

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

CONTRACT CHANGE NOTICE

Change Notice Number 15

to

Contract Number 071B3200061

CONTRACTOR	SAS INSTITUTE INC	STATE Program Manager Contract Administrator	Linda Pung	MULTI
	100 SAS Campus Drive		517-241-5498	
	Cary, NC 27513		Pungl2@michigan.gov	
	Wayne Kuipers		Malu Natarajan	DTMB
	616-403-2275		(517) 284-7030	
	wayne.kuipers@sas.com		natarajanm@michigan.gov	
	*****3017			

CONTRACT SUMMARY

ENTERPRISE FRAUD DETECTION SOFTWARE PROJECT

INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW
December 12, 2012	December 20, 2015	5 - 1 Year	December 20, 2018
PAYMENT TERMS		DELIVERY TIMEFRAME	
		N/A	
ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING
<input type="checkbox"/> P-Card <input type="checkbox"/> Direct Voucher (DV) <input type="checkbox"/> Other			<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
MINIMUM DELIVERY REQUIREMENTS			
N/A			

DESCRIPTION OF CHANGE NOTICE

OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
<input type="checkbox"/>		<input type="checkbox"/>		December 20, 2018
CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE		
\$14,264,326.00	\$0.00	\$14,264,326.00		

DESCRIPTION

Effective January 23, 2018, Change Notice 13 to this Contract is amended to extend Cycle 2 milestone under section 4. Project milestones table by three weeks to compensate for lack of system availability and changes to this schedule will be managed by the established project change request process under the EFDS Governance.

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



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

CONTRACT CHANGE NOTICE

Change Notice Number **13**

to

Contract Number **071B3200061**

CONTRACTOR	SAS INSTITUTE INC
	100 SAS Campus Drive
	Cary, NC 27513
	Wayne Kuipers
	616-403-2275
	wayne.kuipers@sas.com
	*****3017

STATE	Program Manager	Linda Pung	DTMB-IT
		517-241-5498	
		Pungl2@michigan.gov	
	Contract Administrator	Simon Baldwin	DTMB
		(517) 284-6997	
		baldwins@michigan.gov	

CONTRACT SUMMARY				
ENTERPRISE FRAUD DETECTION SOFTWARE PROJECT				
INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW	
December 12, 2012	December 20, 2015	5 - 1 Year	December 20, 2017	
PAYMENT TERMS		DELIVERY TIMEFRAME		
ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING	
<input type="checkbox"/> P-Card <input type="checkbox"/> Direct Voucher (DV) <input type="checkbox"/> Other			<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
MINIMUM DELIVERY REQUIREMENTS				
DESCRIPTION OF CHANGE NOTICE				
OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
<input type="checkbox"/>	N/A	<input type="checkbox"/>	N/A	December 20, 2017
CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE		
\$14,264,326.00	\$0.00	\$14,264,326.00		
DESCRIPTION				
Effective 4/26/2017, two initiatives have been added to this Contract, per the attached Statement of Work and utilizing \$316,535.00 existing funds. All other terms, conditions, specifications, and pricing remain the same. Per Contractor and Agency agreement and DTMB Procurement approval.				



**MICHIGAN DEPARTMENT OF TECHNOLOGY,
MANAGEMENT AND BUDGET
IT SERVICES
STATEMENT OF WORK**

Project Title: Contract 071B3200061 Change Notice: SAS Scope of Work Amendments	Period of Coverage:
Requesting Department: Department of Health and Human Services (MDHHS)	Effective Date: 4//2017
DTMB Program Manager: Kemal Tekinel	Phone: (517) 241-5779
DTMB Contract Administrator: Simon Baldwin	Phone: (517) 284-6997

This Statement of Work (SOW) is made a part of a Change Notice to Contract No. 071B3200061 (Contract) between the State of Michigan (State) and SAS (Contractor or SAS) effective as of the date set forth on the signature page of this Agreement.

SUMMARY

SAS and the State of Michigan Department of Health and Human Services (DHHS or the "State") have agreed to pursue two short-term services initiatives ("Services") with respect to the Medicaid Provider Fraud Detection Module ("Medicaid Provider Module"), part of the Enterprise Fraud Detection System ("EFDS"). The first services initiative will enable the EFDS to operate as an ad-hoc scenario modeling tool, and will be implemented if chosen by The State, at its sole discretion, as solution for long term ad hoc analytics as a result of a joint DTMB/DHHS business assessment. The second will deliver to DHHS a select number of Highly Suspicious Alerts (as defined herein).

BACKGROUND

The State and SAS first signed Contract No. 071B3200061 (as amended, the "Contract") to install the first two modules of EFDS: Unemployment Insurance and Food Assistance Program. The State subsequently added the Medicaid Provider Module and the Medicaid Eligibility Fraud Detection Module pursuant to separate change notices to the Contract. The Medicaid Provider Module was added pursuant to Change Notice Number 2, effective December 20, 2013 ("Change Notice No. 2").

This Statement of Work deals solely with services relating to the Medicaid Provider Module. All other terms and conditions of the Contract remain unchanged, including with respect to any other modules delivered thereunder. The primary components of the Medicaid Provider Module, Home Help and Healthcare, entered production in July and August 2016. In a meeting on October 31, 2016, the State informed SAS that it was evaluating the return-on-investment of the Medicaid Provider Module. Increased focus has been placed on the ability to do "ad-hoc" queries to evaluate the ongoing viability of existing scenarios, and to model new ones.

Change Notice No. 9, effective July 15, 2016 ("Change Notice No. 9") which clarified the scope of services performed by SAS for the Medicaid Provider Module, also modified certain outstanding payments set forth under Change Notice No. 2. To date, a remaining amount of \$316,535 is still available with respect to the Medicaid Provider Module. Until completion of the Services, the parties acknowledge and agree that the sole scope of services to be performed with respect to the Medicaid Provider Module will be those Services set forth in this Statement of Work.

DURATION

SAS will deliver the Services according to the following two concurrent work streams:

Initiative One Services: Enterprise Guide "Ad-hoc" Deployment

Initiative Two Services: Highly Suspicious Alerts

These two services initiatives will begin on a mutually agreeable date to the parties following execution of a change notice to the Contract. Initiative One Services and Initiative Two Services will thereafter run concurrently until completed in accordance with this Statement of Work.

Initiative One Services will be completed within six months following the State of Michigan notifying SAS of its decision to use Enterprise Guide. Configuration of a development environment where a group of DHHS users will have access

to EFDS data is a pre-requisite for this work. Data brought into this environment will be identified by the State and agreed upon by SAS.

Initiative Two Services will occur in three (3) cycles each (each, a “Cycle”), each Cycle to last for 13 weeks. A new cycle will start on Monday. (“Initiative Two Services Period”). During each Cycle, State feedback on alert utility and progress will be evaluated and organized into categories of possible product enhancements. SAS will also work with the State to identify the highest priority, highest value modifications. The first Cycle will begin once the parties have agreed upon a mutually acceptable process for review and acceptance of the Highly Suspicious Alerts generated pursuant to Initiative Two Services. The parties anticipate a start date of May 1, 2017 for both Initiative One Services and Initiative Two Services. Implementation of Initiative One Services will be determined by the State. The State will decide, if and when, based on the results of an independent State initiated evaluation, if and when Initiative One Services will be used.

ONGOING GOVERNANCE AND OVERSIGHT

During the term of this Statement of Work, SAS will provide status reports to the State twice monthly. The State reserves the right to request more reports as needed. Reports will be delivered to:

Name	Role
Kemal Tekinel	Technical Owner
Andrew Mason	Technical Owner
Noelle Rose	Project Manager
David Russell	Business Owner
Casey Barton	Business Owner
Dale Gores	Technical Manager
Brian Turner	PMO Manager
Linda Pung	DTMB General Manager

The reports to the executive steering committee will track progress metrics, which will include the following information:

- number of Highly Suspicious Alerts generated by SAS
- alerts accepted by DHHS
- identified feedback issues
- For the prior period's accepted alerts, provide documentation on methods by which each alert was identified by SAS
- Ad Hoc report status
- Other mutually agreed upon criteria.
- An Executive Steering Committee meeting (“Executive Meeting”) will be established for the duration of this Statement of Work. These meetings will be co-facilitated by SAS and the State and will occur no more than once monthly.

- Below is a suggested meeting cadence

Project Governance Reporting Cycle							
	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
Weekly		Operations Meeting to review project milestones, issues, risks Program Managers create Program Dashboards	PMO Manager creates PMO Dashboard	BIC Enterprise Steering Committee Meeting		Project Manager updates project schedule(s) Project Managers create project status reports	
		Issue/Risk/Change Control Management					
		Stakeholder Management					
Bi-Weekly				Ownership Meeting (Day of the week varies by Program) Leadership Meeting			
		BIC Executive Steering Committee Meeting					
As Needed							

INITIATIVE ONE SERVICES – Enterprise Guide (Ad-hoc) Deployment:

- Goals:
 - SAS to provide the State with the ability to perform ad-hoc analyses against State data sources within the existing EFDS.
 - SAS will participate in a SDT (Solution Design Team) review to assist the State's review of an Ad Hoc solution
 - SAS will configure SAS Enterprise Guide within the EFDS development environment, which is already licensed by the State pursuant to the Contract, as the State's main ad-hoc engine.
 - The State will create a business case and do a pilot to evaluate the SAS and DTMB provided Ad hoc tools.
- The following shall be the Deliverables provided in connection with the Initiative One Services:
 - Provide up to 100 hours of training in Enterprise Guide, as well as coaching and consultative analysis in the early stages of the State's pilot program.
 - This deliverable will be deemed accepted upon the earlier of delivery of all hours have been delivered or when the Initiative Two Services Period has expired.
 - The State will be responsible for identifying to SAS a proposed pilot user group for the Services described in this Statement of Work, as well as providing necessary data storage capacity, and user ID management.

INITIATIVE TWO SERVICES – Highly Suspicious Alerts:

- Definitions: The following definitions will apply to delivery of alerts contemplated by Initiative Two Services.
 - Estimated Potential Recovery Value (EPRV):
 - The potential monetary value, in dollars, of an individual alert, as scored by the existing EFDS and evaluated by SAS. The EPRV represents an estimation of the monetary loss incurred by the State in the payment of Medicaid claims to a specified provider
 - Initial EPRV will be calculated as follows:
 - All claims and claim lines that violated scenarios for claims and claim lines are extracted and put in a table

- All claims involved in outlier or predictive modeling scenarios are extracted and added to the table created in the previous step
 - Duplicates in this table are removed to ensure that claim lines are only counted once
 - The sum of all paid amounts in remaining claim lines is calculated and reported as “Value at Risk”
- Highly Suspicious Alerts:
 - Risk-scored alerts (a measure of violation severity) that have undergone an analytic review by SAS subject matter experts. Each alert will demonstrate a measure of violation severity.
 - Each alert will present only fee-for-service related claims.
 - It is anticipated that each Highly Suspicious Alert provided to the State hereunder should have an estimated overpayment by the State in an amount greater than \$55,000. Unless agreed to by the State, SAS will not present Highly Suspicious Alerts for amounts less than such monetary threshold.
 - Highly Suspicious Alerts will also include information for review by the State that explains a policy-specific or other related violation or other suspicious behavior patterns. Such information will be presented in fashion that outlines why the scenario was triggered as well as identification of the level of importance each scenario contributed to the identification of the Highly Suspicious Alert.
- Deliverables:
 1. SAS will provide the State with Highly Suspicious Alerts:
 - Estimated Potential Recovery Value (EPRV) and Highly Suspicious Alerts must align with the definitions as stated above.
 - Highly Suspicious Alerts will be clearly displayed and will be surfaced at the top of the predictive analytics view provided to the State.
 - Unless agreed to with the State, each Highly Suspicious Alert presented to the State will relate to separate instances of potential fraud; alerts previously submitted will not be presented to the State again unless underlying related data changes to an extent that materially changes the nature of the alert.
 - These views will be provided by SAS in either Word or Excel document format as requested by the State. SAS will provide a template for documenting the alert for State review.
 - For Highly Suspicious Alerts that have been accepted by the State, SAS will provide documentation relating to methodology utilized by SAS. Documentation must be approved by the State.
 2. During each Cycle, SAS will conduct collaborative meetings (“Collaborative Meeting”) every other week with the State of for a minimum of two (2) and a maximum of four (4) hours (Additional hours if mutually agreed upon) in order to exchange feedback on the Highly Suspicious Alerts generated to date and the investigative process as a part of the documentation for process improvement and product optimization. Such meetings will be conducted either remotely or onsite at the State’s location.
 - SAS will provide a proposed agenda a minimum of five days prior to each Collaborative Meeting.
 - Collaborative Meetings and each monthly Executive Meeting will be scheduled at a time and location mutually agreed upon by the parties. The parties anticipate all meetings will follow the proposed schedule each month:
 - Week 1: Collaborative Meeting
 - Week 3: Collaborative Meeting
 - Week 4: Executive Meeting
 3. The State will work with SAS to identify changes to the Medicaid Provider Module (which may include additional scenarios, small-scale “quick hits” enhancements, etc.) whose scope will be set by both DHHS and DTMB Agency Services, taking into account any specific recommendations from SAS. SAS will provide up to 500 hours for this specific purpose at any time during the duration of this SOW. This deliverable will be deemed accepted upon the earlier of delivery of all service hours or when the Initiative Two Services Period has expired.
 4. Project milestones are listed below.

Milestone	Completion Date	Payment Amount
Cycle 1	13 weeks following mutually agreed upon start date as identified in the project schedule	N/A
Cycle 2	13 weeks following conclusion of cycle 1	N/A
Cycle 3	13 weeks following conclusion of cycle 2	N/A
Acceptance and Closeout	7 business days following cycle 3	\$316,535.00 upon completion of Final Acceptance and Closeout. Payment of such fees will be contingent upon acceptance by the State of Highly Suspicious Alerts that meet the Total EPRV threshold.

- The following criteria and processes will be used by SAS when generating Highly Suspicious Alerts:
 - Accepted alerts are expected to result in one of the following outcomes:
 - Provider education resulting in cost avoidance
 - Claim adjustment resulting in reimbursement
 - Medical record review leading to reimbursement
 - Potential factors that may impact the State's estimated likelihood of recovery based on such Highly Suspicious Alert.
 - Confirm potentially suspicious billing patterns by reviewing the following relevant business factors:
 - Reviewing the patient/claim count
 - Evaluating the likelihood of a valid overpayment and that policy supports such recovery
 - Considering whether there is evidence of motivation to commit fraud
 - Conducting an examination of related claims and triggering services
 - Assess the potential extent of required investigation (e.g. assess whether or not verification of services rendered would have to be done to investigate the alert)
 - Ongoing collaborative feedback sessions with SAS to discuss progress relating to investigative processes and scenario and alert suitability:
 - Provide feedback on steps taken by the State to assess the Highly Suspicious Alerts delivered by SAS in order to determine whether to take further action
 - Within two weeks after delivery of Highly Suspicious Alerts, the State will provide feedback on alerts.
 - During each Cycle, SAS will continually evaluate its processes during the Initiative Two Services. As part of such evaluation, a small number of Highly Suspicious Alerts selected by SAS will be presented to the State for further detailed discussion.
- Acceptance Criteria:
 - The State will approve or reject each Highly Suspicious Alert individually based on the results of the collaborative process with the SAS and criteria specified above.
 - If a Highly Suspicious Alert is approved by the State, the EPRV will be credited towards the Total EPRV (defined below).
 - If a Highly Suspicious Alert is rejected, the State will document its reasons for rejection, including whether any further actions or details may be required in order to reevaluate the status of such Highly Suspicious Alert.
 - In the event of a rejection, SAS and the State will determine whether:

- A product change is possible to render the alert acceptable
 - A process change by SAS or the State, as applicable, is appropriate to re-evaluate the alert
 - The general analysis methodology utilized by SAS requires modification – and whether the ad-hoc process can be used to model the desired change
- SAS will provide a maximum of fifty (50) Highly Suspicious Alerts to the State during each month of the Initiative Two Services Period. Highly Suspicious Alerts that were initially rejected by the State and, after reevaluation and consideration by SAS, which are resubmitted to the State will count as a new Highly Suspicious Alert subject to this cap.
- At the end of the Initiative Two Services Period, SAS will be required to demonstrate a minimum EPRV of \$14 million to the State in accepted Highly Suspicious Alerts (“Total EPRV”). Only those Highly Suspicious Alerts accepted by the State will count towards the Total EPRV.
- Formal Acceptance Procedures:
 - At the end of each Cycle, the State will notify SAS which of the Highly Suspicious Alerts delivered have been accepted or rejected. Formal notification of acceptance or rejection of all Highly Suspicious Alerts will occur within two (2) weeks at the end of each Cycle.
 - SAS will provide HSA within the first 8 weeks of each cycle
 - For each Highly Suspicious Alert, the State will also either accept or reject the SAS proposed EPRV value. In the event the State rejects or contests the proposed EPRV, the State will be required to state reasons for such rejection and the parties will mutually agree on an applicable EPRV for such alert.
 - The mutually agreed upon EPRV for each Highly Suspicious Alert accepted by the State will be counted towards the Total EPRV.
- Assumptions:
 - The State may, or may not, at its discretion, choose to take action on Highly Suspicious Alerts generated by SAS under this Statement of Work.
 - A choice by the State not to take action will not invalidate Highly Suspicious Alerts presented by SAS and accepted by the State. Accepted Highly Suspicious Alerts will be added to SAS’ Total EPRV.
 - A designation by SAS of a Highly Suspicious Provider Alert is not a guarantee that the alert will result in fraud conviction or actual revenue recovery.
- Deliverable schedule and EPRV Targets:
 - SAS will slowly increase the number of Highly Suspicious Alerts delivered to the State during each month of the three Cycles. This gradual pace will allow both parties to assess the effectiveness of the delivery process, and to evaluate feedback to both the quality and EPRV. Notwithstanding the foregoing, the total number of Highly Suspicious Alerts delivered to the State each month shall not exceed a total of fifty (50).
 - SAS will be required to demonstrate satisfaction of the Total EPRV at the end of the Initiative Two Services Period. SAS estimates that the Total EPRV will be demonstrated in accordance with the following:

ITEM	First Cycle	Second Cycle	Third Cycle
EPRV in \$ millions	\$ 2	\$ 4	\$ 8

- Of the total number of Highly Suspicious Alerts that SAS will deliver to the State each month, an estimated 70% (“Acceptance Threshold”) must satisfy the general criteria and processes identified previously; *provided, however*, that if at the end of the Initiative Two Services Period SAS has satisfied the Total EPRV notwithstanding failing to meet the Acceptance Threshold each month, SAS will be deemed to have satisfied its delivery requirements under this Statement of Work.

Continuance of Pilot:

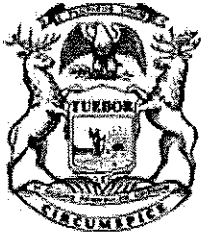
- The State will perform an ROI assessment at the end of each cycle. The calculations will utilize a State calculated “expected overpayment” rather than the EPRV provided by SAS. The State will share with SAS any significant deviation from EPRV and ROI calculation.
- If the ROI assessment is not satisfactory at the end of the first cycle, the State may decide to end the pilot at the completion of the second cycle.
- If the ROI assessment is not satisfactory at the end of the second cycle, the State may decide to end the pilot at the completion of the second cycle.
- The final ROI assessment will be a primary component in the determination of a successful pilot project.

- Estimated FFS Overpayment: > \$1.6 million per month as an average over the life of the pilot.
- The demonstrated SAS SME triage process will be translated into the automated alert generation system
- Future scoring must be based on both FFS dollars, using encounters as support for the identification of outliers, and on encounter dollars, using FFS as support for the identification of outliers
- Future alerts must be centered on the billing provider as this is the primary avenue for recoupment. SAS will work to address these changes using the 500 allotted hours with the understanding that changes that above the 500 hrs would occur in a future contract period. In the event the State determines to proceed with additional services beyond the scope of those set forth in this Statement of Work, the parties will enter into a new change notice to the Contract outlining the specific terms of any additional work.
- The State reserves the right to discontinue this Initiative Two if, after six months, the State, in its sole discretion, deems at least 40% or more of the Alerts as false positives or not cost-effective to pursue.

PAYMENTS:

Notwithstanding the Payment Schedule specified on Change Notice No. 9, the following payments shall be due with respect to the Services described in this Statement of Work:

- Initiative One Services:
 - SAS will provide the Initiative One Services at no additional cost to the State during the term of this Statement of Work.
- Initiative Two Services:
 - Upon completion of the Initiative Two Services Period, SAS will invoice the State \$316,535.00, the outstanding amount currently contemplated by Change Notice No. 9 for deliverables defined within this SOW. These funds are currently on the Contract. Payment of such fees will be contingent upon acceptance by the State of Highly Suspicious Alerts that meet the Total EPRV threshold.
 - Meeting the EPRV target is the agreed upon methodology for determining SAS delivering sufficient HSA's for review. As it is not a true indicator of actual cost avoidance or potential recoveries, an independent assessment will be conducted to determine an ROI of the Medicaid Provider Module.
- The parties acknowledge and agree that for the remainder of the Contract term, the warranty, maintenance and support fees set forth in Table 2 and Table 2b of Exhibit B to Change Notice No. 2 are suspended for the duration of the Services.



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

CONTRACT CHANGE NOTICE

Change Notice Number 12

to

Contract Number 071B3200061

CONTRACTOR	SAS INSTITUTE INC
	100 SAS Campus Drive
	Cary, NC 27513
	Wayne Kuipers
	616-403-2275
	wayne.kuipers@sas.com
*****3017	

STATE	Linda Pung	DTMB-IT
	517-241-5498	
	Pungl2@michigan.gov	
	Simon Baldwin	DTMB
	(517) 284-6997	
baldwins@michigan.gov		

CONTRACT SUMMARY

ENTERPRISE FRAUD DETECTION SOFTWARE PROJECT

INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW
December 12, 2012	December 20, 2015	5 - 1 Year	December 20, 2016

PAYMENT TERMS

DELIVERY TIMEFRAME

ALTERNATE PAYMENT OPTIONS

EXTENDED PURCHASING

☐ P-Card ☐ Direct Voucher (DV) ☐ Other ☒ Yes ☐ No

MINIMUM DELIVERY REQUIREMENTS

DESCRIPTION OF CHANGE NOTICE

OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
<input type="checkbox"/>		<input type="checkbox"/>	N/A	
CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE		
\$14,264,326.00	\$0.00	\$14,264,326.00		

DESCRIPTION

Effective 3/1/2017, the State is adding the attached Statement of work which will stop work on certain projects associated with the State Food Assistance Program and the State Medicaid Eligibility Program. All other terms, conditions, specifications, and pricing remain the same. Per Contractor and Agency agreement and DTMB Procurement approval.



**MICHIGAN DEPARTMENT OF TECHNOLOGY,
MANAGEMENT AND BUDGET
IT SERVICES
STATEMENT OF WORK**

Project Title: Contract 071B3200061 Change Notice: SAS Stop Work	Period of Coverage: 1/12/17-12/20/17
Requesting Department: Michigan Department of Health and Human Services (MDHHS)	Date: 1/18/17
DTMB Project Manager: Kemal Tekinel	Phone: (517) 241-3888
DTMB Contract Administrator: Simon Baldwin	Phone: (517) 284-6997

This Statement of Work is made a part of Change Notice No. 12 to Contract No. 071B3200061 (Contract) between the State of Michigan (State) and SAS (Contractor or SAS) effective as of the date set forth on the signature page of this Agreement.

1. BACKGROUND

- 1.1 The purpose of this amendment will be to formalize changes to the following components of Contract 071B3200061 regarding stoppage of work and pursuit of additional scenarios/alerts.

2. SCOPE OF WORK/SERVICES AND DELIVERABLES

- 2.1 **State Food Assistance Program.** Regarding the State Food Assistance Program, the State will continue to use the current production solution and the State will pay SAS annual software maintenance for food assistance. The State may, in its sole discretion, choose whether to pursue additional scenarios or alerts for the State Food Assistance Program. At the time this Statement of Work was executed, the State elected not to pursue additional the State Food Assistance Program scenarios or alerts unless and until it provides other direction to SAS at a later date.
- 2.2 **State Medicaid Eligibility Program.** Regarding the State Medicaid Eligibility Program, SAS will stop all work on all active projects as directed by the DTMB Program Manager, SAS will not receive any further payment from the State for Medicaid Eligibility services/deliverables, and no alerts for Eligibility will be used in production.
- 2.3 **Entire Agreement.** This SOW, together with the existing Contract, constitutes the Parties' complete and exclusive statement. Apart from the amendments made in this SOW, all Contract terms and conditions must remain in full force and effect.



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

CONTRACT CHANGE NOTICE

Change Notice Number **11**

to

Contract Number **071B3200061**

CONTRACTOR	SAS INSTITUTE INC
	100 SAS Campus Drive
	Cary, NC 27513
	Wayne Kuipers
	616-403-2275
	wayne.kuipers@sas.com
	*****3017

STATE	Program Manager	Linda Pung	DTMB-IT
		517-241-5498	
		Pungl2@michigan.gov	
	Contract Administrator	Simon Baldwin	DTMB
		(517) 284-6997	
		baldwins@michigan.gov	

CONTRACT SUMMARY				
ENTERPRISE FRAUD DETECTION SOFTWARE PROJECT				
INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW	
December 12, 2012	December 20, 2015	5 - 1 Year	December 20, 2016	
PAYMENT TERMS		DELIVERY TIMEFRAME		
ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING	
<input type="checkbox"/> P-Card <input type="checkbox"/> Direct Voucher (DV) <input type="checkbox"/> Other			<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
MINIMUM DELIVERY REQUIREMENTS				
DESCRIPTION OF CHANGE NOTICE				
OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
<input checked="" type="checkbox"/>	1-Year	<input type="checkbox"/>		December 20, 2017
CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE		
\$14,264,326.00	\$0.00	\$14,264,326.00		
DESCRIPTION				
Effective, 12/21/2016, the State is exercising the second option year. The revised Contract expiration date is 12/20/2017. All other terms, conditions, specifications and pricing remain the same. Per Contractor and Agency agreement, and DTMB Procurement approval.				



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

CONTRACT CHANGE NOTICE

Change Notice Number **10**

to

Contract Number **071B3200061**

CONTRACTOR	SAS INSTITUTE INC
	100 SAS Campus Drive
	Cary, NC 27513
	Wayne Kuipers
	616-403-2275
	wayne.kuipers@sas.com
	*****3017

STATE	Program Manager	Linda Pung	DTMB-IT
		517-241-5498	
	Contract Administrator	Pungl2@michigan.gov	
		Simon Baldwin	DTMB
		(517) 284-7000	
		baldwins@michigan.gov	

CONTRACT SUMMARY				
ENTERPRISE FRAUD DETECTION SOFTWARE PROJECT				
INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE	
December 12, 2012	December 20, 2015	5 - 1 Year	December 20, 2016	
PAYMENT TERMS		DELIVERY TIMEFRAME		
ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING	
<input type="checkbox"/> P-Card		<input type="checkbox"/> Direct Voucher (DV)	<input type="checkbox"/> Other	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
MINIMUM DELIVERY REQUIREMENTS				
DESCRIPTION OF CHANGE NOTICE				
OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
<input type="checkbox"/>	N/A	<input type="checkbox"/>	N/A	December 20, 2016
CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE		
\$14,264,326.00	\$0.00	\$14,264,326.00		
DESCRIPTION				

Effective 9/27/2016, the following Statement of Work is added to this Contract and will finalize the maintenance and support terms for Phase 1 FAP and Phase 2 UIA. The implementation of these phases was delayed leading to maintenance and support periods starting on August 9, 2016 and December 31, 2016. Funds for maintenance and support are currently on the Contract and costs remain the same. All other terms, conditions, specifications, and pricing remain the same per Contractor and Agency agreement and DTMB Procurement approval.



**MICHIGAN DEPARTMENT OF TECHNOLOGY,
MANAGEMENT AND BUDGET
IT SERVICES
STATEMENT OF WORK**

Project Title: Contract 071B3200061 Change Notice: SAS	Period of Coverage:
Requesting Department: Department of Health and Human Services (DHHS)	Date: 8/1/16
DTMB Project Manager: Kemal Tekinel	Phone: (517) 241-3888
DTMB Contract Administrator: Simon Baldwin	Phone: (517) 284-6997

This Statement of Work is made a part of Change Notice No. 10 to Contract No. 071B3200061 (Contract) between the State of Michigan (State) and SAS (Contractor or SAS) effective as of the date set forth on the signature page of this Agreement.

1. CONTRACTOR'S SERVICES AND DELIVERABLES

- 1.1 The Parties wish to hereby replace the existing Table 2 and Table 2(b) for FAP and UIA services in their entirety and replace them with the following:

Table 2.a.1 – Warranty, Maintenance and Support for Phase 1 FAP

Task	Warranty, Maintenance and Support Activities	Cost
A	Warranty (One Year) Complete	\$ Included in first year software costs
9.1	Maintenance and Support (Support Year 1) Complete	\$ Included in first year software costs
9.1	Maintenance and Support (Support Year 2) Complete	\$336,584.50
9.1	Maintenance and Support (Support Year 3) Complete	\$346,682.00

Table 2.a.2 – Warranty, Maintenance and Support for Phase 2 UIA

Task	Warranty, Maintenance and Support Activities	Cost
-------------	---	-------------

Task	Warranty, Maintenance and Support Activities	Cost
8.1	Warranty (One Year) Complete	\$ Included in first year software costs
9.1	Maintenance and Support (Support Year 1) Complete	\$ Included in first year software costs
9.1	Maintenance and Support (Support Year 2) Complete	\$336,584.50
9.1	Maintenance and Support (Support Year 3) Complete	\$346,682.00

Table 2.b.1 –Maintenance and Support for Optional Years for Phase 1 FAP

Task	Warranty, Maintenance and Support Activities Option Years	Services Accrual
9.1	Optional Maintenance and Support (Support Year 4) Complete	\$357,082.00
9.1	Maintenance and Support (Support Year 5) Complete	\$367,794.50
9.1	Maintenance and Support (Support Year 6) Complete	\$378,828.50
9.1	Maintenance and Support (Support Year 7) Complete	\$390,193.50
9.1	Maintenance and Support (Support Year 8) Complete	\$401,899.00

Table 2.b.2 –Maintenance and Support for Optional Years for Phase 2 UIA

Task	Warranty, Maintenance and Support Activities Option Years	Services Accrual
9.1	Optional Maintenance and Support (Support Year 4) Complete	\$357,082.00
9.1	Maintenance and Support (Support Year 5) Complete	\$367,794.50
9.1	Maintenance and Support (Support Year 6) Complete	\$378,828.50
9.1	Maintenance and Support (Support Year 7) Complete	\$390,193.50

Task	Warranty, Maintenance and Support Activities Option Years	Services Accrual
9.1	Maintenance and Support (Support Year 8) Complete	\$401,899.00

1.2 **Warranty.** Includes Costs for One (1) Year of Warranty as Described in Section 1.104.8. Note that Year 1 of Warranty begins following Acceptance of either Phase 1 or Phase 2, whichever occurs first. Notwithstanding the preceding sentence, the parties clarify that Phase 1 FAP Warranty Period will end on August 8, 2016 and Phase 2 UIA Warranty Period will end on December 30, 2016.

1.3 **Maintenance and Support.** Payment for Support Year 2 is made upon the end of FAP and UIA. the applicable Contract Warranty Period specified above. For the avoidance of doubt, the following periods of performance will apply to the Maintenance and Support Periods identified in Tables 2.a.1 and Tables 2.a.2 above:

Maintenance and (Support Year 2) Complete – Phase 1 FAP	09August2016-08August2017
Maintenance and (Support Year 3) Complete – Phase 1 FAP	09August2017-08August2018
Maintenance and (Support Year 2) Complete – Phase 2 UIA	31December2016-30December2017
Maintenance and (Support Year 3) Complete – Phase 2 UIA	31December2017-30December2018

1.4 **Maintenance and Support – Optional Years.** Payment for Maintenance and Support for Optional Years specified in Tables 2.b.1 and 2.b.2 will be invoiced for Phase 1 and Phase 2 on an annual basis corresponding the periods of performance specified in Note 2 above.

1.5 The State reserves all rights and remedies under the Contract. Apart from the amendments made in this Statement of Work, all Contract terms and conditions must remain in full force and effect.

IN WITNESS WHEREOF, the Parties, intending to be legally bound, have caused their duly authorized officers to execute this Statement of Work Agreement via a contract change notice signature page, which is incorporated herein by reference.



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

CONTRACT CHANGE NOTICE

Change Notice Number 9
to
Contract Number 071B3200061

CONTRACTOR	SAS INSTITUTE INC
	100 SAS Campus Drive
	Cary, NC 27513
	Wayne Kuipers
	616-403-2275
	Wayne.Kuipers@sas.com
	*****3017

STATE	Program Manager	Pung, Linda	DTMB
		517-241-5498	
		Pungl2@michigan.gov	
	Contract Administrator	Simon Baldwin	DTMB
		(517) 284-6997	
		BaldwinS@michigan.gov	

CONTRACT SUMMARY				
DESCRIPTION: Enterprise Fraud Detection Software Project				
INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW	
December 12, 2012	December 20, 2015	5 - 1 Year	December 20, 2016	
PAYMENT TERMS		DELIVERY TIMEFRAME		
N/A		N/A		
ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING	
<input type="checkbox"/> P-card <input type="checkbox"/> Direct Voucher (DV) <input type="checkbox"/> Other			<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
MINIMUM DELIVERY REQUIREMENTS				
DESCRIPTION OF CHANGE NOTICE				
OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
<input type="checkbox"/>	N/A	<input type="checkbox"/>	N/A	December 20, 2016
CURRENT VALUE		VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE	
\$14,264,326.00		\$ 0.00	\$14,264,326.00	

DESCRIPTION: Effective May, 2016, the following Statement of Work is hereby added to this Contract. All other terms, conditions, specifications, and pricing remain the same per Contractor and Agency agreement and DTMB Procurement approval.



**MICHIGAN DEPARTMENT OF TECHNOLOGY,
MANAGEMENT AND BUDGET
IT SERVICES
STATEMENT OF WORK**

Project Title: Revised SAS Medicaid Fraud Detection Software Payment Schedule; Additional Services	Period of Coverage: 12/21/2012 – 12/20/2016
Requesting Department: DHHS	Date: 6/2/2016
Agency Project Manager: Cynthia Edwards	Phone: (517) 241-9998
DTMB Contract Administrator: Simon Baldwin	Phone: (517) 284-6997

Brief Description of Services to be provided:
Enterprise Fraud Detection Software Project

BACKGROUND:

PROJECT OBJECTIVE:

This request will revise the pricing schedule for Medicaid Provider Fraud Detection Module (Phase 3). The payment structure below shall replace Services Payment Amount specified following Task 12.7 and Task 13.3 of Table 1 included in Exhibit B to Change Notice 2.

ORIGINAL PAYMENT STRUCTURE AND PAYMENT AMOUNT:

	Original Payment Milestone	Original Payment Amount
1	Construction and Testing Completion	\$444,260.00
2	Implementation Acceptance	\$188,810.00
	Total	\$633,070.00

MODIFIED PAYMENT STRUCTURE AND PAYMENT AMOUNTS:

New Payment Milestone	New Payment Amount	Payment Date
Release 1 – Provider (deployed)	\$316,534	Upon execution of this Change Notice
Release 2- Home Help	\$0	N/A
Release 2 – Provider Carryover	\$0	N/A
Release 2 - SSOD Health Care Code Alert Queue Update	\$316,535	After Final Acceptance of Medicaid Provider Fraud Detection Module (per Contract 2.256)

TASKS:

Reserved

DELIVERABLES:

Completion of certain deliverables originally identified within the Contract have now been divided into two releases and payments to Contractor have been bifurcated accordingly. Additional services as specified below are added to the Contract.

- a. Release 1 (completed in October 2015) creates alerts and scenarios based on Provider Pharmacy, Provider Professional and Provider Dental behaviors. These scenarios have already gone through construction and testing completion as well as implementation and acceptance. Provider pharmacy is associated with 304 scenarios, Provider Professional with 259 scenarios, and Provider Dental with 155 Scenarios. The "Release 1" payment amount (\$316,354) was previously invoiced to Customer. Release 1 shall be considered part of the original services set forth in Change Notice No. 2.
- b. Release 2 – Home Help will finalize all home help scenarios, 25 scenarios in total. This release shall be considered part of the original services set forth in Change Notice No. 2.
- c. Release 2 – Provider Carryover will provide the State with additional customizations related to Release 1. These customizations shall be considered part of the original services set forth in Change Notice No. 2. There are a total of 20 scenarios, including 1 new scenario for Provider Professional, 4 new scenarios for Provider Pharmacy, 5 new scenarios for Provider Dental, and 10 enhancements to the standard healthcare scenarios delivered in Release 1. In addition, this release includes changes to pharmacy data ETL code which represents additional services to be provided to the State under the Contract. The sole deliverable for this release shall be the 20 scenario customizations described in this paragraph.
- d. Release 2 - SSOD Health Care Code Alert Queue Update will implement requested changes to the Pharmacy alert queue and additional customizations that are dependent upon the Health Care Code Update. These are additional services to be provided to the State under the Contract. The primary deliverable for this release shall be completion of the Health Care Code Update and related scenario customization along with modification to the alert queue.

ACCEPTANCE CRITERIA:

Per Original Contract

PROJECT CONTROL AND REPORTS:

Reserved

SPECIFIC DEPARTMENT STANDARDS:

Reserved

PAYMENT SCHEDULE:

Payment will be made on a Fixed Firm basis. DTMB will pay CONTRACTOR upon receipt of properly completed invoices which shall be submitted to the billing address on the State issued purchase order not more often than monthly. DTMB Contracts area will coordinate obtaining Agency Project Manager and DTMB Project Manager approvals. All invoices should reflect actual work completed by payment date, and must be approved by the Agency Project Manager and DTMB Project Manager prior to payment. The invoices shall describe and document to the State's satisfaction a description of the work performed, the progress of the project, and fees. When expenses are invoiced, receipts will need to be provided along with a detailed breakdown of each type of expense.

Payment shall be considered timely if made by the DTMB within forty-five (45) days after receipt of properly completed invoices.

WARRANTY PERIOD:

The parties acknowledge and agree that the Warranty Period with respect to Phase 3 Medicaid Provider Fraud Detection shall be the one year period beginning after acceptance of Release 2 – SSOD Health Care Code Alert Queue Update.

EXPENSES:

The State will not pay for any travel expenses, including hotel, mileage, meals, parking, etc.

PROJECT SCHEDULE:

Reserved

PROJECT CONTACTS:

The DTMB Contract Administrator for this project is:

Simon Baldwin
Michigan Department of Technology, Management and Budget
525 W. Allegan Street
Lansing, MI 48933
517-284-6997
Email: baldwins@michigan.gov

AGENCY RESPONSIBILITIES:

Reserved

LOCATION OF WHERE THE WORK IS TO BE PERFORMED:

Reserved

EXPECTED CONTRACTOR WORK HOURS AND CONDITIONS:

Work hours are not to exceed eight (8) hours a day, forty (40) hours a week. Normal working hours of 8:00 am to 5:00 pm are to be observed unless otherwise agreed to in writing.

No overtime will be permitted.

STATE OF MICHIGAN
DEPARTMENT OF TECHNOLOGY, MANAGEMENT & BUDGET
PROCUREMENT

525 W. ALLEGAN STREET
LANSING, MI 48933

P.O. BOX 30026
LANSING, MI 48909

CHANGE NOTICE NO. 8
to
CONTRACT NO. 071B3200061
between
THE STATE OF MICHIGAN
and

NAME & ADDRESS OF CONTRACTOR	PRIMARY CONTACT	EMAIL
SAS Institute Inc. 100 SAS Campus Drive Cary, NC 27513	Wayne Kuipers	wayne.kuipers@sas.com
	PHONE	CONTRACTOR'S TAX ID NO. (LAST FOUR DIGITS ONLY)
	(616) 403-2275	3017

STATE CONTACTS	AGENCY	NAME	PHONE	EMAIL
PROGRAM MANAGER / CCI	DTMB	Linda Pung	(517) 241-5498	Pungl2@michigan.gov
CONTRACT ADMINISTRATOR	DTMB	Simon Baldwin	(517) 284-6997	baldwins@michigan.gov

CONTRACT SUMMARY			
DESCRIPTION: Enterprise Fraud Detection Software Project			
INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW
December 21, 2012	December 20, 2015	(5) 1-Year Options	December 20, 2016
PAYMENT TERMS		DELIVERY TIMEFRAME	
N/A		N/A	
ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING
<input type="checkbox"/> P-card <input type="checkbox"/> Direct Voucher (DV) <input type="checkbox"/> Other			<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
MINIMUM DELIVERY REQUIREMENTS			
N/A			

DESCRIPTION OF CHANGE NOTICE				
EXERCISE OPTION?	LENGTH OF OPTION	EXERCISE EXTENSION?	LENGTH OF EXTENSION	REVISED EXP. DATE
<input type="checkbox"/>	N/A	<input type="checkbox"/>	N/A	December 20, 2016
CURRENT VALUE		VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE	
\$14,264,326.00		\$0.00	\$14,264,326.00	
DESCRIPTION: Effective February 29, 2016, the following Statement of Work is hereby added to this Contract. Please note, the Program Manger has been changed to Linda Pung. All other terms, conditions, specifications, and pricing remain the same per Contractor and Agency agreement and DTMB Procurement approval.				



**MICHIGAN DEPARTMENT OF TECHNOLOGY,
MANAGEMENT AND BUDGET
IT SERVICES
STATEMENT OF WORK**

Project Title: SAS Training Courses Added/Medicaid Fraud Detection Software Payment Schedule Revised	Period of Coverage: 12/21/2012 – 12/20/2016
Requesting Department: DHHS	Date: 12/22/2015
Agency Project Manager: Cynthia Edwards	Phone: (517) 241-9998
DTMB Contract Administrator: Simon Baldwin	Phone: (517) 284-6997

Brief Description of Services to be provided:
Enterprise Fraud Detection Software Project

BACKGROUND:

PROJECT OBJECTIVE:

This request will revise the current training pricing schedule as well as add new trainings.

SCOPE OF WORK:

The following training courses listed in this Change Notice are proposed for 2016. Additional training may be purchased during any renewal term at the same prices set forth below, provided that such training course is available during such renewal year.

Course Title	New Pricing for existing and new Training based on "Training Points"			
	Public Course Fee	Private Course Fee	Estimated Expenses	Total Estimate
SAS Enterprise Guide 1: Querying and Reporting		7800	2394	10194
Using SAS Web Report Studio		4400	1890	6090
Getting Started with the Platform for SAS Business Analytics	1300			1300
SAS Platform Administration: System Administration	1600			1600
	2900	12200	4084	19184
SAS Fraud Framework: Implementation the SAS Social Network Analysis Interface		8800	2394	11194
SAS Business Intelligence Reporting: Fast Track (up to 5 people)		13521	3662	17183
SAS Programming 1: Essentials	1650			1650
SAS Programming 2: Data Manipulation Techniques		11700	3239	14939
SAS Programming 3: Advanced Techniques and Efficiencies (2 People)	3900			3900
SAS SQL1: Essentials		8800	2394	11194
	5550	42821	11689	60060
Total Training Points				79244
Total Cost of Training Points at GSA Rate				\$56,263.00
Fees are documented in "Training Points"				
The public course fees are for 1 person unless otherwise noted.				
The private course fees are for up to 15 students at the State of Michigan unless otherwise noted and facility must pass a virtual lab test for the number of students participating.				

TASKS:

Reserved

DELIVERABLES:

- a) The State shall receive 79,244 SAS Training Points (the "Training Points") in consideration of payment in the amount of \$56,263.
- b) The source of payment for the SAS Training Points shall be the Reserved Contingency Fund referenced on page 117 of the Contract in "Table 3 – Contingency Fund – Task 1.104.10" contained in "Appendix C. Payment Schedule" to the Contract.
- c) The Training Points shall expire on December 20, 2020.
- d) The Training Points shall be used solely by the following State agencies: the Department of Technology, Management and Budget; Department of Health and Human Services; and Unemployment Insurance Agency. No other agency may use the Training Points without the State's written consent.
- e) Exhibit A to this Attachment sets forth the guidelines that apply to the State's use of the Training Points.

Training	Overview	Learn How to:	Duration
SAS Enterprise Guide 1: Querying and Reporting	This course is for users who do not have SAS programming experience but need to access, manage, and summarize data from different sources, and present results in reports and graphs. This course focuses on using the menu-driven tasks in SAS Enterprise Guide, the point-and-click interface to SAS, to create queries and	Access and manipulate local and remote data of various types, Create queries that filter and summarize data, compute new columns, and join multiple tables, Create frequency and tabular reports, Create interactive graphs, Automate output results.	(16) Hours
Using SAS Web Report Studio	This course shows how to build reports and analyze data using SAS Web Report Studio.	View and interact with several types of reports, Build new reports using different data sources, Interact with multidimensional data, Enhance existing SAS reports.	(1) Day or (3) 1/2 Day Sessions
Getting Started with the Platform for SAS Business Analytics	This course provides a comprehensive, hands-on overview of the platform for SAS Business Analytics applications, including SAS Data Integration Studio.	Understand the types of metadata created by the SAS platform, Use SAS platform applications to access and build data sources for reporting and analysis, Build dashboards, Build information maps to provide business views of data, Create stored processes, Create reports using a web application, Access and interact with SAS content using a web-based portal, Access and analyze data using Microsoft Office applications.	(2) Days or (4) 1/2 Day Sessions
SAS Platform Administration: System Administration	This course provides students with the essential knowledge to perform the job functions of a SAS platform administrator.	Administer and back up SAS metadata, Administer SAS Metadata Server, Administer SAS servers, Monitor, log, and troubleshoot SAS servers , Utilize SAS Environment Manager.	(2) Days or (5) 1/2 Day Sessions
SAS Fraud Framework: Implementation the SAS Social Network Analysis Interface	This course provides the knowledge and skills needed to implement the investigator interface of SAS Social Network Analysis 6.2, a component of SAS Fraud Framework. The course addresses the use of eight stored processes for populating the interface, and provides an understanding of the tasks that must be completed before implementation. This course does not address	Create configuration RDB tables, Create, register, and deploy eight interface stored processes, Write stored process programs to populate the Alerts window, Details tab, and Social Network Analysis tab, Create the nodes and links tables used for the social network, Configure the Advanced Search and Alert Disposition windows.	(2) Days or (5) 1/2 Day Sessions
SAS Business Intelligence Reporting: Fast Track (up to 5 people)	This course provides information on how to access and build reports as well as analyze data using several of the information consumer applications in the platform for SAS Business	Identify types of reports, Create and share reporting presentations, Interact with multidimensional data, Access SAS data sources, Work with SAS analyses.	(4) Days
SAS Programming 1: Essentials	This course is for users who want to learn how to write SAS programs. It is the entry point to learning SAS programming and is a prerequisite to many other SAS courses.	Navigate the SAS Studio programming environment, Navigate the SAS Enterprise Guide programming environment, Navigate the SAS windowing environment, Read various types of data into SAS data sets, Create SAS variables and subset data, Combine SAS data sets, Create and enhance listing and summary reports.	(3) Days or (6) 1/2 Day Sessions
SAS Programming 2: Data Manipulation Techniques	This course is for those who need to learn data manipulation techniques using SAS DATA and procedure steps to access, transform, and summarize SAS data sets. The course builds on the concepts that are presented in the SAS	Control SAS data set input and output, Combine SAS data sets, Summarize, read, and write different types of data, Perform DO loop and SAS array processing, Transform character, numeric, and date variables.	(3) Days or (6) 1/2 Day Sessions
SAS Programming 3: Advanced Techniques and Efficiencies (2 People)	This course is for SAS programmers who prepare data for analysis. The comparisons of manipulation techniques and resource cost benefits are designed to help programmers choose the most appropriate technique for their data situation.	Benchmark computer resource usage, Control memory, I/O, and CPU resources, Create and use indexes, Combine data horizontally, Use hash and hiter DATA step component objects and arrays as lookup tables, Compress SAS data sets, Sample your SAS data sets, Create and use SAS data views, Safely reduce the length of numeric variables, Create user-defined functions and informat.	(3) Days or (6) 1/2 Day Sessions
SAS SQL1: Essentials	This course teaches you how to process SAS data using Structured Query Language (SQL).	Query and subset data, Summarize and present data, Combine tables, including complex joins and merges, Create and modify table views and indexes, Replace multiple DATA and PROC steps with one SQL query.	(2) Days or (5) 1/2 Day Sessions

ACCEPTANCE CRITERIA:

Courses shall be deemed accepted upon completion and alignment with the course descriptions identified in the table above.

PROJECT CONTROL AND REPORTS:

Reserved

SPECIFIC DEPARTMENT STANDARDS:

Reserved

PAYMENT SCHEDULE:

Payment will be made on a Fixed Firm basis. DTMB will pay CONTRACTOR upon receipt of properly completed invoices which shall be submitted to the billing address on the State issued purchase order not more often than monthly. DTMB Contracts area will coordinate obtaining Agency Project Manager and DTMB Project Manager approvals. All invoices should reflect actual work completed by payment date, and must be approved by the Agency Project Manager and DTMB Project Manager prior to payment. The invoices shall describe and document to the State's satisfaction a description of the work performed, the progress of the project, and fees. When expenses are invoiced, receipts will need to be provided along with a detailed breakdown of each type of expense.

Payment shall be considered timely if made by the DTMB within forty-five (45) days after receipt of properly completed invoices.

EXPENSES:

The State will not pay for any travel expenses, including hotel, mileage, meals, parking, etc.

PROJECT SCHEDULE:

Reserved

PROJECT CONTACTS:

The DTMB Contract Administrator for this project is:

Simon Baldwin
Michigan Department of Technology, Management and Budget
525 W. Allegan Street
Lansing, MI 48933
517-2846997
Email: baldwins@michigan.gov

AGENCY RESPONSIBILITIES:

Reserved

LOCATION OF WHERE THE WORK IS TO BE PERFORMED:

Reserved

EXPECTED CONTRACTOR WORK HOURS AND CONDITIONS:

Work hours are not to exceed eight (8) hours a day, forty (40) hours a week. Normal working hours of 8:00 am to 5:00 pm are to be observed unless otherwise agreed to in writing.

No overtime will be permitted.

EXHIBIT A

Training Points Guidelines

1. The Customer must designate a representative to serve as the contact to register employees for public courses, on-site courses, Business Knowledge Series courses, Live Web courses, Six Sigma courses, license fees for all e-Learning products, SAS Certification exam vouchers, training development, SAS training center rental fees, selected conferences, or any other preapproved services performed by SAS (collectively "SAS Training Points-Eligible Products and Services").
2. The SAS Training Points offer applies only to eligible courses and events scheduled in the United States.
3. The purchase of SAS Training Points or the use of SAS Training Points to attend courses in certain states might require payment of additional state taxes. This amount is not included in SAS Training Points pricing. If required these taxes will be included in the invoice for the purchase of the SAS Training Points or a separate invoice will be sent for payment remittal.
4. SAS Training Points can be used to register and pay for SAS Training Points-Eligible Products and Services. These events will have varying SAS Training Points assigned to them according to their registration or license fees or standard charges.
5. All SAS Training Points licensed pursuant to this Supplement shall expire on December 20, 2020.
6. Class and conference sizes are limited and space is not guaranteed. On-site classes are limited to 15 students per class.
7. SAS reserves the right to cancel or reschedule any and all SAS Training Points-Eligible Products and Services at its discretion. SAS is not responsible for airline penalties related to the cancellation of SAS courses or events. Please be aware of all airline restrictions regarding nonrefundable airline tickets when purchasing an airline ticket.
8. The SAS Training Points Administrator will issue an account number to the designated contact upon receipt of its SAS Training Points order. Payment terms are net 30 days. The contact may begin using its SAS Training Points as soon as it receives an account number, but not before then.
9. No other discounts are applicable.
10. SAS Training Points fees are non-refundable.

Cancellation Policy

11. Public Courses: SAS Training Points may be reinstated to the account if cancellations are received by mail or e-mail at least 8 calendar days prior to the scheduled start date of an event; after that (7 calendar days or less), SAS Training Points accounts will be charged the full number of corresponding SAS Training Points. Substitutions (name changes) are accepted at any time prior to the event. Transfers are accepted up to 24 hours before the event start date and students are allowed one transfer per course registration.

On-Site Cancellation Policy

12. On-site and Private Live Web Courses: The Customer may cancel on-site courses without charge if notification is received by SAS by phone or in writing no later than 21 days prior to the course start date. Rescheduling a course less than 21 days prior to course start date is considered a cancellation, and a cancellation fee of 25% of the total fee for the scheduled training will be charged and invoiced separately. In addition, if non-refundable airline tickets have been purchased for SAS personnel with Customer's approval, Customer will be responsible for the cost of these tickets.

STATE OF MICHIGAN
DEPARTMENT OF TECHNOLOGY, MANAGEMENT & BUDGET
PROCUREMENT

525 W. ALLEGAN STREET
LANSING, MI 48933

P.O. BOX 30026
LANSING, MI 48909

CHANGE NOTICE NO. 7
to
CONTRACT NO. **071B3200061**
between
THE STATE OF MICHIGAN
and

NAME & ADDRESS OF CONTRACTOR	PRIMARY CONTACT	EMAIL
SAS Institute Inc. 100 SAS Campus Drive Cary, NC 27513	Wayne Kuipers	wayne.kuipers@sas.com
	PHONE	CONTRACTOR'S TAX ID NO. (LAST FOUR DIGITS ONLY)
	(616) 403-2275	3017

STATE CONTACTS	AGENCY	NAME	PHONE	EMAIL
PROGRAM MANAGER / CCI	DTMB	John Karlik	(517) 335-4062	karlikj@michigan.gov
CONTRACT ADMINISTRATOR	DTMB	Simon Baldwin	(517) 284-6997	baldwins@michigan.gov

CONTRACT SUMMARY			
DESCRIPTION: Enterprise Fraud Detection Software Project			
INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW
December 21, 2012	December 20, 2015	(5) 1-Year Options	December 20, 2015
PAYMENT TERMS		DELIVERY TIMEFRAME	
N/A		N/A	
ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING
<input type="checkbox"/> P-card <input type="checkbox"/> Direct Voucher (DV) <input type="checkbox"/> Other			<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
MINIMUM DELIVERY REQUIREMENTS			
N/A			

DESCRIPTION OF CHANGE NOTICE				
EXERCISE OPTION?	LENGTH OF OPTION	EXERCISE EXTENSION?	LENGTH OF EXTENSION	REVISED EXP. DATE
<input checked="" type="checkbox"/>	1-Year Option	<input type="checkbox"/>	N/A	December 20, 2016
CURRENT VALUE		VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE	
\$14,264,326.00		\$0.00	\$14,264,326.00	
DESCRIPTION: Effective November 19, 2015, The first option year available for this Contract is hereby exercised. The revised Contract expiration date is December 20, 2016. Please note, the Contract Administrator has been changed to Simon Baldwin. All other terms, conditions, specifications, and pricing remain the same per Contractor and Agency agreement and DTMB Procurement approval.				

STATE OF MICHIGAN
DEPARTMENT OF TECHNOLOGY, MANAGEMENT AND BUDGET
PROCUREMENT
P.O. BOX 30026, LANSING, MI 48909
OR
525 W. ALLEGAN, LANSING, MI 48933

CHANGE NOTICE NO. 6
to
CONTRACT NO. 071B3200061
between
THE STATE OF MICHIGAN
and

NAME & ADDRESS OF CONTRACTOR	PRIMARY CONTACT	EMAIL
SAS Institute Inc. 100 SAS Campus Drive Cary, NC 27513	Wayne Kuipers(See Section 2.025 for Legal Notices)	Wayne.Kuipers@sas.com
	PHONE	VENDOR FEIN # (LAST FOUR DIGITS ONLY)
	616-403-2275	3017

STATE CONTACTS	AGENCY	NAME	PHONE	EMAIL
PROGRAM MANAGER	DTMB	John Karklik	517-335-4062	KarlikJ@michigan.gov
CONTRACT ADMINISTRATOR	DTMB	Mike Breen	517-284-7002	BreenM@michigan.gov

CONTRACT SUMMARY			
DESCRIPTION: Enterprise Fraud Detection Software Project			
INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW
December 21, 2012	December 20, 2015	5, one year	December 20, 2015
PAYMENT TERMS	F.O.B.	SHIPPED TO	
N/A	N/A	N/A	
ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING
<input type="checkbox"/> P-card <input type="checkbox"/> Direct Voucher (DV) <input type="checkbox"/> Other			<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
MINIMUM DELIVERY REQUIREMENTS			
N/A			

DESCRIPTION OF CHANGE NOTICE				
EXTEND CONTRACT EXPIRATION DATE	EXERCISE CONTRACT OPTION YEAR(S)	EXTENSION BEYOND CONTRACT OPTION YEARS	LENGTH OF OPTION/EXTENSION	EXPIRATION DATE AFTER CHANGE
<input checked="" type="checkbox"/> No <input type="checkbox"/> Yes	<input type="checkbox"/>	<input type="checkbox"/>		
CURRENT VALUE		VALUE/COST OF CHANGE NOTICE	ESTIMATED REVISED AGGREGATE CONTRACT VALUE	
\$14,264,326.00		\$0.00	\$14,264,326.00	
DESCRIPTION: Effective September 2, 2015, this contract is hereby amended to clarify the "warranty" language with Section 1.104 of the existing contract per agency (DHHS) request and DTMB-Procurement approval. All other terms, conditions, specifications and pricing remain the same.				

STATE OF MICHIGAN
 DEPARTMENT OF TECHNOLOGY, MANAGEMENT AND BUDGET
 PROCUREMENT
 P.O. BOX 30026, LANSING, MI 48909
 OR
 525 W. ALLEGAN, LANSING, MI 48933

CHANGE NOTICE NO. 5
 to
CONTRACT NO. 071B3200061
 between
THE STATE OF MICHIGAN
 and

NAME & ADDRESS OF CONTRACTOR	PRIMARY CONTACT	EMAIL
SAS Institute Inc. 100 SAS Campus Drive Cary, NC 27513	Wayne Kuipers(See Section 2.025 for Legal Notices)	Wayne.Kuipers@sas.com
	PHONE	VENDOR FEIN # (LAST FOUR DIGITS ONLY)
	616-403-2275	3017

STATE CONTACTS	AGENCY	NAME	PHONE	EMAIL
PROGRAM MANAGER	DTMB	John Karklik	517-335-4062	KarlikJ@michigan.gov
CONTRACT ADMINISTRATOR	DTMB	Mike Breen	517-284-7002	BreenM@michigan.gov

CONTRACT SUMMARY			
DESCRIPTION: Enterprise Fraud Detection Software Project			
INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW
December 21, 2012	December 20, 2015	5, one year	December 20, 2015
PAYMENT TERMS	F.O.B.	SHIPPED TO	
N/A	N/A	N/A	
ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING
<input type="checkbox"/> P-card <input type="checkbox"/> Direct Voucher (DV) <input type="checkbox"/> Other			<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
MINIMUM DELIVERY REQUIREMENTS			
N/A			

DESCRIPTION OF CHANGE NOTICE				
EXTEND CONTRACT EXPIRATION DATE	EXERCISE CONTRACT OPTION YEAR(S)	EXTENSION BEYOND CONTRACT OPTION YEARS	LENGTH OF OPTION/EXTENSION	EXPIRATION DATE AFTER CHANGE
<input checked="" type="checkbox"/> No <input type="checkbox"/> Yes	<input type="checkbox"/>	<input type="checkbox"/>		
CURRENT VALUE		VALUE/COST OF CHANGE NOTICE	ESTIMATED REVISED AGGREGATE CONTRACT VALUE	
\$14,264,326.00		\$0.00	\$14,264,326.00	

DESCRIPTION:

Effective March 20, 2015, clarification to the DCH Medicaid provider module enterprise fraud protection system is hereby added to the contract (protection of DCH Data within the confines of the system).

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

STATE OF MICHIGAN
DEPARTMENT OF TECHNOLOGY, MANAGEMENT AND BUDGET
PROCUREMENT
P.O. BOX 30026, LANSING, MI 48909 OR 530 W. ALLEGAN, LANSING, MI 48933

CHANGE NOTICE NO. 4
to
CONTRACT NO. 071B3200061
between
THE STATE OF MICHIGAN

NAME & ADDRESS OF CONTRACTOR:	PRIMARY CONTACT	EMAIL
SAS Institute Inc. 100 SAS Campus Drive Cary, NC 27513	Wayne Kuipers (See Section 2.025 for Legal Notices)	Wayne.Kuipers@sas.com
	TELEPHONE	CONTRACTOR #, MAIL CODE
	616-403-2275	

STATE CONTACTS	AGENCY	NAME	PHONE	EMAIL
CONTRACT COMPLIANCE INSPECTOR	DTMB	John Karlik	517-335-4062	KarlikJ@michigan.gov
BUYER	DTMB	Mike Breen	517-284-7002	BreenM@michigan.gov

CONTRACT SUMMARY:

DESCRIPTION: **Enterprise Fraud Detection Software Project**

INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW
12/21/2012	12/20/2015	Five One-Year	12/20/2015
PAYMENT TERMS	F.O.B	SHIPPED	SHIPPED FROM
N/A	N/A	N/A	N/A
ALTERNATE PAYMENT OPTIONS:			AVAILABLE TO MIDEAL PARTICIPANTS
<input type="checkbox"/> P-card <input type="checkbox"/> Direct Voucher (DV) <input type="checkbox"/> Other			<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
MINIMUM DELIVERY REQUIREMENTS: N/A			

DESCRIPTION OF CHANGE NOTICE:

EXTEND CONTRACT EXPIRATION DATE	EXERCISE CONTRACT OPTION YEAR(S)	EXTENSION BEYOND CONTRACT OPTION YEARS	LENGTH OF OPTION/EXTENSION	EXPIRATION DATE AFTER CHANGE
<input checked="" type="checkbox"/> No <input type="checkbox"/> Yes	<input type="checkbox"/>	<input type="checkbox"/>	N/A	
VALUE/COST OF CHANGE NOTICE:			ESTIMATED AGGREGATE CONTRACT VALUE REMAINS:	
\$0.00			\$14,264,326.00	

Effective November 24, 2014, Appendix C – Payment Schedule, Table 1 (for DHS portion only) 4.3 Phase I FAP Initial Deployment (estimated October 2014) is revised. Revised Appendix C – for DHS only attached. All other pricing, terms and conditions remain the same. Per Contractor and DTMB Procurement approval.

REVISED Contract Change Notice # 4 for (***change to DHS Phase 1 FAP Deployment)

Appendix C. Payment Schedule

SUMMARY TOTAL CONTRACT COST:

Table Number	Table Description	
Table 1	Work and Deliverables Services and Software Payment Schedule	\$4,210,658
Table 2	Warranty, Maintenance and Support	\$1,366,533
Table 3	Contingency Fund - Task 1.104.10	\$430,500
Estimate Contract Value		\$6,007,691

Table 1 - Column Definitions:

Task	The reference to the task number identified in the Contract.
Project Milestone	The description of the Task as outlined in the Contract.
Services Accrual	The amount of Services Payments withheld until the completion and acceptance of both FAP and UIA Implementations.
Services Payment	The amount paid upon completion and acceptance of both FAP and UIA Implementations.
Licensing Cost	The portion of total software license that will be paid the sooner of the Invoice Date or the completion of the Project Milestone.

Table 1 – Work and Deliverables Services and Software Payment Schedule

Task	Project Milestones	Services Accrual	Services Payment	Licensing Cost (Invoice Date)
	Contract Execution			\$700,000 (Contract Execution)
1	Initiation and Planning			
1.1	Project Planning			
1.2	General Timeline			
1.3	Confirm Infrastructure			
1.4	Product Installation			
	Initiation and Planning Complete	\$162,360	\$0	\$150,000 (2/28/2013)
2	Phase 1 FAP Requirements & Design			
2.1	Requirements Definition			
2.2	Functional Design			
3	Phase 1 FAP Construction & Testing			
3.1	Construction and Testing Plan			
3.2	Data Preparation			
3.3	Configure FAP Fraud Detection Analysis Scenarios			
3.4	Integrations			
3.5	Transition and Operations Planning			
3.6	System Testing			

Task	Project Milestones	Services Accrual	Services Payment	Licensing Cost (Invoice Date)
3.7	User Acceptance Testing			
	Phase 1 FAP Construction & Testing Complete			\$500,000 (5/31/2013)
4	Phase 1 FAP Implementation			
4.1	Production Cutover			
4.2	Installation Testing			
4.3	Post Implementation Evaluation Report			
***	Phase 1 FAP Initial Deployment (estimated October 2014)	\$421,080	\$200,000	\$500,000 (7/31/2013)
5	Phase 2 UIA Requirements & Design			
5.1	Requirements Definition			
5.2	Functional Design			
	Phase 2 UIA Functional Design Approved			\$150,000 (8/30/2013)
6	Phase 2 UIA Construction & Testing			
6.1	Construction and Testing Plan			
6.2	Data Preparation			
6.3	Configure UIA Benefit and Tax Fraud Detection Analysis Scenarios			
6.4	Integrations			
6.5	Transition and Operations Planning			
6.6	System Testing			
6.7	User Acceptance Testing			
	Phase 2 UIA Construction & Testing Complete			\$500,000 (8/30/2013)
7	Phase 2 UIA Implementation			
7.1	Production Cutover			
7.2	Installation Testing			
7.3	Post Implementation Evaluation Report			
	Phase 2 UIA Implementation Acceptance	\$567,358	\$ 950,798	\$559,860 (9/30/2013)
	Total Services and Software Payments		\$1,150,798	\$3,059,860

STATE OF MICHIGAN
DEPARTMENT OF TECHNOLOGY, MANAGEMENT AND BUDGET
PROCUREMENT
P.O. BOX 30026, LANSING, MI 48909 OR 530 W. ALLEGAN, LANSING, MI 48933

CHANGE NOTICE NO. 3
to
CONTRACT NO. 071B3200061
between
THE STATE OF MICHIGAN

NAME & ADDRESS OF CONTRACTOR:	PRIMARY CONTACT	EMAIL
SAS Institute Inc. 100 SAS Campus Drive Cary, NC 27513	Wayne Kuipers (See Section 2.025 for Legal Notices)	Wayne.Kuipers@sas.com
	TELEPHONE	CONTRACTOR #, MAIL CODE
	616-403-2275	

STATE CONTACTS	AGENCY	NAME	PHONE	EMAIL
CONTRACT COMPLIANCE INSPECTOR	DTMB	John Karlik	517-335-4062	KarlikJ@michigan.gov
BUYER	DTMB	Mike Breen	517-241-3215	BreenM@michigan.gov

CONTRACT SUMMARY:

DESCRIPTION: **Enterprise Fraud Detection Software Project**

INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW
12/21/2012	12/20/2015	Five One-Year	12/20/2015
PAYMENT TERMS	F.O.B	SHIPPED	SHIPPED FROM
N/A	N/A	N/A	N/A
ALTERNATE PAYMENT OPTIONS:			AVAILABLE TO MIDEAL PARTICIPANTS
<input type="checkbox"/> P-card <input type="checkbox"/> Direct Voucher (DV) <input type="checkbox"/> Other			<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
MINIMUM DELIVERY REQUIREMENTS: N/A			

DESCRIPTION OF CHANGE NOTICE:

EXTEND CONTRACT EXPIRATION DATE	EXERCISE CONTRACT OPTION YEAR(S)	EXTENSION BEYOND CONTRACT OPTION YEARS	LENGTH OF OPTION/EXTENSION	EXPIRATION DATE AFTER CHANGE
<input checked="" type="checkbox"/> No <input type="checkbox"/> Yes	<input type="checkbox"/>	<input type="checkbox"/>	N/A	12/20/2015
VALUE/COST OF CHANGE NOTICE:			ESTIMATED AGGREGATE CONTRACT VALUE REMAINS:	
\$3,379,557.00			\$14,264,326.00	
Effective March 11, 2014, via State Administrative Board approval, \$3,379,557.00 is hereby added to this contract. All other pricing, terms and conditions remain the same.				

ATTACHMENT

WHEREAS, this Attachment is made a part of Change Notice No. 3 ("Change Notice") and entered into by and between the State of Michigan ("State") and SAS Institute Inc. ("SAS" or "Contractor") to Contract No. 071B3200061 (as amended, the "Contract");

WHEREAS, the Contract contemplates that additional modules may be added by State agencies from time to time;

WHEREAS, the State and Contractor wish to enter into this Change Notice for the additional module pursuant to Section 2.024 of the Contract in order to assist the Department of Human Services with the detection of Medicaid eligibility fraud and abuse, to operate in conjunction with the software originally licensed pursuant to the Contract;

WHEREAS, Consultant and the State desire to modify the Contract in consideration of further benefits to each to license additional software and order additional services related to the additional module described herein; and

NOW, THEREFORE, notwithstanding any provision to the contrary contained in the Contract to the contrary, the parties hereby agree to amend the Contract as set forth herein:

1. The recitals set forth above are incorporated into this Change Notice.
2. All capitalized terms used but not defined herein shall have the meaning set forth in the Contract.
3. As the term is used herein, the Effective Date of this Change Notice shall be March 31, 2014.
4. The paragraph entitled "Description" in Section 1.104.1 ("Project Initiation and Planning Phase") is hereby deleted in its entirety and replaced with the following:

"The following activities are performed during initiation and planning and continue through the project execution, as appropriate and necessary to control and report on the project. The ongoing activities detailed in this section apply to Phase 1 FAP, Phase 2 UIA, Phase 3 Medicaid Provider Fraud Detection, and Phase 4, Medicaid Eligibility Fraud Detection."

5. The following shall be added as a new paragraph under the "Objective" paragraph of Section 1.104.8 ("Warranty") of the Contract:

"The parties acknowledge and agree that the "Warranty Period" with respect to Phase 4 Medicaid Eligibility Fraud Detection shall be the one year period beginning after Implementation Acceptance of the Medicaid Eligibility Fraud Detection Module."

6. The following shall be added as a new paragraph under the "Warranty Period" paragraph of Section 1.104.8 ("Warranty") of the Contract:

"The Warranty Period with respect to Phase 4 Medicaid Eligibility Fraud Detection shall be the one year period beginning after Implementation Acceptance of the Medicaid Eligibility Fraud Detection Module."

7. The description of services included as Exhibit A to this Change Notice shall be added as a new Section 1.900: "Scope of Work and Deliverables for Phase 4 Medicaid Eligibility Fraud Detection Module" to the Contract.
8. The Medicaid Eligibility Fraud Detection Module Payment Schedule included as Exhibit B to this Change Notice is hereby added to the Contract as a new Appendix C.2.
9. Section 1 ("License Grant; Authorized Use; Purpose") of the Master License Agreement, which is included as Appendix G to the Contract, is hereby deleted in its entirety and replaced with the following:

SAS grants Customer a nonexclusive, nontransferable and nonassignable license to use the Software for the Purpose with designated operating systems under the Agreement. Except as otherwise provided in the Agreement, the Software may be accessed only by Customer's

employees and on site contractors ("Users") doing work in the United States solely for the following State of Michigan governmental agencies: Unemployment Insurance Agency, Department of Human Services, the Office of Inspector General, and the Department of Community Health. The license is an annual license renewed at the mutual agreement of the parties. Renewal is accomplished by SAS sending an invoice for the applicable Software license renewal fees and Customer paying the invoice.

"Purpose" means use by four (4) authorized State of Michigan agencies (Unemployment Insurance Agency, Department of Human Services ("DHS"), the Office of Inspector General, and the Department of Community Health) to provide data integration, analytics and reporting capabilities solely to support fraud and improper payments detection, investigation and prevention efforts within Customer's UIA, FAP, and Medicaid Provider programs.

The parties acknowledge and agree that solely with respect to the Medicaid Eligibility Fraud Detection Module, Users shall only include those current employees and on-site contractors of DHS, provided such number of Users shall not exceed the total number of authorized Users. The parties further acknowledge and agree that solely with respect to the Medicaid Eligibility Fraud Detection Module, the Purpose shall be limited to assisting the Department of Human Services with the detection of fraud and improper payments within DHS' Medicaid Eligibility Programs.

10. As required by Section 2.072 of the Contract, the Department of Technology, Management and Budget, Procurement hereby gives its consent to SAS to delegate a portion of the services to Kforce Inc..
11. This Change Notice, together with the Contract, constitute the parties' complete and exclusive statement regarding the Medicaid Eligibility Fraud Detection Module. Should a conflict arise between this Change Notice and the Contract, this Change Notice shall control. Except as herein modified, all terms and conditions of the Contract shall remain in full force and effect.

EXHIBIT A

SECTION 1.900

1.900: Medicaid Eligibility Fraud Detection Module

The following services shall be provided with respect to the Medicaid Eligibility Fraud Detection Module ("Medicaid Eligibility Module"), which will be part of the State of Michigan Enterprise Fraud Detection Software Project.

1.901: Phase 4 - Medicaid Eligibility Fraud Detection Module: Requirements & Design

Objective

The objective of the Phase 4 Medicaid Eligibility: Requirements & Design Phase is to develop a mutual understanding between the Medicaid business owners/users and the project team with regards to the business requirements for Medicaid Eligibility Module of the State of Michigan Enterprise Fraud Detection Software Project. The Contractor will map the 'what to do' of the requirements specification into the 'how to do' of the design specifications. Finally, the user-oriented functional design specifications will be translated into a set of technical system design specifications.

Description

Requirements & Design Phase kickoff is the first major milestone of the fourth project phase. Project Teams are defined in this phase and the Contractor will hold a definition session with the State to understand the State's requirements and overall functionality of the Medicaid Eligibility Fraud Detection Module. The following tasks are performed during the requirements and design phase and will continue through the project execution, as appropriate and necessary to control and report on the project.

Task 14: Stage 0 - Project Initiation and Planning Phase

The objective of the Project Initiation and Planning Phase is for the project management team to develop the project definition, planning tools and artifacts for Medicaid Eligibility Module. The planning phase and the associated kick-off meeting will be a collaboration between the Contractor and the State of Michigan. It provides opportunities to formally recognize the start of the project, meet project participants, and communicate a shared view of the scope of the project. Contractor will work with the State to produce related project documentation, including a Project Management Methodology (PMM) documentation, Documentation Management Plan, Communication Plan, Resource Management Plan, Change Control Management Plan, Risk Management Plan, and Quality Management Plan

Deliverables

- Summary notes from kick-off meeting.
- Documentation Management Plan
- Communication Plan
- Resource Management Plan
- Change Management Plan
- Risk Management Plan
- Quality Management Plan
- Project Plan/Work Breakdown Structure (WBS)
- Project Schedule

State Responsibility

- Provide input for agenda for kick-off meetings
- Attend and participate in the kick-off meeting
- Provide input into the project plan
- Review and provide input into the contractors PMM and associated content
- Make available appropriate resources within the State of Michigan for meetings and planning sessions
- Develop/revise the required project management documentation
- Schedule status meetings

Contractor Responsibility

- Facilitate the kickoff meeting

- Develop specific objectives and agenda for the Kick-off Meetings
- Schedule and chair the kick-off Meetings
- Generate meeting record for the kick-off Meetings

Acceptance Criteria

- The kick-off meeting will be deemed accepted upon completion of the meeting. Other Deliverables set forth above are subject to the acceptance procedures set forth in Sections 1.501, 2.253, 2.254 and 2.255.

Task 14.1: Stage 1 - Requirements Definition

The Requirements Definition task develops a basis of mutual understanding between the business owner/users and the project team with regards to the Medicaid Eligibility Module. The result of this understanding is a mutually agreed upon Requirements Specification – which becomes the initial baseline for implementation design. The functional and technical/general requirements for the system are also reviewed and confirmed during this stage. In addition, the services requirements for the Medicaid Eligibility fraud detection analysis scenario configuration are also defined.

Activities associated with this stage include:

- Select the Requirements Analysis Technique to be utilized by Contractor
- Define Phase 4 Medicaid Eligibility System Requirements
- Compile and Document Phase 4 Medicaid Eligibility System Requirements
- Develop Phase 4 Medicaid Eligibility System Test Plan Requirements
- Develop Phase 4 Medicaid Eligibility Acceptance Test Plan Requirements
- Establish Phase 4 Medicaid Eligibility Functional Baseline

Deliverables

- Initiation and Requirement sections of the Initiation, Requirements and Design Plan.

State Responsibility

- Complete Infrastructure Services Request (DIT-0184) provided by Contractor to the State
- Develop Acceptance Test Requirements
- Create Initiation, Requirements and Design Plan
- Participate in system requirement workshops and sessions as needed
- Review Initiation and Requirements sections of the Initiation, Requirements and Design Plan

Contractor Responsibility

- Review baseline functional requirements
- Verification of technical/general requirements
- Verification of services requirements for Medicaid Eligibility fraud detection analysis scenario configuration.
- Lead requirement workshops and sessions to confirm and finalize functional, technical/general and services requirements with the State
- Provide input and clarifications to the State as needed
- Complete initiation and requirements sections of the Initiation, Requirements and Design Plan
- Develop System Test Requirements
- Provide input to State on Initiation and Requirements sections of the Initiation, Requirements and Design Plan

Acceptance Criteria

- Completion and acceptance of Initiation and Requirements sections of the Initiation, Requirements and Design Plan

Task 14.1a: Stage 1 -Development Environment Install and Configuration

The objective of this task is to prepare a development environment for the deployment of the Medicaid Eligibility Module. This stage involves verifying that the proposed hardware and the software are ready for deploying a development environment. Upon completion, the development environment will be made available to the Contractor and State development teams. Contractor will install and configure the Medicaid Eligibility Module within the development ready environment.

“Install” means the process of loading the software in Customer’s hardware environment and ensuring that the software is operating properly in accordance with the software documentation. “Configure” means the process of electing between pre-defined options in order to allow the software to operate as desired within Customer’s environment

Deliverable

- Installation of the Medicaid Eligibility Module onto the development environment
- Related Report Documentation

State Responsibility

- Provide Contractor with necessary hardware, as well as appropriate network and remote access to the State’s development environment
- Provide support during the implementation, including making available appropriate personnel
- Attendance Appropriate Personnel
- Review Installation Plan and provision of feedback to such plan to Contractor
- Facilitate Michigan security and technical architecture reviews, as needed

Contractor Responsibility

- The Contractor must provide the necessary resources to install the Medicaid Eligibility onto the development hardware, per the Installation Plan.
- Update the Installation Plan
- Follow the Installation Plan
- Document the installation
- Installation of the Medicaid Eligibility Module onto the development environment

Acceptance Criteria

- Completion of environment build. Installation documentation will be deemed accepted upon delivery by Contractor.

Task 14.2: Functional Design

During Functional Design, the ‘what to do’ of the requirements specification are mapped into the ‘how to do it’ of the design specifications. During this activity, the overall structure of the solution is defined from a functional viewpoint for Phase 4 Medicaid Eligibility. The functional design describes the logical system flow, data organization, system inputs and scenario configuration. The goal of this activity is to define and document the functions of the solution to the extent necessary to obtain the system owner and users’ approval to the level of detail necessary to configure the system. The functional, technical/general and Medicaid Eligibility fraud detection analysis scenario configuration requirements are mapped to system design specifications.

Activities include:

- Design Content of Phase 4 Medicaid Eligibility System Inputs
- Design Phase 4 Medicaid Eligibility System Security Controls
- Develop Phase 4 Medicaid Eligibility Functional Design
- Develop Phase 4 Medicaid Eligibility Test Cases

Deliverables

- Design Plan section of Initiation, Requirements and Design Plan including required templates
- Documentation for test cases

State Responsibility

- Review Initiation, Requirements and Design Plan
- Provide input to Contractor on Initiation and Requirements
- Participate in functional design workshops and sessions
- Develop User Acceptance Test Cases
- Attend walkthrough of Initiation, Requirements and Design Plan Provide access to data and working environment necessary for any design tasks or data analysis

Contractor Responsibility

- Lead functional design workshops and sessions to confirm and finalize functional design with the State.
- Provide input and clarifications to the State as needed

- Complete functional system design
- Complete technical/general design
- Complete Medicaid Eligibility fraud detection analysis scenario configuration design
- Develop System Test Cases
- Complete Design section of Initiation, Requirements and Design Plan Update Initiation, Requirements and Design Plan
- Conduct walkthrough of Initiation, Requirements and Design Plan

Acceptance Criteria

- Approval of the Initiation, Requirements and Design Plan per the criteria set forth in the Contract.
- Test case documentation will be deemed accepted upon delivery to the State.

1.902 Phase 4 Medicaid Eligibility: Deployment & Testing

Objective

The objective of the Phase 4 Medicaid Eligibility: Deployment and Testing Phase is to configure the system to conform to the system design specifications.

Description

The tasks and activities of this stage will result in the transformation of the system design into the complete executable representation of the solution. Functionality is tested to determine the solution meets predetermined functionality, performance, quality, and security requirements. System testing is conducted to validate the solution will operate in its intended environment, satisfies all the user requirements, and is supported with complete and accurate documentation. User Acceptance Testing (UAT) follows system testing, and solicits feedback from users for the Contractor to make any final adjustments before releasing the solution for implementation.

Associated Tasks

- 15.1 Create Deployment and Testing Plan
- 15.2 Data Exploration and Preparation
- 15.3 Data Load and Match
- 15.4 Configure Business Rule Detection
- 15.5 Anomaly Detection
- 15.6 Advanced Analysis & Networks
- 15.7 Transition and Operations Planning
- 15.8 System Testing
- 15.9 User Acceptance Testing (UAT)

Task 15.1: Deployment and Testing Plan

The Contractor is responsible for completing the Deployment and Testing Plan which contains the essentials for test reporting, transition planning, installation planning and State acceptance of the tested system.

Deliverables

- Deployment and Testing Plan

State Responsibility

- Provide timely feedback and information required by the Contractor
- Attend walkthrough of Deployment and Testing Plan
- Review Deployment and Testing Plan
- Complete initial Deployment and Testing Plan

Contractor Responsibility

- Solicit information from the State as needed
- Conduct walkthrough of Deployment and Testing Plan
- Provide input to State on the Deployment and Testing Plan

Acceptance Criteria

- Approval of Deployment and Testing Plan per the acceptance criteria set forth in the Contract.

Task 15.2: Stage 1 - Data Exploration and Preparation

The Contractor will assist the State with identifying data needed to support the Medicaid Eligibility Module. The Contractor will, in consultation with the State, assist the State with its research and assessment of the viability and relevance of potential data sources for analyzing Medicaid eligibility. Following such consultation between the parties, the State and the Contractor will agree to include up to eight (8) data sources ("Data Sources"), with a maximum of ten (10) tables per data source, with an average of 3 tables per data source from which data may be received.

The following list represents the types of data sources which may be applicable. It is not intended to be an exhaustive list, and all Data Sources must be agreed upon by both parties.

- Investigative outcomes from other eligibility and fraud monitoring systems – used for building predictive models and evaluating rules and outlier methods.
- Information from other programs (such as Work First/TANF, Special Assistance, Adoption Services, Refugee Services, SNAP etc.) – used to baseline typical usage of these programs for outlier detection, for determining providers who are also recipients and for comparing information given at time of application
- Medicaid claims history – used to baseline typical usage for outlier detection and for determining providers who are also recipients
- Medicaid Prescription history (MAPS) – used to baseline typical usage for outlier detection and for determining providers who are also recipients
- Treasury Data – Used to verify income and assets
- MSHDA Data – used to baseline usage of housing voucher and utility assistance
- Lottery – Used to verify income and assets
- SSA Master Death Index – Used to verify death. Note that the SSA file is better for verification of death when the death occurred outside of the state
- ESC/Employment Securities Commission – Used to verify income/employment
- Census data – Used to baseline norms for physical areas
- Employment Program Information System – Used to determine participation in program
- Vital Statistics – Used to verify death. Note that this is the better source for verification of death when the death occurs within the state.
- Division of Motor Vehicles - Used to verify personal assets as well as demographic information
- County Property Tax Records – Used for asset verification.
- Register of Deeds – State level, used to verify information.
- Uniform Commercial Code Records – Used to verify business ownership/interests
- Trust and Annuity Records – Used for asset verification
- State Health Plan Data – Used to verify income and determine double dipping with Medicaid
- Department of Justice – Used to verify sex offender status and demographics.
- Department of Correction – Used to verify Jail/Prison times/locations.
- Lexis Nexis – Used to verify demographics, bankruptcies, convictions for felonies, assets, business ownership stakes, etc.
- 3rd Party Financial data – Used to verify insurance carried as well as credit status
 - Equifax
 - Insurance Carrier Information

Contractor will review and analyze the data relating to the Data Sources, to the extent such data is provided by the State, as well as identify data feeds for minimal data architecture and identify key variables and identifiers from the Data Sources.

Deliverables

- Demonstration of data exploration results.
- Documentation for agreed upon Data Sources
- Preliminary Requirements Matrix
- Preliminary design specifications
- Preliminary test plans

State Responsibility

- Provide timely feedback and information required by the Contractor
- Attend demonstration of data preparation for required patterns and analysis scenarios completed by the Contractor
- Provide Contractor preliminary user-acceptance test (UAT) criteria.
- Provide timely access to data required by the Contractor.
- Ensure data quality and provision of Clean Data (see definition provided in “Assumptions” herein). Contractor will not be able to complete the tasks described herein without the delivery of data by the State.

Contractor Responsibility

- Processing of data provided by the State for to detect patterns and analyze scenarios
- Solicit information from the State as needed
- Lead demonstration to the State of the data exploration for Data Sources.

Acceptance Criteria

- Contractor’s demonstration of the data exploration results will be deemed accepted upon delivery of such results to the State.
- Approval of preliminary requirements matrix, preliminary test plan, preliminary data source documentation, and preliminary design specifications per the acceptance criteria set forth in the Contract.

Task 15.3: Stage 2 - Data Load and Match

Contractor will load the Data Sources within the Medicaid Eligibility Module, validate the data, and perform initial matching of recipients across the various sources. Assumptions about clean and unclean data can be in the “Assumptions” section of this Exhibit A.

Deliverables

- Data quality report
- Data integration design document.

State Responsibility

- Provide timely feedback and information required by the Contractor
- Make Clean Data (as defined in the “Assumptions” section herein) available in the development environment to the Contractor within mutually agreeable timeframes.

Contractor Responsibility

- Assess data quality
- Filter unwanted records included in data provided by the State
- Examine suspicious records and update metadata before adding to warehouse
- Build data integration process for selected data sources
- Configure initial set of mutually agreed data matching rules

Acceptance Criteria

- Demonstration by Contractor to the State that the Medicaid Eligibility fraud detection analysis scenarios have been completed and configured.
- Acceptance of the data quality report and data integration design document.

Task 15.4: Stage 2 - Configure Business Rule Detection

Configure the software detection engine with the agreed upon business rules and processes to identify and rank Medicaid enrollees who have inconsistent eligibility information. For purposes of this section, “business rules” are those rules or parameters which are mutually agreed to by the parties which best detect potential instances of fraud, waste, or abuse. Contractor will verify the software functions and performs in accordance with the approved requirement matrix content. Contractor will use the business rules to perform initial retrospective analysis of current enrollee population across the various data sources using the software and results of the initial data matching performed by Contractor.

The Initial Retrospective Recipient Analysis Report is a one-time report delivered by Contractor to the State prior to production that evaluates information across Data Sources. This report will leverage existing matching techniques that compare information provided to various agencies across time. This report, which will be delivered in a mutually agreeable format (HTML, PDF, Excel, etc.), includes the following: Identification of potential fraud cases for customer validation of rules as configured, and will provide consolidated information relating to recipients to assist in improved investigation

Deliverables

- A report to document the eligibility status of Medicaid recipients that was derived based on the business rules.
- Initial Retrospective Recipient Analysis Report
- Ranking Criteria Document

State Responsibility

- Provide feedback and input regarding the deployed business rules
- Provide a primary point of contact for questions or issues
- Review initial retrospective recipient analysis report

Contractor Responsibility

- Design and build initial eligibility rules Identification
- Create documentation regarding the ranking criteria within development environment.

Acceptance Criteria

- Approval of the initial Eligibility Results from business rules, and ranking criteria document per the acceptance criteria set forth in the Contract.
- Delivery of the initial eligibility results will be deemed accepted upon delivery by Contractor.

Task 15.5: Stage 3 - Anomaly Detection

Stage 3 will focus on anomaly detection. Whereas Stage 2 analysis focused on identifying discrepancies across data sources for an individual recipient, Stage 3 will be geared towards identifying demographic norms (as defined herein) and comparing recipient eligibility data to those norms to assist the State with the identification of potentially anomalous individuals. Contractor will begin the initial design and configuration of interfaces and investigation screens, which includes defining business rules for use in the alerting interface. As in Stage 2, a report will be provided showing those recipients who meet certain anomaly thresholds so the State may consider what actions may need to be taken. As in Stage 2 this report will be delivered in a mutually agreeable format, however in future phases the information will be presented using the SAS Fraud Framework User Interface ("SFF UI"). Configuration of the user interface will also commence in Stage 3, and continue into Stage 4 and 5.

For purposes of this section, "norms" are determined using various statistical methods to determine what normal usage of services is in terms of individual programs as well as how recipients use multiple programs. In general, various statistical distributions are fit to the data and the influence of outliers is determined. Depending on the results of this analysis, norms may be determined based on the data distribution as-is, the distribution of the data when a robust method is used (e.g. trimming or Winsorizing), or after a normalizing transformation is used.

Deliverables

- Initial Anomaly Retrospective Recipient Analysis Report. This report, which will be delivered in a mutually agreeable format (HTML, PDF, Excel, etc.), will be aimed towards the following:
 1. Identification of the most likely potential fraud cases as determined by the anomaly methods, that is the cases that are most abnormal, and detailed in the aforementioned report to assist the State with early intervention
 2. Prioritization of recipients to assist the State with better resource allocation, automated routing, and assignment to State investigators
 3. Providing consolidated information related to recipients

State Responsibility

- Provide feedback and input with respect to the Anomaly Retrospective Recipient Analysis Report
- Provide a primary point of contact for questions or issues

Contractor Responsibility

- Design and build anomaly Retrospective Recipient Analysis Report
- Deploy anomaly detection techniques

Acceptance Criteria

- Per sections 1.501, 2.253, 2.254 and 2.255, approval of the Anomaly Retrospective Recipient Analysis Report

Task 15.6: Stage 4 - Advanced Analysis & Networks

This stage will consist of performing an analysis of the State's Medicaid Eligibility network as well as an advanced matching analysis of the data. Network analysis will consist of identifying obvious and non-obvious relationships between eligible individuals and entities, as mutually agreed to by the parties during the requirements gathering phase, to assist the State in determining family relationships or groups of associated individuals. This analysis will then be used to cross match family information or identify anomalies relative to such identified groups. Advanced matching analysis of the data will extend the direct matching performed in Stage 2 to include non-direct matches. This will be aimed towards providing the State with an enhanced capability geared towards positively identifying recipients that may not have a common, unique identifier across all the different data source systems, as well as identifying those recipients that may be providing inconsistent identity information. As in Stage 2 and 3, a report (once in production the information is supplied in the SFF UI), which will be delivered in a mutually agreeable format (HTML, PDF, Excel, etc.), will be provided identifying such individuals.

Within this stage, Contractor will also configure the Software's social network analysis capability to define networks of related enrollees and assist the State with analyzing Medicaid eligibility data across family units and previously unknown relationships. Such configuration will include verification of the following:

- Review matching rules and criteria from previous phases
- Application of advanced patented matching algorithms to recipient data
- Design and build social network eligibility rules
- Identify and document ranking criteria

Contractor will also utilize retrospective analysis using the Software and advanced matching techniques of current enrollee population across the Data Sources. Such analysis will be geared towards the following:

- Identification of the most likely potential fraud cases to assist the State with early intervention as determined by the advanced methods and detailed in the aforementioned report, prioritized to assist the State with better resource allocation, automating routing, and assignment to State investigators
- Providing consolidated information related to recipients through the configured UI

Deliverables

- Advanced retrospective analysis report
- Deployed analytical detection and network analysis

State Responsibility

- Provide feedback and input with respect to the Advanced retrospective analysis report
- Provide a primary point of contact for questions or issues
- Finalize UAT testing criteria

Contractor Responsibility

- Design and deploy Advanced Retrospective Recipient Analysis Report
- Deploy advanced analytical and network detection techniques

Acceptance Criteria

- Per sections 1.501, 2.253, 2.254 and 2.255, approval of the Advanced Retrospective Recipient Analysis Report

Task 15.7: Transition and Operations Planning

The plan to complete the operations transition will be documented by the Contractor in the Operations Transition Plan. This plan will include the following:

- Transition schedules and tasks
- Contractor assistance with the State's hardware and software deployment strategy
- Personnel requirements
- Management Controls
- Reporting

Deliverables

- Operations Transition Plan

State Responsibility

- Review and approve the Operations Transition Plan
- Provide input and clarifications to the Contractor as needed

Contractor Responsibility

- Develop an Operations Transition Plan
- Define the relationships and responsibilities between the Contractor and State personnel for State of Michigan Enterprise Fraud Detection Software operations

Acceptance Criteria

- Per sections 1.501, 2.253, 2.254 and 2.255, approval of the Operations Transition Plan

Task 15.8: System Testing

The Test Plan created in the Deployment and Testing Template will be executed for system testing. Once the product is fully integrated, system testing is conducted to validate that the product will operate in its intended environment, satisfies all user requirements, and is supported with complete and accurate operating documentation. Anomalies identified at this step are recorded and tracked to resolution.

The Contractor must schedule, coordinate, and perform all system testing activities. The State is responsible for producing all test data required for the system testing activities. The Contractor will provide guidance and input to assist the State with the compilation of appropriate test data.

The Contractor will address issues discovered during system testing by following normal application development procedures, which may include modifying the appropriate configuration items in the development environment, unit and integration testing the change, and promoting the configuration and new development items within the testing environment.

The State is responsible for supporting the Contractor in system testing of the entire State of Michigan Enterprise Fraud Detection Software Project.

The Contractor will lead periodic problem review meetings with the State, to analyze issues and failed scenarios. The Contractor will review common issues and failed scenarios reported in system testing and collaborate with the State to improve configuration, development and testing processes with the objective of minimizing the occurrence of these issues and improving the efficiency. The Contractor will also provide knowledge transfer of the plan which is designed to meet conversion, implementation, operation, and development needs of the State

Deliverables

- Documented System Test results

State Responsibility

- Provide assistance and input to Contractor on data necessary to support testing
- The State is responsible for supporting the Contractor in system testing
- Provide a functional test environment
- Review test data
- Assist with the create of the system test schedule and test procedures

- Review failed test scenarios
- Participate in status meetings

Contractor Responsibility

- Create test scripts
- Review test data
- Create test procedures
- Execute test scripts
- Document test results
- Record issues
- Modify test scripts and scenarios, if needed
- Create additional test scripts and scenarios, if needed
- Retest resolved issues and perform regression testing
- Ensure that data is loaded to the Test Environment
- Address issues found

Acceptance Criteria

- All system tests pass. Test result documentation will be deemed accepted upon delivery by Contractor.

Task 15.9: User Acceptance Testing (UAT)

The UAT Test Plan created by the State is executed for User Acceptance Testing. Anomalies identified at this step are recorded and tracked to resolution. User Acceptance Testing begins upon completion of System Testing.

The State will schedule, coordinate, and monitor all UAT activities. The State is responsible for providing end users and Subject Matter Experts to perform UAT.

The State is responsible for producing all test data required for the UAT test activities, as mutually agreed to by the parties.

The Contractor will provide support for the duration of UAT. The testing process must include the ability to advance the testing clock from a historical position to provide for a complete test of the lifecycle of cases over many simulated months or years.

The Contractor will also address issues discovered during UAT by following normal application development procedures – modifying the appropriate configuration items in the development environment, unit and integration testing the change, and promoting the configuration and new development items to the testing environment. Issues shall not include any customer enhancements, changes or other modifications to previously State approved requirements and design. Promotions to the testing environment will occur on a mutually agreed upon regularly scheduled basis (e.g., daily) and emergencies (e.g., UAT cannot continue until the problem is resolved).

The State will take the lead on scheduling, conducting, and validating UAT issues. This activity includes specifying dates and times for end users to conduct testing. The Contractor is responsible for supporting the State users in UAT for the State of Michigan Enterprise Fraud Detection Software Medicaid Eligibility Module and., knowledge transfer on any tools to assist end users on how test results will be produced, viewed, and reported.

The Contractor will provide knowledge transfer to the State UAT team in the functionality and capabilities of State of Michigan Enterprise Fraud Detection Software Medicaid module before conducting the UAT task. The State will lead periodic problem review meetings with the Contractor, to analyze issues and failed scenarios.

The Contractor will review common issues reported in UAT testing and collaborate with the State to improve configuration, development and testing processes with the objective of minimizing the occurrence of these issues and improving the efficiency.

Deliverables

- UAT results
- Knowledge transfer plan designed to meet implementation, operation, and configuration needs of the State for the Medicaid Eligibility Module.
- Up to 3 Business Days (not to exceed eight (8) hours each day) investigator knowledge transfer taught at customer location at mutually agreeable times.

State Responsibility

- Schedule State UAT Testers for training
- Attend training
- Provide input to Contractor on data necessary to support testing
- Review test data
- Create UAT schedule and test procedures
- Conduct tests to validate results
- Document test results
- Record issues
- Document issues using Jira Issue tracking
- Conduct Problem Review meeting
- Modify the Test Scenarios, if needed
- Create additional Test Scenarios, if needed
- Retest resolved issues and perform regression testing
- Attend status meetings

Contractor Responsibility

- Ensure all modifications to the Medicaid Eligibility Module are thoroughly system tested
- Ensure data is loaded to the Test Environment
- Configure and run simulations which enable the State to execute test cases.
- Provide knowledge transfer
- Assist with the creation of the UAT Test schedule and test procedures
- Review failed test scenarios and recommend most efficient and accurate resolutions
- Participate in Problem Review meeting(s)
- Address issue with the State on any issues found
- Assist with coordination of regression testing, as needed
- Conduct status meetings

Acceptance Criteria

- UAT test cases pass
- Approval of knowledge transfer plan designed to meet implementation, operation, and configuration needs for the Medicaid Eligibility Module.
- Knowledge transfer sessions will be deemed complete upon completion of such training courses

1.903: Phase 4 Medicaid Eligibility: Implementation**Objective**

The objective of Phase 4 Medicaid Eligibility: Implementation is to prepare a production environment for deployment of the system.

Description

The Implementation Phase involves verification that the production environment hardware and software is production ready. The system security plan is finalized to ensure the product environment meets all security requirements for the system. Contractor will assist the State with adopting disaster recovery procedures for the system to the State's business continuity plan.

Once the preparation is complete, a detailed cutover task list and schedule are prepared. Each step to be performed is included, along with checkpoints and rollback procedures. The production software goes live, and the system data and functionality is validated. The results of this validation will drive a "go/no go" decision from the State. If there are significant issues, the system deployment may be rolled back, per procedures.

Related Tasks

- 16.1 Eligibility Model Deployment
- 16.2 Production Cutover
- 16.3 Installation Testing
- 16.4 Post Implementation Evaluation Report (PIER)

Task 16.1: Stage 5 - Eligibility Model Deployment

Stage 5 will consist of the rollout of the solution including the operationalizing of the matching, social networking, and reporting and analysis capabilities defined in Stage 2, 3 and 4. In connection with this stage, Contractor will perform the following:

- Operationalize the methods implemented in Stage 2, 3 and 4; deliver the scored results within the SFF UI, aimed towards the following:
 - Identification of the most likely potential fraud cases to assist the State with early intervention
 - Prioritization of recipients to assist the State with better resource allocation, automating routing, and assignment to State investigators
 - Providing consolidated information related to recipients
- Perform recurring social network analysis as defined and agreed upon during the application requirements and project plan creation phases. This analysis will be geared towards allowing State investigators to visualize relationships between people and data in order to help uncover potential organized fraud networks or suspicious or previously unknown relationships. This tool will focus on providing the following types of analyses:
 - Analyze data for suspicious relationships
 - Define relationships between providers and participants
 - Link referred cases to other individuals in the program
- Operationalize Social Network Analysis - The Social Network Analysis Interface is an HTML based user interface (UI) for exploring and investigating networks. The web based UI will include tabular and graphical content and will be geared towards assisting investigators with the following:
 - Identification of suspects involved in known historic collusions
 - Identification of new suspects in potential collusion rings
 - Identification of potentially new collusion rings from both referred cases and statistically designed risk factors
 - Provide graphical output for enhanced reporting and visualization

Deliverables

- Quality Assurance (QA) testing results. "Quality Assurance" means the process by which Contractor ensures the Medicaid Eligibility Module conforms to the technical requirements set forth herein.
- Deliver specific user documentation.
- Design Document
- Provide knowledge transfer for up to fifteen (15) participants for two (2) half day training session at customer location. Training will focus on using the software to conduct eligibility analysis and investigations.

State Responsibility

- Review and sign off on Design Documentation
- Appropriate personnel made available to address questions and issues in a timely manner
- Ensure knowledge transfer sessions as described above have occurred.

Contractor Responsibility

- Deploy solution Development environment
- Promote to Test Environment for UAT (if applicable)
- Finalize and deliver design documentation
- Complete QA testing and documentation
- Conduct Knowledge Transfer

Acceptance Criteria

- Approval of design document, specific user documentation, and QA testing documentation per the acceptance criteria set forth in the Contract.
- Knowledge Transfer sessions will be deemed completed upon completion of the two half day training sessions.

Task 16.2: Production Cutover

The System goes live. Desk-side support is provided to end users and operations are carefully monitored.

The Contractor updates the Installation Plan which provides the list of interrelated steps and activities that must be coordinated to ensure a smooth and successful rollout. The Installation Plan is followed during Production Cutover.

A high-level checklist is prepared for general consumption within the agency to communicate the general schedule. A detailed, step-by-step checklist is prepared for the project team to follow.

Perform Software Implementation

The Contractor must provide the necessary resources to install the State of Michigan Enterprise Fraud Detection Software onto the production hardware per the Installation Plan. Any and all issues must be resolved during the installation procedures prior to cutover to the new software.

Deliverable

- Installation of the Medicaid Eligibility Module onto the production environment
- "Go/no go" Check List

State Responsibility

- Provide support/ desk-side support during the implementation
- Attendance of Appropriate Personnel in the "go/no-go" review meeting
- Review Installation Plan
- Prepare the "go/no-go" checklist
- Make "go/no go" decision

Contractor Responsibility

- Update the Installation Plan
- Follow the Installation Plan
- Review the "go/no-go" Check List
- Installation of the Medicaid Eligibility Module onto the production environment

Acceptance Criteria

- The Installation Plan will be deemed accepted upon delivery by Contractor.
- Installation of the Medicaid Eligibility Module.

Task 16.3: Installation Testing

The Contractor must test the Medicaid Eligibility Module in the State production environment to ensure the software is installed and functioning properly. These tests should work to:

- Ensure the environment is properly installed and configured
- Ensure the State of Michigan Enterprise Fraud Detection Software is completely functional
- Ensure data is ported to the production environment
- Ensure the implementation of the Medicaid Eligibility Module does not alter any other modules licensed by the State already in production
- Identify any issues or problems in the environment against expected results for all tests

Deliverables

- Conduct Installation Testing

State Responsibility

- Provide staff to assist the Contractor in the Installation Testing activity
- Review and approve Installation Test results
- Review and approve Regression Test results

Contractor Responsibility

- Test the production environment to ensure it is fully installed and operating properly
- Ensure data is ported to the production environment
- Resolve any issues/problems for installation
- Regression test any modules already in production
- Provide installation test results

Acceptance Criteria

- Completion of Production Installation Testing

Task 16.4: Post Implementation Evaluation Report (PIER)

The Contractor is responsible, with input from the State, for completing the Post-Implementation Evaluation Report for Phase 4 Medicaid Eligibility.

Deliverable

- Post Implementation Evaluation Report (PIER)

State Responsibility

- Review the Post Implementation Evaluation Report
- Provide feedback to Contractor
- Approve the Post Implementation Evaluation Report

Contractor Responsibility

- Complete the Post Implementation Evaluation Report
- Correct any identified deficiencies

Acceptance Criteria

- Acceptance of the Post Implementation Evaluation Report per the acceptance criteria set forth in the Contract.

ASSUMPTIONS

The description of the services contained in this statement of work was developed using the following assumptions. Any changes to these assumptions may impact the scope of the services to be accomplished hereunder, or may result in the imposition of additional fees. Such changes will be addressed using the Change Management process provided for in the Contract.

Access to Subject Matter Experts:

- The State will provide personnel resources to assist SAS to understand unique business rules and processes for each System function and related data sources.

Data-Related Items:

- The State is responsible for providing all required data to SAS and obtaining any data use agreements that may be required.
- The State will provide data in a mutually agreed upon format and timeframe.
- File format is the same for historical data and ongoing data and will remain consistent throughout the Term.
- The State will provide sample data, data dictionaries, and entity diagrams (if applicable) for the required data sources.
- After identification of the Data Sources, SAS will assess the quality of the source data. If SAS determines there to be significant data integrity issues, SAS' ability to deliver the customized services may be impacted. If this occurs, the state shall re-prioritize requirements. Data quality and any other factors regarding usability of the source data will be the responsibility of the State.
- A Clean Data Extract - A data extract delivered to the SAS that is representative and identical to the source system it was extracted from. Source system fields, tables, and subsets based on timeframe will be defined during the requirements gathering and definition phase. Examples of unclean data include but are not limited to:
 - Truncated fields or Otherwise Incomplete data
 - Invalid Dates or Codes
 - Outdated data
 - Incorrect data associated with a field
 - Extract layout does not match the data layout provided with the extract
- Customer and SAS mutually agree on scheduled data refreshes, based on the availability of data feeds.
- Customer provides delta changes in production data feeds, if possible

General

- The State and SAS will enter into a contract, which shall be an amendment to the Original Contract, which will outline the services to be provided, and any other relevant terms and conditions.

- The State will provide and make available all hardware and infrastructure related items including, but not limited to: physical hardware, third-party software required (Oracle DB, JBoss or Weblogic), disk storage, network and security configurations within 60 days of contract signature.
- The State will provide SAS with remote connectivity for VPN and remote system access.
- The State will assign a project manager to work with SAS' project manager to coordinate service related activities.
- The State will provide any State specific business requirements as it pertains to Eligibility Business Rules.
- The State project manager will be responsible for coordinating and obtaining any third parties or third party data needed to satisfy the requirements.
- Changes to requirements will be managed through the SOM change control process.
- The State will make available resources to assist with business questions, application construction, data modeling, database administration, and IT functions. The State will also make available content experts to validate functionality, usability, and accuracy of results.
- The State will be available during normal business hours to participate in discussions, meetings, and walk-throughs of interim work products and deliverables based on the project plan deliverables, weekly status meetings, monthly steering meeting and ad hoc meetings based on project needs.
- The project team will leverage SAS' online collaboration tools for issue tracking, account requests, change management and documentation delivery.
- The State will lead and coordinate UAT efforts. The SAS team will play a support and issue resolution role to assist the State with the UAT effort.
- The State will provide timely investigation into any alerts provided and communicate results/findings back to the project team for enhancement of the business rules.
- All estimated timeframes are based on receipt of verified Clean Data into the State of Michigan Enterprise Fraud Detection Software Project.
- The State will provide timely feedback and approvals of Deliverables described herein
- The technical requirements stipulated in the Contract shall otherwise apply to the services described herein.
- The SAS team will also include remote deployment resources engaged solely for delivery of the services described in this Exhibit. SAS remote resources will travel to the customer site for key meetings and deliverables, as mutually agreed to by SAS and State project managers.

EXHIBIT B

PAYMENT SCHEDULE FOR MEDICAID PROVIDER FRAUD DETECTION MODULE

SUMMARY TOTAL COST FOR MEDICAID PROVIDER FRAUD DETECTION MODULE:

Table Number	Table Description	
Table 1	Work and Deliverables Services and Software Payment Schedule	\$2,683,831
Table 2	Warranty, Maintenance and Support	\$695,726
Estimated Value		\$3,379,557

Table 1 - Column Definitions:

Task	The reference to the task number identified in the Contract.
Project Milestone	The description of the Task as outlined in the Contract.
Services Payment	The amount paid upon completion and acceptance of Medicaid Eligibility Fraud Detection Module implementation milestones.
Licensing Cost	The total software license that will be paid on the Invoice Date.

Table 1 – Work and Deliverables Services and Software Payment Schedule

Task	Project Milestones: Phase 4 Medicaid Eligibility Fraud Detection Module	*Services Payment	Licensing Cost (Invoice Date)
	Contract Execution		\$1,557,828

Task	Project Milestones: Phase 4 Medicaid Eligibility Fraud Detection Module	*Services Payment	Licensing Cost (Invoice Date)
			(Change Notice Execution)
14			
14	Stage 0 - Project Initiation and Planning Phase		
	Initiation and Planning Complete	\$202,681	
	Requirements & Design		
14.1	Requirements Definition		
14.1a	Development Environment Install and Configuration		
14.2	Functional Design Complete		
	Functional Design Approved	\$337,801	
15	Deployment and Testing		
15.1	Create Deployment and Testing Plan		
15.2	Stage 1 - Data Exploration and Preparation		
15.3	Stage 2 -Data Load and Match		
15.4	Stage 2 - Configure Business Rule Detection		
15.5	Stage – 3 Anomaly Detection		
15.6	Stage 4 - Advanced Analysis & Networks		
15.7	Transition and Operations Planning		
15.8	System Testing		
15.9	User Acceptance Testing		
	Deployment & Testing Complete	\$394,101	
16	Implementation		
16.1	Stage 5 - Eligibility Model Deployment		
16.2	Production Cutover		
16.3	Installation Testing		
16.4	Post Implementation Evaluation Report		
	Implementation Acceptance	\$191,420	
	Total Services and Software Payments	\$1,126,003	\$1,557,828

****Implementation services do not include services for future years related to installation of software upgrades, patches, hotfixes etc...***

Notes:

1. The Contractor will provide the Medicaid Eligibility Fraud Detection Module as part of the Michigan Enterprise Fraud Detection System, which is an Enterprise License. Note (2)(a) of Appendix C of the Contract is hereby deleted and replaced with the following:
 - a. The Michigan Enterprise Fraud Detection System is comprised of the following SAS offerings: SAS Fraud Framework for Government, SAS Fraud Framework for Healthcare, DataFlux Data Management Server and Studio Enrichment, DataFlux DataPack (DF) – US Address Verification. Contractor shall also provide a separate limited license to SAS Visual Analytics, solely for use in connection with the Medicaid Provider Fraud Detection Module and the Medicaid Eligibility Fraud Detection Module. Includes four modules, UIA Benefits

Overpayments, FAP (SNAP) Fraud Detection, Medicaid Provider Fraud Detection, and Medicaid Eligibility Fraud Detection. Up to five (5) SAS Access Engine licenses and the associated services to implement them. Four authorized agencies at this time are Unemployment Insurance Agency, Department of Human Services, Department of Community Health, and The Office of Inspector General. Except as otherwise provided herein, includes eighty (80) Fraud Framework clients, not concurrent, and five (5) DF Client users, not concurrent and an unlimited number of Investigative Workbench clients (web-based GUI). Use by DCH of the Medicaid Eligibility Fraud Detection Module shall be further subject to the User restrictions set forth in Section 1 of Appendix G. Additional clients, fraud modules and expansion of use to other agencies are available from SAS for additional fees. Use of SAS Visual Analytics is included, but may only be used by Users (as such term is defined in connection with the Medicaid Eligibility Fraud Detection Module) for the Purpose (as such term is defined in connection with the Medicaid Eligibility Fraud Detection Module) in connection with the Medicaid Eligibility Fraud Detection Module.

3. With respect to the Medicaid Provider Fraud Detection Module, the License Costs will be paid as defined in the Licensing Cost Column in Table 1. Invoices will be due on the dates listed in the Licensing Cost column of Table 1.

Table 2 – Warranty, Maintenance and Support

Task	Warranty, Maintenance and Support Activities for Phase 3 Medicaid Provider Fraud Detection Module	Cost
8.1	Warranty (One Year) Complete Begins on the effective date of this Change Notice	\$ Included in first year software costs
9.1	Maintenance and Support (Support Year 1) Complete	\$ Included in first year software costs
9.1	Maintenance and Support (Support Year 2) Complete	\$342,722
9.1	Maintenance and Support (Support Year 3) Complete	\$353,004
	Total for Support years 1-3.	\$695,726

Notes:

1. Warranty: Includes Costs for One (1) Year of Warranty as described in Section 1.104.8.
2. Maintenance and Support: Payment for Support Year 2 is made upon the end of the Contract Warranty Period identified in Section 1.104.8.

STATE OF MICHIGAN
DEPARTMENT OF TECHNOLOGY, MANAGEMENT AND BUDGET
PROCUREMENT
P.O. BOX 30026, LANSING, MI 48909 OR 530 W. ALLEGAN, LANSING, MI 48933

CHANGE NOTICE NO. 2
to
CONTRACT NO. 071B3200061
between
THE STATE OF MICHIGAN

NAME & ADDRESS OF CONTRACTOR:	PRIMARY CONTACT	EMAIL
SAS Institute Inc. 100 SAS Campus Drive Cary, NC 27513	Wayne Kuipers (See Section 2.025 for Legal Notices)	Wayne.Kuipers@sas.com
	TELEPHONE	CONTRACTOR #, MAIL CODE
	616-403-2275	

STATE CONTACTS	AGENCY	NAME	PHONE	EMAIL
CONTRACT COMPLIANCE INSPECTOR	DTMB	John Karlik	517-335-4062	KarlikJ@michigan.gov
BUYER	DTMB	Mike Breen	517-241-3215	BreenM@michigan.gov

CONTRACT SUMMARY:

DESCRIPTION: **Enterprise Fraud Detection Software Project**

INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW
12/21/2012	12/20/2015	Five One-Year	12/20/2015
PAYMENT TERMS	F.O.B	SHIPPED	SHIPPED FROM
N/A	N/A	N/A	N/A
ALTERNATE PAYMENT OPTIONS:			AVAILABLE TO MIDEAL PARTICIPANTS
<input type="checkbox"/> P-card <input type="checkbox"/> Direct Voucher (DV) <input type="checkbox"/> Other			<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
MINIMUM DELIVERY REQUIREMENTS: N/A			

DESCRIPTION OF CHANGE NOTICE:

EXTEND CONTRACT EXPIRATION DATE	EXERCISE CONTRACT OPTION YEAR(S)	EXTENSION BEYOND CONTRACT OPTION YEARS	LENGTH OF OPTION/EXTENSION	EXPIRATION DATE AFTER CHANGE
<input checked="" type="checkbox"/> No <input type="checkbox"/> Yes	<input type="checkbox"/>	<input type="checkbox"/>	N/A	12/20/2015
VALUE/COST OF CHANGE NOTICE:			ESTIMATED AGGREGATE CONTRACT VALUE REMAINS:	
\$0.00			\$10,884,769.00	

Effective immediately this contract amended to include the Medicaid Fraud Software, Implementation Services and Maintenance and Support as outlined in Appendix H of the Contract and further described Attachment. This Change notice finalizes the requirements and invoice/payment schedule for this module that was included in the Contract through Change Notice #1.

All other pricing, terms and conditions remain the same.

ATTACHMENT

WHEREAS, this Attachment is made a part of Change Notice No. 2 ("Change Notice") and entered into by and between the State of Michigan ("State") and SAS Institute Inc. ("SAS" or "Contractor") to Contract No. 071B3200061 (as amended, "Contract");

WHEREAS, Appendix H of the Contract contemplates the addition of an additional module ("Additional Module") designed to assist with the detection of Medicaid provider fraud and abuse to operate in conjunction with the software originally licensed pursuant to the Contract;

WHEREAS, the State and Contractor previously entered into Change Notice No. 1 contemplating the addition of the software and services described in this Attachment;

WHEREAS, the State and Contractor wish to enter into this Attachment to the Change Notice for the Additional Module pursuant to Section 2.024 of the Contract;

WHEREAS, Contractor and the State desire to modify the Contract in consideration of further benefits to each to license additional software and order additional services related to such Additional Module; and

NOW, THEREFORE, notwithstanding any provision to the contrary contained in the Contract to the contrary, the parties hereby agree to amend the Contract as set forth herein:

1. The recitals set forth above are incorporated into this Change Notice.
2. All capitalized terms used but not defined herein shall have the meaning set forth in the Contract.
3. As the term is used herein, the Effective Date of this Change Notice shall be December 31, 2013.
4. The paragraph entitled "Description" in Section 1.104.1 ("Project Initiation and Planning Phase") is hereby deleted in its entirety and replaced with the following:

"The following activities are performed during initiation and planning and continue through the project execution, as appropriate and necessary to control and report on the project. The ongoing activities detailed in this section apply to Phase 1 FAP, Phase 2 UIA, and Phase 3 Medicaid Provider Fraud Detection."

5. The following shall be added as a new paragraph under the "Objective" paragraph of Section 1.104.8 ("Warranty") of the Contract:

"The parties acknowledge and agree that the "Warranty Period" with respect to Phase 3 Medicaid Provider Fraud Detection shall be the one year period beginning on the effective date of this Change Notice and shall run concurrently with the Maintenance and Support for Year 1."

6. The following shall be added as a new paragraph under the "Warranty Period" paragraph of Section 1.104.8 ("Warranty") of the Contract:

"The Warranty Period with respect to Phase 3 Medicaid Provider Fraud Detection shall be the one year period beginning on the effective date of this Change Notice."

7. The following shall be added as a new sentence at the end of the first paragraph of Task 8.1 of Section 1.104.8 ("Warranty"):

"The parties acknowledge and agree that any Deliverables required in connection with this task shall be provided to the State after the warranty period begins with respect to Phase 1 or Phase 2 (as such period is described in the first sentence of the "Objective" paragraph of this Section 1.104.8)."

8. The description of services included as Exhibit A to this Change Notice shall be added as a new Section 1.800: "Scope of Work and Deliverables for Phase 3 Medicaid Provider Fraud Detection Module" to the Contract.

9. The Additional Module Payment Schedule included as Exhibit B to this Change Notice is hereby added to the Contract as a new Appendix C.1.
10. Section 1 ("License Grant; Authorized Use; Purpose") of the Master License Agreement, which is included as Appendix G to the Contract, is hereby deleted in its entirety and replaced with the following:

SAS grants Customer a nonexclusive, nontransferable and nonassignable license to use the Software for the Purpose with designated operating systems under the Agreement. Except as otherwise provided in the Agreement, the Software may be accessed only by Customer's employees and on site contractors ("Users") doing work in the United States solely for the following State of Michigan governmental agencies: Unemployment Insurance Agency, Department of Human Services, the Office of Inspector General, and the Department of Community Health. The license is an annual license renewed at the mutual agreement of the parties. Renewal is accomplished by SAS sending an invoice for the applicable Software license renewal fees and Customer paying the invoice. "Purpose" means use by four (4) authorized State of Michigan agencies (Unemployment Insurance Agency, Department of Human Services, the Office of Inspector General, and the Department of Community Health) to provide data integration, analytics and reporting capabilities solely to support fraud and improper payments detection, investigation and prevention efforts within Customer's UIA, FAP, and Medicaid Provider programs.

11. Appendix G to the Contract is hereby amended to include the addition of Supplement Number 2, which is included as Exhibit C to this Change Notice.
12. This Change Notice, including this Attachment, together with the Contract, constitute the parties' complete and exclusive statement regarding the Additional Module. Should a conflict arise between this Attachment and the Contract, this Attachment shall control. Except as herein modified, all terms and conditions of the Contract shall remain in full force and effect.

EXHIBIT A

SECTION 1.800

1.800: Medicaid Provider Fraud Detection Module

The following services shall be provided with respect to the Medicaid Provider Fraud Detection Module.

1.801: Phase 3 Medicaid Provider Fraud Detection: Requirements & Design

Objective

The objective of the Phase 3 Medicaid Provider: Requirements & Design Phase is to develop a mutual understanding between the Medicaid business owners/users and the project team with regards to the business requirements for Phase 3 Medicaid Provider of the State of Michigan Enterprise Fraud Detection Software Project. The Contractor will map the 'what to do' of the requirements specification into the 'how to do' of the design specifications. Finally, the user-oriented functional design specifications are translated into a set of technical system design specifications.

Description

Requirements & Design Phase kickoff is the first major milestone of the third project phase. Project Teams are defined and the Contractor completes the definition sessions to understand the State's requirements and overall functionality of the State of Michigan Enterprise Fraud Detection Software for Phase 3 Medicaid Provider Fraud Detection. The following tasks are performed during the requirements and design phase and continue through the project execution, as appropriate and necessary to control and report on the project.

Tasks

- 11.0 Initiation and Planning
- 11.1 Requirements Definition
- 11.2 Functional Design

Task 11.0: Initiation and Planning

Contractor will perform Tasks 1.1, 1.2, 1.3, and 1.4, each as set forth in the Contract, in connection with the Medicaid Provider Fraud Detection Module. References to "Phase 1 FAP" or "Phase 2 UIA" in such sections shall be deemed to include references to "Phase 3 Medicaid Provider Fraud Detection." The parties acknowledge and agree that any specific dates or deadlines referenced in such sections shall be scheduled upon mutual agreement by the parties in connection with Phase 3 Medicaid Provider Fraud Detection.

Task 11.1: Requirements Definition

The Requirements Definition task develops a basis of mutual understanding between the business owner/users and the project team with regards to the Phase 3 Medicaid Provider business requirements of the State of Michigan Enterprise Fraud Detection Software Project. The result of this understanding is a mutually agreed upon Requirements Specification – which becomes the initial baseline for implementation design. The functional and technical/general requirements for the system are reviewed and confirmed. In addition, the services requirements for the Medicaid provider fraud detection analysis scenario configuration are defined.

Activities include:

- Select Requirements Analysis Technique
- Define Phase 3 Medicaid Provider System Requirements
- Compile and Document Phase 3 Medicaid Provider System Requirements
- Develop Phase 3 Medicaid Provider System Test Plan Requirements
- Develop Phase 3 Medicaid Provider Acceptance Test Plan Requirements
- Establish Phase 3 Medicaid Provider Functional Baseline

Deliverables

- Initiation and Requirement sections of the Initiation, Requirements and Design Plan (SEM 01-Exp), including attached SEM templates

State Responsibility

- Complete Infrastructure Services Request (DIT-0184), based on an Enterprise Architecture Solutions Assessment (EASA), to be prepared by the State
- Develop Acceptance Test Requirements
- Provide input to Contractor on Initiation and Requirements sections of SEM 01-Exp
- Participate in system requirement workshops and sessions as needed
- Review Initiation and Requirements sections of the Initiation, Requirements and Design Plan (SEM 01-Exp) including required SEM templates

Contractor Responsibility

- Verification of functional requirements
- Verification of technical/general requirements
- Verification of services requirements for Medicaid Provider fraud detection analysis scenario configuration.
- Lead requirement workshops and sessions to confirm and finalize functional, technical/general and services requirements with the State
- Provide input and clarifications to the State as needed
- Complete Initiation and Requirements sections of Initiation, Requirements and Design Plan (SEM 01-Exp)
- Develop System Test Requirements
- Review and provide input to State in connection with its preparation of EASA.

Acceptance Criteria

- Completion of Initiation and Requirements sections of the Initiation, Requirements and Design Plan (SEM 01-Exp) including required SEM templates

Task 11.2: Functional Design

During Functional Design the 'what to do' of the requirements specification are mapped into the 'how to do it' of the design specifications. During this activity, the overall structure of the solution is defined from a functional viewpoint for Phase 3 Medicaid Provider. The functional design describes the logical system flow, data organization, system inputs and scenario configuration. The goal of this activity is to define and document the functions of the solution to the extent necessary to obtain the system owner and users' approval to the level of detail necessary to configure the system. The functional, technical/general and Medicaid Provider fraud detection analysis scenario configuration requirements are mapped to system design specifications.

Activities include:

- Determine Phase 3 Medicaid Provider System Structure
- Initial Data intake, data validation, and exploratory data analysis
- Design Content of Phase 3 Medicaid Provider System Inputs
- Design Phase 3 Medicaid Provider System Security Controls
- Develop Phase 3 Medicaid Provider Functional Design
- Develop Phase 3 Medicaid Provider Test Cases

Deliverables

- Design Plan section of Initiation, Requirements and Design Plan (SEM 01-Exp) including required SEM templates

State Responsibility

- Review Initiation, Requirements and Design Plan (SEM 01-Exp)
- Provide input to Contractor on Initiation and Requirements sections of SEM 01-Exp
- Participate in functional design workshops and sessions
- Develop User Acceptance Test Cases
- Attend walkthrough of Initiation, Requirements and Design Plan (SEM 01-Exp)
- Provide access to data and working environment necessary for any design tasks or data analysis

Contractor Responsibility

- Lead functional design workshops and sessions to confirm and finalize functional design with the State.
- Provide input and clarifications to the State as needed
- Complete functional system design
- Complete technical/general design
- Complete Medicaid Provider fraud detection analysis scenario configuration design
- Develop System Test Scenarios
- Complete Design section of Initiation, Requirements and Design Plan (SEM 01-Exp)
- Update Initiation, Requirements and Design Plan (SEM 01-Exp)
- Conduct walkthrough of Initiation, Requirements and Design Plan (SEM 01-Exp)

Acceptance Criteria

- Per section 1.501, 2.253, 2.254 & 2.255, approval of the Initiation, Requirements and Design Plan (SEM 01-Exp) including required SEM templates.

1.802 Phase 3 Medicaid Provider: Deployment & Testing

Objective

The objective of the Phase 3 Medicaid Provider: Deployment and Testing Phase is to configure the system to conform to the system design specifications.

Description

The tasks and activities of this stage result in the transformation of the system design into the complete executable representation of the solution. Functionality is tested to determine the solution meets predetermined functionality, performance, quality, and security requirements. System testing is conducted to validate the solution will operate in its intended environment, satisfies all the user requirements, and is supported with complete and accurate documentation. User Acceptance Testing (UAT) follows system testing, and solicits feedback from users for the Contractor to make any final adjustments before releasing the solution for implementation.

Tasks

- 12.1 Deployment and Testing Plan (SEM 02-Exp)
- 12.2 Data Preparation
- 12.3 Configure Medicaid Provider Fraud Detection Analysis Scenarios
- 12.4 Integrations
- 12.5 Transition and Operations Planning
- 12.6 System Testing
- 12.7 User Acceptance Testing (UAT)

Task 12.1: Deployment and Testing Plan (SEM 02-Exp)

The Contractor is responsible for completing the Deployment and Testing Plan which contains the essentials for test reporting, transition planning, installation planning and State acceptance of the tested system.

Deliverables

- Deployment and Testing Plan (SEM 02-Exp)

State Responsibility

- Provide timely feedback and information required by the Contractor
- Attend walkthrough of Deployment and Testing Plan

Contractor Responsibility

- Solicit information from the State as needed
- Complete initial Deployment and Testing Plan (SEM 02-Exp)
- Conduct walkthrough of Deployment and Testing Plan

Acceptance Criteria

- Per section 1.501, 2.253, 2.254 & 2.255, approval of Deployment and Testing Plan (SEM 02-Exp)

Task 12.2: Data Preparation

The Contractor will assist the State with completing data processing needed to support the Phase 3 Medicaid Provider fraud detection analysis from the DTMB warehouse. This includes analyzing the available data from the warehouse, potentially working with DTMB warehouse staff to modify or augment the contents of the data warehouse if needed, and preparing any necessary extract/transform/load (ETL) procedures necessary to support the State of Michigan Enterprise Fraud Detection Software COTS product.

As defined in the Contract, "Clean Data" means a data extract delivered to the contractor/SAS that is representative and identical to the source system it was extracted from. Source system fields, tables, and subsets based on timeframe will be defined during the requirements gathering and definition phase. Examples of dirty data include:

- Truncated fields or Otherwise Incomplete data
- Invalid Dates or Codes
- Outdated data
- Incorrect data associated with a field

- Extract layout does not match the data layout provided with the extract

Deliverables

- Data preparation for required Phase 3 Medicaid Provider fraud detection patterns and analysis scenarios

State Responsibility

- Provide timely feedback and information required by the Contractor
- Attend demonstration of data preparation for required patterns and analysis scenarios completed by the Contractor
- Provide access to appropriate data dictionaries describing the data model(s) involved prior to data delivery
- Provide timely access to data required by the Contractor.
- Ensure data quality and provision of Clean Data.

Contractor Responsibility

- Complete data processing of data/data access provided by the State for required Phase 3 Medicaid Provider fraud detection patterns and analysis scenarios
- Solicit information from the State as needed
- Lead demonstration of the completed data preparation for required Phase 3 Medicaid Provider fraud detection patterns and analysis scenarios to the State which will include a demonstration / walkthrough of data processing and Runbook.

Acceptance Criteria

- Determination by the State of the successful data processing for required Phase 3 Medicaid Provider fraud detection patterns and analysis scenarios in the State of Michigan Enterprise Fraud Detection Software

Task 12.3: Configure Medicaid Provider Fraud Detection Analysis Scenarios

The Contractor is responsible for configuring their existing scenarios for fraud analysis for Medicaid fraud detection as well as configuration of new scenarios from Appendix H that are desired.

Deliverables

- Configuration of fraud detection scenarios as agreed upon in requirements gathering.

State Responsibility

- Provide timely feedback and information required by the Contractor
- Attend demonstration of the fraud detection analysis scenarios by the Contractor

Contractor Responsibility

- Configuration of fraud detection analysis scenarios
- Solicit information to obtain information from the State as needed
- Lead demonstration of the fraud detection analysis scenarios to the State

Acceptance

- Demonstration by Contractor to the State that the Medicaid Provider fraud detection analysis scenarios have been successfully completed and configured

Task 12.4: Integrations

If required, the Contractor solution will integrate the Medicaid provider fraud detection beneficiary analysis results periodically with up to one downstream case management system, to be mutually determined by the parties, based on the severity and priority of the potential cases. The interfaces must be automated.

The Contractor is responsible for documenting, development and testing the interfaces to such system. The data requirements and protocols for each must be defined. The interfaces to be developed along with the communication protocol will be based on the approved Initiation, Requirements and Design Plan (SEM 01-Exp). The State currently anticipates that the communication protocol will be a mutually agreed upon flat file format transmitted via secure FTP or access to mutually agreed upon database tables or views from Contractor. Electronic notifications of success or failure are generated from each interface.

The scope of this task includes integration with any required middleware, testing through the middleware and through the systems components.

The Contractor will work with the State to identify formatted messages that will be exchanged for each interface. The State of Michigan Enterprise Fraud Detection Software will utilize the existing format for interfaces, unless otherwise

directed by the State. The Contractor will perform unit testing to validate the transaction messages match the data layouts.

Deliverables

- Interface Design documents
- Integration of fraud detection scenario results from State of Michigan Enterprise Fraud Detection Software to the Medicaid Provider case management systems

State Responsibility

- Assist in creating the Interface Design documents
- Provide documentation on required interfaces
- Provide input and clarifications to the Contractor as needed

Contractor Responsibility

- Coordinate with the State on questions and problems relating to interfaces
- Identify modifications needed to required interfaces
- Create Interface Design documents
- Develop interfaces
- Perform unit testing on interfaces

Acceptance Criteria

- Approval of Contractor prepared Interface Design document
- Demonstration of successful integration with such mutually agreed upon system

Task 12.5: Transition and Operations Planning

The plan to complete the operations transition must be documented by the Contractor in the Operations Transition Plan. This plan shall include, at a minimum:

- Transition schedules and tasks
- Contractor assistance with the State's hardware and software deployment strategy
- Personnel requirements
- Facilities
- Risk Mitigation Strategies
- Management Controls
- Reporting
- Acceptance Criteria

Deliverables

- Operations Transition Plan

State Responsibility

- Review and approve the Operations Transition Plan
- Provide input and clarifications to the Contractor as needed

Contractor Responsibility

- Develop an Operations Transition Plan
- Define the relationships and responsibilities between the Contractor and State personnel for State of Michigan Enterprise Fraud Detection Software operations

Acceptance Criteria

- Approval of Operations Transition Plan

Task 12.6: System Testing

The Test Plan created in the Deployment and Testing Template (SEM 02-Exp) is executed for system testing. Once the product is fully integrated, system testing is conducted to validate that the product will operate in its intended environment, satisfies all user requirements, and is supported with complete and accurate operating documentation. Anomalies identified at this step are recorded and tracked to resolution.

The Contractor must schedule, coordinate, and perform all system testing activities. The State is responsible for producing all test data required for the system testing activities. The Contractor will provide guidance and input to assist the State with the compilation of appropriate test data.

The Contractor must also correct defects discovered during system testing by following normal application development procedures – modifying the appropriate configuration items in the development environment, unit and integration testing the change, and promoting the configuration and new development items to the testing environment.

The State is responsible for supporting the Contractor in system testing of the entire State of Michigan Enterprise Fraud Detection Software Project.

The Contractor will lead periodic problem review meetings with the State, to analyze defects and failed scenarios. The Contractor will review common defects and failed scenarios reported in system testing and collaborate with the State to improve configuration, development and testing processes with the objective of minimizing the occurrence of these issues and improving the efficiency.

Deliverables

- System Test results
- Comprehensive training plan designed to meet conversion, implementation, operation, and development needs of the State

State Responsibility

- Provide assistance and input to Contractor on data necessary to support testing
- Provide a functional test environment
- Review test data
- Assist with the create of the system test schedule and test procedures
- Review failed test scenarios
- Participate in status meetings

Contractor Responsibility

- Create test scripts
- Review test data
- Create test procedures
- Execute test scripts
- Conduct tests to validate results
- Document test results
- Record defects
- Modify test scripts and scenarios, if needed
- Create additional test scripts and scenarios, if needed
- Retest resolved defects and perform regression testing
- Ensure that data is loaded to the Test Environment
- Provide customized data or interface files, as needed, to complete test scenario execution
- Assist with the creation of the UAT Test schedule and test procedures
- Review failed test scenarios and recommend most efficient and accurate resolutions
- Correct defects found
- Conduct status meetings

Acceptance Criteria

- All system tests pass
- Approval of comprehensive training plan designed to meet conversion, implementation, operation, and development needs of the State

Task 12.7: User Acceptance Testing (UAT)

The Test Plan created in the Deployment and Testing Template (SEM 02-Exp) is executed for User Acceptance Testing. Anomalies identified at this step are recorded and tracked to resolution. User Acceptance Testing begins upon completion of System Testing.

The Contractor will work with the State to schedule, coordinate, and monitor all UAT activities. The State is responsible for providing end users and Subject Matter Experts to perform UAT.

The Contractor is responsible for loading all test data for the UAT and Training activities. The State is responsible for producing all test data required for the system testing activities.

The Contractor must provide support for the duration of UAT. The testing process must include the ability to advance the testing clock to provide for a complete test of the lifecycle of cases over many simulated months or years.

The Contractor must also address defects discovered during UAT by following normal application development procedures – modifying the appropriate configuration items in the development environment, unit and integration testing the change, and promoting the configuration and new development items to the testing environment. Defects shall not include any customer enhancements, changes or other modifications to a previously Contractor approved requirements and design. Promotions to the testing environment must occur on a mutually agreed upon regularly scheduled basis (e.g., daily) and emergencies (e.g., UAT cannot continue until the problem is resolved).

The State will take the lead on conducting UAT. The Contractor is responsible for participating and supporting the State users in UAT of the entire State of Michigan Enterprise Fraud Detection Software Project. This activity includes specifying dates and time for end users to conduct testing, training on any tools to assist end users on how test results will be produced, viewed, and reported.

The Contractor will train the State UAT team in the functionality and capabilities of State of Michigan Enterprise Fraud Detection Software before conducting the UAT task. The State will lead periodic problem review meetings with the Contractor, to analyze defects and failed scenarios.

The Contractor will review common defects and failed scenarios reported in UAT testing and collaborate with the State to improve configuration, development and testing processes with the objective of minimizing the occurrence of these issues and improving the efficiency.

The Contractor will develop a training plan documenting how State staff will be trained on how to operate and maintain the State of Michigan Enterprise Fraud Detection Software. The plan must include a list of all formal courses provided by the Contractor to State staff along with who should attend each class. The Contractor must also provide a list of any pre-requisite classes the State staff needs to operate and maintain the System.

Deliverables

- UAT results
- Comprehensive training plan designed to meet implementation, operation, and configuration needs of the State for Phase 3 Medicaid Provider
- Listing of formal training courses (via a mutually agreed upon training plan), recommended audience, duration and a current schedule for each course
- Description of training courses taught locally
- Provide recommendations as pre-requisite skills and the level of expertise required to support and operate the State of Michigan Enterprise Fraud Detection Software

State Responsibility

- Schedule State UAT Testers for training
- Attend training
- Provide input to Contractor on data necessary to support testing
- Review test data
- Create UAT schedule and test procedures
- Conduct tests to validate results
- Document test results
- Record defects
- Document defects using Incident Reports
- Conduct Problem Review meeting
- Modify the Test Scenarios, if needed
- Create additional Test Scenarios, if needed
- Retest resolved defects and perform regression testing
- Attend status meetings

Contractor Responsibility

- Ensure all modifications to the State of Michigan Enterprise Fraud Detection Software are thoroughly system tested prior to transferring new versions to UAT Testing
- Ensure data is loaded to the Test Environment
- Configure and run simulations which enable the State to execute test cases.
- Provide training
- Assist with the creation of the UAT Test schedule and test procedures
- Review failed test scenarios and recommend most efficient and accurate resolutions
- Participate in Problem Review meeting(s)
- Address with the State any defects found
- Assist with coordination of regression testing as needed

- Conduct status meetings

Acceptance Criteria

- All UAT test cases pass
- Approval of comprehensive training plan designed to meet implementation, operation, and configuration needs for Phase 3 Medicaid Provider
- Approval of listing of formal training courses, recommended audience, duration and a current schedule for each course
- Approval of description of training courses that will be taught locally
- Approval of recommendations as pre-requisite skills and the level of expertise required to support and operate the State of Michigan Enterprise Fraud Detection Software

1.803 Phase 3 Medicaid Provider: Implementation

Objective

The objective of the Phase 3 Medicaid Provider: Implementation is to prepare a production environment for deployment of the system.

Description

The Implementation Phase involves verification that the production environment hardware and software is production ready. The system security plan is finalized to ensure the product environment meets all security requirements for the system and data, including data at rest and data in transit. The disaster recovery procedures for the system are added to the State business continuity plan for the State.

Once the preparation is complete, a detailed cutover task list and schedule are prepared. Each step to be performed is included, along with checkpoints and rollback procedures. The production software goes live, and the system data and functionality is validated. The results of this validation will drive a “go/no go” decision from the State. If there are significant issues, the system deployment may be rolled back, per procedures.

Tasks

- 13.1 Production Cutover
- 13.2 Installation Testing
- 13.3 Post Implementation Evaluation Report (PIER)

Task 13.1: Production Cutover

The System goes live. Desk-side support is provided to end users and operations are carefully monitored.

The Contractor updates the Installation Plan (SEM-0702) which provides the list of interrelated steps and activities that must be coordinated to ensure a smooth and successful rollout. The Installation Plan is followed during Production Cutover.

A high-level checklist is prepared for general consumption within the agency to communicate the general schedule. A detailed, step-by-step checklist is prepared for the project team to follow.

Perform Software Implementation

The Contractor must provide the necessary resources to install the State of Michigan Enterprise Fraud Detection Software onto the production hardware per the Installation Plan. Any and all issues must be resolved during the installation procedures prior to cutover to the new software.

Deliverable

- Installation of the State of Michigan Enterprise Fraud Detection Software onto the production environment
- “Go/no go” Check List

State Responsibility

- Provide support during the implementation
- Attendance of Appropriate Personnel in the “go/no-go” review meeting
- Review Installation Plan
- Prepare the “go/no-go” checklist
- Make “go/no go” decision

Contractor Responsibility

- Update the Installation Plan
- Follow the Installation Plan
- Review the “go/no-go” Check List
- Installation of the State of Michigan Enterprise Fraud Detection Software onto the production environment

Acceptance Criteria

- Per section 1.501, 2.253, 2.254 & 2.255, approval of the Installation Plan
- Approval of State of Michigan Enterprise Fraud Detection Software installation

Task 13.2: Installation Testing

The Contractor must test the State of Michigan Enterprise Fraud Detection Software in the State production environment to ensure the software is installed and functioning properly. These tests should:

- Ensure the environment is properly installed and configured
- Ensure the State of Michigan Enterprise Fraud Detection Software is completely functional
- Ensure data is ported to the production environment
- Identify any defects or problems in the environment against expected results for all tests

Deliverables

- Conduct Installation Testing

State Responsibility

- Provide staff to assist the Contractor in the Installation Testing activity
- Review and approve Installation Test results

Contractor Responsibility

- Properly test the production environment to ensure it is fully installed and operating properly
- Ensure data is ported to the production environment
- Resolve any issues/problems for installation
- Provide installation test results

Acceptance Criteria

- Approval of Installation Testing results

Task 13.3: Post Implementation Evaluation Report (PIER)

The Contractor is responsible – with input from the State – for completing the Post-Implementation Evaluation Report for Phase 3 Medicaid Provider.

Deliverable

- Post Implementation Evaluation Report (PIER)

State Responsibility

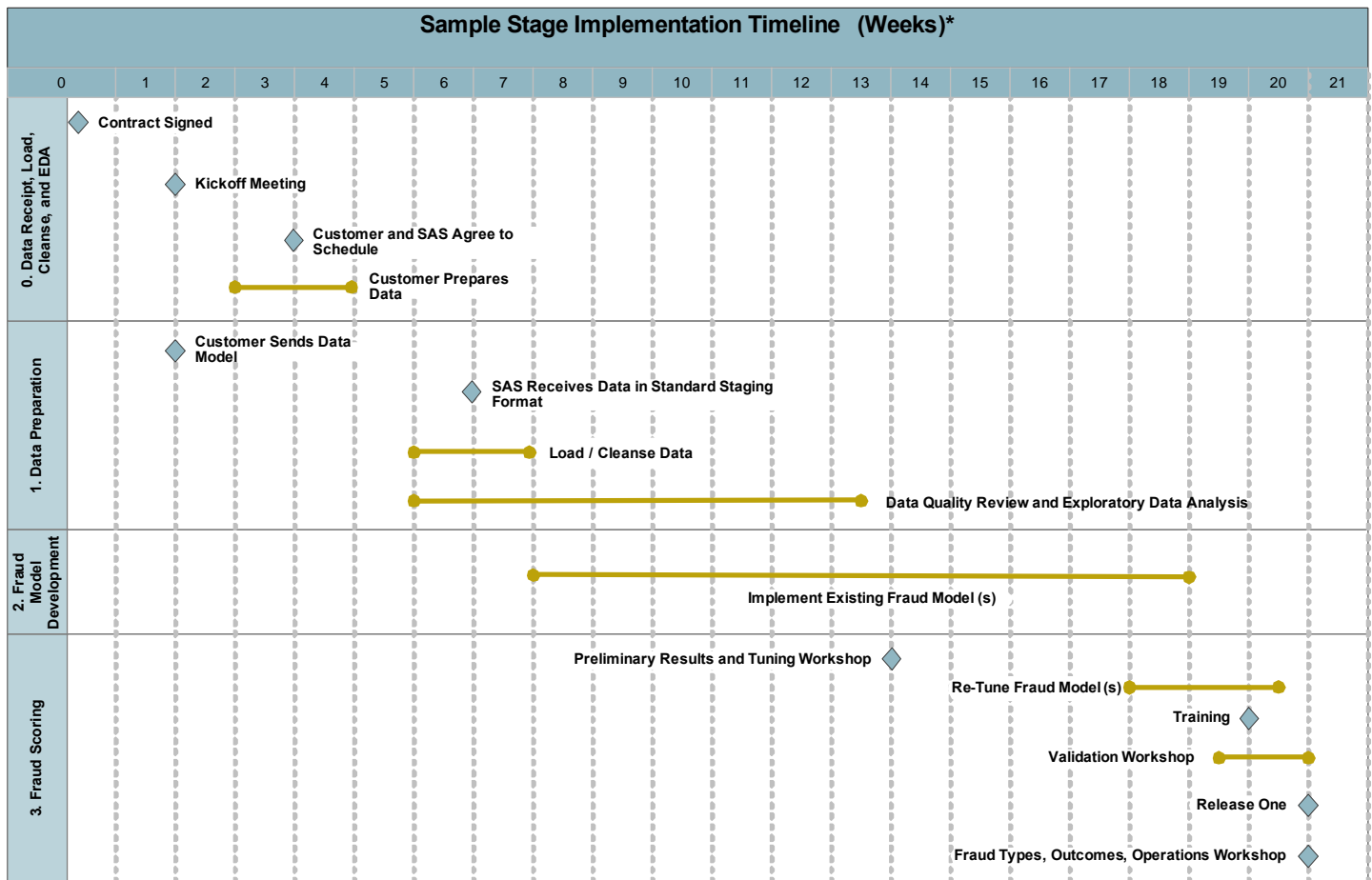
- Review the Post Implementation Evaluation Report
- Provide feedback to Contractor
- Approve the Post Implementation Evaluation Report

Contractor Responsibility

- Complete the Post Implementation Evaluation Report
- Correct any identified deficiencies

Acceptance Criteria

- Per section 1.501, 2.253, 2.254 & 2.255, approval of Post Implementation Evaluation Report



The chart above provides an estimated timeline for the delivery of Services relating to the Medicaid Provider Fraud Detection Module and is not otherwise intended to impose any obligations on the part of Contractor, or the State, as applicable, to provide such Services in the timeframes set forth above. Specific timeframes will be mutually agreed upon by the parties and documented in the project plan that will guide the delivery of the Services relating to the Medicaid Provider Fraud Detection Module and will be based on certain assumptions, which will include but are not limited to the following:

- Occurrence of any Phase 0 activities are based on customer availability.
- Hardware environment for the State is ready for development use.
- The State will provide answers to all questions posed by Contractor within a reasonable period of time, or such other time frame specifically requested by Contractor.
- All changes to the Statement of Work for the Medicaid Provider Fraud Detection Module will be mutually agreed upon by the parties and managed through the change control process. Contractor's obligation with respect to the delivery of services in connection with the Medicaid Provider Fraud Detection Module shall be only those services set forth in Section 1.800.
- The timeline set forth may be materially affected by any additional requests by the State for additional services outside the scope contemplated in Section 1.800.
- The State will provide necessary resources and expertise, as required by this Change Notice; including, but not limited to, resources to assist with business questions, application construction, data modeling, database administration, and IT functions. The timeframes set forth above are also based on the assumption the State will also make available content experts to validate functionality, usability, and accuracy of results.
- Contractor receives all required historical clean data from the State as contemplated in Section 1.800. The State shall also be responsible for ensuring quality of data and other factors regarding usability of various data sources. The State will also provide all required data (Customer Materials) to Contractor in a timely manner to meet the required deliverables set forth in Section 1.800.

- The State provides Contractor clean data in a mutually agreed upon format that remains consistent for the duration of the implementation of the Medicaid Provider Fraud Detection Module, and on an agreed upon frequency.
- The State provides any required data dictionaries / descriptions for each data source (that is, information about each data field: field name, data type, data length, label, and so on).
- The State and Contractor mutually agree on scheduled data refreshes, based on the availability of each data feed.

EXHIBIT B

PAYMENT SCHEDULE FOR MEDICAID PROVIDER FRAUD DETECTION MODULE

SUMMARY TOTAL COST FOR ADDITIONAL MODULE:

Table Number	Table Description	
Table 1	Work and Deliverables Services and Software Payment Schedule	\$3,023,015
Table 2	Warranty, Maintenance and Support	\$854,063
Table 3	Contingency Fund - Task 1.104.10	\$1,000,000
Estimated Value		\$4,877,078

Table 1 - Column Definitions:

Task	The reference to the task number identified in the Contract.
Project Milestone	The description of the Task as outlined in the Contract.
Services Payment	The amount paid upon completion and acceptance of related tasks.
Licensing Cost	The portion of total software license that will be paid the sooner of the Invoice Date or the completion of the Project Milestone.

Table 1 – Work and Deliverables Services and Software Payment Schedule

Task	Project Milestones: Phase 3 Medicaid Provider Fraud Detection Module	Services Payment	Licensing Cost (Invoice Date)
	Contract Execution		\$1,912,365 (Upon Change Notice Execution)
11.0	Initiation and Planning		
1.1	Project Planning		
1.2	General Timeline		
1.3	Confirm Infrastructure		
1.4	Product Installation		
	Initiation and Planning Complete	\$199,917	
11	Requirements & Design		
11.1	Requirements Definition		
11.2	Functional Design		
	Functional Design Approved	\$277,663	
12	Construction & Testing		
12.1	Construction and Testing Plan		
12.2	Data Preparation		
12.3	Configure FAP Fraud Detection Analysis Scenarios		
12.4	Integrations		
12.5	Transition and Operations Planning		
12.6	System Testing		
12.7	User Acceptance Testing		
	Construction & Testing Complete	\$444,260	
13	Implementation		
13.1	Production Cutover		
13.2	Installation Testing		
13.3	Post Implementation Evaluation Report		

Task	Project Milestones: Phase 3 Medicaid Provider Fraud Detection Module	Services Payment	Licensing Cost (Invoice Date)
	Implementation Acceptance	\$188,810	
	Total Services and Software Payments	\$1,110,650	\$1,912,365

Notes:

1. The Contractor will provide the Medicaid Provider Fraud Detection Module as part of the Michigan Enterprise Fraud Detection System, which is an Enterprise License. Note (2)(a) of Appendix C of the Contract is hereby deleted and replaced with the following:
 - a. The Michigan Enterprise Fraud Detection System is comprised of the following SAS offerings: SAS Fraud Framework for Government, SAS Fraud Framework for Healthcare, DataFlux Data Management Server and Studio Enrichment, DataFlux DataPack (DF) – US Address Verification. Contractor shall also provide a separate limited license to SAS Visual Analytics, solely for use in connection with respect to the Medicaid Provider Fraud Detection Module. The System includes three modules, UIA Benefits Overpayments, FAP (SNAP) Fraud Detection, and Medicaid Provider Fraud Detection. Up to five (5) SAS Access Engine licenses and the associated services to implement them. Four authorized agencies at this time are Unemployment Insurance Agency, Department of Human Services, Department of Community Health, and The Office of Inspector General. Includes sixty (60) Fraud Framework clients, not concurrent, and five (5) DF Client users, not concurrent and an unlimited number of Investigative Workbench clients (web-based GUI). Additional clients, fraud modules and expansion of use to other agencies are available from SAS for additional fees. Use of SAS Visual Analytics is included, but may only be used by Users in connection with the Medicaid Provider Fraud Detection Module.
3. With respect to the Medicaid Provider Fraud Detection Module, the License Costs will be paid as defined in the Licensing Cost Column in Table 1. Invoices will be due on the dates listed in the Licensing Cost column of Table 1.

Table 2 – Warranty, Maintenance and Support

Task	Warranty, Maintenance and Support Activities for Phase 3 Medicaid Provider Fraud Detection Module	Cost
8.1	Warranty (One Year) Complete Begins on the effective date of this Change Notice	\$ Included in first year software costs
9.1	Maintenance and Support (Support Year 1) Complete	\$ Included in first year software costs
9.1	Maintenance and Support (Support Year 2) Complete	\$420,721
9.1	Maintenance and Support (Support Year 3) Complete	\$433,342
	Total for Support years 1-3.	\$854,063

Table 2b –Maintenance and Support for Optional Years

Task	Warranty, Maintenance and Support Activities Option Years	Services Accrual
9.1	Optional Maintenance and Support (Support Year 4) Complete	\$446,342
9.1	Maintenance and Support (Support Year 5) Complete	\$459,732
9.1	Maintenance and Support (Support Year 6) Complete	\$473,524
9.1	Maintenance and Support (Support Year 7) Complete	\$487,730
9.1	Maintenance and Support (Support Year 8) Complete	\$502,362

Notes:

1. Warranty: Includes Costs for One (1) Year of Warranty as described in Section 1.104.8. Note that Year 1 of Warranty begins on the effective date of this Change Notice and shall run concurrently with the Maintenance and Support period for Year 1.
2. Maintenance and Support: Payment for Support Year 2 is made upon the end of the Contract Warranty Period identified in Section 1.104.8, which shall be on the one year anniversary of the effective date of this Change Notice.

Table 3 – Contingency Fund - Task 1.104.10

Contractor Staffing Category	Firm Fixed Hourly Rate
Senior Project Manager	\$200
Tech Lead	\$225
Analytical Lead	\$225
Developer	\$225
Analyst	\$225
Tester	\$200
SAS Admin	\$200
SSOIT	\$200
Documentation	\$200
Reserved Contingency Fund	\$1,000,000

Notes:

1. Hourly rates provided are firm, fixed rates for the duration of the contract. Travel and other expenses will not be reimbursed.
2. The State will utilize the firm fixed fully loaded hourly rates detailed above for each staff that will be used as fixed rates for responses to separate statements of work.

3. The State intends to establish funding for additional enhancements. Actual funding for enhancements will occur on a yearly basis, and there is no guarantee as to the level of funding, if any, available to the project.
4. This funding may also be utilized towards additional software licensing, software services or other related matters.

EXHIBIT C

SUPPLEMENT NUMBER 2

[SEE ATTACHED]



Supplement Number 2 ("Supplement")

to Master License Agreement ("MLA")

						FOR SAS USE ONLY	
Software and Subcomponents ¹		Applicable Pricing Metric, Number of Authorized Units ²	Operating System ³	Authorized Hardware (CPU/Server Manufacturer, Model type/Serial No.) ³	Initial Fees ⁴ (in above Currency Type)	License Beginning Date	Anniversary Date
Software:	SAS Visual Analytics – Non-Distributed Environment	Solution Test and Development; Limited Use; Processor Core Based (16)	To be defined by Customer in writing to SAS	To be defined by Customer in writing to SAS	As set forth in the Contract	Effective Date of Change Notice No. 2	One Year from Effective Date of Change Notice No. 2

¹ Pricing metrics, operating systems and/or Authorized Hardware for subcomponents which differ from that of the Software with which they are associated are listed in the column that corresponds to the applicable subcomponent. Unless otherwise noted, subcomponents listed here are included in the Software license fee for the Software product with which they are licensed or provided.

² The pricing metric is used to derive license fees; for example, but without limitation, Capacity Based, Total Users, PC Use, etc. as described on page 2 of this Supplement. Certain pricing metrics contain additional terms that pertain to Customer's use of the Software.

³ Customer must provide Operating System and Authorized Hardware information to SAS prior to shipment of Software.

⁴ Unless otherwise described in this Supplement, these are the first year license fees for the Software.

License of Software. This Supplement is an attachment to the MLA (collectively, "Agreement").

Pricing Metrics. The pricing metrics described herein apply to the Software and any Software subcomponents. For the avoidance of doubt, only those pricing metrics listed on page 1 apply to the Software and Software subcomponents licensed hereunder.

SAS Visual Analytics Processor Core Based (16) – The Software license fee is based on the number of physical processor cores or virtual processor cores, as applicable, contained within the Authorized Hardware. If the Authorized Hardware is a physical server, the license fee is based on the total number of physical processor cores contained within the physical server. If the Software is installed on a partition of a physical server, the Software license fee is based on the total number of physical processor cores contained within the server partition of the Authorized Hardware and Customer must use software or other technological means, as specified by the Authorized Hardware manufacturer, to limit, at all times, the partition to no more than the licensed number of physical processor cores. If the Authorized Hardware is a Virtual Machine, the Software license fee is based on the total number of virtual processor cores allocated to the Virtual Machine. A "Virtual Machine" is a single virtual environment, identified by a unique name as specified on the first page of this Supplement, created using commercially available virtualization software, in which use of the Software is isolated, at all times, to a specified maximum number of virtual processor cores. The Virtual Machine may run only on a single physical host machine at any given time but may be moved from one physical host machine to another so long as the Virtual Machine name and maximum number of virtual processor cores allocated to it remain unchanged. Unless otherwise authorized in this Supplement, the physical host machine must be located on Customer's premises. The Software is comprised of subcomponents. Each Software subcomponent may be used only in conjunction with the Software and may not be used or deployed for any other purpose.

Solution Test and Development - The license granted hereunder authorizes Customer to implement a single configured installation of the Software in one (1) production environment, one (1) test environment and one (1) development environment. Customer may use the Software installed in the production environment for Customer's internal production purposes ("Production Environment"). Customer may use the Software installed in the test environment solely for the purpose of testing the Software and Software applications and code prior to installation in Customer's Production Environment ("Test Environment"). Customer may use the Software installed in the development environment solely for the purposes of developing and creating applications and code with the Software for use in Customer's Production Environment ("Development Environment"). Customer must identify in writing the Authorized Hardware for the Production Environment, the Test Environment and the Development Environment. The operating system for the Test Environment and the Development Environment must be the same as the operating system for the Production Environment. The Test Environment and Development Environment shall be used only for the test and development purposes described above and shall at no time be used for production purposes or as a fail-over system.

Limited Use - Use of SAS Visual Analytics may only be used by Users in connection with the Medicaid Provider Fraud Detection Module for the Purpose.

Subcomponent Installations. Some Software consists of subcomponents which may be used only in connection with a single Software configuration. When the Software requires installation of subcomponents on more than one hardware tier, the server-tier subcomponents may be installed only on the Authorized Hardware listed on page 1 of this Supplement. If authorized by SAS, however, some server-tier subcomponents also may be installed on separate hardware. Where the license fee is based on hardware capacity, then the separate hardware must have the same or lower classification as the Authorized Hardware. Software or subcomponents licensed to SAS by third parties may only be installed once.

STATE OF MICHIGAN
DEPARTMENT OF TECHNOLOGY, MANAGEMENT AND BUDGET
PROCUREMENT

September 13, 2013

P.O. BOX 30026, LANSING, MI 48909 OR 530 W. ALLEGAN, LANSING, MI 48933

CHANGE NOTICE NO. 1
to
CONTRACT NO. 071B3200061
between
THE STATE OF MICHIGAN

NAME & ADDRESS OF CONTRACTOR:	PRIMARY CONTACT	EMAIL
SAS Institute Inc. 100 SAS Campus Drive Cary, NC 27513	Wayne Kuipers (See Section 2.025 for Legal Notices)	Wayne.Kuipers@sas.com
	TELEPHONE	CONTRACTOR #, MAIL CODE
	616-403-2275	

STATE CONTACTS	AGENCY	NAME	PHONE	EMAIL
CONTRACT COMPLIANCE INSPECTOR	DTMB	John Karlik	517-335-4062	KarlikJ@michigan.gov
BUYER	DTMB	Mike Breen	517-241-3215	BreenM@michigan.gov

CONTRACT SUMMARY:

DESCRIPTION: **Enterprise Fraud Detection Software Project**

INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW
12/21/2012	12/20/2015	Five One-Year	12/20/2015
PAYMENT TERMS	F.O.B	SHIPPED	SHIPPED FROM
N/A	N/A	N/A	N/A
ALTERNATE PAYMENT OPTIONS:			AVAILABLE TO MI DEAL PARTICIPANTS
<input type="checkbox"/> P-card <input type="checkbox"/> Direct Voucher (DV) <input type="checkbox"/> Other			<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
MINIMUM DELIVERY REQUIREMENTS: N/A			

DESCRIPTION OF CHANGE NOTICE:

EXTEND CONTRACT EXPIRATION DATE	EXERCISE CONTRACT OPTION YEAR(S)	EXTENSION BEYOND CONTRACT OPTION YEARS	LENGTH OF OPTION/EXTENSION	EXPIRATION DATE AFTER CHANGE
<input checked="" type="checkbox"/> No <input type="checkbox"/> Yes	<input type="checkbox"/>	<input type="checkbox"/>	N/A	12/20/2015
VALUE/COST OF CHANGE NOTICE:			ESTIMATED REVISED AGGREGATE CONTRACT VALUE:	
\$4,877,078.00			\$10,884,769.00	

Effective immediately this contract is INCREASED by \$4,877,078.00 to provide funding for the Medicaid Fraud Software, Implementation Services and Maintenance and Support as outlined in Appendix H of the Contract. This increase includes the cost items in Appendix H and \$1,000,000.00 towards a reserved bank of hours for future enhancements. The State will finalize the requirements and invoice/payment schedule for this module in a future Change Notice. The Contractor will not receive payment for any deliverables that are part of this amendment until the future Change Notice is completed and approved by the State and Contractor. This change is issued per State Administrative Board Approval on 9/13/2013.

Please note: The Buyer has been changed to Mike Breen. All other pricing, terms and conditions remain the same.

STATE OF MICHIGAN
 DEPARTMENT OF TECHNOLOGY, MANAGEMENT AND BUDGET
 PROCUREMENT
 P.O. BOX 30026, LANSING, MI 48909
 OR
 530 W. ALLEGAN, LANSING, MI 48933

**NOTICE
 OF
 CONTRACT NO. 071B3200061
 between
 THE STATE OF MICHIGAN
 and**

NAME & ADDRESS OF CONTRACTOR:	PRIMARY CONTACT	EMAIL
SAS Institute Inc. 100 SAS Campus Drive Cary, NC 27513	Wayne Kuipers (See Section 2.025 for Legal Notices)	Wayne.Kuipers@sas.com
	TELEPHONE	CONTRACTOR #, MAIL CODE
	616-403-2275	

STATE CONTACTS	AGENCY	NAME	PHONE	EMAIL
CONTRACT COMPLIANCE INSPECTOR:	DTMB	John Karlik	(517) 335-4062	KarlikJ@michigan.gov
BUYER:	DTMB	Steve Motz	(517) 241-3215	motzs@michigan.gov

CONTRACT SUMMARY:			
DESCRIPTION:			
Enterprise Fraud Detection Software Project			
INITIAL TERM	EFFECTIVE DATE	INITIAL EXPIRATION DATE	AVAILABLE OPTIONS
3 Years	12/21/2012	12/20/2015	Five One-Year
PAYMENT TERMS	F.O.B	SHIPPED	SHIPPED FROM
Net 45	Shipment	N/A	N/A
ALTERNATE PAYMENT OPTIONS:			AVAILABLE TO MIDEAL PARTICIPANTS
<input type="checkbox"/> P-card <input type="checkbox"/> Direct Voucher (DV) <input type="checkbox"/> Other			<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
MINIMUM DELIVERY REQUIREMENTS:			
N/A			
MISCELLANEOUS INFORMATION:			
N/A			
ESTIMATED CONTRACT VALUE AT TIME OF EXECUTION:		\$6,007,691.00	

STATE OF MICHIGAN
 DEPARTMENT OF TECHNOLOGY, MANAGEMENT AND BUDGET
 PROCUREMENT
 P.O. BOX 30026, LANSING, MI 48909
 OR
 530 W. ALLEGAN, LANSING, MI 48933

CONTRACT NO. 071B3200061
 between
THE STATE OF MICHIGAN
 and

NAME & ADDRESS OF CONTRACTOR:	PRIMARY CONTACT	EMAIL
SAS Institute Inc. 100 SAS Campus Drive Cary, NC 27513	Wayne Kuipers (See Section 2.025 for Legal Notices)	Wayne.Kuipers@sas.com
	TELEPHONE	CONTRACTOR #, MAIL CODE
	616-403-2275	

STATE CONTACTS	AGENCY	NAME	PHONE	EMAIL
CONTRACT COMPLIANCE INSPECTOR:	DTMB	John Karlik	(517) 335-4062	KarlikJ@michigan.gov
BUYER:	DTMB	Steve Motz	(517) 241-3215	motzs@michigan.gov

CONTRACT SUMMARY:			
DESCRIPTION:			
Enterprise Fraud Detection Software Project			
INITIAL TERM	EFFECTIVE DATE	INITIAL EXPIRATION DATE	AVAILABLE OPTIONS
3 Years	12/21/2012	12/20/2015	Five One-Year
PAYMENT TERMS	F.O.B	SHIPPED	SHIPPED FROM
Net 45	Shipment	N/A	N/A
ALTERNATE PAYMENT OPTIONS:			AVAILABLE TO MiDEAL PARTICIPANTS
<input type="checkbox"/> P-card <input type="checkbox"/> Direct Voucher (DV) <input type="checkbox"/> Other			<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
MINIMUM DELIVERY REQUIREMENTS:			
N/A			
MISCELLANEOUS INFORMATION:			
N/A			
ESTIMATED CONTRACT VALUE AT TIME OF EXECUTION:			\$6,007,691.00

THIS IS NOT AN ORDER: This Contract Agreement is awarded on the basis of our inquiry bearing the solicitation #071I2200091. Orders for delivery will be issued directly by the Department of Technology, Management & Budget through the issuance of a Purchase Order Form.

Notice of Contract #:071B3200061

FOR THE CONTRACTOR:	FOR THE STATE:
SAS Institute Inc.	
Firm Name	Signature
	Greg Faremouth, IT Division Director
Authorized Agent Signature	Name/Title
	DTMB, Procurement
Authorized Agent (Print or Type)	Enter Name of Agency
Date	Date



STATE OF MICHIGAN
Department of Technology, Management and Budget
DTMB-Procurement

Contract No. [071B3200061](#)
[Enterprise Fraud Detection Software Project](#)

Buyer Name: [Steve Motz](#)
Telephone Number: [517-241-3215](#)
E-Mail Address: motzs@michigan.gov



Table of Contents

Article 1 – Statement of Work (SOW)	9
1.000 Project Identification	9
1.001 Project Request	9
1.002 Background	9
1.100 Scope of Work and Deliverables	10
1.101 In Scope	10
1.102 Out Of Scope	11
1.103 Environment	11
1.104 Work And Deliverables	13
1.200 Roles and Responsibilities	61
1.201 Contractor Staff, Roles, And Responsibilities	61
1.202 State Staff, Roles, And Responsibilities	62
1.203 Other Roles And Responsibilities	63
1.300 Project Plan	64
1.301 Project Plan Management	64
1.302 Reports	64
1.400 Project Management	64
1.401 Issue Management	64
1.402 Risk Management	65
1.403 Change Management	65
1.500 Acceptance	65
1.501 Criteria	65
1.502 Final Acceptance	66
1.600 Compensation and Payment	66
1.601 Compensation And Payment	66
1.700 Additional Terms and Conditions Specific to this SOW	67
1.701 State unemployment Tax Avoidance (SUTA) Dumping	67
Article 2, Terms and Conditions	68
2.000 Contract Structure and Term	68
2.001 Contract Term	68
2.002 Options to Renew	68
2.003 Legal Effect	68
2.004 Appendices Attachments & Exhibits	68
2.005 Ordering	68
2.006 Order of Precedence	68
2.007 Headings	69
2.008 Form, Function & Utility	69
2.009 Reformation and Severability	69
2.010 Consents and Approvals	69
2.011 No Waiver of Default	69
2.012 Survival	69
2.020 Contract Administration	69
2.021 Issuing Office	69
2.022 Contract Compliance Inspector	69
2.023 Project Manager	70
2.024 Change Requests	70
2.025 Notices	71
2.026 Binding Commitments	71
2.027 Relationship of the Parties	71
2.028 Covenant of Good Faith	71
2.029 Assignments	71
2.030 General Provisions	72
2.031 Media Releases	72
2.032 Contract Distribution	72
2.033 Permits	72



2.034	Website Incorporation	72
2.035	Future Bidding Preclusion	72
2.036	Freedom of Information	72
2.037	Disaster Recovery	72
2.040	Financial Provisions	73
2.041	Fixed Prices for Services/Deliverables	73
2.042	Adjustments for Reductions in Scope of Services/Deliverables	73
2.043	Services/Deliverables Covered	73
2.044	Invoicing and Payment – In General	73
2.045	RESERVED - Pro-ration	73
2.046	Antitrust Assignment	73
2.047	Final Payment	74
2.048	Electronic Payment Requirement	74
2.050	Taxes	74
2.051	Employment Taxes	74
2.052	Sales and Use Taxes	74
2.060	Contract Management	74
2.061	Contractor Personnel Qualifications	74
2.062	Contractor Key Personnel	74
2.063	Re-assignment of Personnel at the State's Request	75
2.064	Contractor Personnel Location	75
2.065	Contractor Identification	75
2.066	Cooperation with Third Parties	75
2.067	Contract Management Responsibilities	76
2.068	Contractor Return of State Equipment/Resources	76
2.070	Subcontracting by Contractor	76
2.071	Contractor full Responsibility	76
2.072	State Consent to delegation	76
2.073	Subcontractor bound to Contract	76
2.074	Flow Down	77
2.075	Competitive Selection	77
2.080	State Responsibilities	77
2.081	Equipment	77
2.082	Facilities	77
2.090	Security	77
2.091	Background Checks	77
2.092	Security Breach Notification	78
2.093	PCI DATA Security Requirements	78
2.100	Confidentiality	78
2.101	Confidentiality	78
2.102	Protection and Destruction of Confidential Information	78
2.103	Exclusions	79
2.104	No Implied Rights	79
2.105	Respective Obligations	79
2.110	Records and Inspections	79
2.111	Inspection of Work Performed	79
2.112	Examination of Records	79
2.113	Retention of Records	80
2.114	Audit Resolution	80
2.115	Errors	80
2.120	Warranties	80
2.121	Warranties and Representations	80
2.122	RESERVED - Warranty of Merchantability	81
2.123	RESERVED - Warranty of Fitness for a Particular Purpose	81
2.124	RESERVED - Warranty of Title	81
2.125	RESERVED - Equipment Warranty	82
2.126	RESERVED - Equipment to be New	82
2.127	RESERVED - Prohibited Products	82
2.128	Consequences for Breach	82
2.130	Insurance	82



2.131	Liability Insurance	82
2.132	Subcontractor Insurance Coverage	83
2.133	Certificates of Insurance and Other Requirements	84
2.140	Indemnification	84
2.141	General Indemnification	84
2.142	Code Indemnification	84
2.143	Employee Indemnification	84
2.144	Patent/Copyright Infringement Indemnification	84
2.145	Continuation of Indemnification Obligations	85
2.146	Indemnification Procedures	85
2.150	Termination/Cancellation	86
2.151	Notice and Right to Cure	86
2.152	Termination for Cause	86
2.153	Termination for Convenience	86
2.154	Termination for Non-Appropriation	87
2.155	Termination for Criminal Conviction	87
2.156	Termination for Approvals Rescinded	87
2.157	Rights and Obligations upon Termination	87
2.158	Reservation of Rights	88
2.160	Termination by Contractor	88
2.161	Termination by Contractor	88
2.170	Transition Responsibilities	88
2.171	Contractor Transition Responsibilities	88
2.172	Contractor Personnel Transition	88
2.173	Contractor Information Transition	88
2.174	Contractor Software Transition	89
2.175	Transition Payments	89
2.176	State Transition Responsibilities	89
2.180	Stop Work	89
2.181	Stop Work Orders	89
2.182	Cancellation or Expiration of Stop Work Order	89
2.183	Allowance of Contractor Costs	89
2.190	Dispute Resolution	90
2.191	In General	90
2.192	Informal Dispute Resolution	90
2.193	Injunctive Relief	90
2.194	Continued Performance	90
2.200	Federal and State Contract Requirements	91
2.201	Nondiscrimination	91
2.202	Unfair Labor Practices	91
2.203	Workplace Safety and Discriminatory Harassment	91
2.204	Prevailing Wage	91
2.210	Governing Law	91
2.211	Governing Law	92
2.212	Compliance with Laws	92
2.213	Jurisdiction	92
2.220	Limitation of Liability	92
2.221	Limitation of Liability	92
2.230	Disclosure Responsibilities	92
2.231	Disclosure of Litigation	92
2.232	Call Center Disclosure	93
2.233	Bankruptcy	93
2.240	Performance	93
2.241	Time of Performance	93
2.242	Service Level Agreement (SLA)	94
2.243	RESERVED - Liquidated Damages	94
2.244	Excusable Failure	94
2.250	Approval of Deliverables	95



2.251	Delivery of Deliverables	95
2.252	Contractor System Testing	95
2.253	Approval of Deliverables, In General	96
2.254	Process for Approval of Written Deliverables	97
2.255	Process for Approval of Custom Software Deliverables	97
2.256	Final Acceptance	98
2.260	Ownership	98
2.261	Ownership of Work Product	98
2.262	Vesting of Rights	98
2.263	Rights in Data	98
2.264	Ownership of Materials	99
2.270	State Standards	99
2.271	Existing Technology Standards	99
2.272	Acceptable Use Policy	99
2.273	Systems Changes	99
2.280	Extended Purchasing	99
2.281	MiDEAL (Michigan Delivery Extended Agreements Locally)	99
2.282	RESERVED - State Employee Purchases	99
2.290	Environmental Provision	99
2.291	Environmental Provision	99
2.300	Deliverables	101
2.301	Software	101
2.302	RESERVED - Hardware	101
2.303	RESERVED - Equipment to Be New	101
2.304	RESERVED - Equipment to be New and Prohibited Products	101
2.310	Software Warranties	101
2.311	Performance Warranty	101
2.312	No Surreptitious Code Warranty	101
2.313	Calendar Warranty	102
2.314	Third-party Software Warranty	102
2.315	Physical Media Warranty	102
2.320	Software Licensing	102
2.321	Cross-License, Deliverables Only, License to Contractor	102
2.322	Cross-License, Deliverables and Derivative Work, License to Contractor	103
2.323	RESERVED - License Back to the State	103
2.324	RESERVED - License Retained by Contractor	103
2.325	RESERVED - Pre-existing Materials for Custom Software Deliverables	103
2.330	RESERVED - Source Code Escrow	103
	Glossary	104
	Appendices	107
	RESERVED - Appendix A. Project Manager Resume Summary Template	107
	Appendix B. Breakdown of Hardware and Related Software	108
	Appendix C. Payment Schedule	115
	RESERVED - Appendix D. Preliminary Project Plan	<i>Error! Bookmark not defined.</i>
	RESERVED - Appendix E. Organization Chart and Staffing Resource table	<i>Error! Bookmark not defined.</i>
	RESERVED - Appendix F. Mandatory Minimum Requirements	<i>Error! Bookmark not defined.</i>
	Appendix G. Master License Agreement	125
	Appendix H. Optional Medicaid Functional Requirements and Pricing	133



Article 1 – Statement of Work (SOW)

1.000 Project Identification

1.001 PROJECT REQUEST

This Contract follows the completion of RFP# 071I2200091 – “Enterprise Fraud Detection Software Project,” released on February 17, 2012, by the State of Michigan (SOM or the State), through the Unemployment Insurance Agency (UIA), as part of the Department of Licensing and Regulatory Affairs (LARA), with the assistance and support of the Michigan Department of Technology, Management and Budget (DTMB). The statement of work describes the specific requirements that will allow the solution to be utilized by the Unemployment Insurance Agency, Department of Human Services (DHS) Food Assistance Program (FAP) and the Office of the Inspector General (OIG).

If additional State agencies choose to utilize this Contract the State will obtain a fixed price proposal that is derived from the hourly rates provided in Appendix C, and the State will seek additional spending authority through the Administrative Board when required.

All project work must be performed in close cooperation with both the State and the UIA Project Control Office (PCO) and Independent Verification and Validation (IV&V) Project Manager. Refer to Section 1.202 for more information about the PCO, IV&V and State Project Managers.

1.002 BACKGROUND

The Michigan Unemployment Insurance Agency (UIA) is responsible for collecting taxes from Employers and disbursing UI benefits to eligible Claimants as defined in the Michigan Employment Security Act (http://www.michigan.gov/documents/ua_mesact_3103_7.pdf).

The Michigan Department of Human Services (DHS) directs the operations of public assistance and service programs, through county family independence agencies, in every county in Michigan. It administers assistance payment programs available within the state. These programs include temporary assistance for needy families (Family Independence Program); Child Day Care; medical assistance jointly funded by the federal government and the state; state disability assistance and state medical services program, which are funded by the state and State Emergency Relief Program; and food stamps, a federally funded program.

The Michigan Office of the Inspector General (OIG) is a criminal justice agency within the Michigan Department of Human Services, created in 1972. The Office assists DHS in maintaining integrity and accountability in the administration of its programs. OIG Agents and their supervisor are strategically located throughout the State of Michigan. The OIG provides investigation and advisory services to ensure appropriate and efficient use of available public resources.

The OIG is responsible for investigating instances of alleged welfare fraud in all programs administered by the Department, as well as reviewing administrative policies and procedures and recommend ways of improving accountability, fraud deterrence and detection. For example, OIG investigates alleged fraud in the Family Independence Program (FIP), the Food Assistance Program (FAP), the Child Development and Care program (CDC) and the Medical Assistance program (MA). This includes investigations of non-Medicaid vendor fraud as well as department employees alleged to be involved in program fraud. All investigations found to contain the elements of fraud are forwarded to the appropriate authority for criminal disposition or are sent to the appropriate area within the Michigan Department of Human Services for administrative action.

STATE PROJECT GOALS

The State goals for this project are to implement a COTS solution able to provide fraud detection based on State and Federal guidelines. The following is a list of goals for the State of Michigan Enterprise Fraud Detection Software Project:

1. Reduce the percentage of UI benefits overpaid due to BYE fraud from the baseline level at the end of the first year of implementation and also by the end of the second year of implementation as detailed in the Improper Payments Elimination and Recovery Act of 2010 (IPERA) and E.O. 13520.
For more information on this goal, go to http://wdr.doleta.gov/directives/corr_doc.cfm?DOCN=3038



2. Identify and report fraud characteristics by individuals or groups based on information derived from multiple data sources using data analytics.
3. Recognize patterns in data that reveal organized attempts to defraud the unemployment insurance system.
4. Reduce the number and amount of improper payments as reported quarterly.
5. Reduce the number and amount of UI overpayments.
6. Recognize patterns in data that reveal organized attempts to defraud public assistance programs.
7. Increase program integrity in public assistance programs.

1.100 Scope of Work and Deliverables

1.101 IN SCOPE

This contract is for the installation and configuration of a COTS software data analytics product which analyzes data for patterns that might reveal an organized attempt to defraud the Michigan Unemployment Insurance Agency (UIA) and the DHS Food Assistance Program (FAP). The State requires a data analytics product which allows staff to query an aggregate dataset populated from multiple disparate agency data sources stored in the DTMB Data Warehouse to conduct real-time ad hoc analysis. The tools must utilize techniques that allow information to be filtered and sorted in varying levels of detail. The technology must allow end-users to conduct analysis without programming and with no advanced knowledge of the underlying data sources and structures.

As this is a Statewide Contract, it is anticipated that additional State agencies and program areas (as well as MiDEAL participants) may utilize the fraud detection software and services in the future. This includes but is not limited to the Department of Community Health (DCH) for the purposes of identifying Medicaid provider fraud and abuse. Appendix H – Optional Medicaid Functional Requirements and Pricing provides a DCH option for future consideration based on the Contractor's proposal dated August 28, 2012. Addition of the Medicaid Functional Requirements to this Contract will require a Change Request pursuant to Section 2.024 below. The Contractor agrees to extend and guarantee to the State of Michigan 2012 pricing on all future fraud modules and licenses purchased within 18 months of signing the contract. Further, the Contractor asserts that it will negotiate and provide pricing and project timelines at the State's earliest convenience upon its conveyance of appropriate specifications for all future modules.

This project is for the procurement of a COTS product and services with the following scope: Requirements Definition, Functional Design, Configuration, Testing, Implementation, Warranty and Maintenance. The State of Michigan Enterprise Fraud Detection Software must encompass all technical and functional requirements provided in Article 1, Section 1.104 – Work and Deliverables. The solution must include the acquisition of software and services necessary for a complete implementation.

The services for this project are broken down into two phases.

Phase 1 FAP: Utilizes data currently stored in the DTMB Data Warehouse for the development of Food Assistance Program (FAP) fraud detection analysis. Integration with LexisNexis for asset verification and integrating the FAP recipient fraud detection analysis results with the FEE legacy system is also required.

Phase 2 UIA: Utilizes data from the DTMB Data Warehouse for the development of UIA Benefit and Tax fraud detection analysis. The integration of UIA fraud detection analysis results based on scoring and priority with the CAMS and FACTS legacy systems and MiDAS (Michigan Integrated Data Automated System), currently under development, is also required.

The State is currently engaged in a modernization project of their legacy UI systems (MiDAS project). The start of Phase 2 is dependent upon the continued successful progress of the MiDAS project.

The solution must provide the functionality and meet the requirements for the functional areas listed below:

- Fraud Functions – General
- Fraud Functions – UI Claimants and PA Recipients
- Fraud Functions – Employers



- Fraud Functions – Internal Staff
- Fraud Functions – Public Assistance Recipient Provider/Retailer
- General System Functionality

The expected Phase 1 and Phase 2 project duration is 18 months from the Contractor's receipt and validation of Clean Data in the State's development hosting environment. Hardware and network will be configured and ready for use.

The State has made significant investment in a number of enterprise, shared solutions or services (see Article 1, Section 1.103, Environment). The solution must take into account that investment and leverage these shared services while meeting the technical and functional requirements of this contract. A detailed description of the software, services (work), and deliverables sought for this project is provided in Article 1, Section 1.104 – Work and Deliverables.

1.102 OUT OF SCOPE

The following tasks and deliverables are out-of-scope for the State of Michigan Enterprise Fraud Detection Software Project:

- Procurement of Hardware.

1.103 ENVIRONMENT

The links below provide information on the State's Enterprise information technology (IT) policies, standards and procedures which includes security policy and procedures, IT strategic plan, eMichigan web development and the State Unified Information Technology Environment (SUITE).

The State has methods, policies, standards and procedures that have been developed over the years. The Contractor is expected to provide proposals that conform to State IT policies and standards. All services and products provided must comply with all applicable State IT policies and standards.

Enterprise IT Policies, Standards and Procedures:

<http://www.michigan.gov/dmb/0,4568,7-150-56355---,00.html>

All software and hardware items provided by the Contractor must run on and be compatible with the Michigan Department of Technology, Management and Budget (DTMB) Standard Information Technology Environment. Additionally, the State must be able to maintain software and other items produced as the result of the Contract. Therefore, non-standard development tools may not be used unless approved by DTMB. The State will complete the necessary documentation as part of the EA Solution Assessment Worksheet outlined in Section 1.3.1 of the Contract to obtain approval to use SAS software. The DTMB Project Manager must approve any tools, in writing, before use on any information technology project.

It is recognized that technology changes rapidly. The Contractor may request, in writing, a change in the standard environment, providing justification for the requested change and all costs associated with any change. The State's Project Manager must approve any changes, in writing, and DTMB, before work may proceed based on the changed environment.

Enterprise IT Security Policy and Procedures:

http://www.michigan.gov/documents/dmb/1310_183772_7.pdf

http://www.michigan.gov/documents/dmb/1310.02_183775_7.pdf

http://www.michigan.gov/documents/dmb/1325_193160_7.pdf

http://www.michigan.gov/documents/dmb/1335_193161_7.pdf

http://www.michigan.gov/documents/dmb/1340_193162_7.pdf

http://www.michigan.gov/documents/dmb/1350.10_184594_7.pdf

**The State's security environment includes:**

1. DTMB Single Login
2. DTMB provided SQL security database
3. Secured Socket Layers
4. SecureID (State Security Standard for external network access and high risk Web systems)

The State's enterprise shared solution environments include:

1. Query and Reporting Functionality through SAP BusinessObjects
2. Address Standardization Functionality through SAP Data Quality Management
3. Extract, Transform, and Load Functionality through IBM DataStage, QualityStage, and Information Analyzer
4. GeoData Services such as a geospatial data warehouse (MS SQL Spatial) and an enterprise ArcGIS Server as an application tier

IT Strategic Plan:

<http://www.michigan.gov/itstrategicplan>

IT eMichigan Web Development Standard Tools:

http://www.michigan.gov/documents/som/Look_and_Feel_Standards_302051_7.pdf

Project Management and Systems Engineering Methodology

The State and Contractor will mutually agree on the project management methodology to be used in the performance of the Michigan Enterprise Fraud Detection Software Project. This may consist of, or be a combination of the State Unified Information Technology Environment (SUITE), the SAS project management methodology, the State Project Management Methodology (PMM) and Systems Engineering Methodology (SEM) Express. The State of Michigan PMM and SEM methodologies include definitions of certain of the Deliverables in the Statement of Work.

Project Management Methodology (PMM) Express was developed as a guide to assist in the management of smaller, less complex projects within the Department of Information Technology. *PMM Express* is a customized version of the State of Michigan Project Management Methodology (PMM) and schedule template.

The SEM Express is a companion guide to the State of Michigan Systems Engineering Methodology (SEM). *SEM Express* offers guidance for smaller, straight-forward systems development projects.

The State Unified Information Technology Environment (SUITE):

<http://www.michigan.gov/suite>

PMM Express:

<http://www.michigan.gov/dmb/0,4568,7-150-56355-58009--,00.html>

SEM Express:

http://www.michigan.gov/suite/0,4674,7-245-45409_46991---,00.html

Solution Platform(s)

The Contractor will utilize a minimum of the following three (3) environments suitable to support the Enterprise Fraud Detection System implementation strategy:

Development

This environment is used to implement and customize the solution. This environment is managed by the Contractor and used for unit testing, software upgrade testing, and any other purposes deemed necessary by the Contractor or State.

User Acceptance Testing (UAT)

This environment is where the State shall conduct all UAT activities.



Production

This environment is where the final integrated solution is deployed.

These environments are not required to reside on distinct hardware, and must operate in a Virtual Machine (VM) environment. The Contractor may include other environments as deemed appropriate for proper use and deployment of the solution.

1.104 WORK AND DELIVERABLES

The purpose of this section is to describe the work and deliverables necessary to provide the required functionality for the State of Michigan Fraud Detection Software Project.

This section describes the project management and systems engineering methodology, as well as additional related activities that must be followed during the execution of this project.

The Deliverables will be developed using the mutually agreed upon Project Management and Systems Engineering Methodologies outlined in section 1.103.

All project Milestones/Deliverables, Tasks or Artifacts are to be reviewed by the State, the PCO, and/or the Independent Verification and Validation (IV&V) Project Manager. Approval of all project Milestones/Deliverables, Tasks or Artifacts shall be the sole responsibility of the State DTMB/UIA Project Managers and/or designees.

I. Services and Deliverables To Be Provided

The following section includes the work and deliverables that are required to be performed and/or submitted during the contract term.

The following table lists the high-level phases as well as the required milestones, deliverables and tasks.

Ref. #	Phase	Milestone/Deliverable Task or Artifact
1.104.1	Project Initiation and Planning	1.1 Project Planning
		1.2 General Timeline
		1.3 Confirm Infrastructure
		1.4 Product Installation
1.104.2	Phase 1 FAP: Requirements & Design	2.1 Requirements Definition
		2.2 Functional Design
1.104.3	Phase 1 FAP: Construction & Testing	3.1 Construction and Testing Plan (SEM 02-Exp)
		3.2 Data Preparation
		3.3 Configure FAP Fraud Detection Analysis Scenarios
		3.4 Integrations
		3.5 Transition and Operations Planning
		3.6 System Testing
		3.7 User Acceptance Testing
1.104.4	Phase 1 FAP: Implementation	4.1 Production Cutover
		4.2 Installation Testing
		4.3 Post Implementation Evaluation Report (PIER)
1.104.5	Phase 2 UIA: Requirements & Design	5.1 Requirements Definition
		5.2 Functional Design



Ref. #	Phase	Milestone/Deliverable Task or Artifact
1.104.6	Phase 2 UIA: Construction & Testing	6.1 Construction and Testing Plan (SEM 02-Exp)
		6.2 Data Preparation
		6.3 Configure UIA Benefit and Tax Fraud Detection Analysis Scenarios
		6.4 Integrations
		6.5 Transition and Operations Planning
		6.6 System Testing
		6.7 User Acceptance Testing
1.104.7	Phase 2 UIA: Implementation	7.1 Production Cutover
		7.2 Installation Testing
		7.3 Post Implementation Evaluation Report (PIER)
1.104.8	Warranty	8.1 Warranty
1.104.9	Maintenance and Support	9.1 System Maintenance
1.104.10	Contingency Fund	10.1 Change Request

1.104.1 Project Initiation and Planning Phase

Objective

The objective of the Project Initiation and Planning Phase is for the project management team to develop the project definition and planning tools and artifacts for the entire State of Michigan Enterprise Fraud Detection Software Project.

Description

The following activities are performed during initiation and planning and continue through the project execution, as appropriate and necessary to control and report on the project. The ongoing activities detailed in this section apply to Phase 1 FAP and Phase 2 UIA.

Tasks

- 1.1 Project Planning
- 1.2 General Timeline
- 1.3 Confirm Infrastructure
- 1.4 Product Installation

Task 1.1: Project Planning

1.1.1 Project Charter (PMM 002)

The Project Charter communicates the existence of a project. It contains vital information about the project and its leadership.

The State – with Contractor input – must create this deliverable.

Deliverables

- Project Charter

State Responsibility



- Create and submit Project Charter

Contractor Responsibility

- Provide input and clarifications to the State as needed

Acceptance Criteria

- None required – State Deliverable

1.1.2 Project Plan (PMM 003-Exp)

The Project Plan must address all components of the SUITE PMM-003-Exp. The Project Management Plan creates a consistent, coherent document that is used to guide both Project execution and Project control. The State - with input from the Contractor - will create the Project Plan and its subcomponents and maintain the document throughout the life of the project. The State is responsible for establishing the overall Project Management Plan. The Contractor is also responsible for creating these plans, as they relate to their project activities. The State will incorporate the Contractor plan into a State document that will be followed during project execution. At a minimum, the Project Plan shall include: General Project Information (points of contact, phone numbers, etc.), Project Executive Summary, Detailed Project Scope Statement, Resource Planning, Communications Planning, Quality Planning and Risk Planning.

Deliverables

- Project Plan (PMM 003-Exp)

State Responsibility

- Create the Project Management Plan (PMM-003-Exp) and subcomponent plans
- Provide access to policies and procedures
- Provide State project resource estimates for State specific tasks
- Review and update the Project Management Plan

Contractor Responsibility

- Provide input and clarifications to the State as needed

Acceptance Criteria

- None required – State Deliverable

1.1.3 Project Phase Kick-off Meetings

The Project Kickoff meeting provides opportunities to recognize the start of the project formally, meet project participants, communicate a shared view of the project, ensure understanding of the approved project charter, and clarify next steps for staff. There will be two separate Kick-off Meetings for the State of Michigan Enterprise Fraud Detection Software Project, one for each Phase.

Timeframe

- Phase 1 FAP Kick-off Meeting must be held within 15 business days of contract start date or as mutually agreed upon
- Phase 2 UIA Kick-off Meeting must be held on scheduled start date for Phase 2 or as mutually agreed upon

Deliverables

- None for this task

State Responsibility

- Provide input to agenda for Kick-off Meetings
- Attend Kick-off Meetings

Contractor Responsibility

- Develop specific objectives and agenda for the Kick-off Meetings
- Schedule and chair the Kick-off Meetings
- Generate meeting record for the Kick-off Meetings

Acceptance Criteria



- Completion of Phase 1 FAP Project Kick-off Meeting
- Completion of Phase 2 UIA Project Kick-off Meeting

1.1.4 Create Status Report - Weekly Reporting

The Contractor must prepare a weekly project status report and submit it to the State project management team. The weekly status report must follow the PMM defined format and content, and cover the previous weekly period.

As part of the Weekly Status Report, the Contractor must submit Action Items, Issues and Risk items, identify any staffing problems and other issues that may affect the project scope, schedule, budget or work products.

Deliverables

- Weekly Status Report

State Responsibility

- Review weekly status reporting format and content
- Review the Weekly Status Reports
- Chair Weekly Status Reporting meetings

Contractor Responsibility

- Comply with the PMM defined Status Report format and content
- Completion of Weekly Project Status Reports
- Attend the Weekly Status Reporting meetings

Acceptance Criteria

- Status reports submitted weekly by the Contractor to the State.

1.1.5 Create/Update Issue & Risk Report – As Needed

The State, with input from the Contractor, is responsible for establishing issues and risk reporting and process, including the identification and recording of issues/risk items, prioritization, definition of mitigation strategies, monitoring of items, and regularly scheduled assessment reviews with the Contractor.

The State will provide a tool for issue and risk tracking. All project staff are requested and encouraged to identify and report issues and risks. Managing, mitigating and/or eliminating assigned issues/risks are the responsibility of the State, with assistance from the Contractor.

Issues shall be escalated for resolution from Level 3 through Level 1, as defined below:

- Level 1 – Executive Subject Matter Experts (SME's)
- Level 2 – Project Managers
- Level 3 – Business leads

Deliverables

- Issue/risk report and process

State Responsibility

- Provide the issue and risk tracking tool
- Identify the criteria to categorize, prioritize and determine the severities for issues and risks
- Submit issues and risks, and determine mitigations/resolutions
- Determine how issues shall be assigned
- Include escalation procedures for issues and risks

Contractor Responsibility

- Submit Issues and Risks, and recommend mitigations/resolutions
- Collaborate with State on tools and processes for issue and risk management
- Provide input to the criteria to categorize, prioritize and determine the severities for issues and risks
- Correction of all issues and risks assigned to the Contractor
- Inclusion of issue/risk reporting as part of the weekly status meetings
- Identify timeframes for resolution and mitigation plans for issues and risks

**Acceptance Criteria**

- None required - State deliverable

Task 1.2: General Timeline

The proposed rollout plan approach and dates are validated, refined, and confirmed. The Contractor detailed Project Schedule artifact is prepared.

1.2.1 Project Schedule

The Contractor is required to provide a project schedule that details the tasks and resources (including State and Contractor staff) loads. The Contractor must work with the State to update the Project Schedule. The updated Project Schedule must contain, at a minimum, the following level of detail:

- Deliverables and Milestone tasks
- Dependency Relationships
- Task expected start and finish dates
- Task actual start and finish dates
- Task durations
- Task actual work effort (percent complete)
- Task description
- Resource allocation (by individual role) for each task, including State positions

This detailed schedule will feed or link to the Master Project Schedule, which will be prepared and maintained by the State.

Timeframe

- The target date for Phase 1 FAP Project Schedule completion is within ten (10) business days from the Phase 1 Project Phase Kick-off meeting
- The target date for Phase 2 UIA Project Schedule completion is within ten (10) business days from the Phase 2 Project Phase Kick-off meeting

Deliverables

- Project Schedule – Phase 1 FAP
- Project Schedule – Phase 2 UIA

State Responsibility

- Incorporate the Contractor Project schedule into Master Project Schedule
- Provide status and clarifications to the project team, as needed
- Provide access to policies and procedures related to Contractor deliverables
- Review, maintain and report on the Master Project Schedule

Contractor Responsibility

- Update the Contractor Project Schedule
- Review, maintain and report on the Contractor Project Schedule
- Provide input and clarifications to the State as needed
- Correct any issues identified by the State

Acceptance Criteria

- Per section 1.501, 2.253, 2.254 & 2.255, approval of Contractor Project Schedule

1.2.2 Update Project Schedule – Weekly Reporting

The Contractor is responsible for updating the Contractor's detailed project schedule (at a minimum) on a weekly basis, and providing any changes to the State, for incorporation into the master project schedule, to maintain accurate status and reporting. The most current project schedules must be available for distribution and review with each Weekly Status report.

Deliverables



- Updated Contractor detailed Project Schedule

State Responsibility

- Create and update the Master Project Schedule

Contractor Responsibility

- Update the Contractor detailed Project Schedule

Acceptance Criteria

- Per section 1.501, 2.253, 2.254 & 2.255, approval of the updated Contractor detailed Project Schedule

Task 1.3: Confirm Infrastructure

This step ensures that the project infrastructure is in place. This includes location, network, hardware, development software, and associated logistics. The Technical Architecture Plan artifact is created.

Confirmation of the project infrastructure is usually done in parallel with a review of the technical infrastructure. This review includes network, hardware, operating system and desktop software, and determination of what changes in infrastructure, if any, are required for the production system.

1.3.1 EA Solution Assessment Worksheet

The Contractor must work with the State to complete the EA Solution Assessment Worksheet. This worksheet documents the Contractor's proposed tools and provides the number of licenses needed for the project team. Any exceptions to the preferred software/tools listed in the Contractor EA Solution Assessment Worksheet require documented justification from the Contractor.

The Contractor must participate in EA solution assessment workshops with the EA group to review, discuss and complete the EA Assessment Worksheet. The State will assign a liaison from the State project team to work with the EA group and track the overall progress of the work sessions and approval of the EA Assessment. The Contractor will provide a complete updated Enterprise Architecture Solution Assessment Worksheet to the State for their review and approval.

Deliverables

- EA Solution Assessment Worksheet

State Responsibility

- Assign a project liaison to work with the EA Assessment group
- Provide input and clarifications to the Contractor as needed
- Collaborate with Contractor to complete the EA Solution Assessment Worksheet
- Review and approve the Contractor's EA Solution Assessment Worksheet

Contractor Responsibility

- Collaborate with State on the necessary hardware and software provisions
- Document all necessary hardware and software
- Document the use of all hardware and software
- Assist State with completion of the EA Solution Assessment Worksheet

Acceptance Criteria

- Per section 1.501, 2.253, 2.254 & 2.255, approval of EA Solution Assessment Worksheet

1.3.2 Project Security Plan & Assessment (DIT-0170)

The Contractor must provide input to Michigan Cyber Security (MCS) to support the Security Plan and Assessment for the State of Michigan Enterprise Fraud Detection Software Project. In this task, the Contractor must engage the Project's Security Liaison, review State and Agency Security Policies, and comply with the process to complete the Security Plan and Assessment (DIT-0170), including Data Classification and System



Criticality sections. When establishing the Security Plan, identify any security risks, and describe how those risks will be mitigated.

Deliverables

- Security & Assessment Plan (DIT-0170)

State Responsibility

- Create the Security Plan & Assessment
- Provide acceptable Contractor security access to project environments

Contractor Responsibility

- Provide input to the Security Plan & Assessment
- Collaborate with State on the necessary security architecture, features, processes and procedures
- Comply with the State's described security approach for the project environments

Acceptance Criteria

- None Required – State deliverable

1.3.3 Technical Architecture Plan

The State and Contractor will jointly develop the Technical Architecture Plan. Hardware related items in the Technical Architecture Plan will be owned by the State and Software Related items in the Technical Architecture Plan will be owned by the Contractor.

The Contractor must provide a Technical Architecture Plan following a detailed requirement gathering session which containing detailed technical architectural diagrams with textual support describing the system, its function, software deployed to it, and how the State of Michigan Enterprise Fraud Detection Software interacts with the other systems contained in the overall architecture. This information must be provided for each of the three (3) environments required for the project: Development, UAT, and Production. The Technical Architecture Plan must be kept up to date throughout the project if any changes are made to the technical architecture. The technical architecture plan must include:

- Overall detailed architectural diagrams, including network topology, protocols and features, such as encryption, connection types and transfer rates where appropriate
- Required servers and their general specifications, identifying each server by its purpose, security zone, and environment
- Required software for each server, including number of licenses and versions
- Encryption for sensitive data in flight and at rest
- Touch points to other systems
- Security Policy, Access Control and Auditing
- Obfuscation of sensitive data and session security
- All major system components, data flows and how they are installed in each server environment
- Other software required, such as client licensing, including the total number of licenses and the structure of pricing and usage of the licenses (floating vs. workstation)

Deliverables

- Technical Architecture Plan

State Responsibility

- Provide input and clarifications to the Contractor as needed
- Provide State of Michigan standards for existing Enterprise Architecture
- Make available the appropriate personnel per the resource plan, to attend in the Technical Architecture requirement/design sessions
- Review and approve the Technical Architecture Plan

Contractor Responsibility

- Review State of Michigan architecture and technical standards
- Compliance with the technical requirements documented in Article 1, Section 1.104 – Work and Deliverables section II
- Create Technical Architecture Plan that is compliant with the State's Enterprise Architecture

Acceptance Criteria



- Per section 1.501, 2.253, 2.254 & 2.255, approval of Technical Architecture Plan

Task 1.4: Product Installation

1.4.1 Environment Installations

The Contractor is responsible for working with the State to install the necessary hardware and software in accordance with the environment installation plans. The Contractor must ensure that all operating systems, services, security controls, and software are properly installed. The Contractor must document the results of each environment build when installed, as per the approved project schedule.

The State of Michigan can typically procure Virtual Machine (VM) environments suitable for a development environment in 30 to 90 days from the procurement date. If the development environment requires non-standard state configurations, it can add substantial time to the procurement process.

Deliverables

- Environments built

State Responsibility

- Provide Contractor access to server environments
- Install all hardware and operating systems as necessary
- Configure hardware and software as necessary
- Configure any network devices as necessary
- Create users as needed and configure users into necessary security groups
- Apply security policy to permit or deny access by Contractor staff
- Install system certificates
- Review and approve all environment builds

Contractor Responsibility

- Install and configure the application and support software once the State has physically installed the hardware and operating systems
- Assist the State with configuration of hardware and software as necessary
- Assist the State with configuration of any network devices as necessary
- Create users as needed and configure users into necessary security groups
- Deploy final installation of all environments

Acceptance Criteria

- Completion of all environment builds

1.4.2 Environment Installation Testing

Upon completion of the installation of the environment, the Contractor must execute their installation tests to validate that installation was executed successfully.

The installation testing must include testing the connectivity to the State network infrastructure, as well as testing of the security access appropriate to the security zone that the environment is installed within. The Contractor must define and document the plan for testing failure points and the appropriate mitigation strategies. The Contractor is expected to work with State to conduct these runs and review the results. The Contractor is responsible for demonstrating that the complete environment can be restored to a fully operation state, with efficiency.

The State's IT organization has existing backup and restore procedures in place. The Contractor will provide the following:

- Provide guidance on solution considerations the State needs to address for backups
 - a. Point in time consistency
 - b. Determining when the point in time is taken with regards to data integration processing and other warehouse updates
 - c. Ensuring SAS metadata, SAS tables, and database point in time are all consistent



- d. Ensuring all applications are tied to CNAMEs versus actual FQDN
- SAS can assist with backup/restore testing by suggesting files to restore and then confirming the 'recovered' files are correct.

Deliverables

- Environments fully tested
- Backup and Recovery Plan

State Responsibility

- Support the Contractor installation tests
- Review the Contractor's Backup and Recovery Plan
- Implement the Backup and Recovery Plan
- Communicate any issues and defects to the Contractor for resolution

Contractor Responsibility

- Creation of the Backup and Recovery Plan
- Complete the environment installation tests

Acceptance Criteria

- Completion of environment installation tests
- Per section 1.501, 2.253, 2.254 & 2.255, approval of Backup and Recovery Plan

1.104.2: Phase 1 FAP: Requirements & Design

Objective

The objective of the Phase 1 FAP: Requirements & Design Phase is to develop a mutual understanding between the FAP business owners/users and the project team with regards to the business requirements for Phase 1 FAP of the State of Michigan Enterprise Fraud Detection Software Project. The Contractor will map the 'what to do' of the requirements specification into the 'how to do' of the design specifications. Finally, the user-oriented functional design specifications are translated into a set of technical system design specifications.

Description

Requirements & Design Phase begins the execution of the first project phase. Project Teams are defined and the Contractor completes the definition sessions to understand the State's requirements and overall functionality of the State of Michigan Enterprise Fraud Detection Software for Phase 1 FAP. The following tasks are performed during the requirements and design phase and continue through the project execution, as appropriate and necessary to control and report on the project.

Tasks

- 2.1 Requirements Definition
- 2.2 Functional Design

Task 2.1: Requirements Definition

The Requirements Definition task develops a basis of mutual understanding between the business owner/users and the project team with regards to the Phase 1 FAP business requirements of the State of Michigan Enterprise Fraud Detection Software Project. The result of this understanding is a mutually agreed upon Requirements Specification – which becomes the initial baseline for product design. The functional and technical/general requirements for the system are reviewed and confirmed. In addition, the services requirements for the benefit and tax fraud detection analysis scenario configuration are defined.

Activities include:

- Define Phase 1 FAP System Requirements
- Compile and Document Phase 1 FAP System Requirements
- Develop Phase 1 FAP System Test Plan Requirements



- Develop Phase 1 FAP Acceptance Test Plan Requirements
- Establish Phase 1 FAP Functional Baseline

Deliverables

- Initiation and Requirement sections of the Initiation, Requirements and Design Plan (SEM 01-Exp), including attached SEM templates

State Responsibility

- Develop Acceptance Test Requirements
- Provide input to Contractor on Initiation and Requirements sections of SEM 01-Exp
- Participate in system requirement workshops and sessions as needed
- Review Initiation and Requirements sections of the Initiation, Requirements and Design Plan (SEM 01-Exp) including required SEM templates

Contractor Responsibility

- Verification of functional requirements
- Verification of technical/general requirements
- Verification of services requirements for FAP fraud detection analysis scenario configuration.
- Lead requirement workshops and sessions to confirm and finalize functional, technical/general and services requirements with the State
- Provide input and clarifications to the State as needed
- Complete Initiation and Requirements sections of Initiation, Requirements and Design Plan (SEM 01-Exp)
- Develop System Test Requirements

Acceptance Criteria

- Completion of Initiation and Requirements sections of the Initiation, Requirements and Design Plan (SEM 01-Exp) including required templates.

Task 2.2: Functional Design

During Functional Design the 'what to do' of the requirements specification are mapped into the 'how to do it' of the design specifications. During this activity, the overall structure of the solution is defined from a functional viewpoint for Phase 1 FAP. The functional design describes the logical system flow, data organization, system inputs and outputs, and processing rules. The goal of this activity is to define and document the functions of the solution to the extent necessary to obtain the system owner and users' approval to the level of detail necessary to configure the system. The functional, technical/general and benefit fraud detection analysis scenario configuration requirements are all mapped to system design specifications.

Activities include:

- Determine Phase 1 FAP System Structure
- Design Content of Phase 1 FAP System Inputs & Outputs
- Design Phase 1 FAP System Interfaces
- Design Phase 1 FAP System Security Controls
- Develop Phase 1 FAP Functional Design
- Develop Phase 1 FAP Test Cases

Deliverables

- Design Plan section of Initiation, Requirements and Design Plan (SEM 01-Exp) including required SEM templates

**State Responsibility**

- Review Initiation, Requirements and Design Plan (SEM 01-Exp)
- Provide input to Contractor on Initiation and Requirements sections of SEM 01-Exp
- Participate in functional design workshops and sessions
- Develop User Acceptance Test Cases
- Attend walkthrough of Initiation, Requirements and Design Plan (SEM 01-Exp)



Contractor Responsibility

- Lead functional design workshops and sessions to confirm and finalize functional design with the State.
- Provide input and clarifications to the State as needed
- Complete functional system design
- Complete technical/general design
- Complete FAP fraud detection analysis scenario configuration design
- Develop System Test Scenarios
- Complete Design section of Initiation, Requirements and Design Plan (SEM 01-Exp)
- Update Initiation, Requirements and Design Plan (SEM 01-Exp)
- Conduct walkthrough of Initiation, Requirements and Design Plan (SEM 01-Exp)

Acceptance Criteria

- Per section 1.501, 2.253, 2.254 & 2.255, approval of the Initiation, Requirements and Design Plan (SEM 01-Exp) including required SEM templates.

1.104.3 Phase 1 FAP: Construction & Testing

Objective

The objective of the Phase 1 FAP: Construction and Testing Phase is to configure the system to conform to the system design specifications.

Description

The tasks and activities of this stage result in the transformation of the system design into the complete executable representation of the solution. Functionality is tested to determine the solution meets predetermined functionality, performance, quality, and security requirements. System testing is conducted to validate the solution will operate in its intended environment, satisfies all the user requirements, and is supported with complete and accurate documentation. User Acceptance Testing (UAT) follows system testing, and solicits feedback from users for the Contractor to make any final adjustments before releasing the solution for implementation.

Tasks

- 3.1 Construction and Testing Plan (SEM 02-Exp)
- 3.2 Data Preparation
- 3.3 Configure FAP Fraud Detection Analysis Scenarios
- 3.4 Integrations
- 3.5 Transition and Operations Planning
- 3.6 System Testing
- 3.7 User Acceptance Testing (UAT)

Task 3.1: Construction and Testing Plan (SEM 02-Exp)

The Contractor is responsible for completing the Construction and Testing Plan which contains the essentials for test reporting, transition planning, installation planning and State acceptance of the tested system.

Deliverables

- Construction and Testing Plan (SEM 02-Exp)

State Responsibility

- Provide timely feedback and information required by the Contractor
- Attend walkthrough of Construction and Testing Plan

Contractor Responsibility

- Solicit information from the State as needed
- Complete initial Construction and Testing Plan (SEM 02-Exp)
- Conduct walkthrough of Construction and Testing Plan

Acceptance Criteria

- Per section 1.501, 2.253, 2.254 & 2.255, approval of Construction and Testing Plan (SEM 02-Exp)



Task 3.2: Data Preparation

The Contractor is responsible for completing any data preparation needed to support the Phase 1 FAP fraud detection analysis from the DTMB warehouse. This includes analyzing the available data from the warehouse, potentially working with DTMB warehouse staff to modify or augment the contents of the data warehouse as needed, and preparing any necessary extract/transform/load (ETL) procedures necessary to support the State of Michigan Enterprise Fraud Detection Software COTS product.

Deliverables

- Data preparation for all required Phase 1 FAP fraud detection patterns and analysis scenarios

State Responsibility

- Provide timely feedback and information required by the Contractor
- Attend demonstration of data preparation for all required patterns and analysis scenarios completed by the Contractor

Contractor Responsibility

- Complete data preparation for all required Phase 1 FAP fraud detection patterns and analysis scenarios
- Solicit information from the State as needed
- Lead demonstration of the completed data preparation for all required Phase 1 FAP fraud detection patterns and analysis scenarios to the State which will include a demonstration / walkthrough of data processing and Runbook

Acceptance Criteria

- Determination by the State of the successful data preparation for all required Phase 1 FAP fraud detection patterns and analysis scenarios in the COTS Fraud Detection solution
-

Task 3.3: Configure FAP Fraud Detection Analysis Scenarios

The Contractor is responsible for configuring fraud analysis for four (4) FAP fraud detection analysis scenarios. The State will consider additional best practice analysis scenarios from the Contractor. These four configured fraud analysis scenarios must at a minimum contain beneficiary, employer, internal staff and provider/retailer criteria and apply pattern analyses such as the following for FAP:

1. New Application/Redetermination Cross Match – Method of identifying potential fraud cases through data comparisons and pattern recognition for new public assistance applications/redeterminations that are filed within a defined time frame using the following criteria as an example:
 - A. Recipient/Beneficiary
 - State ID pattern
 - Birthday pattern
 - Address pattern
 - Close-to-recipient address
 - Education level
 - Repeated phone number for PA application/redetermination
 - Repeated ID Address
 - Employer has not reported wages
 - User ID pattern
 - Prior detection
 - Incarceration
 - Social network pattern
 - B. Employer
 - Fictitious employer
 - Office building pattern
 - Abandoned building pattern
 - Terminated building pattern



- C. Provider/Retailer
 - N/A
 - D. Internal Staff
 - Employee filing as a PA recipient
 - Validate internal staff wages
 - Employee address cross match
2. FinCEN Cross Match – Method of identifying potential financial crime fraud cases through data comparisons and pattern recognition for new and ongoing public assistance cases that are filed within a defined time frame using the following criteria as an example:
- A. Recipient/Beneficiary
 - State ID pattern
 - Birthday pattern
 - Address pattern
 - Close-to-recipient address
 - Education level
 - Repeated phone number for PA application/redetermination
 - Repeated ID Address
 - Employer has not reported wages
 - Prior detection
 - Incarceration
 - Social network pattern
 - B. Employer
 - N/A
 - C. Provider/Retailer
 - N/A
 - D. Internal Staff
 - Employee filing as a PA recipient
 - Validate internal staff wages
 - Employee address cross match
3. MI Department of Treasury Cross Match – Method of identifying potential wage and employer fraud cases through data comparisons and pattern recognition for new and ongoing public assistance cases that are filed within a defined time frame using the following criteria as an example:
- A. Recipient/Beneficiary
 - State ID pattern
 - Birthday pattern
 - Address pattern
 - Close-to-recipient address
 - Education level
 - Repeated phone number for PA application/redetermination
 - Repeated ID Address
 - Employer has not reported wages
 - Validate claimant wages (1099 output)
 - B. Employer
 - Fictitious employer
 - Office building pattern
 - Abandoned building pattern
 - Terminated building pattern
 - C. Provider/Retailer
 - N/A
 - D. Internal Staff
 - Validate internal staff wages
 - Employee address cross match



4. Trafficking Cross Match – Method of identifying potential public assistance trafficking fraud cases through data comparisons and pattern recognition for new and ongoing public assistance cases that are file within a defined time frame using the following criteria as an example:

A. Recipient/Beneficiary

- Distance from case address
- High volume of recipient redemptions
- Even dollar transaction
- Identical transaction amount
- Transaction type
- Off-hours redemption
- Time period between transactions pattern
- Exceeded threshold amount transaction
- Social network pattern

B. Employer

- N/A

C. Provider/Retailer

- High volume of provider/retailer redemptions
- Multiple redemptions for a single recipient pattern
- Even dollar transaction
- Identical transaction amount
- Transaction type
- Off-hour redemption pattern
- Time period between transactions pattern
- Exceeded threshold amount transaction pattern

D. Internal Staff

- N/A

Deliverables

- Configuration of four (4) FAP fraud detection analysis scenarios for FAP: New Application/Redetermination Cross Match, FinCEN Cross Match, MI Department of Treasury Cross Match and Trafficking Cross Match

State Responsibility

- Provide timely feedback and information required by the Contractor
- Attend demonstration of completed configured FAP fraud detection analysis scenarios by the Contractor

Contractor Responsibility

- Configuration of four (4) fraud detection analysis scenarios for FAP: New Application/Redetermination Cross Match, FinCEN Cross Match, MI Department of Treasury Cross Match and Trafficking Cross Match
- Solicit information to obtain information from the State as needed
- Lead demonstration of completed FAP fraud detection analysis scenarios to the State

Acceptance

- Demonstration by Contractor to the State that the FAP fraud detection analysis scenarios have been successfully configured and completed

Task 3.4: Integrations

The Contractor solution must integrate the FAP beneficiary analysis results periodically with FEE, based on the severity and priority of the potential cases. The interfaces must be automated.

The State of Michigan Enterprise Fraud Detection Software must also integrate with LexisNexis for asset verification.



The Contractor is responsible for documenting, development and testing the interfaces to FEE and LexisNexis. The data requirements and protocols for each must be defined. The interfaces to be developed along with the communication protocol will be based on the approved Initiation, Requirements and Design Plan (SEM 01-Exp). The State currently anticipates that the communication protocol will be a mutually agreed upon flat file format transmitted via secure FTP. Electronic notifications of success or failure are generated from each interface.

The scope of this task includes integration with any required middleware, testing through the middleware and through the systems components.

The Contractor will work with the State to identify formatted messages that will be exchanged for each interface. The State of Michigan Enterprise Fraud Detection Software will utilize the existing format for interfaces, unless otherwise directed by the State. The Contractor will perform unit testing to validate the transaction messages match the data layouts.

Deliverables

- Interface Design documents
- Integration from State of Michigan Enterprise Fraud Detection Software to FEE potential beneficiary FAP cases from fraud detection analysis scenario results
- Integration from State of Michigan Enterprise Fraud Detection Software to LexisNexis for asset verification

State Responsibility

- Assist in creating the Interface Design documents
- Provide documentation on required interfaces
- Provide input and clarifications to the Contractor as needed

Contractor Responsibility

- Coordinate with the State on questions and problems relating to interfaces
- Identify modifications needed to required interfaces
- Create Interface Design documents
- Develop interfaces
- Perform unit testing on interfaces

Acceptance Criteria

- Approval of Contractor prepared Interface Design document
- Demonstration of successful integration with FEE
- Demonstration of successful integration with LexisNexis

Task 3.5: Transition and Operations Planning

The plan to complete the operations transition must be documented by the Contractor in the Operations Transition Plan. This plan shall include, at a minimum:

- Transition schedules and tasks
- Hardware and software deployment strategy
- Personnel requirements
- Facilities
- Risk Mitigation Strategies
- Management Controls
- Reporting
- Acceptance Criteria

Deliverables

- Update Operations Transition Plan, as needed

**State Responsibility**

- Review and approve the Operations Transition Plan
- Provide input and clarifications to the Contractor as needed

Contractor Responsibility

- Update the Operations Transition Plan, as needed
- Define the relationships and responsibilities between the Contractor and State personnel for State of Michigan Enterprise Fraud Detection Software operations

Acceptance Criteria

- Approval of Updated Operations Transition Plan

Task 3.6: System Testing

The Test Plan created in the Construction and Testing Template (SEM 02-Exp) is executed for system testing. Once the product is fully integrated, system testing is conducted to validate that the product will operate in its intended environment, satisfies all user requirements, and is supported with complete and accurate operating documentation. Anomalies identified at this step are recorded and tracked to resolution.

The Contractor must schedule, coordinate, and perform all system testing activities. The Contractor is responsible for generating all test data for the system testing activities. The State will provide assistance and input to assist Contractor with the development of appropriate test data.

The Contractor must also correct defects discovered during system testing by following normal application development procedures – modifying the appropriate configuration items in the development environment, unit and integration testing the change, and promoting the configuration and new development items to the testing environment.

The State is responsible for supporting the Contractor in system testing of the entire State of Michigan Enterprise Fraud Detection Software.

The Contractor will lead periodic problem review meetings with the State, to analyze defects and failed scenarios. The Contractor will review common defects and failed scenarios reported in system testing and collaborate with the State to improve configuration, development and testing processes with the objective of minimizing the occurrence of these issues and improving the efficiency.

Deliverables

- System Test results

State Responsibility

- Provide assistance and input to Contractor on data necessary to support testing
- Review test data
- Assist with the create of the system test schedule and test procedures
- Review failed test scenarios
- Participate in status meetings

Contractor Responsibility

- Create test scripts
- Review test data
- Create test procedures
- Execute test scripts
- Conduct tests to validate results
- Document test results
- Record defects
- Modify test scripts and scenarios, if needed
- Create additional test scripts and scenarios, if needed
- Retest resolved defects and perform regression testing
- Ensure that data is loaded to the Test Environment



- Provide customized data or interface files, as needed, to complete test scenario execution
- Review failed test scenarios and recommend most efficient and accurate resolutions
- Correct defects found
- Conduct status meetings

Acceptance Criteria

- All system tests pass

Task 3.7: User Acceptance Testing (UAT)

The Test Plan created in the Construction and Testing Template (SEM 02-Exp) is executed for User Acceptance Testing. Anomalies identified at this step are recorded and tracked to resolution. User Acceptance Testing begins upon completion of System Testing.

The Contractor will work with the State to schedule, coordinate, and monitor all UAT activities. The State is responsible for providing end users and SMEs to perform UAT.

The Contractor is responsible for loading all test data for the UAT and Training activities. The State will provide assistance and input to assist Contractor with the development of appropriate test data.

The Contractor must provide support for the duration of UAT. The testing process must include the ability to advance the testing clock to provide for a complete test of the lifecycle of cases over many simulated months or years.

The Contractor must also correct defects discovered during UAT by following normal application development procedures – modifying the appropriate configuration items in the development environment, unit and integration testing the change, and promoting the configuration and new development items to the testing environment. Promotions to the testing environment must occur on a mutually agreed upon regularly scheduled basis (e.g., daily) and emergencies (e.g., UAT cannot continue until the problem is resolved).

The State will take the lead on conducting UAT. The Contractor is responsible for participating and supporting the State users in UAT of the entire State of Michigan Enterprise Fraud Detection Software. This activity includes specifying dates and time for end users to conduct testing, training on any tools to assist end users on how test results will be produced, viewed, and reported.

The Contractor will train the State UAT team in the functionality and capabilities of State of Michigan Enterprise Fraud Detection Software before conducting the UAT task. The State will lead periodic problem review meetings with the Contractor, to analyze defects and failed scenarios.

The Contractor will review common defects and failed scenarios reported in UAT testing and collaborate with the State to improve configuration, development and testing processes with the objective of minimizing the occurrence of these issues and improving the efficiency.

Deliverables

- UAT results
- Comprehensive training plan designed to meet conversion, implementation, operation, and development needs of the State for Phase 1 FAP

State Responsibility

- Schedule State UAT Testers for training
- Attend training
- Provide input to Contractor on data necessary to support testing
- Review test data
- Create UAT schedule and test procedures



- Conduct tests to validate results
- Document test results
- Record defects
- Document defects using Incident Reports
- Conduct Problem Review meeting
- Modify the Test Scenarios, if needed
- Create additional Test Scenarios, if needed
- Retest resolved defects and perform regression testing
- Attend status meetings

Contractor Responsibility

- Ensure that all modifications to the State of Michigan Enterprise Fraud Detection Software are thoroughly system tested prior to transferring new versions to UAT Testing
- Ensure that data is loaded to the Test Environment
- Provide customized data or interface files to the State, as needed, to complete test scenario execution
- Provide training
- Assist with the creation of the UAT Test schedule and test procedures
- Review failed test scenarios and recommend most efficient and accurate resolutions
- Participate in Problem Review meeting(s)
- Correct defects found
- Assist with coordination of regression testing as needed
- Conduct status meetings

Acceptance Criteria

- All UAT test cases pass
- Approval of comprehensive training plan designed to meet conversion, implementation, operation, and development needs of the State for Phase 1 FAP

1.104.4 Phase 1 FAP: Implementation

Objective

The objective of the Phase 1 FAP: Implementation is to prepare a production environment for deployment of the system.

Description

The Implementation Phase involves verification that the production environment hardware and software is production ready. The system security plan is finalized to ensure the product environment meets all security requirements for the system and data, including data at rest and data in transit. The disaster recovery procedures for the system are added to the State business continuity plan for the State.

Once the preparation is complete, a detailed cutover task list and schedule are prepared. Each step to be performed is included, along with checkpoints and rollback procedures. The production software goes live, and the system data and functionality is validated. The results of this validation will drive a “go/no go” decision from the State. If there are significant issues, the system deployment may be rolled back, per procedures.

Tasks

- 4.1 Production Cutover
- 4.2 Installation Testing
- 4.3 Post Implementation Evaluation Report (PIER)

Task 4.1: Production Cutover

The system goes live. Desk-side support is provided to end users and operations are carefully monitored.

The Contractor develops an Installation Plan (SEM-0702) which provides the list of interrelated steps and activities that must be coordinated to ensure a smooth and successful rollout. The Installation Plan is followed during Production Cutover.



A high-level checklist is prepared for general consumption within the agency to communicate the general schedule. A detailed, step-by-step checklist is prepared for the project team to follow.

Perform Software Implementation

The Contractor must provide the necessary resources to install the State of Michigan Enterprise Fraud Detection Software solution onto the production hardware per the Installation Plan. Any and all issues must be resolved during the installation procedures prior to cutover to the new software.

Deliverable

- Installation of the State of Michigan Enterprise Fraud Detection Software onto the production environment
- Installation Plan (SEM-0702)
- "Go/no go" Check List

State Responsibility

- Provide support during the implementation
- Attendance of Appropriate Personnel in the "go/no-go" review meeting
- Review Installation Plan
- Prepare the "go/no-go" checklist
- Make "go/no go" decision

Contractor Responsibility

- Prepare the Installation Plan (SEM-0702)
- Follow the Installation Plan
- Review the "go/no-go" Check List
- Installation of the State of Michigan Enterprise Fraud Detection Software onto the production environment

Acceptance Criteria

- Approval of State of Michigan Enterprise Fraud Detection Software installation

Task 4.2: Installation Testing

The Contractor must test the State of Michigan Enterprise Fraud Detection Software with the Phase 1 configurations in the State production environment to ensure the software is installed and functioning properly. These tests should:

- Ensure the environment is properly installed and configured
- Ensure the System is completely functional
- Ensure data is ported to the production environment
- Identify any defects or problems in the environment against expected results for all tests

Deliverables

- Conduct Installation Testing

State Responsibility

- Provide staff to assist the Contractor in the Installation Testing activity
- Review and approve Installation Test results

Contractor Responsibility

- Properly test the production environment to ensure it is fully installed and operating properly
- Ensure data is ported to the production environment
- Resolve any issues/problems for installation
- Provide installation test results

Acceptance Criteria

- Approval of Installation Testing results



Task 4.3: Post Implementation Evaluation Report (PIER)

The Contractor is responsible – with input from the State – for completing the Post-Implementation Evaluation Report for Phase 1 FAP.

Deliverable

- Post Implementation Evaluation Report (PIER)

State Responsibility

- Review the Post Implementation Evaluation Report
- Provide feedback to Contractor
- Approve the Post Implementation Evaluation Report

Contractor Responsibility

- Complete the Post Implementation Evaluation Report
- Correct any identified deficiencies

Acceptance Criteria

- Per section 1.501, 2.253, 2.254 & 2.255, approval of Post Implementation Evaluation Report

1.104.5: Phase 2 UIA: Requirements & Design**Objective**

The objective of the Phase 2 UIA: Requirements & Design Phase is to develop a mutual understanding between the UIA business owners/users and the project team with regards to the business requirements for Phase 2 UIA of the State of Michigan Enterprise Fraud Detection Software Project. The Contractor will map the 'what to do' of the requirements specification into the 'how to do' of the design specifications. Finally, the user-oriented functional design specifications are translated into a set of technical system design specifications.

Description

Requirements & Design Phase begins the execution of the second project phase. Project Teams are defined and the Contractor completes the definition sessions to understand the State's requirements and overall functionality of the State of Michigan Enterprise Fraud Detection Software for Phase 2 UIA. The following tasks are performed during the requirements and design phase and continue through the project execution, as appropriate and necessary to control and report on the project.

Tasks

- 5.1 Requirements Definition
- 5.2 Functional Design

Task 5.1: Requirements Definition

The Requirements Definition task develops a basis of mutual understanding between the business owner/users and the project team with regards to the Phase 2 UIA business requirements of the State of Michigan Enterprise Fraud Detection Software Project. The result of this understanding is a mutually agreed upon Requirements Specification – which becomes the initial baseline for product design. The functional and technical/general requirements for the system are reviewed and confirmed. In addition, the services requirements for the benefit and tax fraud detection analysis scenario configuration are defined.

Activities include:

- Select Requirements Analysis Technique
- Define Phase 2 UIA System Requirements
- Compile and Document Phase 2 UIA System Requirements
- Develop Phase 2 UIA System Test Plan Requirements
- Develop Phase 2 UIA Acceptance Test Plan Requirements
- Establish Phase 2 UIA Functional Baseline



Deliverables

- Initiation and Requirement sections of the Initiation, Requirements and Design Plan (SEM 01-Exp), including attached SEM templates

State Responsibility

- Complete Infrastructure Services Request (DIT-0184)
- Develop Acceptance Test Requirements
- Provide input to Contractor on Initiation and Requirements sections of SEM 01-Exp
- Participate in system requirement workshops and sessions as needed
- Review Initiation and Requirements sections of the Initiation, Requirements and Design Plan (SEM 01-Exp) including required SEM templates

Contractor Responsibility

- Verification of functional requirements
- Verification of technical/general requirements
- Verification of services requirements for UIA benefit and tax fraud detection analysis scenario configuration.
- Lead requirement workshops and sessions to confirm and finalize functional, technical/general and services requirements with the State
- Provide input and clarifications to the State as needed
- Complete Initiation and Requirements sections of Initiation, Requirements and Design Plan (SEM 01-Exp)
- Develop System Test Requirements

Acceptance Criteria

- Completion of Initiation and Requirements sections of the Initiation, Requirements and Design Plan (SEM 01-Exp) including required SEM templates

Task 5.2: Functional Design

During Functional Design the 'what to do' of the requirements specification are mapped into the 'how to do it' of the design specifications. During this activity, the overall structure of the solution is defined from a functional viewpoint for Phase 2 UIA. The functional design describes the logical system flow, data organization, system inputs and outputs, and processing rules. The goal of this activity is to define and document the functions of the solution to the extent necessary to obtain the system owner and users' approval to the level of detail necessary to configure the system. The functional, technical/general and benefit and tax fraud detection analysis scenario configuration requirements are all mapped to system design specifications.

Activities include:

- Determine Phase 2 UIA System Structure
- Design Content of Phase 2 UIA System Inputs & Outputs
- Design Phase 2 UIA System Interfaces
- Design Phase 2 UIA System Security Controls
- Develop Phase 2 UIA Functional Design
- Develop Phase 2 UIA Test Cases

Deliverables

- Design Plan section of Initiation, Requirements and Design Plan (SEM 01-Exp) including required SEM templates

State Responsibility

- Review Initiation, Requirements and Design Plan (SEM 01-Exp)
- Provide input to Contractor on Initiation and Requirements sections of SEM 01-Exp
- Participate in functional design workshops and sessions
- Develop User Acceptance Test Cases
- Attend walkthrough of Initiation, Requirements and Design Plan (SEM 01-Exp)



Contractor Responsibility

- Lead functional design workshops and sessions to confirm and finalize functional design with the State.
- Provide input and clarifications to the State as needed
- Complete functional system design
- Complete technical/general design
- Complete UIA benefit and tax fraud detection analysis scenario configuration design
- Develop System Test Scenarios
- Complete Design section of Initiation, Requirements and Design Plan (SEM 01-Exp)
- Update Initiation, Requirements and Design Plan (SEM 01-Exp)
- Conduct walkthrough of Initiation, Requirements and Design Plan (SEM 01-Exp)

Acceptance Criteria

- Per section 1.501, 2.253, 2.254 & 2.255, approval of the Initiation, Requirements and Design Plan (SEM 01-Exp) including required SEM templates.

1.104.6 Phase 2 UIA: Construction & Testing

Objective

The objective of the Phase 2 UIA: Construction and Testing Phase is to configure the system to conform to the system design specifications.

Description

The tasks and activities of this stage result in the transformation of the system design into the complete executable representation of the solution. Functionality is tested to determine the solution meets predetermined functionality, performance, quality, and security requirements. System testing is conducted to validate the solution will operate in its intended environment, satisfies all the user requirements, and is supported with complete and accurate documentation. User Acceptance Testing (UAT) follows system testing, and solicits feedback from users for the Contractor to make any final adjustments before releasing the solution for implementation.

Tasks

- 6.1 Construction and Testing Plan (SEM 02-Exp)
- 6.2 Data Preparation
- 6.3 Configure UIA Benefit and Tax Fraud Detection Analysis Scenarios
- 6.4 Integrations
- 6.5 Transition and Operations Planning
- 6.6 System Testing
- 6.7 User Acceptance Testing (UAT)

Task 6.1: Construction and Testing Plan (SEM 02-Exp)

The Contractor is responsible for completing the Construction and Testing Plan which contains the essentials for test reporting, transition planning, installation planning and State acceptance of the tested system.

Deliverables

- Construction and Testing Plan (SEM 02-Exp)

State Responsibility

- Provide timely feedback and information required by the Contractor
- Attend walkthrough of Construction and Testing Plan

Contractor Responsibility

- Solicit information from the State as needed
- Complete initial Construction and Testing Plan (SEM 02-Exp)
- Conduct walkthrough of Construction and Testing Plan

Acceptance Criteria

- Per section 1.501, 2.253, 2.254 & 2.255, approval of Construction and Testing Plan (SEM 02-Exp)



Task 6.2: Data Preparation

The Contractor is responsible for completing any data preparation needed to support the Phase 2 UIA fraud detection analysis from the DTMB warehouse. This includes analyzing the available data from the warehouse, potentially working with DTMB warehouse staff to modify or augment the contents of the data warehouse if needed, and preparing any necessary extract/transform/load (ETL) procedures necessary to support the State of Michigan Enterprise Fraud Detection Software COTS product.

Deliverables

- Data preparation for all required Phase 2 UIA fraud detection patterns and analysis scenarios

State Responsibility

- Provide timely feedback and information required by the Contractor
- Attend demonstration of data preparation for all required patterns and analysis scenarios completed by the Contractor

Contractor Responsibility

- Complete data preparation for all required Phase 2 UIA fraud detection patterns and analysis scenarios
- Solicit information from the State as needed
- Lead demonstration of the completed data preparation for all required Phase 2 UIA fraud detection patterns and analysis scenarios to the State which will include a demonstration / walkthrough of data processing and Runbook

Acceptance Criteria

- Determination by the State of the successful data preparation for all required Phase 2 UIA fraud detection patterns and analysis scenarios in the State of Michigan Enterprise Fraud Detection Software

Task 6.3: Configure UIA Benefit and Tax Fraud Detection Analysis Scenarios

The Contractor is responsible for configuring fraud analysis for four (4) UIA benefit and tax fraud detection analysis scenarios. The State will consider additional best practice analysis scenarios from the Contractor. These four configured fraud analysis scenarios must at a minimum contain claimant, employer and internal staff criteria and apply pattern analyses such as the following for UIA:

1. New Claims Cross Match – Method of identifying potential UIA fraud cases through data comparisons and pattern recognition for new unemployment claims that are filed within a defined time frame using the following criteria as an example:
 - A. Claimant Criteria:
 - State ID pattern
 - Birthday pattern
 - Address pattern
 - Close-to-claimant address
 - Multiple claims to the same address
 - Education Level
 - Repeated phone number for initial claims
 - IP Address
 - Repeated IP Address
 - Separating employer not in base period
 - Employer has not reported wages for claimant
 - User ID pattern
 - Social Security Act Disability and UI Benefit Payments
 - Prior detection
 - Incarceration
 - B. Employer Criteria:
 - Fictitious employer
 - Employer filing as claimant



- C. Internal Staff Criteria
 - Employee filing as claimant
- 2. Continued Claims Cross Match: Method of identifying potential UIA fraud cases through data comparisons and pattern recognition for continued unemployment claims (certifications) that are filed within a defined time frame using the following criteria as an example:
 - A. Claimant Criteria:
 - IP Address
 - Repeated IP Address
 - Same originating telephone number for continued claims
 - User ID pattern
 - Prior detection
 - Incarceration
 - B. Employer Criteria: N/A
 - Internal Staff Criteria:
 - Telephone number source
 - Repeated employee involvement on claims certifications
 - IP Address
- 3. Base Period Wages: Method of identifying potential UIA fraud cases through data comparisons and pattern recognition for unusual patterns within the base period on new claims that are filed within a defined time frame using the following criteria as an example:
 - A. Claimant Criteria:
 - High number of base period employers
 - Self-reported wages on same employer (multiple claimants)
 - Separating employer not in base period
 - B. Employer Criteria:
 - Fictitious employer
 - Recently liable employers in the base period
 - C. Verify Internal Staff Criteria:
 - Staff data entry of wages
- 4. Employer Tax Liability: Method of identifying potential fraud cases through data comparisons and pattern recognition for underpayment of tax liabilities by an employer using the following criteria as an example:
 - A. Claimant Criteria:
 - Self-reported wages on same employer
 - B. Employer Criteria:
 - Wage pattern
 - Tax pattern
 - C. Internal Staff Criteria: N/A

Deliverables

- Configuration of four (4) UIA benefit and tax fraud detection analysis scenarios: New Claims Cross Match, Continued Claims Cross Match, Base Period Wages and Employer Tax Liability

State Responsibility

- Provide timely feedback and information required by the Contractor
- Attend demonstration of the four (4) completed/configured UIA benefit and tax fraud detection analysis scenarios by the Contractor

Contractor Responsibility

- Configuration of four (4) UIA benefit and tax fraud detection analysis scenarios: New Claims Cross Match, Continued Claims Cross Match, Base Period Wages and Employer Tax Liability



- Solicit information to obtain information from the State as needed
- Lead demonstration of the four (4) completed/configured UIA benefit and tax fraud detection analysis scenarios to the State

Acceptance

- Demonstration by Contractor to the State that the UIA benefit and tax fraud detection analysis scenarios have been successfully completed and configured

Task 6.4: Integrations

The Contractor solution must integrate the UIA fraud analysis results periodically with FACTS and CAMS, and the UIA MiDAS system, based on the severity and priority of the potential cases. The interfaces must be automated. High Priority UIA cases will be sent to FACTS while Medium and Low Priority UIA cases will be sent to CAMS. Analysis results for potential fraud cases will be integrated with the MiDAS system workflow engine and cases will be routed to the appropriate work queues based on priority and severity. Scoring information must be included with the work item when passed to MiDAS.

The Contractor is responsible for documenting, development and testing the interfaces to FACTS, CAMS and MiDAS. The data requirements and communication protocols must be defined. The interfaces to be developed along with the communication protocol will be based on the approved Initiation, Requirements and Design Plan (SEM 01-Exp). The State currently anticipates that the communication protocol will be a mutually agreed upon flat file format transmitted via secure FTP. Electronic notifications of success or failure are generated from each interface.

The scope of this task includes integration with any identified middleware or other communication methods, and testing these integration points.

The Contractor will work with the State to identify formatted messages that will be exchanged for each interface. The State of Michigan Enterprise Fraud Detection Software will utilize the existing format for interfaces, unless otherwise directed by the State. The Contractor will perform unit testing to validate the transaction messages match the data layouts.

Deliverables

- Interface Design documents
- Integration from State of Michigan Enterprise Fraud Detection Software to FACTS for High Priority potential UIA cases from fraud detection analysis scenario results
- Integration from State of Michigan Enterprise Fraud Detection Software to CAMS for Medium and Low Priority potential UIA cases from fraud detection analysis scenario results
- Integration from State of Michigan Enterprise Fraud Detection solution to MiDAS workflow engine based on priority/severity of potential UIA cases

State Responsibility

- Assist in creating the Interface Design documents
- Provide documentation on required interfaces
- Provide input and clarifications to the Contractor as needed

Contractor Responsibility

- Coordinate with the State on questions and problems relating to interfaces
- Identify modifications needed to required interfaces
- Create Interface Design documents
- Develop interfaces
- Perform unit testing on interfaces

Acceptance Criteria

- Approval of Contractor prepared Interface Design documents
- Demonstration of successful integration of UIA analysis scenario results by priority with FACTS and CAMS
- Demonstration of successful integration with MiDAS



Task 6.5: Transition and Operations Planning

The plan to complete the operations transition must be documented by the Contractor in the Operations Transition Plan. This plan shall include, at a minimum:

- Transition schedules and tasks
- Hardware and software deployment strategy
- Personnel requirements
- Facilities
- Risk Mitigation Strategies
- Management Controls
- Reporting
- Acceptance Criteria

Deliverables

- Operations Transition Plan

State Responsibility

- Review and approve the Operations Transition Plan
- Provide input and clarifications to the Contractor as needed

Contractor Responsibility

- Develop an Operations Transition Plan
- Define the relationships and responsibilities between the Contractor and State personnel for State of Michigan Enterprise Fraud Detection Software operations

Acceptance Criteria

- Approval of Operations Transition Plan

Task 6.6: System Testing

The Test Plan created in the Construction and Testing Template (SEM 02-Exp) is executed for system testing. Once the product is fully integrated, system testing is conducted to validate that the product will operate in its intended environment, satisfies all user requirements, and is supported with complete and accurate operating documentation. Anomalies identified at this step are recorded and tracked to resolution.

The Contractor must schedule, coordinate, and perform all system testing activities. The Contractor is responsible for generating all test data for the system testing activities. The State will provide assistance and input to assist Contractor with the development of appropriate test data.

The Contractor must also correct defects discovered during system testing by following normal application development procedures – modifying the appropriate configuration items in the development environment, unit and integration testing the change, and promoting the configuration and new development items to the testing environment.

The State is responsible for supporting the Contractor in system testing of the entire State of Michigan Enterprise Fraud Detection Software Project.

The Contractor will lead periodic problem review meetings with the State, to analyze defects and failed scenarios. The Contractor will review common defects and failed scenarios reported in system testing and collaborate with the State to improve configuration, development and testing processes with the objective of minimizing the occurrence of these issues and improving the efficiency.

Deliverables

- System Test results
- Comprehensive training plan designed to meet conversion, implementation, operation, and development needs of the State

**State Responsibility**

- Provide assistance and input to Contractor on data necessary to support testing
- Review test data
- Assist with the create of the system test schedule and test procedures
- Review failed test scenarios
- Participate in status meetings

Contractor Responsibility

- Create test scripts
- Review test data
- Create test procedures
- Execute test scripts
- Conduct tests to validate results
- Document test results
- Record defects
- Modify test scripts and scenarios, if needed
- Create additional test scripts and scenarios, if needed
- Retest resolved defects and perform regression testing
- Ensure that data is loaded to the Test Environment
- Provide customized data or interface files, as needed, to complete test scenario execution
- Assist with the creation of the UAT Test schedule and test procedures
- Review failed test scenarios and recommend most efficient and accurate resolutions
- Correct defects found
- Conduct status meetings

Acceptance Criteria

- All system tests pass
- Approval of comprehensive training plan designed to meet conversion, implementation, operation, and development needs of the State

Task 6.7: User Acceptance Testing (UAT)

The Test Plan created in the Construction and Testing Template (SEM 02-Exp) is executed for User Acceptance Testing. Anomalies identified at this step are recorded and tracked to resolution. User Acceptance Testing begins upon completion of System Testing.

The Contractor will work with the State to schedule, coordinate, and monitor all UAT activities. The State is responsible for providing end users and Subject Matter Experts to perform UAT.

The Contractor is responsible for loading all test data for the UAT and Training activities. The State will provide assistance and input to assist Contractor with the development of appropriate test data.

The Contractor must provide support for the duration of UAT. The testing process must include the ability to advance the testing clock to provide for a complete test of the lifecycle of cases over many simulated months or years.

The Contractor must also correct defects discovered during UAT by following normal application development procedures – modifying the appropriate configuration items in the development environment, unit and integration testing the change, and promoting the configuration and new development items to the testing environment. Promotions to the testing environment must occur on a mutually agreed upon regularly scheduled basis (e.g., daily) and emergencies (e.g., UAT cannot continue until the problem is resolved).

The State will take the lead on conducting UAT. The Contractor is responsible for participating and supporting the State users in UAT of the entire State of Michigan Enterprise Fraud Detection Software Project. This activity includes specifying dates and time for end users to conduct testing, training on any tools to assist end users on how test results will be produced, viewed, and reported.



The Contractor will train the State UAT team in the functionality and capabilities of State of Michigan Enterprise Fraud Detection Software before conducting the UAT task. The State will lead periodic problem review meetings with the Contractor, to analyze defects and failed scenarios.

The Contractor will review common defects and failed scenarios reported in UAT testing and collaborate with the State to improve configuration, development and testing processes with the objective of minimizing the occurrence of these issues and improving the efficiency.

The Contractor will develop a training plan documenting how State staff will be trained on how to operate and maintain the State of Michigan Enterprise Fraud Detection Software. The plan must include a list of all formal courses provided by the Contractor to State staff along with who should attend each class. The Contractor must also provide a list of any pre-requisite classes the State staff needs to operate and maintain the System.

Deliverables

- UAT results
- Comprehensive training plan designed to meet implementation, operation, and configuration needs of the State for Phase 2 UIA
- Listing of formal training courses, recommended audience, duration and a current schedule for each course
- Description of training courses that will be taught locally
- Provide recommendations as pre-requisite skills and the level of expertise required to support and operate the State of Michigan Enterprise Fraud Detection Software

State Responsibility

- Schedule State UAT Testers for training
- Attend training
- Provide input to Contractor on data necessary to support testing
- Review test data
- Create UAT schedule and test procedures
- Conduct tests to validate results
- Document test results
- Record defects
- Document defects using Incident Reports
- Conduct Problem Review meeting
- Modify the Test Scenarios, if needed
- Create additional Test Scenarios, if needed
- Retest resolved defects and perform regression testing
- Attend status meetings

Contractor Responsibility

- Ensure that all modifications to the State of Michigan Enterprise Fraud Detection Software are thoroughly system tested prior to transferring new versions to UAT Testing
- Ensure that data is loaded to the Test Environment
- Provide customized data or interface files to the State, as needed, to complete test scenario execution
- Provide training
- Assist with the creation of the UAT Test schedule and test procedures
- Review failed test scenarios and recommend most efficient and accurate resolutions
- Participate in Problem Review meeting(s)
- Correct defects found
- Assist with coordination of regression testing as needed
- Conduct status meetings



Acceptance Criteria

- All UAT test cases pass
- Approval of comprehensive training plan designed to meet implementation, operation, and configuration needs for Phase 2 UIA
- Approval of listing of formal training courses, recommended audience, duration and a current schedule for each course
- Approval of description of training courses that will be taught locally
- Approval of recommendations as pre-requisite skills and the level of expertise required to support and operate the State of Michigan Enterprise Fraud Detection Software

1.104.7 Phase 2 UIA: Implementation

Objective

The objective of the Phase 2 UIA: Implementation is to prepare a production environment for deployment of the system.

Description

The Implementation Phase involves verification that the production environment hardware and software is production ready. The system security plan is finalized to ensure the product environment meets all security requirements for the system and data, including data at rest and data in transit. The disaster recovery procedures for the system are added to the State business continuity plan for the State.

Once the preparation is complete, a detailed cutover task list and schedule are prepared. Each step to be performed is included, along with checkpoints and rollback procedures. The production software goes live, and the system data and functionality is validated. The results of this validation will drive a “go/no go” decision from the State. If there are significant issues, the system deployment may be rolled back, per procedures.

Tasks

- 7.1 Production Cutover
- 7.2 Installation Testing
- 7.3 Post Implementation Evaluation Report (PIER)

Task 7.1: Production Cutover

The System goes live. Desk-side support is provided to end users and operations are carefully monitored.

The Contractor updates the Installation Plan (SEM-0702) which provides the list of interrelated steps and activities that must be coordinated to ensure a smooth and successful rollout. The Installation Plan is followed during Production Cutover.

A high-level checklist is prepared for general consumption within the agency to communicate the general schedule. A detailed, step-by-step checklist is prepared for the project team to follow.

Perform Software Implementation

The Contractor must provide the necessary resources to install the State of Michigan Enterprise Fraud Detection Software onto the production hardware per the Installation Plan. Any and all issues must be resolved during the installation procedures prior to cutover to the new software.

Deliverable

- Installation of the State of Michigan Enterprise Fraud Detection Software onto the production environment
- “Go/no go” Check List

State Responsibility

- Provide support during the implementation
- Attendance of Appropriate Personnel in the “go/no-go” review meeting



- Review Installation Plan
- Prepare the “go/no-go” checklist
- Make “go/no go” decision

Contractor Responsibility

- Update the Installation Plan
- Follow the Installation Plan
- Review the “go/no-go” Check List
- Installation of the State of Michigan Enterprise Fraud Detection Software onto the production environment

Acceptance Criteria

- Per section 1.501, 2.253, 2.254 & 2.255, approval of the Installation Plan
- Approval of State of Michigan Enterprise Fraud Detection Software installation

Task 7.2: Installation Testing

The Contractor must test the State of Michigan Enterprise Fraud Detection Software in the State production environment to ensure the software is installed and functioning properly. These tests should:

- Ensure the environment is properly installed and configured
- Ensure the State of Michigan Enterprise Fraud Detection Software is completely functional
- Ensure data is ported to the production environment
- Identify any defects or problems in the environment against expected results for all tests

Deliverables

- Conduct Installation Testing

State Responsibility

- Provide staff to assist the Contractor in the Installation Testing activity
- Review and approve Installation Test results

Contractor Responsibility

- Properly test the production environment to ensure it is fully installed and operating properly
- Ensure data is ported to the production environment
- Resolve any issues/problems for installation
- Provide installation test results

Acceptance Criteria

- Approval of Installation Testing results

Task 7.3: Post Implementation Evaluation Report (PIER)

The Contractor is responsible – with input from the State – for completing the Post-Implementation Evaluation Report for Phase 2 UIA.

Deliverable

- Post Implementation Evaluation Report (PIER)

State Responsibility

- Review the Post Implementation Evaluation Report
- Provide feedback to Contractor
- Approve the Post Implementation Evaluation Report

Contractor Responsibility

- Complete the Post Implementation Evaluation Report
- Correct any identified deficiencies

Acceptance Criteria

- Per section 1.501, 2.253, 2.254 & 2.255, approval of Post Implementation Evaluation Report



1.104.8: Warranty

Objective

The Contractor is required to support the system for the duration of the one (1) year warranty period, which begins after **Implementation Acceptance of the first phase completed (regardless of whether Phase 1 or Phase 2) as identified in Section 1.104** have been granted by the State. The Contractor is required to provide maintenance and support until final contract completion.

Description

For the warranty period, the Contractor warrants that the system must conform in all respects to the requirements of the system as set out in the Contract and the accepted deliverables.

If, within the warranty period, the State of Michigan Enterprise Fraud Detection Software fails to comply with this warranty, Contractor must repair defects as necessary at no cost to bring the system into compliance with the warranty.

The State is responsible for notifying the Contractor of the failure in writing, describing the correct operation, providing the Contractor with adequate documentation and evidence to reproduce the failure, and, when necessary, demonstrating the failure so that the cause of the failure may be traced and corrected. The Contractor must make such warranty repairs as expeditiously as necessary, following written notification or such longer period as may be necessary using diligence and dispatch. For the purpose of this project, "Defect" means any error in the State of Michigan Enterprise Fraud Detection Software that prevents the State of Michigan Enterprise Fraud Detection Software from performing in compliance with the required functionality.

Warranty Period

- Software Maintenance through the end of the warranty period
- One (1) year warranty

Task 8.1: Warranty

For the duration of the Contract and warranty period, the Contractor will ensure that the new system is current on service packs as well as any new versions and/or releases. The installation of new and future releases will be mutually agreed upon by State and Contractor.

The Contractor must create the Warranty Services Plan which must include:

- How the Contractor must provide State of Michigan Fraud Detection solution performance tuning, defect repair and service pack releases
- How the Contractor must provide continuity of existing operational functionalities
- How the Contractor must provide warranty services such as:
 - Service packs are installed
 - Upgrades are installed
 - Defects with core code are resolved
 - Defects resulting from configurations are resolved

Deliverables

- Warranty Services Plan
- Warranty Services

State Responsibility

- Review and approval of the Warranty Services Plan
- Report and classify all defects in the defect-tracking tool
- Approval of Release packages
- Retest all reported defects before releasing back into production
- Participation in system changes during warranty period



Contractor Responsibility

- Create Warranty Services Plan
- Provide warranty services as defined in the Warranty Service Plan
- Provide State of Michigan Enterprise Fraud Detection Software performance tuning, defect repair and service pack releases

Acceptance Criteria

- Documentation of the Warranty Services Plan
- Execution of Warranty Services Plan
- Implementation of State of Michigan Enterprise Fraud Detection Software release packages as agreed upon by the State
- State of Michigan Enterprise Fraud Detection Software is functional, in production and current on all service pack and upgrades at the end of the Warranty Period
- Per section 1.501, 2.253, 2.254 & 2.255, approval of Warranty Services Plan
- End of Warranty Period

1.104.9: Maintenance and Support

Objective

The Contractor will provide maintenance and support starting at the **end of the Contract Warranty Period defined in Section 1.104.8: Warranty.**

The Contractor must work with the State to perform a knowledge transfer on the State of Michigan Fraud Detection solution. This knowledge transfer shall include involving State personnel in ongoing configuration activities.

Description

The Contractor will provide Level 1 maintenance and support which includes items such as:

- Access to service packs
- Access to new versions of the Enterprise Fraud Detection Software
- Access to new and revised documentation
- Phone support
- Defect repair - core Enterprise Fraud Detection Software bugs repaired at no cost to State

Tasks

- 9.1 System Maintenance

Task 9.1: System Maintenance

The Contractor is required to develop a System Maintenance Plan (SEM-0301). The Contractor will include a complete description of their maintenance and support services within the Plan.

The State intends to identify individuals to participate on a full-time basis in ongoing production support activities. Staff shall have the requisite skills to participate on the team as identified by the Contractor in the Transition Plan. The Contractor must communicate concerns regarding specific areas/individuals if the Contractor feels there is an elevated level of schedule risk. The State shall pursue other methods of performing the knowledge transfer for the given area in this situation.

For the duration of the contract, the Contractor will ensure that the new system is current on service packs as well as any new versions and / or releases.

The Contractor must include support services during the maintenance and support period at sufficient levels to ensure, at a minimum, that:

- service packs are installed
- upgrades are installed
- hot fixes are installed
- defects with code are resolved



- defects resulting from configurations are resolved
- the overall system is kept in good running order

Deliverable

- System Maintenance Plan (SEM-0301)

State Responsibility

- Provide qualified State resources to assist in Maintenance and Support
- Provide qualified State resources to assist in performing upgrades
- Report and classify all defects
- Approval of Release packages
- Retest all reported defects before releasing back into production
- Review and approval of the System Maintenance Plan

Contractor Responsibility

- Develop System Maintenance Plan (SEM-0301)
- Provide services as defined in the System Maintenance Plan
- Provide State of Michigan Enterprise Fraud Detection Software performance tuning, defect repair and service pack releases

Acceptance Criteria

- Per section 1.501, 2.253, 2.254 & 2.255, approval of System Maintenance Plan (SEM-0301)

1.104.10: Contingency Fund

Objective

This section is intended to facilitate the handling of requests for new functionality and/or changes to the proposed system, as well as new services and/or changes to existing services provided via this contract.

The contingency fund may be utilized towards additional software licensing, software services or other related matters.

Description

For any changes in functionality or services, the Contractor must perform an impact analysis to determine the functional areas impacted by the change, and the associated requirements and deliverables that must be modified to incorporate the change. Once the impact analysis has been completed, the Contractor must submit a change request detailing the proposed changes to incorporate the new/changed functionality. A change request should additionally include impact to the project schedule, and the FTEs required to incorporate and to implement the change. The change request will follow the defined and approved process.

Task 10.1 Change Requests

The State has established funding for system enhancements and services from the Contractor beyond those listed in the Contract, such as additional enhancements and legislative changes. Actual funding for enhancements shall occur on a yearly basis, and there is no guarantee as to the level of funding for enhancements, if any, available to the project. Enhancement requests must go through a rigorous review process established by the State before being submitted to the Contractor for impact assessment and estimates.

A limited amount of Contractor time will be required in this review process, but only to provide a cursory review of the request. The requests considered potentially viable shall then be passed to the Contractor for impact assessment (i.e., impact on existing plans and estimates). Requests may be considered for inclusion in an existing release, for a future planned release or bundled for an entirely new release. Requests for impact assessment and estimates may be made on an individual (request-by-request) basis or on a request group basis.



The Change Management Plan must be followed for requests for any modifications to a Statement of Work, which are not part of this contract. Enhancements must not affect the schedule, service level, or cost of the other activities and tasks requested in this Contract without the express acknowledgement and consent of the State.

Deliverables

- Change Request

State Responsibility

- The State will review and either approve or deny a change request based on impact to the project schedule, resources and budget

Contractor Responsibility

- The Contractor must submit a change request detailing the proposed changes to incorporate the new/changed functionality; a change request should additionally include impact to the project schedule, and FTEs required to incorporate and implement the change; the change request will follow the defined and approved process

Acceptance Criteria

- Per section 1.501, 2.253, 2.254 & 2.255, approval of Change Request



II. Requirements

A. Technical/General System Requirements

Technical/General System requirements will identify the general framework in which the product must work, such as: system architecture, documentation, audit and backup and recovery. Contractor Comments are provided within the requirement and labeled under the header "Contractor Comments"

Technical/General Requirement	
1: Service Architecture	
1-1	The system must employ web-based architecture with an intelligent workstation client accessing a central database through software on one or more servers.
1-2	<p>The system must be an open system, supporting Service Oriented Architecture (SOA) with no dependency on the use of specific models or models of equipment operating systems, and provide horizontal and vertical scalability based on amount of data processed, quantity of users, and number of business solutions to allow the State to expand beyond UI and FAP (e.g. Medicaid, Treasury).</p> <p>Contractor Comments: The SAS solutions are inherently platform vendor independent, allowing the applications to operate and produce the same results whether used with UNIX or Windows based systems.</p> <p>Below is a link to SAS supported operating systems. http://support.sas.com/resources/sysreq/hosts/</p>
1-3	<p>The system must function with the following desktop Operating System (OS), and must be updated to function on new versions of such OS's in the future if prior versions are no longer supported and/or become obsolete.</p> <p>Windows 7</p>
1-4	<p>The system's desktop client install must function on the following standard SOM desktop hardware:</p> <p>Link to SOM Desktop Standard: http://www.michigan.gov/dmb/0,4568,7-150-56355-108231--,00.html</p> <p>Contractor Comments: SAS does not foresee this as limiting ability to comply with an on premises deployment.</p>
2: Security	
2-1	<p>The system must operate in a secure manner and comply with State Enterprise IT Security Policy and Procedures as found in the following:</p> <p>http://www.michigan.gov/documents/dmb/1310_183772_7.pdf http://www.michigan.gov/documents/dmb/1310.02_183775_7.pdf http://www.michigan.gov/documents/dmb/1325_193160_7.pdf http://www.michigan.gov/documents/dmb/1335_193161_7.pdf</p> <p>Contractor Comments: The Fraud Framework does support some capability for branding applications using the SOM brand. Since this software product is a COTS solution branding will be mutually agreed upon.</p>
2-2	<p>The system must adhere to SOM Policy 1340.00 regarding "Information Security":</p> <p>http://www.michigan.gov/documents/dmb/1340_193162_7.pdf</p> <p>Contractor Comments: The Fraud Framework does support some capability for branding applications using the SOM brand. Since this software product is a COTS solution branding will be mutually agreed upon.</p>
2-3	<p>The system must adhere to SOM Policy 1350.10 regarding "Access to Networks, Systems, Computers, Databases, and Applications":</p> <p>http://www.michigan.gov/documents/dmb/1350.10_184594_7.pdf</p>



	<p>Contractor Comments: Below are links to SAS supported security technologies and integration components.</p> <p>http://support.sas.com/documentation/cdl/en/bisecag/63082/HTML/default/viewer.htm#n0iqe26rd4ui8ln1sqq5g7cs4ghc.htm</p> <p>http://support.sas.com/documentation/cdl/en/bisecag/63082/HTML/default/viewer.htm#p0sajzx39gs312n18ud96czemphr.htm</p> <p>SAS does not foresee this as limiting SOM's ability to comply with an on premises deployment.</p>
2-4	The system must ensure that the integrity and confidentiality of data is protected by safeguards to prevent release of information without proper consent.
2-5	The system must ensure a secure sign-on through user ID and password.
3: Security Access/Control	
3-1	The system must provide security at database, workstation, and individual operator levels. The SOM DBA will apply database security and local IT will ensure workstation security.
3-2	<p>The system must provide secure access control based upon unique user login for groups and roles in addition to individual users.</p> <p>Contractor Comments: Covered by SAS metadata groups/roles. Specific details will need to be collected during detail requirement session(s). Below are links to SAS supported security technologies and integration components.</p> <p>http://support.sas.com/documentation/cdl/en/bisecag/63082/HTML/default/viewer.htm#n0iqe26rd4ui8ln1sqq5g7cs4ghc.htm</p> <p>http://support.sas.com/documentation/cdl/en/bisecag/63082/HTML/default/viewer.htm#p0sajzx39gs312n18ud96czemphr.htm</p>
3-3	The system must check each user's access privileges at login, and automatically disable or enable client functions (in real time) based upon the user's profile, including access to reports, stored processes which produce them, and client functions.
3-4	<p>The system must provide varying levels of access within the application (e.g. Administrators). Team leaders and supervisors must be able to see the status of their team's workload and progress as well as the progress of each individual team member.</p> <p>Contractor Comments: This will be delivered by as part of Standard BI Fraud Operational Reports</p>
3-5	The system must provide a means for adding new roles and removing or disabling existing roles.
4: Application Specifications	
4-1	The system must allow for the accurate and timely input, extraction and integration of State data including data cleansing, validation, structuring, standardization, and de-duplication techniques as needed. Data cleansing means processing data to resolve data quality issues.
4-2	The system must allow for processing of all State business identified in this Contract.
4-3	The system must provide a single Graphical User Interface (GUI) that is user-friendly, user-definable, configurable, and provide capabilities to State users as identified in this Contract. The GUI will be configured as mutually agreed during the detailed requirements and design sessions.
4-4	The system must be able to be installed and operate on virtual server software.
5: Reporting	
5-1	The reporting product technology must be compatible with n-Tier architecture (client-server and Web).
6: Capacity	
6-1	The system must support at least 25 concurrent users.
	Contractor Comments:



	The SAS system scales to the Hardware. This is dependent on SOM's hardware and sizing. EEC will go through the sizing exercise for the hardware.
7: System Auditing	
7-1	<p>The system must maintain an audit trail of all system usage (analysis scenarios, scoring, etc.), changes to data and metadata and any changes that affect the security of the environment including login IDs and permissions.</p> <p>Contractor Comments: Since hosted at the SOM log in ID's and modification of the ID's are the responsibility of the State.</p> <p>Application level authorization in the SAS metadata is auditable. The specifics around usage tracking will be determined during detailed requirements gathering and design session(s)</p>
7-2	The system must provide the ability for the end user to purge audit trail history.
7-3	<p>The system must ensure that all system events for software, hardware, interfaces, operating system, network, etc. are written to a system event log in a manner that facilitates debugging of all system problems.</p> <p>Contractor Comments: System event monitoring will be handled by SOM Admins.</p> <p>SAS will not limit SOM ability to meet this requirement.</p>
7-4	<p>The system must provide the ability to query, view, filter, and sort the system audit trail.</p> <p>Contractor Comments: SAS can produce logs for SAS technologies and the logs will be available for review. See comment in Section 7-1</p>
8: Error Handling	
8-1	The system must ensure that all errors are written to an error log.
8-2	The system must allow for an administrator to view, filter, sort, and search the error log.
8-3	<p>The contractor must provide a list of system error codes with explanation and provide system-generated automatic email notifications for critical errors.</p> <p>Contractor Comments: This will be part of the ETL process. List of error codes are in the link below: http://support.sas.com/documentation/cdl/en/mcrolref/61885/HTML/default/viewer.htm#a000208995.htm</p>
9: Backup and Recovery	
9-1	<p>The system must have the ability to provide a complete backup and recovery process for all database tables and system files.</p> <p>Contractor Comments: Database back up is the responsibility of the SOM DBA's.</p> <p>Furthermore the standards for backup and restoration of the SAS metadata are in the following URL: http://support.sas.com/documentation/cdl/en/bisag/64088/HTML/default/viewer.htm#a003267606.htm</p>
10: Additional	
10-1	Error Correction. Upon notice by the State of a problem, reasonable efforts must be made to correct or provide a working solution for the problem.
10-2	Material Defects. The State will be notified of any material errors or defects in the deliverables known, or made known to the contractor from any source during the Contract term that could cause the production of inaccurate, or otherwise materially incorrect, results and shall initiate actions as may be commercially necessary or proper to effect corrections of any such errors or defects.
10-3	The system must be upgradable by State information technology staff when a new version is available without the need for onsite contractor support. The contractor is responsible for correcting any product errors or problems associated with new version releases.



10-4	On-site Support: The contractor must provide on-site presence as outlined in Section 1.201 (B) of the Contract.
11: Documentation and Standards	
11-1	The contractor must provide a full set of standard product and project-specific documentation both in electronic and print format.
11-2	The contractor must provide User Manuals covering all user roles including administrators.
11-3	The contractor must provide Help-Desk for supporting users. <u>Contractor Comments:</u> The State will handle level 1 triage and any application level support will be directed by Contractor technical support to address Contractor technology issues.
11-4	The system must provide context-sensitive online help and tool-tips.
11-5	The contractor must provide a logical network diagram that describes how the infrastructure components will meet the functional requirements.
11-6	The contractor must provide conceptual and logical data-flow diagrams.
11-7	The contractor must provide a complete installation and configuration documentation library including installation and configuration notes specific to Michigan.
11-8	The contractor must provide a high-level architecture diagram, including logical and physical components.
11-9	The system documentation must describe error logging capabilities including instructions for modifying logging levels and how to access the error logs.
11-10	The system documentation must describe Disaster Recovery capabilities (including Hot and Cold standby options, licensing implications, and critical vs. non-critical functionality and data).
11-11	The system documentation must describe any batch processing requirements for the application.
11-12	The contractor must state their provisions and/or procedures for updating or enhancing any manuals provided in response to this Contract.
11-13	When product and technical manuals are revised, the contractor must notify Michigan in advance and provide an entire new set, or furnish the replacement pages electronically. All associated costs, if any, must be identified.
12: Installation	
12-1	The contractor must provide a detailed work plan (in hours) and duration (in days) of a typical installation of the base package, including all modules. Include both SOM and contractor effort.
12-2	The contractor must provide a high-level project plan outlining activity descriptions, work effort, duration and resources for a typical base-package installation.
13: Training	
13-1	Operational Training: The system must require minimal training and include operational training as part of knowledge transfer sessions.
14: Storage	
14-1	The system must implement data compression techniques that will minimize the agency's need for additional storage.
14-2	The system must implement data compression techniques without compromising functionality or performance. <u>Contractor Comments:</u> The Contractor will be considerate of disk space and ensure the user experience is minimally impacted.



B. Functional Requirements

Functional requirements identify what the fraud detection system must do to enable performance of work tasks and any applicable service levels.

Please note the following definitions of terms concerning the first column in the header row:

- **UI:** This requirement is only applicable to the Unemployment Insurance Agency (UIA)
- **PA:** This requirement is only applicable to Public Assistance
- **Both:** This requirement is applicable to both UI and PA.

UI PA Both	Functional Requirement	
1. Fraud Functions: General		
Both	1-1	<p>The system must identify and report attempted fraud, waste and abuse by individuals and groups using predicative analytics, employing business rules, anomaly detection and social network analysis based on information derived from the DTMB Data Warehouse.</p> <p><u>Contractor Comments:</u> SOM specific rules will be implemented. Predictive models and networks will be configured using the SOM's data.</p>
Both	1-2	<p>The system must analyze and identify possible characteristics of Unemployment Insurance (UI) and Public Assistance (PA) programs fraud, waste and abuse perpetrated by all entities including employers, providers and individuals using predictive analytics, employing business rules, anomaly detection and social network analysis.</p> <p><u>Contractor Comments:</u> SOM specific rules will be implemented. Predictive models and networks will be configured using the SOM's data.</p>
Both	1-3	<p>The system must analyze and identify possible characteristics of UI and PA fraud, waste and abuse perpetrated by State staff using predictive analytics, employing business rules, anomaly detection and social network analysis.</p> <p><u>Contractor Comments:</u> Project scope currently included UI and PA the SAS Fraud Framework can be extended to support future Fraud/Waste & Abuse initiatives.</p>
UI	1-4	<p>The system must identify the potential individual, organized and collusive fraud, waste and abuse using predicative analytics, employing business rules, anomaly detection and social network analysis in Unemployment Insurance (UI).</p> <p><u>Contractor Comments:</u> SOM specific rules will be implemented. Predictive models and networks will be configured using the SOM's data.</p>
UI	1-5	<p>The system must analyze and identify possible characteristics of UI fraud, waste and abuse perpetrated by claimants using predictive analytics, employing business rules, anomaly detection and social network analysis.</p> <p><u>Contractor Comments:</u> SOM specific rules will be implemented. Predictive models and networks will be configured using the SOM's data.</p>
PA	1-6	<p>The system must analyze and identify the potential individual, organized and collusive fraud, waste and abuse using predictive analytics, employing business rules, anomaly detection and social network analysis in PA programs.</p> <p><u>Contractor Comments:</u> SOM specific rules will be implemented. Predictive models and networks will be configured using the SOM's data.</p>



PA	1-7	<p>The system must analyze and identify possible characteristics of PA fraud, waste and abuse perpetrated by PA recipients using predictive analytics, employing business rules, anomaly detection and social network analysis.</p> <p>Contractor Comments: SOM specific rules will be implemented. Predictive models and networks will be configured using the SOM's data.</p>
PA	1-8	<p>The system must analyze and identify possible characteristics of PA fraud, waste and abuse by PA providers/retailers using predictive analytics, employing business rules, anomaly detection and social network analysis.</p> <p>Contractor Comments: SOM specific rules will be implemented. Predictive models and networks will be configured using the SOM's data.</p>
Fraud Functions: UI Claimants and PA Recipients		
Both	2-1	<p>The system must compare and verify information from a UI claimant and PA recipient and flag discrepancies.</p> <p>Contractor Comments: Entity resolution methods will be tailored to SOM's data.</p>
Both	2-2	<p>The system must use multiple sources in the DTMB Data Warehouse for UI claimant and PA recipient data to verify claim authenticity and flag discrepancies.</p> <p>Contractor Comments: Entity resolution methods will be tailored to SOM's data.</p>
Both	2-3	<p>The system must be flexible enough to allow for ad hoc and analysis and reporting that can be performed on an ad hoc /on demand basis.</p>
Both	2-4	<p>Data Analysis: The system must use data analytics to analyze accumulated data from the DTMB Data Warehouse to verify information from a UI claimant and PA recipient and utilize data analytics by employing business rules, anomaly detection, predictive modeling and social network analysis to detect potential patterns of fraud, waste, and abuse.</p> <p>Contractor Comments: SOM specific rules will be implemented. Predictive models and networks will be configured using the SOM's data.</p>
Both	2-5	<p>User ID pattern: The system must identify user IDS that are the same or have slight variations, e.g. ABC123, ABC1234 by using data quality, data matching and entity resolution capabilities that allow for the identification of entities with slight variations, including individuals, companies and addresses.</p> <p>Contractor Comments: Entity resolution methods will be tailored to SOM's data.</p>
Both	2-6	<p>State ID pattern: The system must analyze UI claimants and PA recipients according to their State ID and/or State Driver License for valid patterns in data fields including Social Security Number (SSN) and phone number.</p>
Both	2-7	<p>Social Security Act (SSA) Disability and UI Benefit Payments: The system must analyze UI claimants and PA benefit recipients against the SSA disability database to identify potential fraudulent UI claims and PA applications/redeterminations and flag discrepancies.</p> <p>Contractor Comments: Entity resolution methods will be tailored to SOM's data.</p>
Both	2-8	<p>Birthday pattern: The system must analyze UI claimants and PA recipients according to their birth date and detect patterns of claims using the same birthday over a period of time.</p>
Both	2-9	<p>Address patterns: The system must analyze UI claimant and PA recipient address discrepancies detected from external data sources and flag discrepancies and slightly different addresses.</p>
Both	2-10	<p>Education Level: The system must analyze and segment UI claimants and recipients according to their citizenship status and education level.</p>



Both	2-11	Repeated IP address: The system must identify multiple UI claims and PA applications/redeterminations originating within a user-defined time period from the same IP address (e.g. UI claims are filed within a week; PA redeterminations can be within 30 days).
Both	2-12	Prior detection: The system must identify UI claimants and PA recipients with a prior history of fraud detection and score the associated risk of such activity.
Both	2-13	Incarceration: The system must verify information from a UI claimant and PA recipient against incarceration records/data and flag potential cross-matches.
Both	2-14	Social network pattern: The system must utilize Web services to detect patterns in social networks to identify fraud in public assistance and unemployment insurance. Web Services is defined as information secured from resources via internet protocols including machine-to-machine interfaces, such as SOAP sources and RSS feeds when possible and traditional online web pages, from which data would be programmatically scraped and harvested.
Both	2-15	Employer has not reported: The system must identify UI claims and PA applications/redeterminations where UI claimant and PA recipient indicated self-reported wages for newly liable employers and multiple employers in a base period and flag discrepancies.
Both	2-16	<p>Validate wages: The system must validate UI claimant and PA recipient wages against 1099s submitted to the IRS within individual tax returns and flag discrepancies.</p> <p>Contractor Comments: Assumption: deployed on premises</p> <p>The SAS system/technology can adhere to the IRS 1075 Safeguards.</p>
UI	2-17	The system must provide the ability for end users to restrict analysis scenario results to Initial, Additional, and Reopened Claims filed within the user-specified range of dates; and to claims with a Weekly Benefit Amount (WBA) equal to or greater than the user-specified amount.
UI	2-18	Close-to-claimant address: The system must analyze related UI claims based on the purified street address to analyze claimant addresses and distance between them and other geographic points.
UI	2-19	<p>Multiple claims to the same address: The system must analyze UI claimants according to the address of record on their unemployment insurance claim based on a requested date range. Matching of addresses should account for variations in spacing, spelling, inconsistent abbreviations, and other techniques which may enhance the efficiency of the analysis scenario.</p> <p>Contractor Comments: Entity resolution methods will be tailored to SOM's data.</p>
UI	2-20	Repeated phone number for initial claims: The system must identify multiple UI claims using the same contact telephone number over a specified time range for user selected claim types.
UI	2-21	Same originating telephone number for continued claims: The system must identify multiple UI claims within a given certification week originating from the same telephone number for a specified time range for user selected claim types.
UI	2-22	Separating employer not in base period: The system must identify UI claims whose separating employer is not a base period employer for a requested time period.
UI	2-23	Self-reported wages on same employer: The system must identify UI claims where multiple claimants indicated self-reported wages on the same employer.
UI	2-24	High number of base period employees: The system must identify UI claims with a high number of base period employers identified for a particular claimant.
PA	2-25	The system must provide the ability for end users to restrict analysis scenario results to PA applications/redeterminations filed within the user-specified range of dates; and to applications /redeterminations with a supplemental benefit amount equal to or greater than the user-specified amount.
PA	2-26	<p>Close-to-recipient address: The system must analyze related PA applications/redeterminations based on the purified street address to analyze recipient addresses and distance between them and other geographic points.</p> <p>Contractor Comments: Entity resolution methods will be tailored to SOM's data.</p>
PA	2-27	Multiple applications / redeterminations to the same address: The system must analyze PA recipients according to the address of record on their PA application /redetermination case based on a requested date range. Matching of addresses should account for variations in spacing,



		<p>spelling, inconsistent abbreviations, and other techniques which may enhance the efficiency of the analysis scenario.</p> <p>Contractor Comments: Entity resolution methods will be tailored to SOM's data.</p>
PA	2-28	Repeated phone number for PA application / redetermination: The system must identify multiple PA applications and/or redeterminations using the same contact telephone number for a specified time range.
PA	2-29	High volume of recipient redemptions: The system must analyze unusually high volumes for redemptions by a recipient.
PA	2-30	The system must provide a user-definable parameter to set the value for unusually high volumes for redemptions by a recipient.
PA	2-31	Even dollar transactions: The system must detect patterns of even dollar transactions for a recipient.
PA	2-32	Identical transaction amounts: The system must detect patterns for identical transaction amounts for a recipient.
PA	2-33	Transaction type: The system must analyze the transaction type as swiped versus keyed for a recipient.
PA	2-34	Off-hours redemptions: The system must detect and analyze off-hour transactions for recipients where 'off-hours' is a configurable time frame.
PA	2-35	Time period between transactions pattern: The system must detect and analyze recipient transactions, which occur within a user-defined time period.
PA	2-36	The system must provide a user-definable parameter to set the time period between transactions by a recipient.
PA	2-37	Exceeded threshold amount transactions: The system must analyze transaction amounts, which have exceeded a user-defined threshold amount for redemptions by a recipient.
PA	2-38	The system must provide user-defined parameters to set the threshold amount for the Exceeded threshold amount by recipients.
PA	2-39	<p>Public assistant recipients and UI Claimants: The system must analyze PA recipients against UI claimants to identify potential fraudulent PA applications/ redeterminations, flag potential cross-matches and score the associated risk of such cross-matches.</p> <p>Contractor Comments: Entity resolution methods will be tailored to SOM's data.</p>
Fraud Functions: Employers		
Both	3-1	The system must compare and verify information from an employer and flag potential discrepancies.
Both	3-2	Fictitious employer: The system must analyze non-labile employers with audit variations of employer names, employer addresses, type of work performed, dates of work performed, employer response to UI notice, phone numbers, how the UI claim or PA application/redetermination was filed (Internet or phone), etc., to identify fictitious employers.
Both	3-3	Abandoned building pattern: The system must analyze UI claims, PA applications/ determinations and employer accounts to detect employers who have registered an address, which is designated as abandoned.
Both	3-4	Terminated building pattern: The system must analyze UI claims, PA applications/ redeterminations and employer accounts to detect employers who have registered an address for a building, which is no longer valid.
Both	3-5	Prior detection: The system must identify employers with a prior history of fraud detection and score the associated risk of such activity.
UI	3-6	<p>The system must use multiple sources of cross match UI claimant, employer and government-supplied related data to verify claim authenticity and flag potential discrepancies in cross-matched data.</p> <p>Contractor Comments: Entity resolution methods will be tailored to SOM's data.</p>
UI	3-7	Data analysis: The system must analyze accumulated data to detect employer fraud.



UI	3-8	High percentage of claims: The system must identify employers that have a high percentage of UI claims filed in relation to the total number of employees.
UI	3-9	The system must identify discrepancies between wage records reported by employers against the wages reported for UI benefit claims.
UI	3-10	Business Telephone Listing: The system must detect employers who are listed in the White Pages telephone directory and do not have employer accounts registered with UIA providing a cross-match of numbers and unregistered employers. <u>Contractor Comments:</u> The SOM will provide or make available the White Pages Phone Number data.
UI	3-11	SUTA dumping: The system must identify potential fraud schemes whereby employers create a "new business" while maintaining the same employees for the purpose of lower taxes.
UI	3-12	SUTA SSN pattern: The system must identify claimant social security numbers moving/transferred between multiple employer account numbers.
UI	3-13	Employer filing as claimant: The system must cross match the Social Security Numbers of company officers provided in employer accounts and UI Claimant Social Security Numbers to identify company officers who are receiving UI Benefits.
UI	3-14	Wage pattern: The system must analyze W2s reported for the same employer FEIN which are greater than the amount the employer reported on the Quarterly Wage Report for individual state and federal income tax returns.
UI	3-15	Tax pattern – existing employer: The system must analyze total wages reported with the same employer FEIN which are greater than the amount the employer reported on the Quarterly Tax Report for employer state and federal income tax returns.
UI	3-16	Tax pattern – transferred employer: The system must analyze total wages reported for transferred employers/business with the same address which are greater than the amount the predecessor employer reported on the Quarterly Tax Report for employer state and federal income tax returns.
UI	3-17	Tax pattern – new employer: The system must analyze total wages reported for new employers /business with the same address which are greater than the amount the previous employer with the same address reported on the Quarterly Tax Report for employer state and federal income tax returns.
UI	3-18	Recently liable employers in the base period: The system must identify recently liable employers in the base period.
UI	3-19	Repeated IP address for registration: The system must identify multiple employer registrations across entities within a given a specified time period originating from the same IP address.
UI	3-20	High number of liable employers in the first quarterly report: The system must identify unusually 'high' employee counts for the employer's first submitted Wage Report.
UI	3-21	1099 pattern: The system must detect pattern changes in the volume of 1099s issued by an employer.
UI	3-22	Paper of Incorporation Filed: The system must analyze and cross-match the Bureau of Commercial Services (BCS) records to UI records to determine if the employer has an account with the UIA in order to detect unregistered employers.
UI	3-23	Participant in Workforce Investment Act (WIA) Program: The system must detect and cross-match employers who have applied for WIA services or participated in WIA programs (train employees, received tax breaks for employees hired from UI rolls and other programs) but have not filed an application to register with UIA in order to detect unregistered employers.
UI	3-24	Worker Compensation Claim Filed Against: The system must detect and cross-match employers who have had worker's compensation claims filed against them and do not have employer accounts registered with UIA in order to detect unregistered employers.
UI	3-25	Request to Import Foreign Labor Filed: The system must detect and cross-match employers who are importing foreign labor and do not have employer accounts registered with UIA in order to detect unregistered employers. <u>Contractor Comments:</u> The SOM will make available the appropriate data to support this requirement.
PA	3-26	Business Telephone Verification: The system must analyze and cross-match business telephone numbers provided by employers against the UIA employer accounts in order to detect unregistered employers.



Fraud Functions: Internal Staff		
Both	4-1	<p>The system must identify internal fraud by an employee of unemployment insurance and public assistance agencies.</p> <p>Contractor Comments: Assumption: Internal fraud as it applies to UI claimant or Program Assistance beneficiaries or UI employers are SOM employee</p>
Both	4-2	<p>Data analysis: The system must use data analytics to analyze accumulated data to detect internal fraud committed by state employees.</p> <p>Contractor Comments: Assumption: Internal fraud as it applies to UI claimant or Program Assistance beneficiaries or UI employers are SOM employees.</p>
Both	4-3	<p>IP Addresses: The system must analyze across entities and time the source of the IP Address to identify continued UI claims and ongoing PA benefits originating from a state agency in order to identify claims and benefits originating from the same IP addresses.</p>
Both	4-4	<p>Employee address cross match: The system must cross match UI Claims and PA applications/ redeterminations against the employee addresses or similar addresses to identify employees who claim UI benefits, PA benefits and model payments while still employed by the State.</p>
UI	4-5	<p>Employee filing as claimant: The system must cross match the UI claims against the State payroll records to identify employees who claim UI benefits while still employed by the State.</p>
UI	4-6	<p>Telephone number source: The system must analyze and cross-match the source of the telephone number to identify continued claims originating from a State agency desk and flag potential discrepancies.</p>
UI	4-7	<p>Repeated employee involvement on UI claims certifications: The system must analyze unusually high volumes of certifications by a particular employee and flag groups or individuals that are anomalous or outliers.</p>
UI	4-8	<p>Staff data entry of wages: The system must analyze wages which are entered by an employee which are unverified against employer reported wages.</p>
UI	4-9	<p>Staff involvement for high number of claims: The system must identify repeated involvement by a particular agency employee on employer accounts with a high number of claims entry activity and flag groups or individuals that are anomalous or outliers.</p>
PA	4-10	<p>Employee filing as recipient: The system must cross match PA applications/ redeterminations against the State payroll records to identify employees who claim PA benefits and model payments while still employed by the state.</p>
PA	4-11	<p>Repeated employee involvement on PA applications: The system must analyze unusually high volumes of opening and/or processing changes to PA applications and ongoing cases by a particular employee relative to the office average and flag groups or individuals that are anomalous or outliers.</p>
PA	4-12	<p>Validate internal staff wages: The system must validate internal staff wages that are greater than or equal to a user defined threshold.</p>
PA	4-13	<p>Validate 1099 wages: The system must validate and cross-match state employee wages against 1099s submitted to the IRS within individual tax returns in order to flag State employees that have discrepancies.</p> <p>Contractor Comments: Assumption: This will be used in the context of supporting UI and PA fraud.</p>
Fraud Functions: Public Assistance Provider/Retailer		
PA	5-1	<p>The system must compare and verify information from a public assistance provider/retailer and flag potential discrepancies.</p> <p>Contractor Comments: SOM will provide the necessary data and make it readily available to support the project. The final set of data sources will be mutually agreed to during detailed requirements gathering.</p>
PA	5-2	<p>High volume of provider/retailer redemptions: The system must analyze unusually high volumes for redemptions by a provider/ retailer and be compared across groups or individuals where those that</p>



		are anomalous or are outliers are flagged.
PA	5-3	The system must provide a user-definable parameter to set the value for unusually high volumes for redemptions by a provider/retailer.
PA	5-4	Multiple redemptions for a single recipient: The system must analyze multiple redemptions for a single claimant within a configurable time frame.
PA	5-5	Even dollar transactions: The system must detect patterns of even dollar transactions for a provider/retailer.
PA	5-6	Identical transaction amounts: The system must detect patterns for identical transaction amounts for a provider/retailer.
PA	5-7	Transaction type: The system must analyze the transaction type as swiped versus keyed.
PA	5-8	Off-hours redemptions: The system must detect and analyze off-hour transactions for providers/retailers where 'off-hours' is a configurable time frame.
PA	5-9	Time period between transactions pattern: The system must detect and analyze provider/retailer transactions, which occur within a user-defined time period.
PA	5-10	The system must provide a user-definable parameter to set the time period between transactions by a provider/retailer.
PA	5-11	Exceeded threshold amount transactions: The system must analyze transaction amounts which have exceeded a user-defined threshold amount for redemptions by a provider /retailer.
PA	5-12	The system must provide user-defined parameters to set the threshold amount for the Exceeded threshold amount by a provider/retailer.
PA	5-13	Data Analysis: The system must analyze accumulated data to detect provider/retailer fraud.
PA	5-14	Prior detection: The system must identify provider/retailers with a prior history of fraud detection and score the associated risk of such activity.
General System Functionality		
Both	6-1	Pattern Analysis: The system must use data analytics to detect patterns from disparate data sources in the DTMB Data Warehouse that could point to fraudulent activity.
Both	6-2	The system must identify known techniques for identity theft and organized fraud and provide a library of program-specific detection methods for detecting opportunistic and organized fraud.
Both	6-3	The system must provide pre-configured data analytics patterns which have been proven to identify theft and organized fraud.
Both	6-4	Data Navigation: The system must provide the ability for the end user to navigate the result set included in a given audit and drill down into results flagged by the detection processes.
Both	6-5	The system must provide the drill down techniques that allow information to be filtered and sorted in varying levels of detail by the end user.
Both	6-6	Data Filtering: The system must provide the ability for the end user to select and configure the level of data filtering to decrease or increase the result set included in a given audit.
Both	6-7	Technical Knowledge Requirements: The system must provide the ability for end users to configure and execute basic analysis scenarios with limited knowledge of query languages (e.g. SQL).
Both	6-8	The system must provide the ability for end users to configure and execute analysis scenarios without assistance from the Information Technology department.
Both	6-9	The system must provide the ability to configure and execute basic analysis scenarios requiring the end user to have limited knowledge of the underlying data sources and structures.
Both	6-10	The system must be deployable with only minimal assistance and support of the Information Technology department.
Both	6-11	Create analysis scenarios: The system must provide the ability for end users to create ad hoc and scheduled analysis scenarios.
Both	6-12	Saving analysis scenarios: The system must provide the ability for end users to save ad hoc analysis scenarios for future reuse and deployment.
Both	6-13	Modify analysis scenarios: The system must provide the ability for end users to modify ad hoc analysis scenarios and re-save for future reuse and deployment.
Both	6-14	Saving results: The system must provide the ability for the end user to save the result set of an audit for future reference.
Both	6-15	The system must provide the ability for the end user to save the result set of an audit in common output formats (e.g. Word, Excel, flat file).
Both	6-16	The system must provide the ability for the end user to export the result set of an audit in common output formats.



Both	6-17	Modify result set: The system must provide the ability for the end user to modify the analysis scenario result set based on a refresh of existing analysis scenarios as they are developed.
Both	6-18	Analysis scenario execution: The system must provide the ability for the end user to execute both ad hoc and saved analysis scenarios.
Both	6-19	The system must provide the ability for the end user to execute and refresh result sets of an analysis scenario immediately.
Both	6-20	The system must provide the ability for the end user to schedule the execution of analysis scenarios as a batch process.
Both	6-21	The system must provide the ability for the end user to modify the parameters of an existing analysis scenario.
Both	6-22	The system must provide predefined analysis scenario parameters. (E.g. previous month, previous quarter, etc.) Pre-defined parameters must be able to be used as-is or modified by end users.
Both	6-23	Scoring framework: The system must provide the ability to assign a probability/weighting to the patterns that make up a potential fraud case to aid in prioritizing cases as well as reducing false positives.
Both	6-24	The system must provide the ability to assign a probability/ weighting based on the likelihood of fraud applying user definable criteria (I.e. length of time a person has had an overpayment).
Both	6-25	The system must provide the ability for end users to define and configure the criteria used for probability/ weighting of the potential fraud characteristics.
Both	6-26	The system must aggregate scores of detected patterns when creating a fraud detection work item for a UI claimant, PA recipient, internal staff, employer and provider/retailer.
Both	6-27	The system must provide the ability for end users to modify the scoring of the analysis scenario.
Both	6-28	The system must provide the ability for designated users to use logic to adjust the scoring of a generated result set.
Both	6-29	The system must provide the ability for end users to score individual cases that could result in an overpayment.
Both	6-30	The system must provide the ability for end users to score individual cases for possible identity theft.
Both	6-31	The system must provide the ability for end users to score individual cases for possible internal staff fraud.
Both	6-32	The system must combine and adjust the score of an existing work item based on the weight of new and existing patterns detected for UI claimants, PA recipients, internal staff, employers, and providers/ retailers.
Both	6-33	The system must provide the ability for end users to designate Opt-in and Opt-out lists for rules scoring.
Both	6-34	Reporting: The system must provide a series of standard reports and the capability to configure user defined reports designed for general business users who want to view, author and share reports on the web.
Both	6-35	The system must provide dashboards and reports for different groups and user roles and/or allow report specification and creation for each agency during the system implementation phase.
Both	6-36	For authorized users and groups, the system must provide the ability for end users to create, customize and modify reports and dashboards that are deployed.
Both	6-37	The system must provide Key Performance Indicators for management staff that the State specifies, including operational metrics.
Both	6-38	The system must provide the ability for end users to create new reports and dashboards.
Both	6-39	The system must provide the ability for end users to create new reports and dashboards by modifying existing reports and dashboards.
Both	6-40	The system must provide the ability for the end user to review and enter data on the outcome of a case to improve the efficiency of future analysis scenario results, improve fraud detection and reduce false positives.
Both	6-41	Performance: The system must execute ad hoc analysis scenarios in seconds or minutes, rather than hours.
Both	6-42	The system must execute scheduled analysis scenarios as a batch process which is assumed to take longer to generate than ad hoc analysis scenarios.
Both	6-43	Data Sources: The system must utilize data from the DTMB Data Warehouse which contains data from multiple agencies.



Both	6-44	The system must use data analytics to detect patterns on data in the DTMB Data Warehouse (i.e. not against production data systems) that might reveal an organized attempt to defraud the state UI and PA systems.
Both	6-45	The system must interface analysis scenario results with agency systems used for fraud investigation based on the priority/scoring of the potential fraud case (e.g. high, medium or low risk) using configurable prioritization parameters.
Both	6-46	The system must provide users the ability to update the analysis scenario results based on the outcome of a fraud investigation to account for past/prior known outcomes for specific entities so that the results can be applied the next time the alert generation process is executed.
UI	6-47	The system must provide the ability for end users to score individual cases for possible underpayment of taxes by employers.
UI	6-48	The system must interface with the FACTS system for High Risk UI cases.
UI	6-49	The system must interface with the CAMs system for Medium and Low Risk UI cases.
UI	6-50	The system must interface with the MiDAS workflow functionality to assign potential UI fraud cases to the correct queue based on priority and scoring.
UI	6-51	The system must interface with MiDAS workflow functionality to update the analysis scenario results based on the outcome of a UI fraud investigation.
PA	6-52	The system must interface with the FEE system for recipient PA fraud cases.
PA	6-53	<p>The system must utilize web services to integrate with LexisNexis to verify assets.</p> <p>Contractor Comments: Examples of integration options are included in the following url: http://www.sas.com/technologies/bi/appdev/inttech/ The Contractor suggests hosting/calling a web service or message queue integration.</p>

**1.200 Roles and Responsibilities****1.201 CONTRACTOR STAFF, ROLES, AND RESPONSIBILITIES****A. Contractor Staff**

The Contractor will provide a Project Manager who will be considered **Key Personnel** to interact with the designated personnel from the State to insure a smooth transition to the new system. The project manager will coordinate all of the activities of the Contractor personnel assigned to the project and create all reports required by State. The Contractor's project manager responsibilities include, at a minimum:

1. Manage all defined Contractor responsibilities in this Scope of Services.
2. Manage Contractor's Subcontractors, if any
3. Develop the project plan and schedule, and update as needed
4. Serve as the point person for all project issues
5. Coordinate and oversee the day-to-day project activities of the project team
6. Assess and report project feedback and status
7. Escalate project issues, project risks, and other concerns
8. Review all project deliverables and provide feedback
9. Proactively propose/suggest options and alternatives for consideration
10. Utilize change control procedures
11. Prepare project documents and materials
12. Manage and report on the project's budget

The Contractor's Assigned Project Manager is listed below:

Name: Andrew Phillips

The requirements for this position are as follows:

- Experience in successfully managing the implementation of the Fraud Detection COTS product to be installed.
- Experience in successfully implementing the Fraud Detection COTS product with data from both a legacy mainframe environment and relational database management systems (RDBMS).
- Minimum 5 years recent experience managing IT projects in a government environment. History of managing a project in a multi-vendor environment.
- Minimum 5 years experience creating and managing comprehensive project plans in Microsoft Project utilizing project management methodologies and tools.
- Minimum 5 years of experience performing scope management for projects including a disciplined change control process.
- Minimum 5 years experience performing issues management across multiple departments.
- Minimum 5 years experience creating and executing implementation plans.
- Minimum 5 years experience in verbal and written communication with clients and technical staff in English. Excellent verbal and written communication skills required.
- Possession of a Bachelor's degree preferably in Information Technology, Engineering or Business or equivalent experience. Current Project Management Professional (PMP) certification preferred.

In addition to the Project Manager, the Contractor will provide sufficient qualified staffing to satisfy the deliverables of this Statement of Work.

The Contractor will provide, and update when changed, an organizational chart indicating lines of authority for personnel involved in performance of this Contract and relationships of this staff to other programs or functions of the firm. This chart must also show lines of authority to the next senior level of management and indicate who within the firm will have prime responsibility and final authority for the work.

B. On Site Work Requirements

No Michigan specific work will be performed offshore.

**1. Location of Work**

The Contractor will perform work at their facilities as well as State facilities as mutually agreed. The State will allow the Contractor to access project resources and State network via Virtual Private Network (VPN) or other agreed upon mode of access, subject to the State security policy. The Contractor will ensure appropriate onsite presence represented during critical deliverables and milestones. The Contractor will conduct remote work to leverage Contractor's full set of skills, roles and resources.

At minimum the Contractor shall have on-site presence for the following activities:

- Monthly Performance Review Meetings (Section 1.301)
- Kick-Off Meeting and Initial Requirements Gathering (Section 1.1.3)
- Initial Design Review (2.2 Functional Design; 5.2 Functional Design)
- Design Review (2.2 Functional Design; 5.2 Functional Design)
- User Acceptance Test Kickoff (1.2.1 Environment Installation Testing; 3.7 User Acceptance Testing; 6.7 User Acceptance Testing)
- Cutover to the New Software (4.1 Production Cutover, 7.1 Production Cutover)

2. Hours of Operation:

- a. Normal State working hours are 8:00 a.m. to 5:00 p.m. EST, Monday through Friday, with work performed as necessary after those hours to meet project deadlines. No overtime will be authorized or paid.
- b. The State is not obligated to provide State management of assigned work outside of normal State working hours. The State reserves the right to modify the work hours in the best interest of the project.
- c. Contractor shall observe the same standard holidays as State employees. The State does not compensate for holiday pay.

3. Travel:

- a. No travel or expenses will be reimbursed. This includes travel costs related to training provided to the State by Contractor.
- b. Travel time will not be reimbursed.

4. Additional Security and Background Check Requirements:

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

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

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

1.202 STATE STAFF, ROLES, AND RESPONSIBILITIES

The State project team will consist of Executive Subject Matter Experts (SME's), project support, and a DTMB and Agency project manager:

Executive Subject Matter Experts

The Executive Subject Matter Experts representing the business units involved will provide the vision for the business design and how the application shall provide for that vision. They shall be available on an as needed basis. The Executive SME's will be empowered to:

1. Resolve project issues in a timely manner
2. Review project plan, status, and issues
3. Resolve deviations from project plan
4. Provide acceptance sign-off
5. Utilize change control procedures
6. Ensure timely availability of State resources



7. Make key implementation decisions, as identified by the Contractor's project manager, within 48-hours of their expected decision date.

The specific Executive Subject Matter experts will be determined during the Initiation and Planning stage.

State Project Manager- (DTMB and Agency)

DTMB will provide a Project Manager who will be responsible for the State's infrastructure and coordinate with the Contractor in determining the system configuration.

The State's Project Managers will provide the following services, including but not limited to:

1. Provide State facilities, as needed
2. Coordinate the State resources necessary for the project
3. Facilitate coordination between various external Contractor s
4. Facilitate communication between different State departments/divisions
5. Provide final acceptance and sign-off of deliverable/milestone
6. Review and sign-off of invoices
7. Resolve project issues
8. Escalate outstanding/high priority issues
9. Utilize change control procedures
10. Conduct regular and ongoing review of the project to confirm that it meets original objectives and requirements
11. Document and archive all important project decisions
12. Arrange, schedule and facilitate State staff attendance at all project meetings.

Name	Agency/Division	Title
Debra J. Patterson	DTMB - UIA	Project Manager
Clayton F. Tierney	UIA	Project Manager
Tess Layman	DTMB - DHS	Project Manager
Richard Staten	UIA – Project Control Office	Project Manager

DTMB shall provide a Contract Administrator whose duties shall include, but not be limited to, supporting the management of the Contract.

Name	Agency/Division	Title
Steve Motz	DTMB	Contract Administrator

1.203 OTHER ROLES AND RESPONSIBILITIES

The State intends to support the system on its own at the completion of this contract. The Contractor must work with the State to transition support for the system to State of Michigan technical (DTMB) staff. This must include involving State personnel in a variety of areas such as – ongoing production support, data conversion, requirements definition, and user acceptance testing. The Contractor must also work and coordinate with other organizations such as the State of Michigan Data Center Staff, Office of Enterprise Security, Enterprise Architecture, and Enterprise Program Management Office.

Project Control Office (PCO)

The State has retained an independent Contractor to perform Project Control Office (PCO) responsibilities during the Project's lifecycle. The major role of the PCO is to manage and control all aspects of UIA projects. The PCO is in place to ensure the overall goals and objectives of the project are met, which must entail periodic reviews of the overall strategy with the Contractor and the State.

The PCO will assign a project manager to this project that will have accountability for administering procedural controls, reviewing content and quality of deliverables, and ensuring progress of all activities in their respective areas of responsibility and expertise. This will also include strong adherence to the State Unified Information Technology Environment (SUITE) and the associated Project Management Methodology (PMM) and Systems Engineering Methodology (SEM).

**Independent Verification and Validation (IV&V)**

The full-time, onsite IV&V Project Manager provides an objective assessment of software products and processes throughout the project lifecycle. This objective assessment is to ensure requirements (such as system and software) are complete, accurate, consistent, and testable. The IV&V Project Manager also provides management insight into processes and risks, objective views of compliance or non-compliance with program performance, schedule, and budget requirements.

Represented State Employees

The Contractor should be aware that some UIA Staff are members of one of three (3) union organizations that operate within DTMB and/or LARA/UIA. These Employees have defined roles, responsibilities, skills, experience, and work hours.

1.300 Project Plan

Project Planning covers those activities that require ongoing administrative oversight throughout all the Project's implementation processes, from initiation to completion of the project. Planning also includes a number of plan documents that guide and govern the project from requirements validation and refinement through deployment, as well as for preparing for the eventual assumption of responsibilities by the State.

1.301 PROJECT PLAN MANAGEMENT

Project Schedule – See Article 1, Section 1.2.1

Kick-Off Meetings

See Article 1, Section 1.1.3 of Contract.

As part of the Kick-Off meeting the Contractor will be required to attend an orientation meeting to discuss the content and procedures of the Contract. The meeting will be held at a date and time mutually acceptable to the State and the Contractor and will be held in person or via teleconference. The State shall bear no cost for the time and travel of the Contractor for attendance at the meeting.

Performance Review Meetings

The State will require the Contractor to attend monthly meetings, at a minimum, to review the Contractor's performance under the Contract. The meetings will be held in Detroit or Lansing, Michigan, or by teleconference, as mutually agreed by the State and the Contractor. The State shall bear no cost for the time and travel of the Contractor for attendance at the meeting.

Project Control

The Contractor will carry out this project under the direction and control of DTMB and UIA Project Managers, with strong support and advice from the Project Control Office (PCO). Additional management will be added as needed through the Change Control Process.

1.302 REPORTS

At a minimum, the Contractor must provide the following identified reports:

- Weekly Project Status Reports must be provided to the State Project Managers, the Executives, Sponsors, and other key project personnel as identified by the State.
- Monthly Project Plan updates must be provided to the State Project Managers, the Executives, Sponsors, and other key project personnel as identified by the State.
- Monthly Performance Reports must be provided to the State Project Managers, the Executives, Sponsors, and other key project personnel as identified by the State.

The Contractor must use the State-defined templates, or other forms as mutually agreed upon for the following reports. Once both parties have agreed to the format of the report, it shall become the standard to follow for the duration of the contract.

1.400 Project Management**1.401 ISSUE MANAGEMENT**

See 1.104.1, Task 1.1.5 Create/Update Issue & Risk Report for issue management requirements



1.402 RISK MANAGEMENT

See 1.104.1, Task 1.1.5 Create/Update Issue & Risk Report for risk management requirements

1.403 CHANGE MANAGEMENT

Change management is defined as the process to communicate, assess, monitor, and control all changes to project scope and the contract. The State employs a change management process as defined within the SUITE Project Management Methodology.

Whenever an adjustment is requested for any portion of the SOW, approved deliverables, previously approved changes, project baseline schedule and/or project cost, a formal change request form must be completed and tracked through closure. The purpose of the Change Management Process is to document and describe:

- The change management approach
- Triggers/Sources of change requests
- Categories and priorities for change requests
- How changes will be processed and tracked
- Roles and responsibilities related to change management activities
- Documentation required for each change request
- Tools needed to support the Change Management Process

The State must ensure all changes that occur within the project are promptly identified, coordinated, agreed upon, and properly managed. The Change Management Process must be followed if the Contractor requests the use of Supplemental or Optional Services, which must be part of this contract.

The Contractor is advised that any legislative, policy or other changes during the life of the Contract may result in changes to the Agency specific requirements and functions. The State will be responsible for submitting appropriate change request to the Contractor. The Contractor must perform an impact analysis to determine the functional areas impacted by the change, and the associated requirements and deliverables that must be modified to incorporate the change. Once the impact analysis has been completed, the Contractor must submit a change request detailing the proposed changes to incorporate the new/changed functionality. The change request should additionally include impact to the project schedule, and FTEs required to incorporate and to implement the change. The change request must follow the defined and approved process.

For proposed contract changes outside the scope of the current approved Purchase Order, the Contract Administrator (with approval of the State Project Managers) must submit a change request to the Department of Technology, Management, and Budget (DTMB), Procurement Buyer, who must make recommendations to the DTMB Chief Procurement Officer regarding ultimate approval or disapproval of the change request. If the DTMB Chief Procurement Officer agrees with the proposed modification, and all required approvals are obtained (including State Administrative Board), the DTMB Procurement Buyer must issue an addendum to the Contract, via a Contract Change Notice.

If products or services are provided by the Contractor prior to the issuance of a Contract Change Notice by DTMB Procurement, the Contractor risks non-payment for out-of-scope pricing, products, or services.

1.500 Acceptance

1.501 CRITERIA

The acceptance criteria for document and software deliverables are specified in the standard terms and conditions of the contract, in Article 2, Section 2.253 – 2.255. The Contractor shall follow this prescribed process for the review and approval of deliverables, milestones and stage exit reviews as required under the Contract.

Upon completion of the deliverable(s), the Contractor shall distribute the document to the reviewers and approvers. The Contractor shall schedule and facilitate a follow-up meeting to collectively walkthrough the deliverable and review feedback from the State. During the review meeting, all deliverable comments, issues and defects should be discussed, resolved and the disposition documented in accordance with the acceptance criteria.



The Contractor PM is responsible for ensuring the approved changes resulting from the deliverable review are documented and incorporated in the appropriate deliverable(s). The review process is iterative until all changes are accepted. Any Deliverable for which agreement cannot be reached after the second (2nd) facilitated review shall follow the defined project escalation process. The deliverable shall be circulated for signature approval once the deliverable is updated to reflect the agreed upon changes. Once signatures are received, the deliverable shall then be scanned and placed in the electronic project repository.

1.502 FINAL ACCEPTANCE

See Section 2.256.

1.600 Compensation and Payment

1.601 COMPENSATION AND PAYMENT

Method of Payment

This contract is a fixed, firm priced contract. The Contractor shall be compensated as per Appendix C - Payment Schedule. Contractor shall be paid according to the terms and conditions defined within the negotiated contract.

Travel

The State will not pay for any travel expenses, including hotel, mileage, meals, parking, etc. Travel time will not be reimbursed.

Out-of-Pocket Expenses

Contractor out-of-pocket expenses are not separately reimbursable by the State unless, on a case-by-case basis for unusual expenses, the State has agreed in advance and in writing to reimburse Contractor for such an expense at the State's current travel reimbursement rates.

If Contractor reduces its prices for any of the software or services during the term of this Contract, the State shall have the immediate benefit of such lower prices for new purchases. Contractor shall send notice to the State's DTMB Contract Administrator with the reduced prices within fifteen (15) Business Days of the reduction taking effect.

Statements of Work and Issuance of Purchase Orders

1. Unless otherwise agreed by the parties, each Statement of Work will include:
 1. Background
 2. Project Objective
 3. Scope of Work
 4. Deliverables
 5. Acceptance Criteria
 6. Project Control and Reports
 7. Specific Department Standards
 8. Payment Schedule
 9. Travel and Expenses
 10. Project Contacts
 11. Agency Responsibilities and Assumptions
 12. Location of Where the Work is to be performed
 13. Expected Contractor Work Hours and Conditions
2. The parties agree that the Services/Deliverables to be rendered by Contractor pursuant to this Contract (and any future amendments of it) will be defined and described in detail in Statements of Work or Purchase Orders (PO) executed under this Contract. Contractor shall not be obliged or authorized to commence any work to implement a Statement of Work until authorized via a PO issued against this Contract. Contractor shall perform in accordance with this Contract, including the Statements of Work/Purchase Orders executed under it.

**Invoicing**

The Contractor shall submit properly itemized invoices to the “Bill To” Address on the Purchase Order.

Invoices must provide and itemize, as applicable:

1. Contract number;
2. Purchase Order number
3. Contractor name, address, phone number, and Federal Tax Identification Number;
4. Description of any commodities/hardware, including quantity ordered;
5. Date(s) of delivery and/or date(s) of installation and set up;
6. Price for each item, or Contractor's list price for each item and applicable discounts;
7. Maintenance charges;
8. Net invoice price for each item;
9. Shipping costs;
10. Other applicable charges;
11. Total invoice price; and
12. Payment terms, including any available prompt payment discount.

Incorrect or incomplete invoices will be returned to Contractor for correction and reissue.

1.602 HOLDBACK

The State shall have the right to hold back an amount as specified in any future Statement of Work.

1.700 Additional Terms and Conditions Specific to this SOW**1.701 STATE UNEMPLOYMENT TAX AVOIDANCE (SUTA) DUMPING**

The Contractor shall agree that during the period of this engagement/contract, it shall refrain from conducting training seminars or publishing instructional or promotional materials in any form that instructs or encourages its clients or potential clients about any aspect of the practice known as “SUTA Dumping”. SUTA Dumping is the practice of manipulating the UI Tax Rate to achieve a lower rate and then using the lower rate to pay lower UI taxes, which is prohibited by Section 22b of the MES Act.



Article 2, Terms and Conditions

2.000 Contract Structure and Term

2.001 CONTRACT TERM

This Contract is for a period of three (3) years beginning December 21, 2012 through December 20, 2015. All outstanding Purchase Orders must also expire upon the termination for any of the reasons listed in **Section 2.150** of the Contract, unless otherwise extended under the Contract. Absent an early termination for any reason, Purchase Orders issued but not expired, by the end of the Contract's stated term, shall remain in effect for the balance of the fiscal year for which they were issued.

2.002 OPTIONS TO RENEW

This Contract may be renewed in writing by mutual agreement of the parties not less than 30 days before its expiration. The Contract may be renewed for up to 5 additional 1 year periods. Prices for such renewal periods will be mutually agreed upon by the parties.

2.003 LEGAL EFFECT

Contractor accepts this Contract by signing two copies of the Contract and returning them to DTMB Procurement. The Contractor shall not proceed with the performance of the work to be done under the Contract, including the purchase of necessary materials, until both parties have signed the Contract to show acceptance of its terms, and the Contractor receives a contract release/purchase order that authorizes and defines specific performance requirements.

Except as otherwise agreed in writing by the parties, the State shall not be liable for costs incurred by Contractor or payment under this Contract, until Contractor is notified in writing that this Contract or Change Order has been approved by the State Administrative Board (if required), signed by all the parties and a Purchase Order against the Contract has been issued.

2.004 APPENDICES ATTACHMENTS & EXHIBITS

All Appendices, Attachments and Exhibits affixed to any and all Statement(s) of Work, or appended to and referencing this Contract, are incorporated in their entirety and form part of this Contract.

2.005 ORDERING

The State must issue an approved written Purchase Order, Blanket Purchase Order, Direct Voucher or Procurement Card Order to order any Services/Deliverables under this Contract. All orders are subject to the terms and conditions of this Contract. No additional terms and conditions contained on either a Purchase Order or Blanket Purchase Order apply unless they are specifically contained in that Purchase Order or Blanket Purchase Order's accompanying Statement of Work. Exact quantities to be purchased are unknown; however, the Contractor will be required to furnish all such materials and services as may be ordered during the Contract period. Quantities specified, if any, are estimates based on prior purchases, and the State is not obligated to purchase in these or any other quantities.

2.006 ORDER OF PRECEDENCE

The Contract, including any Statements of Work and Exhibits, to the extent not contrary to the Contract, each of which is incorporated for all purposes, constitutes the entire agreement between the parties with respect to the subject matter and supersedes all prior agreements, whether written or oral, with respect to the subject matter and as additional terms and conditions on the purchase order must apply as limited by **Section 2.005**.

In the event of any inconsistency between the terms of the Contract and a Statement of Work, the terms of the Statement of Work shall take precedence (as to that Statement of Work only); provided, however, that a Statement of Work may not modify or amend the terms of the Contract (other than with respect to the Statement of Work in question). The Contract may be modified or amended only by a formal Contract amendment.



2.007 HEADINGS

Captions and headings used in the Contract are for information and organization purposes. Captions and headings, including inaccurate references, do not, in any way, define or limit the requirements or terms and conditions of the Contract.

2.008 FORM, FUNCTION & UTILITY

If the Contract is for use of more than one State agency and if the Deliverable/Service does not meet the form, function, and utility required by that State agency, that agency may, subject to State purchasing policies, procure the Deliverable/Service from another source.

2.009 REFORMATION AND SEVERABILITY

Each provision of the Contract is severable from all other provisions of the Contract and, if one or more of the provisions of the Contract is declared invalid, the remaining provisions of the Contract remain in full force and effect.

2.010 Consents and Approvals

Except as expressly provided otherwise in the Contract, if either party requires the consent or approval of the other party for the taking of any action under the Contract, the consent or approval must be in writing and must not be unreasonably withheld or delayed.

2.011 NO WAIVER OF DEFAULT

If a party fails to insist upon strict adherence to any term of the Contract then the party has not waived the right to later insist upon strict adherence to that term, or any other term, of the Contract.

2.012 SURVIVAL

Any provisions of the Contract that impose continuing obligations on the parties, including without limitation the parties' respective warranty, indemnity and confidentiality obligations, survive the expiration or termination of the Contract for any reason. Specific references to survival in the Contract are solely for identification purposes and not meant to limit or prevent the survival of any other section

2.020 Contract Administration

2.021 ISSUING OFFICE

This Contract is issued by the Department of Technology, Management and Budget, Procurement and is a Statewide Contract (collectively, including all other relevant State of Michigan departments and agencies, the "State"). DTMB Procurement is the sole point of contact in the State with regard to all procurement and contractual matters relating to the Contract. The DTMB Procurement Contract Administrator for this Contract is:

Steve Motz, Buyer

Department of Technology, Management and Budget - Procurement
Mason Bldg, 2nd Floor
PO Box 30026
Lansing, MI 48909
motzs@michigan.gov
517-241-3215

2.022 CONTRACT COMPLIANCE INSPECTOR

The Chief Procurement Officer of DTMB Procurement directs the person named below, or his or her designee, to monitor and coordinate the activities for the Contract on a day-to-day basis during its term. **Monitoring Contract activities does not imply the authority to change, modify, clarify, amend, or otherwise alter the prices, terms, conditions and specifications of the Contract. DTMB Procurement is the only State office authorized to change, modify, amend, alter or clarify the prices, specifications, terms and conditions of this Contract.** The Contract Compliance Inspector is identified on the cover page of this Contract.



2.023 PROJECT MANAGER

The individuals identified as Project Managers in Section 1.202 of the Contract will oversee the project for the State.

2.024 CHANGE REQUESTS

The State reserves the right to request from time to time any changes to the requirements and specifications of the Contract and the work to be performed by the Contractor under the Contract. During the course of ordinary business, it may become necessary for the State to discontinue certain business practices or create Additional Services/Deliverables. At a minimum, to the extent applicable, Contractor shall provide a detailed outline of all work to be done, including tasks necessary to accomplish the Additional Services/Deliverables, timeframes, listing of key personnel assigned, estimated hours for each individual per task, and a complete and detailed cost justification.

If the State requests or directs the Contractor to perform any Additional Services/Deliverables that are outside the scope of the Contractor's responsibilities under the Contract ("New Work"), the State will notify the Contractor that the requested Services/Deliverables are a New Work request, if the state fails to notify the Contractor, the Contractor must notify the State promptly before commencing performance of the requested activities it believes are New Work. If the Contractor fails to notify the State before commencing performance of the requested activities, any such activities performed before the Contractor gives notice shall be conclusively considered to be in-scope Services/Deliverables and not New Work.

If the State requests or directs the Contractor to perform any services or provide deliverables that are consistent with and similar to the Services/Deliverables being provided by the Contractor under the Contract, but which the Contractor reasonably and in good faith believes are not included within the Statements of Work, then before performing such services or providing such deliverables, the Contractor shall notify the State in writing that it considers the services or deliverables to be an Additional Service/Deliverable for which the Contractor should receive additional compensation. If the Contractor does not so notify the State, the Contractor shall have no right to claim thereafter that it is entitled to additional compensation for performing that Service or providing that Deliverable. If the Contractor does so notify the State, then such a Service or Deliverable shall be governed by the Change Request procedure in this Section.

In the event prices or service levels are not acceptable to the State, the Additional Services or New Work shall be subject to competitive bidding based upon the specifications.

(1) Change Request at State Request

If the State requires Contractor to perform New Work, Additional Services or make changes to the Services that would affect the Contract completion schedule or the amount of compensation due Contractor (a "Change"), the State shall submit a written request for Contractor to furnish a proposal for carrying out the requested Change (a "Change Request").

(2) Contractor Recommendation for Change Requests:

Contractor shall be entitled to propose a Change to the State, on its own initiative, should Contractor believe the proposed Change would benefit the Contract.

(3) Upon receipt of a Change Request or on its own initiative, Contractor shall examine the implications of the requested Change on the technical specifications, Contract schedule and price of the Deliverables and Services and shall submit to the State without undue delay a written proposal for carrying out the Change. Contractor's proposal shall include any associated changes in the technical specifications, Contract schedule and price and method of pricing of the Services. If the Change is to be performed on a time and materials basis, the firm fixed hourly rate provided in **Appendix C, Table 3 shall apply to the provision of such Services. If Contractor provides a written proposal and should Contractor be of the opinion that a requested Change is not to be recommended, it shall communicate its opinion to the State but shall nevertheless carry out the Change as specified in the written proposal if the State directs it to do so and a mutually agreeable Contract Change Notice is executed by the parties.**

(4) By giving Contractor written notice within a reasonable time, the State shall be entitled to accept a Contractor proposal for Change, to reject it, or to reach another agreement with Contractor. Should the parties agree on carrying out a Change, a written Contract Change Notice must be prepared and issued



under this Contract, describing the Change and its effects on the Services and any affected components of this Contract (a "Contract Change Notice").

- (5) No proposed Change shall be performed until the proposed Change has been specified in a duly executed Contract Change Notice issued by the Department of Technology, Management and Budget, Procurement.
- (6) If the State requests or directs the Contractor to perform any activities that Contractor believes constitute a Change, the Contractor must notify the State that it believes the requested activities are a Change before beginning to work on the requested activities. If the Contractor fails to notify the State before beginning to work on the requested activities, then the Contractor waives any right to assert any claim for additional compensation or time for performing the requested activities. If the Contractor commences performing work outside the scope of this Contract and then ceases performing that work, the Contractor must, at the request of the State, retract any out-of-scope work that would adversely affect the Contract.

2.025 NOTICES

Any notice given to a party under the Contract must be deemed effective, if addressed to the party as addressed below, upon: (i) delivery, if hand delivered; (ii) receipt of a confirmed transmission by facsimile if a copy of the notice is sent by another means specified in this Section; (iii) the third Business Day after being sent by U.S. mail, postage pre-paid, return receipt requested; or (iv) the next Business Day after being sent by a nationally recognized overnight express courier with a reliable tracking system.

State:

State of Michigan
DTMB Procurement
Attention: Steve Motz
PO Box 30026
530 West Allegan
Lansing, Michigan 48909

Contractor: SAS Institute Inc.

Name: General Counsel

Address: 100 SAS Campus Drive, Cary, NC 27613

Either party may change its address where notices are to be sent by giving notice according to this Section.

2.026 BINDING COMMITMENTS

Representatives of Contractor must have the authority to make binding commitments on Contractor's behalf within the bounds set forth in the Contract. Contractor may change the representatives from time to time upon giving written notice.

2.027 RELATIONSHIP OF THE PARTIES

The relationship between the State and Contractor is that of client and independent Contractor. No agent, employee, or servant of Contractor or any of its Subcontractors shall be deemed to be an employee, agent or servant of the State for any reason. Contractor shall be solely and entirely responsible for its acts and the acts of its agents, employees, servants and Subcontractors during the performance of the Contract.

2.028 COVENANT OF GOOD FAITH

Each party shall act reasonably and in good faith. Unless stated otherwise in the Contract, the parties shall not unreasonably delay, condition or withhold the giving of any consent, decision or approval that is either requested or reasonably required of them in order for the other party to perform its responsibilities under the Contract.

2.029 ASSIGNMENTS

Neither party may assign the Contract, or assign or delegate any of its duties or obligations under the Contract, to any other party (whether by operation of law or otherwise), without the prior written consent of the other party; provided, however, that the State may assign the Contract to any other State agency, department, division or department without the prior consent of Contractor and Contractor may assign the Contract to an affiliate so long as the affiliate is adequately capitalized and can provide adequate assurances that the affiliate



can perform the Contract. The State may withhold consent from proposed assignments, subcontracts, or novations when the transfer of responsibility would operate to decrease the State's likelihood of receiving performance on the Contract or the State's ability to recover damages.

Contractor may not, without the prior written approval of the State, assign its right to receive payments due under the Contract. If the State permits an assignment, the Contractor is not relieved of its responsibility to perform any of its contractual duties and the requirement under the Contract that all payments must be made to one entity continues. Any costs associated with transfer of the Services to another agency of the State shall be borne by the State.

If the Contractor intends to assign the contract or any of the Contractor's rights or duties under the Contract, the Contractor must notify the State in writing at least 90 days before the assignment. The Contractor also must provide the State with adequate information about the assignee within a reasonable amount of time before the assignment for the State to determine whether to approve the assignment.

2.030 General Provisions

2.031 MEDIA RELEASES

News releases (including promotional literature and commercial advertisements) pertaining to the RFP and Contract or project to which it relates shall not be made without prior written State approval, and then only in accordance with the explicit written instructions from the State. No results of the activities associated with the RFP and Contract are to be released without prior written approval of the State and then only to persons designated.

2.032 CONTRACT DISTRIBUTION

DTMB Procurement retains the sole right of Contract distribution to all State agencies and local units of government unless other arrangements are authorized by DTMB Procurement.

2.033 PERMITS

Contractor must obtain and pay any associated costs for all required governmental permits, licenses and approvals for the delivery, installation and performance of the Services. The State shall pay for all costs and expenses incurred in obtaining and maintaining any necessary easements or right of way.

2.034 WEBSITE INCORPORATION

The State is not bound by any content on the Contractor's website, even if the Contractor's documentation specifically referenced that content and attempts to incorporate it into any other communication, unless the State has actual knowledge of the content and has expressly agreed to be bound by it in a writing that has been manually signed by an authorized representative of the State.

2.035 FUTURE BIDDING PRECLUSION

Contractor acknowledges that, to the extent this Contract involves the creation, research, investigation or generation of a future RFP; it may be precluded from bidding on the subsequent RFP. The State reserves the right to disqualify any Bidder if the State determines that the Bidder has used its position (whether as an incumbent Contractor, or as a Contractor hired to assist with the RFP development, or as a Vendor offering free assistance) to gain a competitive advantage on the RFP

2.036 FREEDOM OF INFORMATION

All information in any proposal submitted to the State by Bidder and this Contract is subject to the provisions of the Michigan Freedom of Information Act, 1976 Public Act No. 442, as amended, MCL 15.231, et seq (the "FOIA").

2.037 DISASTER RECOVERY

Contractor and the State recognize that the State provides essential services in times of natural or man-made disasters. Therefore, except as so mandated by Federal disaster response requirements, Contractor personnel dedicated to providing Services/Deliverables under this Contract shall provide the State with priority service for repair and work around in the event of a natural or man-made disaster.



2.040 Financial Provisions

2.041 FIXED PRICES FOR SERVICES/DELIVERABLES

Each Statement of Work or Purchase Order issued under this Contract shall specify (or indicate by reference to the appropriate Contract Exhibit) the firm, fixed prices for all Services/Deliverables, and the associated payment milestones and payment amounts.

2.042 ADJUSTMENTS FOR REDUCTIONS IN SCOPE OF SERVICES/DELIVERABLES

If the scope of the Services/Deliverables under any Statement of Work issued under this Contract is subsequently reduced by the State, the parties shall negotiate an equitable reduction in Contractor's charges under such Statement of Work commensurate with the reduction in scope.

2.043 SERVICES/DELIVERABLES COVERED

The State shall not be obligated to pay any amounts in addition to the charges specified in this Contract for all Services/Deliverables to be provided by Contractor and its Subcontractors, if any, under this Contract.

2.044 INVOICING AND PAYMENT – IN GENERAL

- (a) Each Statement of Work issued under this Contract shall list (or indicate by reference to the appropriate Contract Exhibit) the prices for all Services/Deliverables to be provided, and the associated payment milestones and payment amounts.
- (b) Each Contractor invoice shall show details as to charges by Service/Deliverable component and location at a level of detail reasonably necessary to satisfy the State's accounting and charge-back requirements. Invoices for Services performed on a time and materials basis shall show, for each role, the number of hours of Services performed during the billing period, the billable skill/labor category for such role and the applicable hourly billing rate. Prompt payment by the State is contingent on the Contractor's invoices showing the amount owed by the State minus any holdback amount to be retained by the State in accordance with **Section 1.600**.
- (c) Correct invoices shall be due and payable by the State, in accordance with the State's standard payment procedure as specified in 1984 Public Act No. 279, MCL 17.51 et seq., within 45 days after receipt, provided the State determines that the invoice was properly rendered.
- (d) All invoices should reflect actual work done. Specific details of invoices and payments shall be agreed upon between the Contract Administrator and the Contractor after the proposed Contract Agreement has been signed and accepted by both the Contractor and the Chief Procurement Officer, Department of Management & Budget. This activity shall occur only upon the specific written direction from DTMB-Procurement.

The specific payment schedule for any Contract(s) entered into, as the State and the Contractor(s) shall mutually agree upon. The schedule should show payment amount and should reflect actual work done by the payment dates. As a general policy statements shall be forwarded to the designated representative by the 15th day of the following month.

The State may make progress payments to the Contractor when requested as work progresses, but not more frequently than monthly, in amounts approved by the Contract Administrator, after negotiation. Contractor must show verification of measurable progress at the time of requesting progress payments.

2.045 RESERVED - PRO-RATION

2.046 ANTITRUST ASSIGNMENT

The Contractor assigns to the State any claim for overcharges resulting from antitrust violations to the extent that those violations concern materials or services supplied by third parties to the Contractor, toward fulfillment of this Contract.

**2.047 FINAL PAYMENT**

The making of final payment by the State to Contractor does not constitute a waiver by either party of any rights or other claims as to the other party's continuing obligations under the Contract, nor shall it constitute a waiver of any claims by one party against the other arising from unsettled claims or failure by a party to comply with this Contract, including claims for Services and Deliverables not reasonably known until after acceptance to be defective or substandard. Contractor's acceptance of final payment by the State under this Contract shall constitute 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 unsettled.

2.048 ELECTRONIC PAYMENT REQUIREMENT

Electronic transfer of funds is required for payments on State Contracts. Contractors are required to register with the State electronically at <http://www.cpexpress.state.mi.us>. As stated in Public Act 431 of 1984, all contracts that the State enters into for the purchase of goods and services shall provide that payment shall be made by electronic fund transfer (EFT).

2.050 Taxes**2.051 EMPLOYMENT TAXES**

Contractor shall collect and pay all applicable federal, state, and local employment taxes relating to its personnel.

2.052 SALES AND USE TAXES

Contractor shall register and remit sales and use taxes on taxable sales of tangible personal property or services delivered into the State. Contractors that lack sufficient presence in Michigan to be required to register and pay tax must do so as a volunteer. This requirement extends to: (1) all members of any controlled group as defined in § 1563(a) of the Internal Revenue Code and applicable regulations of which the company is a member, and (2) all organizations under common control as defined in § 414(c) of the Internal Revenue Code and applicable regulations of which the company is a member that make sales at retail for delivery into the State are registered with the State for the collection and remittance of sales and use taxes. In applying treasury regulations defining "two or more trades or businesses under common control" the term "organization" means sole proprietorship, a partnership (as defined in § 701(a) (2) of the Internal Revenue Code), a trust, an estate, a corporation, or a limited liability company.

2.060 Contract Management**2.061 CONTRACTOR PERSONNEL QUALIFICATIONS**

All persons assigned by Contractor to the performance of Services under this Contract must be employees of Contractor or its majority-owned (directly or indirectly, at any tier) subsidiaries (or a State-approved Subcontractor) and must be fully qualified to perform the work assigned to them. Contractor must include a similar provision in any subcontract entered into with a Subcontractor. For the purposes of this Contract, independent Contractors engaged by Contractor solely in a staff augmentation role must be treated by the State as if they were employees of Contractor for this Contract only; however, the State understands that the relationship between Contractor and Subcontractor is an independent Contractor relationship.

2.062 CONTRACTOR KEY PERSONNEL

- (a) The Contractor must provide the Contract Compliance Inspector with the names of the Key Personnel.
- (b) Key Personnel must be dedicated as defined in the Statement of Work to the Project for its duration in the applicable Statement of Work with respect to other individuals designated as Key Personnel for that Statement of Work.
- (c) The State shall have 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 shall notify the State of the proposed assignment, shall introduce the individual to the appropriate State representatives, and shall 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 shall provide a written explanation including reasonable detail outlining



the reasons for the rejection. Additionally, the State's request must be based on legitimate, good faith reasons.

- (d) Contractor must not remove any Key Personnel from their assigned roles on the 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"). Unauthorized Removals 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. Unauthorized Removals does not include replacing Key Personnel because of promotions or other job movements allowed by Contractor personnel policies or Collective Bargaining Agreement(s) as long as the State receives prior written notice before shadowing occurs and Contractor provides 30 days of shadowing unless parties agree to a different time period. The Contractor with the State must review any Key Personnel replacements, and appropriate transition planning will be established. Any Unauthorized Removal may be considered by the State to be a material breach of the Contract, in respect of which the State may elect to exercise its termination and cancellation rights.
- (e) The Contractor must notify the Contract Compliance Inspector and the Contract Administrator at least 5 business days before redeploying non-Key Personnel, who are working primarily to the Project, to other projects. If the State does not object to the redeployment by its scheduled date, the Contractor may then redeploy the non-Key Personnel.

2.063 RE-ASSIGNMENT OF PERSONNEL AT THE STATE'S REQUEST

The State reserves the right to require the removal from the Project of 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. Additionally, the State's request must be based on legitimate, good faith reasons. Replacement personnel for the removed person must be fully qualified for the position. If the State exercises this right, and the Contractor cannot immediately replace the removed personnel, the State agrees to an equitable adjustment in schedule or other terms that may be affected by the State's required removal. If any incident with removed personnel results in delay not reasonably anticipatable under the circumstances and which is attributable to the State, the applicable SLAs for the affected Service shall not be counted for a time as agreed to by the parties.

2.064 CONTRACTOR PERSONNEL LOCATION

All staff assigned by Contractor to work on the Contract shall perform their duties either primarily at Contractor's offices and facilities or at State facilities. Without limiting the generality of the foregoing, Key Personnel shall, at a minimum, spend at least the amount of time on-site at State facilities as indicated in the applicable Statement of Work. Subject to availability, selected Contractor personnel may be assigned office space to be shared with State personnel.

2.065 CONTRACTOR IDENTIFICATION

Contractor employees must be clearly identifiable while on State property by wearing a State-issued badge, as required. Contractor employees are required to clearly identify themselves and the company they work for whenever making contact with State personnel by telephone or other means.

2.066 COOPERATION WITH THIRD PARTIES

Contractor agrees to cause its personnel and the personnel of any Subcontractors to cooperate with the State and its agents and other Contractors including the State's Quality Assurance personnel. As reasonably requested by the State in writing, the Contractor shall provide to the State's agents and other Contractors reasonable access to Contractor's Project personnel, systems and facilities to the extent the access relates to activities specifically associated with this Contract and shall not interfere or jeopardize the safety or operation of the systems or facilities. The State acknowledges that Contractor's time schedule for the Contract is very specific and agrees not to unnecessarily or unreasonably interfere with, delay or otherwise impeded Contractor's performance under this Contract with the requests for access.

**2.067 CONTRACT MANAGEMENT RESPONSIBILITIES**

Contractor shall be responsible for all acts and omissions of its employees, as well as the acts and omissions of any other personnel furnished by Contractor to perform the Services. Contractor shall have overall responsibility for managing and successfully performing and completing the Services/Deliverables, subject to the overall direction and supervision of the State and with the participation and support of the State as specified in this Contract. Contractor's duties shall include monitoring and reporting the State's performance of its participation and support responsibilities (as well as Contractor's own responsibilities) and providing timely notice to the State in Contractor's reasonable opinion if the State's failure to perform its responsibilities in accordance with the Project Plan is likely to delay the timely achievement of any Contract tasks.

The Contractor shall provide the Services/Deliverables directly or through its affiliates, subsidiaries, Subcontractors or resellers. Regardless of the entity providing the Service/Deliverable, the Contractor shall act as a single point of contact coordinating these entities to meet the State's need for Services/Deliverables. Nothing in this Contract, however, shall be construed to authorize or require any party to violate any applicable law or regulation in its performance of this Contract.

2.068 CONTRACTOR RETURN OF STATE EQUIPMENT/RESOURCES

The Contractor shall return to the State any State-furnished equipment, facilities and other resources when no longer required for the Contract in the same condition as when provided by the State, reasonable wear and tear excepted.

2.070 Subcontracting by Contractor**2.071 CONTRACTOR FULL RESPONSIBILITY**

Contractor shall have full responsibility for the successful performance and completion of all of the Services and Deliverables. The State shall consider Contractor to be the sole point of contact with regard to all contractual matters under this Contract, including payment of any and all charges for Services and Deliverables.

2.072 STATE CONSENT TO DELEGATION

Contractor shall not delegate any duties under this Contract to a Subcontractor unless the Department of Technology, Management and Budget, Procurement has given written consent to such delegation. The State shall have the right of prior written approval of all Subcontractors and to require Contractor to replace any Subcontractors found, in the reasonable judgment of the State, to be unacceptable. The State's request shall be written with reasonable detail outlining the reasons for the removal request. Additionally, the State's request shall be based on legitimate, good faith reasons. Replacement Subcontractor(s) for the removed Subcontractor shall be fully qualified for the position. If the State exercises this right, and the Contractor cannot immediately replace the removed Subcontractor, the State shall agree to an equitable adjustment in schedule or other terms that may be affected by the State's required removal. If any such incident with a removed Subcontractor results in delay not reasonable anticipatable under the circumstances and which is attributable to the State, the applicable SLA for the affected Work shall not be counted for a time agreed upon by the parties.

2.073 SUBCONTRACTOR BOUND TO CONTRACT

In any subcontracts entered into by Contractor for the performance of the Services, Contractor shall require the Subcontractor, to the extent of the Services to be performed by the Subcontractor, to be bound to Contractor by the terms of this Contract and to assume toward Contractor all of the obligations and responsibilities that Contractor, by this Contract, assumes toward the State. The State reserves the right to receive copies of and review all subcontracts, although Contractor may delete or mask any proprietary information, including pricing, contained in such contracts before providing them to the State. The management of any Subcontractor shall be the responsibility of Contractor, and Contractor shall remain responsible for the performance of its Subcontractors to the same extent as if Contractor had not subcontracted such performance. Contractor shall make all payments to Subcontractors or suppliers of Contractor. Except as otherwise agreed in writing by the State and Contractor, the State shall not be obligated to direct payments for the Services other than to



Contractor. The State's written approval of any Subcontractor engaged by Contractor to perform any obligation under this Contract shall not relieve Contractor of any obligations or performance required under this Contract. A list of the Subcontractors, if any, approved by the State as of the execution of this Contract, together with a copy of the applicable subcontract is attached.

2.074 FLOW DOWN

Except where specifically approved in writing by the State on a case-by-case basis, Contractor shall flow down the obligations in **Sections 2.031, 2.060, 2.100, 2.110, 2.120, 2.130, and 2.200** in all of its agreements with any Subcontractors.

2.075 COMPETITIVE SELECTION

The Contractor shall select Subcontractors (including suppliers) on a competitive basis to the maximum practical extent consistent with the objectives and requirements of the Contract.

2.080 State Responsibilities

2.081 EQUIPMENT

The State shall provide only the equipment and resources identified in the Statement of Work and other Contract Exhibits.

2.082 FACILITIES

The State must designate space as long as it is available and as provided in the Statement of Work, to house the Contractor's personnel whom the parties agree will perform the Services/Deliverables at State facilities (collectively, the "State Facilities"). The Contractor shall have reasonable access to, and unless agreed otherwise by the parties in writing must observe and comply with all rules and regulations relating to each of the State Facilities (including hours of operation) used by the Contractor in the course of providing the Services. Contractor agrees that it shall not, without the prior written consent of the State, use any State Facilities or access any State information systems provided for the Contractor's use, or to which the Contractor otherwise gains access in the course of performing the Services, for any purpose other than providing the Services to the State.

2.090 Security

2.091 BACKGROUND CHECKS

On a case-by-case basis, the State may investigate, at State expense, the Contractor's personnel before they may have access to State facilities and systems. The Contractor will be responsible for the costs of the required background checks. The scope of the background check is at the discretion of the State and the results shall be used to determine Contractor personnel eligibility for working within State facilities and systems. The investigations shall include Michigan State Police Background checks (ICHAT) and may include the National Crime Information Center (NCIC) Finger Prints. Proposed Contractor personnel may be required to complete and submit an RI-8 Fingerprint Card for the NCIC Finger Print Check. Any request for background checks shall be initiated by the State and shall be reasonably related to the type of work requested.

All Contractor personnel shall also be expected to comply with the State's security and acceptable use policies for State IT equipment and resources. See http://www.michigan.gov/documents/dmb/1460.00_384290_7.pdf.

Furthermore, Contractor personnel shall be expected to agree to the State's security and acceptable use policies before the Contractor personnel shall be accepted as a resource to perform work for the State. It is expected the Contractor shall present these documents to the prospective employee before the Contractor presents the individual to the State as a proposed resource. Contractor staff shall be expected to comply with all Physical Security procedures in place within the facilities where they are working.



2.092 SECURITY BREACH NOTIFICATION

If the Contractor breaches this Section, the Contractor must (i) promptly cure any deficiencies and (ii) comply with any applicable federal and state laws and regulations pertaining to unauthorized disclosures. Contractor and the State shall cooperate to mitigate, to the extent practicable, the effects of any breach, intrusion, or unauthorized use or disclosure. Contractor must report to the State in writing any use or disclosure of Confidential Information, whether suspected or actual, other than as provided for by the Contract within 10 days of becoming aware of the use or disclosure or the shorter time period as is reasonable under the circumstances.

2.093 PCI DATA SECURITY REQUIREMENTS

This Section 2.093 shall be applicable only to contractors that process, transmit or store credit/debit cardholder data.

(a) Contractors that process, transmit or store credit/debit cardholder data, must adhere to the Payment Card Industry (PCI) Data Security Standards. The Contractor is responsible for the security of cardholder data in its possession. The data may only be used to assist the State or for other uses specifically authorized by law.

(b) The Contractor must notify the CCI (within 72 hours of discovery) of any breaches in security where cardholder data has been compromised. In that event, the Contractor must provide full cooperation to the Visa, MasterCard, Discover and state Acquirer representative(s), and/or a PCI approved third party to conduct a thorough security review. The Contractor must make the forensic report available within two weeks of completion. The review must validate compliance with the current PCI Data Security Standards for protecting cardholder data.

(c) The Contractor must properly dispose of cardholder data, in compliance with DTMB policy, when it is no longer needed. The Contractor must continue to treat cardholder data as confidential upon contract termination.

(d) The Contractor must provide the CCI with an annual Attestation of Compliance (AOC) or a Report on Compliance (ROC) showing the contractor is in compliance with the PCI Data Security Standards. The Contractor must notify the CCI of all failures to comply with the PCI Data Security Standard.

2.100 Confidentiality

2.101 CONFIDENTIALITY

Contractor and the State each acknowledge that the other possesses and shall continue to possess confidential information that has been developed or received by it. As used in this Section, "Confidential Information" of Contractor must mean all non-public proprietary information of Contractor (other than Confidential Information of the State as defined below), which is marked confidential, restricted, proprietary, or with a similar designation. "Confidential Information" of the State must mean any information which is retained in confidence by the State (or otherwise required to be held in confidence by the State under applicable federal, state and local laws and regulations) or which, in the case of tangible materials provided to Contractor by the State under its performance under this Contract, is marked as confidential, proprietary or with a similar designation by the State. "Confidential Information" excludes any information (including this Contract) that is publicly available under the Michigan FOIA.

2.102 PROTECTION AND DESTRUCTION OF CONFIDENTIAL INFORMATION

The State and Contractor shall each use at least the same degree of care to prevent disclosing to third parties the Confidential Information of the other as it employs to avoid unauthorized disclosure, publication or dissemination of its own confidential information of like character, but in no event less than reasonable care. Neither Contractor nor the State shall (i) make any use of the Confidential Information of the other except as contemplated by this Contract, (ii) acquire any right in or assert any lien against the Confidential Information of the other, or (iii) if requested to do so, refuse for any reason to promptly return the other party's Confidential Information to the other party. Each party shall limit disclosure of the other party's Confidential Information to



employees and Subcontractors who must have access to fulfill the purposes of this Contract. Disclosure to, and use by, 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 scope of responsibility, and (C) Contractor obligates the Subcontractor in a written Contract to maintain the State's Confidential Information in confidence. At the State's request, any employee of Contractor and of any Subcontractor having access or continued access to the State's Confidential Information may be required to execute an acknowledgment that the employee has been advised of Contractor's and the Subcontractor's obligations under this Section and of the employee's obligation to Contractor or Subcontractor, as the case may be, to protect the Confidential Information from unauthorized use or disclosure.

Promptly upon termination or cancellation of the Contract for any reason, Contractor must certify to the State that Contractor has destroyed all State Confidential Information.

2.103 EXCLUSIONS

Notwithstanding the foregoing, the provisions in this Section shall not apply to any particular information which the State or Contractor can demonstrate (i) was, at the time of disclosure to it, in the public domain; (ii) after disclosure to it, is published or otherwise becomes part of the public domain through no fault of the receiving party; (iii) was in the possession of the receiving party at the time of disclosure to it without an obligation of confidentiality; (iv) was received after disclosure to it from a third party who had a lawful right to disclose the information to it without any obligation to restrict its further disclosure; or (v) was independently developed by the receiving party without reference to Confidential Information of the furnishing party. Further, the provisions of this Section shall not apply to any particular Confidential Information to the extent the receiving party is required by law to disclose the Confidential Information, provided that the receiving party (i) promptly provides the furnishing party with notice of the legal request, and (ii) assists the furnishing party in resisting or limiting the scope of the disclosure as reasonably requested by the furnishing party.

2.104 NO IMPLIED RIGHTS

Nothing contained in this Section must be construed as obligating a party to disclose any particular Confidential Information to the other party, or as granting to or conferring on a party, expressly or impliedly, any right or license to the Confidential Information of the other party.

2.105 RESPECTIVE OBLIGATIONS

The parties' respective obligations under this Section must survive the termination or expiration of this Contract for any reason.

2.110 Records and Inspections

2.111 INSPECTION OF WORK PERFORMED

The State's authorized representatives shall at all reasonable times and with 10 days prior written request, have the right to enter Contractor's premises, or any other places, where the Services are being performed, and shall have access, upon reasonable request, to interim drafts of Deliverables or work-in-progress. Upon 10 Days prior written notice and at all reasonable times, the State's representatives shall be allowed to inspect, monitor, or otherwise evaluate the work being performed and to the extent that the access will not unreasonably interfere or jeopardize the safety or operation of the systems or facilities. Contractor shall provide all reasonable facilities and assistance for the State's representatives.

2.112 EXAMINATION OF RECORDS

For seven years after the Contractor provides any work under this Contract (the "Audit Period"), the State may examine and copy any of Contractor's books, records, documents and papers pertinent to establishing Contractor's compliance with the Contract and with applicable laws and rules. The State shall notify the Contractor 30 days before examining the Contractor's books and records. The State does not have the right to review any information deemed confidential by the Contractor to the extent access would require the confidential information to become publicly available. This provision also applies to the books, records, accounts, documents and papers, in print or electronic form, of any parent, affiliated or subsidiary organization of Contractor, or any Subcontractor of Contractor performing services in connection with the Contract.

**2.113 RETENTION OF RECORDS**

Contractor shall maintain at least until the end of the Audit Period all pertinent financial and accounting records (including time sheets and payroll records, and information pertaining to the Contract and to the Services, equipment, and commodities provided under the Contract) pertaining to the Contract according to generally accepted accounting principles and other procedures specified in this Section. Financial and accounting records shall be made available, upon request, to the State at any time during the Audit Period. If an audit, litigation, or other action involving Contractor's records is initiated before the end of the Audit Period, the records shall be retained until all issues arising out of the audit, litigation, or other action are resolved or until the end of the Audit Period, whichever is later.

2.114 AUDIT RESOLUTION

If necessary, the Contractor and the State shall meet to review each audit report promptly after issuance. The Contractor shall respond to each audit report in writing within 30 days from receipt of the report, unless a shorter response time is reasonably specified in the report. The Contractor and the State shall develop, agree upon and monitor an action plan to promptly address and resolve any deficiencies, concerns, and/or recommendations in the audit report.

2.115 ERRORS

If the audit demonstrates any errors in the documents provided to the State, then the amount in error shall be reflected as a credit or debit on the next invoice and in subsequent invoices until the amount is paid or refunded in full. However, a credit or debit may not be carried for more than four invoices. If a balance remains after four invoices, then the remaining amount shall be due as a payment or refund within 45 days of the last quarterly invoice that the balance appeared on or termination of the contract, whichever is earlier.

In addition to other available remedies, the difference between the payment received and the correct payment amount is greater than 10%, then the Contractor shall pay all of the reasonable costs of the audit.

All access to Contractor's premises and records set forth in this Contract are subject to Contractor's reasonable security and confidentiality policies and procedures.

2.120 Warranties**2.121 WARRANTIES AND REPRESENTATIONS**

The Contractor represents and warrants:

- (a) It is capable in all respects of fulfilling and must fulfill all of its obligations under this Contract. The performance of all obligations under this Contract must be provided in a timely, professional, and workman-like manner and must meet the performance and operational standards required under this Contract. The exclusive warranty law remedy for breach of this warranty is refund of fees paid for the Services, Work Product or Deliverable at issue.
- (b) The Contract Appendices, Attachments and Exhibits identify the equipment and software and services necessary for the Deliverable(s) to perform and Services to operate in compliance with the Contract's requirements and other standards of performance.
- (c) It is the lawful owner or licensee of any Deliverable licensed or sold to the State by Contractor or developed by Contractor under this Contract, and Contractor has all of the rights necessary to convey to the State the ownership rights or licensed use, as applicable, of any and all Deliverables. None of the Deliverables provided by Contractor to the State under neither this Contract, nor their use by the State shall infringe the patent, copyright, trade secret, or other proprietary rights of any third party. The exclusive warranty law remedy for breach of this warranty is Contractor's intellectual property indemnification obligations set forth in Section 2.144 hereof.
- (d) If, under this Contract, Contractor procures any equipment, software or other Deliverable for the State (including equipment, software and other Deliverables manufactured, re-marketed or otherwise sold by Contractor under Contractor's name), then in addition to Contractor's other responsibilities with respect to the items in this Contract, Contractor must assign or otherwise transfer to the State or its designees, or afford the State the benefits of, any manufacturer's warranty for the Deliverable.



- (e) The contract signatory has the power and authority, including any necessary corporate authorizations, necessary to enter into this Contract, on behalf of Contractor.
- (f) It is qualified and registered to transact business in all locations where required.
- (g) Neither the Contractor nor any affiliates, nor any employee of either, has, must have, or must acquire, any contractual, financial, business, or other interest, direct or indirect, that would conflict in any manner or degree with Contractor's performance of its duties and responsibilities to the State under this Contract or otherwise create an appearance of impropriety with respect to the award or performance of this Agreement. Contractor must notify the State about the nature of the conflict or appearance of impropriety within two days of learning about it.
- (h) Neither Contractor nor any affiliates, nor any employee of either has accepted or must accept anything of value based on an understanding that the actions of the Contractor or affiliates or employee on behalf of the State would be influenced. Contractor must not attempt to influence any State employee by the direct or indirect offer of anything of value.
- (i) Neither Contractor nor any affiliates, nor any employee of either has paid or agreed to pay any person, other than bona fide employees and consultants working solely for Contractor or the Affiliate, any fee, commission, percentage, brokerage fee, gift, or any other consideration, contingent upon or resulting from the award or making of this Contract.
- (j) The prices proposed by Contractor were arrived at independently, without consultation, communication, or agreement with any other Contractor for the purpose of restricting competition; the prices quoted were not knowingly disclosed by Contractor to any other Contractor; and no attempt was made by Contractor to induce any other person to submit or not submit a proposal for the purpose of restricting competition.
- (k) All financial statements, reports, and other information furnished by Contractor to the State as part of its response to the RFP or otherwise in connection with the award of this Contract fairly and accurately represent the business, properties, financial condition, and results of operations of Contractor as of the respective dates, or for the respective periods, covered by the financial statements, reports, other information. Since the respective dates or periods covered by the financial statements, reports, or other information, there have been no material adverse changes in the business, properties, financial condition, or results of operations of Contractor.
- (l) All written information furnished to the State by or for the Contractor in connection with this Contract, including its bid, is true, accurate, and complete, and contains no untrue statement of material fact or omits any material fact necessary to make the information not misleading.
- (m) It is not in material default or breach of any other contract or agreement that it may have with the State or any of its departments, commissions, boards, or agencies. Contractor further represents and warrants that it has not been a party to any contract with the State or any of its departments that was terminated by the State or the department within the previous five years for the reason that Contractor failed to perform or otherwise breached an obligation of the contract.
- (n) If any of the certifications, representations, or disclosures made in the Contractor's original bid response change after contract award, the Contractor is required to report those changes immediately to the Department of Technology, Management and Budget, Procurement.

The exclusive warranty law remedy for breach of the warranties set forth in subsections (b) and (e) through and including (n) above is termination of this Contract and refund of fees paid hereunder.

EXCEPT FOR THOSE WARRANTIES SPECIFICALLY SET FORTH HEREIN FOR SERVICES, WORK PRODUCT OR DELIVERABLES, SAS DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THE WORK PRODUCT, SERVICES OR DELIVERABLES PROVIDED HEREUNDER OR THE RESULTS OBTAINED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND THOSE ARISING BY STATUTE OR OTHERWISE IN LAW OR FROM A COURSE OF DEALING.

2.122 RESERVED - WARRANTY OF MERCHANTABILITY

2.123 RESERVED - WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE

2.124 RESERVED - WARRANTY OF TITLE

**2.125 RESERVED - EQUIPMENT WARRANTY****2.126 RESERVED - EQUIPMENT TO BE NEW****2.127 RESERVED - PROHIBITED PRODUCTS****2.128 CONSEQUENCES FOR BREACH**

In addition to any remedies available in law, if the Contractor breaches any of the warranties contained in this section, the breach may be considered as a default in the performance of a material obligation of this Contract. Exclusive remedies listed herein do not limit other, non-warranty remedies available in law or equity.

2.130 Insurance**2.131 LIABILITY INSURANCE**

The Contractor must provide proof of the minimum levels of insurance coverage as indicated below. The insurance must protect the State from claims that may arise out of or result from the Contractor's performance of services under the terms of this Contract, whether the services are performed by the Contractor, or by any Subcontractor, or by anyone directly or indirectly employed by any of them, or by anyone for whose acts they may be liable.

The Contractor waives all rights against the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees and agents for recovery of damages to the extent these damages are covered by the insurance policies the Contractor is required to maintain under this Contract(except with regard to errors & omissions and crime coverages).

All insurance coverage provided relative to this Contract/Purchase Order is PRIMARY and NON-CONTRIBUTING (except errors & omissions is contributing) to any comparable liability insurance (including self-insurances) carried by the State.

The insurance must be written for not less than any minimum coverage specified in this Contract or required by law, whichever is greater.

The insurers selected by Contractor must have an A.M. Best rating of A or better, or as otherwise approved in writing by the State, or if the ratings are no longer available, with a comparable rating from a recognized insurance rating agency.

All policies of insurance required in this Contract must be issued by companies that have been approved to do business in the State.

See www.michigan.gov/dleg.

Where specific limits are shown, they are the minimum acceptable limits. If Contractor's policy contains higher limits, the State must be entitled to coverage to the extent of the higher limits.

The Contractor is required to pay for and provide the type and amount of insurance checked ☐ below:

- ☒ 1. Commercial General Liability with the following minimum coverage:
 \$2,000,000 General Aggregate Limit other than Products/Completed Operations
 \$2,000,000 Products/Completed Operations Aggregate Limit
 \$1,000,000 Personal & Advertising Injury Limit
 \$1,000,000 Each Occurrence Limit

The Contractor must list the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees and agents as ADDITIONAL INSURED on the Commercial General Liability certificate. The Contractor also agrees to provide evidence that insurance policies contain a waiver of subrogation by the insurance company.



- ☒ 2. If a motor vehicle is used to provide services or products under this Contract, the Contractor must have vehicle liability insurance on any auto including owned, hired and non-owned vehicles used in Contractor's business for bodily injury and property damage as required by law.

The Contractor must list the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees and agents as ADDITIONAL INSURED on the vehicle liability certificate. The Contractor also agrees to provide evidence that insurance policies contain a waiver of subrogation by the insurance company.

- ☒ 3. Workers' compensation coverage must be provided according to applicable laws governing the employees and employers work activities in the state of the Contractor's domicile. If a self-insurer provides the applicable coverage, proof must be provided of approved self-insured authority by the jurisdiction of domicile. For employees working outside of the state of qualification, Contractor must provide appropriate certificates of insurance proving mandated coverage levels for the jurisdictions where the employees' activities occur.

Any certificates of insurance received must also provide a list of states where the coverage is applicable.

The Contractor also agrees to provide evidence that insurance policies contain a waiver of subrogation by the insurance company. This provision must not be applicable where prohibited or limited by the laws of the jurisdiction in which the work is to be performed.

- ☒ 4. Employers liability insurance with the following minimum limits:
 \$100,000 each accident
 \$100,000 each employee by disease
 \$500,000 aggregate disease

- ☒ 5. Employee Fidelity, including Computer Crimes, insurance naming the State as a loss payee, providing coverage for direct loss to the State and any legal liability of the State arising out of or related to fraudulent or dishonest acts committed by the employees of Contractor or its Subcontractors, acting alone or in collusion with others, in a minimum amount of one million dollars (\$1,000,000.00) with a maximum deductible of one hundred thousand dollars (\$100,000.00).

- ☒ 6. Umbrella or Excess Liability Insurance in a minimum amount of ten million dollars (\$10,000,000.00), which must apply, at a minimum, to the insurance required in Subsection 1 (Commercial General Liability) above.

- ☒ 7. Professional Liability (Errors and Omissions) Insurance with the following minimum coverage: three million dollars (\$3,000,000.00) each occurrence and three million dollars (\$3,000,000.00) annual aggregate.

- ☐ 8. Fire and Personal Property Insurance covering against any loss or damage to the office space used by Contractor for any reason under this Contract, and the equipment, software and other contents of the office space, including without limitation, those contents used by Contractor to provide the Services to the State, up to its replacement value, where the office space and its contents are under the care, custody and control of Contractor. The policy must cover all risks of direct physical loss or damage, including without limitation, flood and earthquake coverage and coverage for computer hardware and software. The State must be endorsed on the policy as a loss payee as its interests appear.

2.132 SUBCONTRACTOR INSURANCE COVERAGE

Except where the State has approved in writing a Contractor subcontract with other insurance provisions, Contractor must require all of its Subcontractors under this Contract to purchase and maintain the insurance coverage as described in this Section for the Contractor in connection with the performance of work by those Subcontractors. Alternatively, Contractor may include any Subcontractors under Contractor's insurance on the coverage required in this Section. Subcontractor(s) must fully comply with the insurance coverage required in this Section. Failure of Subcontractor(s) to comply with insurance requirements does not limit Contractor's liability or responsibility.



2.133 CERTIFICATES OF INSURANCE AND OTHER REQUIREMENTS

Contractor must furnish to DTMB Procurement, certificate(s) of insurance verifying insurance coverage or providing satisfactory evidence of self-insurance as required in this Section (the "Certificates"). The Certificate must be on the standard "acord" form or equivalent. **The Contract Number or the Purchase Order Number must be shown on the Certificate Of Insurance To Assure Correct Filing.** All Certificate(s) are to be prepared and submitted by the Insurance broker. If coverage under the policies is CANCELLED, MATERIALLY CHANGED, OR NOT RENEWED, SAS will provide 30 days prior written notice to DTMB Procurement. The notice must include the Contract or Purchase Order number affected. Before the Contract is signed, and when the insurance renews every year thereafter, the Contractor must provide evidence that the State and its agents, officers and employees are listed as additional insured under each commercial general liability and commercial automobile liability policy. In the event the State approves the representation of the State by the insurer's attorney, the attorney may be required to be designated as a Special Assistant Attorney General by the Attorney General of the State of Michigan.

The Contractor must maintain all required insurance coverage throughout the term of the Contract and any extensions and, in the case of claims-made Commercial General Liability policies, must secure tail coverage for at least three years following the expiration or termination for any reason of this Contract. The minimum limits of coverage specified above are not intended, and must not be construed; to limit any liability or indemnity of Contractor under this Contract to any indemnified party or other persons. Contractor is responsible for all deductibles with regard to the insurance. If the Contractor fails to pay any premium for required insurance as specified in this Contract, or if any insurer cancels or significantly reduces any required insurance as specified in this Contract without the State's written consent, then the State may, after the State has given the Contractor at least 30 days written notice, pay the premium. The State may deduct any part of the cost from any payment due the Contractor, or the Contractor must pay that cost upon demand by the State.

2.140 Indemnification

2.141 GENERAL INDEMNIFICATION

To the extent permitted by law, the Contractor must indemnify, defend and hold harmless the State from liability, including all claims and losses, and all related costs and expenses (including reasonable attorneys' fees and costs of investigation, litigation, settlement, judgments, interest and penalties), for bodily injury, death or damage to tangible property, excluding damage to software or files, accruing or resulting to any person, firm or corporation that may be injured or damaged by the Contractor in the performance of this Contract and that are attributable to the negligence or tortious acts of the Contractor or any of its Subcontractors, or by anyone else for whose acts any of them may be liable.

2.142 CODE INDEMNIFICATION

To the extent permitted by law, the Contractor shall indemnify, defend and hold harmless the State from any claim, loss, or expense arising from Contractor's breach of the No Surreptitious Code Warranty.

2.143 EMPLOYEE INDEMNIFICATION

In any claims against the State of Michigan, its departments, divisions, agencies, sections, commissions, officers, employees and agents, by any employee of the Contractor or any of its Subcontractors, the indemnification obligation under the Contract must not be limited in any way by the amount or type of damages, compensation or benefits payable by or for the Contractor or any of its Subcontractors under worker's disability compensation acts, disability benefit acts or other employee benefit acts. This indemnification clause is intended to be comprehensive. Any overlap in provisions, or the fact that greater specificity is provided as to some categories of risk, is not intended to limit the scope of indemnification under any other provisions.

2.144 PATENT/COPYRIGHT INFRINGEMENT INDEMNIFICATION

To the extent permitted by law, the Contractor must indemnify, defend and hold harmless the State from and against all losses, liabilities, damages (including taxes), and all related costs and expenses (including reasonable attorneys' fees and costs of investigation, litigation, settlement, judgments, interest and penalties) incurred in connection with any action or proceeding threatened or brought against the State to the extent that the action or proceeding is based on a claim that any Software, service, Work Product or Deliverable supplied



by the Contractor or its Subcontractors, or the operation of the Software, service, Work Product or Deliverable, or the use or reproduction of any documentation provided with the Software, service, Work Product or Deliverable infringes any United States patent, copyright, trademark or trade secret of any person or entity, which is enforceable under the laws of the United States.

In addition, should the Software, service, Work Product or Deliverable, or its operation, become or in the State's or Contractor's opinion be likely to become the subject of a claim of infringement, the Contractor must at the Contractor's sole expense (i) procure for the State the right to continue using the Software, service, Work Product or Deliverable or, if the option is not reasonably available to the Contractor, (ii) replace or modify to the State's reasonable satisfaction the same with Software, service, Work Product or Deliverable of equivalent function and performance so that it becomes non-infringing, or, if the option is not reasonably available to Contractor, (iii) accept its return by the State with appropriate credits to the State against the Contractor's charges and reimburse the State for any losses or costs incurred as a consequence of the State ceasing its use and returning it; provided that, such reimbursement for such losses or cost is subject to the Limitation of Liability set forth in section 2.220.

Notwithstanding the foregoing, the Contractor has no obligation to indemnify or defend the State for, or to pay any costs, damages or attorneys' fees related to, any claim based upon (i) Work Product or Deliverables developed based on written specifications of the State; (ii) use of the Software, Work Product or Deliverables in a configuration other than implemented or approved in writing by the Contractor, including, but not limited to, any modification of the same by the State; or (iii) the combination, operation, or use of the Software, Work Product or Deliverable with intellectual property or software not supplied by the Contractor under this Contract.

2.145 CONTINUATION OF INDEMNIFICATION OBLIGATIONS

The Contractor's duty to indemnify under this Section continues in full force and effect, notwithstanding the expiration or early cancellation of the Contract, with respect to any claims based on facts or conditions that occurred before expiration or cancellation.

2.146 INDEMNIFICATION PROCEDURES

The procedures set forth below must apply to all indemnity obligations under this Contract.

- (a) After the State receives notice of the action or proceeding involving a claim for which it shall seek indemnification, the State must promptly notify Contractor of the claim in writing and take or assist Contractor in taking, as the case may be, any reasonable action to avoid the imposition of a default judgment against Contractor. No failure to notify the Contractor relieves the Contractor of its indemnification obligations except to the extent that the Contractor can prove damages attributable to the failure. Within 20 days following receipt of written notice from the State relating to any claim, the Contractor must notify the State in writing whether Contractor agrees to assume control of the defense and settlement of that claim (a "Notice of Election"). After notifying Contractor of a claim and before the State receiving Contractor's Notice of Election, the State is entitled to defend against the claim, at the Contractor's expense, and the Contractor will be responsible for any reasonable costs incurred by the State in defending against the claim during that period.
- (b) If Contractor delivers a Notice of Election relating to any claim: (i) the State is entitled to participate in the defense of the claim and to employ counsel at its own expense to assist in the handling of the claim and to monitor and advise the State about the status and progress of the defense; (ii) the Contractor must, at the request of the State, demonstrate to the reasonable satisfaction of the State, the Contractor's financial ability to carry out its defense and indemnity obligations under this Contract; (iii) the Contractor must periodically advise the State about the status and progress of the defense and must obtain the prior written approval of the State before entering into any settlement of the claim or ceasing to defend against the claim and (iv) to the extent that any principles of Michigan governmental or public law may be involved or challenged, the State has the right, at its own expense, to control the defense of that portion of the claim involving the principles of Michigan governmental or public law. But the State may retain control of the defense and settlement of a claim by notifying the Contractor in writing within 10 days after the State's receipt of Contractor's information requested by the State under clause (ii) of this paragraph if the State determines that the Contractor has failed to demonstrate to the reasonable satisfaction of the State the Contractor's financial ability to carry out its defense and indemnity obligations under this Section



(in which event Contractor's indemnification obligations will not apply to such 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. In the event the insurer's attorney represents the State under this Section, the insurer's attorney may be required to be designated as a Special Assistant Attorney General by the Attorney General of the State of Michigan.

- (c) If Contractor does not deliver a Notice of Election to any claim of which it is notified by the State as provided above, the State may defend the claim in the manner as it may deem appropriate, at the cost and expense of Contractor. If it is determined that the claim was one against which Contractor was required to indemnify the State, upon request of the State, Contractor must promptly reimburse the State for all the reasonable costs and expenses.

2.150 Termination/Cancellation

2.151 NOTICE AND RIGHT TO CURE

If the Contractor breaches the contract, and the State in its sole discretion determines that the breach is curable, then the State shall provide the Contractor with written notice of the breach and a time period (not less than 30 days) to cure the Breach. The notice of breach and opportunity to cure is inapplicable for successive or repeated breaches or if the State determines in its sole discretion that the breach poses a serious and imminent threat to the health or safety of any person or the imminent loss, damage, or destruction of any real or tangible personal property.

2.152 TERMINATION FOR CAUSE

- (a) The State may terminate this contract, for cause, by notifying the Contractor in writing, if the Contractor (i) breaches any of its material duties or obligations under this Contract (including a Chronic Failure to meet any particular SLA), or (ii) fails to cure a breach within the time period specified in the written notice of breach provided by the State
- (b) If this Contract is terminated for cause, the Contractor must pay all costs incurred by the State in terminating this Contract, including but not limited to, State administrative costs, reasonable attorneys' fees and court costs, and any reasonable additional costs the State may incur to procure the Services/Deliverables required by this Contract from other sources. Re-procurement costs are not consequential, indirect or incidental damages, and cannot be excluded by any other terms otherwise included in this Contract, provided the costs are not in excess of 50% more than the prices for the Service/Deliverables provided under this Contract.
- (c) If the State chooses to partially terminate this Contract for cause, charges payable under this Contract shall be equitably adjusted to reflect those Services/Deliverables that are terminated and the State must pay for all Services/Deliverables for which Final Acceptance has been granted provided up to the termination date. Services and related provisions of this Contract that are terminated for cause must cease on the effective date of the termination.
- (d) If the State terminates this Contract for cause under this Section, and it is determined, for any reason, that Contractor was not in breach of contract under the provisions of this section, that termination for cause must be deemed to have been a termination for convenience, effective as of the same date, and the rights and obligations of the parties must be limited to that otherwise provided in this Contract for a termination for convenience.

2.153 TERMINATION FOR CONVENIENCE

The State may terminate this Contract for its convenience, in whole or part, if the State determines that a termination is in the State's best interest. Reasons for the termination must be left to the sole discretion of the State and may include, but not necessarily be limited to (a) the State no longer needs the Services or products specified in the Contract, (b) relocation of office, program changes, changes in laws, rules, or regulations make implementation of the Services no longer practical or feasible, (c) unacceptable prices for Additional Services or New Work requested by the State, or (d) falsification or misrepresentation, by inclusion or non-inclusion, of information material to a response to any RFP issued by the State. The State may terminate this Contract for its convenience, in whole or in part, by giving Contractor written notice at least 30 days before the date of termination. If the State chooses to terminate this Contract in part, the charges payable under this Contract must be equitably adjusted to reflect those Services/Deliverables that are terminated. Services and related



provisions of this Contract that are terminated for convenience must cease on the effective date of the termination.

2.154 TERMINATION FOR NON-APPROPRIATION

- (a) Contractor acknowledges that, if this Contract extends for several fiscal years, continuation of this Contract is subject to appropriation or availability of funds for this Contract. If funds to enable the State to effect continued payment under this Contract are not appropriated or otherwise made available, the State must terminate this Contract and all affected Statements of Work, in whole or in part, at the end of the last period for which funds have been appropriated or otherwise made available by giving written notice of termination to Contractor. The State must give Contractor at least 30 days advance written notice of termination for non-appropriation or unavailability (or the time as is available if the State receives notice of the final decision less than 30 days before the funding cutoff).
- (b) If funding for the Contract is reduced by law, or funds to pay Contractor for the agreed-to level of the Services or production of Deliverables to be provided by Contractor are not appropriated or otherwise unavailable, the State may, upon 30 days written notice to Contractor, reduce the level of the Services or change the production of Deliverables in the manner and for the periods of time as the State may elect. The charges payable under this Contract shall be equitably adjusted to reflect any equipment, services or commodities not provided by reason of the reduction.
- (c) If the State terminates this Contract, eliminates certain Deliverables, or reduces the level of Services to be provided by Contractor under this Section, the State must pay Contractor for all Work-in-Process performed through the effective date of the termination or reduction in level, as the case may be and as determined by the State, to the extent funds are available. This Section shall not preclude Contractor from reducing or stopping Services/Deliverables or raising against the State in a court of competent jurisdiction, any claim for a shortfall in payment for Services performed or Deliverables finally accepted before the effective date of termination.

2.155 TERMINATION FOR CRIMINAL CONVICTION

The State may terminate this Contract immediately and without further liability or penalty in the event Contractor, an officer of Contractor, or an owner of a 25% or greater share of Contractor is convicted of a criminal offense related to a State, public or private Contract or subcontract.

2.156 TERMINATION FOR APPROVALS RESCINDED

The State may terminate this Contract if any final administrative or judicial decision or adjudication disapproves a previously approved request for purchase of personal services under Constitution 1963, Article 11, § 5, and Civil Service Rule 7-1. In that case, the State shall pay the Contractor for only the work completed to that point under the Contract. Termination may be in whole or in part and may be immediate as of the date of the written notice to Contractor or may be effective as of the date stated in the written notice.

2.157 RIGHTS AND OBLIGATIONS UPON TERMINATION

- (a) If the State terminates this Contract for any reason, the Contractor must (a) stop all work as specified in the notice of termination, (b) take any reasonable action that may be necessary, or that the State may direct, for preservation and protection of Deliverables or other property derived or resulting from this Contract that may be in Contractor's possession, (c) return all materials and property provided directly or indirectly to Contractor by any entity, agent or employee of the State, (d) transfer title in, and deliver to, the State, unless otherwise directed, all Deliverables intended to be transferred to the State at the termination of the Contract and which are resulting from the Contract (which must be provided to the State on an "As-Is" basis except to the extent the amounts paid by the State in respect of the items included compensation to Contractor for the provision of warranty services in respect of the materials), and (e) take any reasonable action to mitigate and limit any potential damages, or requests for Contractor adjustment or termination settlement costs, to the maximum practical extent, including terminating or limiting as otherwise applicable those subcontracts and outstanding orders for material and supplies resulting from the terminated Contract.
- (b) If the State terminates this Contract before its expiration for its own convenience, the State must pay Contractor for all charges due for Services provided before the date of termination and, if applicable, as a separate item of payment under this Contract, for Work In Process, on a percentage of completion basis



at the level of completion determined by the State. Regardless of the basis for the termination, the State is not obligated to pay, or otherwise compensate, Contractor for any lost expected future profits, costs or expenses incurred with respect to Services not actually performed for the State.

- (c) Upon a good faith termination, the State may assume, at its option, any subcontracts and agreements for services and deliverables provided under this Contract, and may further pursue completion of the Services/Deliverables under this Contract by replacement contract or otherwise as the State may in its sole judgment deem expedient.

2.158 RESERVATION OF RIGHTS

Any termination of this Contract or any Statement of Work issued under it by a party must be with full reservation of, and without prejudice to, any rights or remedies otherwise available to the party with respect to any claims arising before or as a result of the termination.

2.160 Termination by Contractor

2.161 TERMINATION BY CONTRACTOR

If the State breaches the Contract, and the Contractor in its sole discretion determines that the breach is curable, then the Contractor will provide the State with written notice of the breach and a time period (not less than 30 days) to cure the breach. The Notice of Breach and opportunity to cure is inapplicable for successive and repeated breaches.

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, (iii) does not cure the breach within the time period specified in a written notice of breach, or (iv) materially violates Contractor's intellectual property. But the Contractor must discharge its obligations under **Section 2.160** before it terminates the Contract (except with regard to subsection (iv) of the preceding sentence).

2.170 Transition Responsibilities

2.171 CONTRACTOR TRANSITION RESPONSIBILITIES

If the State terminates this contract, for convenience or cause, or if the Contract is otherwise dissolved, voided, rescinded, nullified, expires or rendered unenforceable, the Contractor shall comply with direction provided by the State to assist in the orderly transition of equipment, services, software, leases, etc. to the State or a third party designated by the State. If this Contract expires or terminates, the Contractor agrees to make all reasonable efforts to effect an orderly transition of services within a period of time that in no event will exceed 360 days. These efforts must include, but are not limited to, those listed in **Section 2.150**.

2.172 CONTRACTOR PERSONNEL TRANSITION

The Contractor shall work with the State, or a specified third party, to develop a transition plan setting forth the specific tasks and schedule to be accomplished by the parties, to effect an orderly transition. The Contractor must allow as many personnel as practicable to remain on the job to help the State, or a specified third party, maintain the continuity and consistency of the services required by this Contract. In addition, during or following the transition period, in the event the State requires the Services of the Contractor's Subcontractors or vendors, as necessary to meet its needs, Contractor agrees to reasonably, and with good-faith, work with the State to use the Services of Contractor's Subcontractors or vendors. Contractor will notify all of Contractor's Subcontractors of procedures to be followed during transition.

2.173 CONTRACTOR INFORMATION TRANSITION

The Contractor shall provide reasonable non-proprietary detailed specifications for all Services/Deliverables needed by the State, or specified third party, to properly provide the Services/Deliverables required under this Contract. The Contractor will provide the State with state data generated from the inception of this Contract through the date on which this Contractor is terminated in a comma-delineated format unless otherwise requested by the State. The Contractor will deliver to the State any remaining owed reports and documentation still in Contractor's possession subject to appropriate payment by the State.



2.174 CONTRACTOR SOFTWARE TRANSITION

The Contractor shall reasonably assist the State in the acquisition of any Contractor software required to perform the Services/use the Deliverables under this Contract. This must include any documentation being used by the Contractor to perform the Services under this Contract. If the State transfers any software licenses to the Contractor, those licenses must, upon expiration of the Contract, transfer back to the State at their current revision level. Upon notification by the State, Contractor may be required to freeze all non-critical changes to Deliverables/Services.

2.175 TRANSITION PAYMENTS

If the transition results from a termination for any reason, the termination provisions of this Contract must govern reimbursement. If the transition results from expiration, the Contractor will be reimbursed for all reasonable transition costs (i.e. costs incurred within the agreed period after contract expiration that result from transition operations) at the rates agreed upon by the State. The Contractor will prepare an accurate accounting from which the State and Contractor may reconcile all outstanding accounts.

2.176 STATE TRANSITION RESPONSIBILITIES

In the event that this Contract is terminated, dissolved, voided, rescinded, nullified, or otherwise rendered unenforceable, the State agrees to reconcile all accounts between the State and the Contractor, complete any pending post-project reviews and perform any others obligations upon which the State and the Contractor agree.

- (a) Reconciling all accounts between the State and the Contractor;
- (b) Completing any pending post-project reviews.

2.180 Stop Work

2.181 STOP WORK ORDERS

The State may, at any time, by written Stop Work Order to Contractor, require that Contractor stop all, or any part, of the work called for by the Contract for a period of up to 90 calendar days after the Stop Work Order is delivered to Contractor, and for any further period to which the parties may agree. The Stop Work Order must be identified as a Stop Work Order and must indicate that it is issued under this **Section**. Upon receipt of the stop work order, Contractor must immediately comply with its terms and take all reasonable steps to minimize incurring costs allocable to the work covered by the Stop Work Order during the period of work stoppage. Within the period of the stop work order, the State must either: (a) cancel the stop work order; or (b) terminate the work covered by the Stop Work Order as provided in **Section 2.182**.

2.182 CANCELLATION OR EXPIRATION OF STOP WORK ORDER

The Contractor shall resume work if the State cancels a Stop Work Order or if it expires. The parties shall agree upon an equitable adjustment in the delivery schedule, personnel, the Contract price, or other affected material matters, and the Contract shall be modified, in writing, accordingly, if: (a) the Stop Work Order results in an increase in the time required for, personnel assigned to the project, Contractor's costs properly allocable to, or any other material matter relating to the performance of any part of the Contract; and (b) Contractor asserts its right to an equitable adjustment within 30 calendar days after the end of the period of work stoppage; provided that, if the State decides the facts justify the action, the State may receive and act upon a Contractor proposal submitted at any time before final payment under the Contract. Any adjustment will conform to the requirements of **Section 2.024**.

2.183 ALLOWANCE OF CONTRACTOR COSTS

If the Stop Work Order is not canceled and the work covered by the Stop Work Order is terminated for reasons other than material breach, the termination shall be deemed to be a termination for convenience under **Section 2.153**, and the State shall pay reasonable costs resulting from the Stop Work Order in arriving at the termination settlement. For the avoidance of doubt, the State shall not be liable to Contractor for loss of profits because of a Stop Work Order issued under this Section.



2.190 Dispute Resolution

2.191 IN GENERAL

Any claim, counterclaim, or dispute between the State and Contractor arising out of or relating to the Contract or any Statement of Work must be resolved as follows. For all Contractor claims seeking an increase in the amounts payable to Contractor under the Contract, or the time for Contractor's performance, Contractor must submit a letter, together with all data supporting the claims, executed by Contractor's Contract Administrator or the Contract Administrator's designee certifying that (a) the claim is made in good faith, (b) the amount claimed accurately reflects the adjustments in the amounts payable to Contractor or the time for Contractor's performance for which Contractor believes the State is liable and covers all costs of every type to which Contractor is entitled from the occurrence of the claimed event, and (c) the claim and the supporting data are current and complete to Contractor's best knowledge and belief.

2.192 INFORMAL DISPUTE RESOLUTION

- (a) All disputes between the parties shall be resolved under the Contract Management procedures in this Contract. If the parties are unable to resolve any dispute after compliance with the processes, the parties must meet with DTMB's Chief Procurement Officer, DTMB, or designee, to resolve the dispute without the need for formal legal proceedings, as follows:
 - (1) The representatives of Contractor and the State must meet as often as the parties reasonably deem necessary to gather and furnish to each other all information with respect to the matter at issue which the parties believe to be appropriate and germane in connection with its resolution. The representatives shall discuss the problem and negotiate in good faith in an effort to resolve the dispute without the necessity of any formal proceeding.
 - (2) During the course of negotiations, all reasonable requests made by one party to another for non-privileged information reasonably related to the Contract shall be honored in order that each of the parties may be fully advised of the other's position.
 - (3) The specific format for the discussions shall be left to the discretion of the designated State and Contractor representatives, but may include the preparation of agreed upon statements of fact or written statements of position.
 - (4) Following the completion of this process within 60 calendar days, the DTMB Chief Procurement Officer, or designee, shall issue a written opinion regarding the issue(s) in dispute within 30 calendar days. The opinion regarding the dispute must be considered the State's final action and the exhaustion of administrative remedies.
- (b) This Section shall not be construed to prevent either party from instituting, and a party is authorized to institute, formal proceedings earlier to avoid the expiration of any applicable limitations period or loss of any remedy at law or equity, to preserve a superior position with respect to other creditors, or under Section 2.193. Section 2.190 will not apply, in the discretion of the aggrieved party, to one party's breach of the other's intellectual property rights. Further, either party may seek any remedy at law or equity following resort to the informal dispute resolution procedure in Section 2.190 if such party determines the resulting resolution is insufficient.
- (c) The State shall not mediate disputes between the Contractor and any other entity, except state agencies, concerning responsibility for performance of work under the Contract.

2.193 INJUNCTIVE RELIEF

The only circumstance in which disputes between the State and Contractor shall not be subject to the provisions of **Section 2.192** is where a party makes a good faith determination that a breach of the terms of the Contract by the other party is that the damages to the party resulting from the breach shall be so immediate, so large or severe and so incapable of adequate redress after the fact that a temporary restraining order or other immediate injunctive relief is the only adequate remedy.

2.194 CONTINUED PERFORMANCE

Each party agrees to continue performing its obligations under the Contract while a dispute is being resolved except to the extent the issue in dispute precludes performance (dispute over payment must not be deemed to preclude performance) and without limiting either party's right to terminate the Contract as provided in **Section 2.150**, as the case may be.



2.200 Federal and State Contract Requirements

2.201 NONDISCRIMINATION

In the performance of the Contract, Contractor agrees not to discriminate against any employee or applicant for employment, with respect to his or her hire, tenure, terms, conditions or privileges of employment, or any matter directly or indirectly related to employment, because of race, color, religion, national origin, ancestry, age, sex, height, weight, and marital status, physical or mental disability. Contractor further agrees that every subcontract entered into for the performance of this Contract or any purchase order resulting from this Contract will contain a provision requiring non-discrimination in employment, as specified here, binding upon each Subcontractor. This covenant is required under the Elliot 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., and any breach of this provision may be regarded as a material breach of the Contract.

2.202 UNFAIR LABOR PRACTICES

Under 1980 PA 278, MCL 423.321, et seq., the State shall not award a Contract or subcontract to an employer whose name appears in the current register of employers failing to correct an unfair labor practice compiled under section 2 of the Act. This information is compiled by the United States National Labor Relations Board. A Contractor of the State, in relation to the Contract, shall not enter into a contract with a Subcontractor, manufacturer, or supplier whose name appears in this register. Under section 4 of 1980 PA 278, MCL 423.324, the State may void any Contract if, after award of the Contract, the name of Contractor as an employer or the name of the Subcontractor, manufacturer or supplier of Contractor appears in the register.

2.203 WORKPLACE SAFETY AND DISCRIMINATORY HARASSMENT

In performing Services for the State, the Contractor shall comply with the Department of Civil Services Rule 2-20 regarding Workplace Safety and Rule 1-8.3 regarding Discriminatory Harassment. In addition, the Contractor shall comply with Civil Service regulations and any applicable agency rules provided to the Contractor. For Civil Service Rules, see <http://www.mi.gov/mdcs/0,1607,7-147-6877---,00.html>.

2.204 PREVAILING WAGE

In the event the Contractor provides laborers under this Contract that are subject to the Michigan Department of Labor and Economic Development, Wage and Hour Bureau prevailing wage and fringe benefits, the wage rates and fringe benefits to be paid each class of individuals employed by the Contractor, its Subcontractors, their Subcontractors, and all persons involved with the performance of this Contract in privity of contract with the Contractor shall not be less than the wage rates and fringe benefits established by the Michigan Department of Labor and Economic Development, Wage and Hour Bureau, schedule of occupational classification and wage rates and fringe benefits for the local where the work is to be performed. The term Contractor shall include all general Contractors, prime Contractors, project managers, trade Contractors, and all of their Contractors or Subcontractors and persons in privity of contract with them.

The Contractor, its Subcontractors, their Subcontractors and all persons involved with the performance of this contract in privity of contract with the Contractor shall keep posted on the work site, in a conspicuous place, a copy of all wage rates and fringe benefits as prescribed in the Contract. Contractor shall also post, in a conspicuous place, the address and telephone number of the Michigan Department of Labor and Economic Development, the agency responsible for enforcement of the wage rates and fringe benefits. Contractor shall keep an accurate record showing the name and occupation of the actual wage and benefits paid to each individual employed in connection with this contract. This record shall be available to the State upon request for reasonable inspection.

If any trade is omitted from the list of wage rates and fringe benefits to be paid to each class of individuals by the Contractor, it is understood that the trades omitted shall also be paid not less than the wage rate and fringe benefits prevailing in the local where the work is to be performed.

2.210 Governing Law

**2.211 GOVERNING LAW**

The Contract shall in all respects be governed by, and construed according to, the substantive laws of the State of Michigan without regard to any Michigan choice of law rules that would apply the substantive law of any other jurisdiction to the extent not inconsistent with, or pre-empted by federal law.

2.212 COMPLIANCE WITH LAWS

Contractor shall comply with all applicable state, federal and local laws and ordinances in providing the Services/Deliverables.

2.213 JURISDICTION

Any dispute arising from the Contract shall be resolved in the State of Michigan. With respect to any claim between the parties, Contractor consents to venue in Ingham County, Michigan, and irrevocably waives any objections it may have to the jurisdiction on the grounds of lack of personal jurisdiction of the court or the laying of venue of the court or on the basis of forum non conveniens or otherwise. Contractor agrees to appoint agents in the State of Michigan to receive service of process. This provision is inapplicable to disputes relating to infringement of intellectual property that fall within the jurisdiction of U.S. Federal courts in Michigan.

2.220 Limitation of Liability**2.221 LIMITATION OF LIABILITY**

Neither the Contractor nor the State shall be liable to each other, regardless of the form of action, for consequential, incidental, indirect, or special damages. This limitation of liability does not apply to claims for infringement of United States patent, copyright, trademark or trade secrets; to claims for personal injury or damage to tangible property caused by the gross negligence or willful misconduct of the Contractor; to claims covered by other specific provisions of this Contract calling for liquidated damages; or to court costs or attorney's fees awarded by a court in addition to damages after litigation based on this Contract.

The Contractor's liability for damages to the State is limited to the value of the Contract. The foregoing limitation of liability does not apply to claims for infringement of United States patent, copyright, trademarks or trade secrets; to claims for personal injury or damage to tangible property caused by the gross negligence or willful misconduct of the Contractor; to claims covered by other specific provisions of this Contract calling for liquidated damages; or to court costs or attorney's fees awarded by a court in addition to damages after litigation based on this Contract.

The State's liability for damages to the Contractor is limited to the value of the Contract.

2.230 Disclosure Responsibilities**2.231 DISCLOSURE OF LITIGATION**

Contractor shall disclose any material criminal litigation, investigations or proceedings involving the Contractor (and each Subcontractor) or any of its officers or directors or any litigation, investigations or proceedings under the Sarbanes-Oxley Act. In addition, each Contractor (and each Subcontractor) shall notify the State of any material civil litigation, arbitration or proceeding which arises during the term of the Contract and extensions, to which Contractor (or, to the extent Contractor is aware, any Subcontractor) is a party, and which involves: (i) disputes that might reasonably be expected to adversely affect the viability or financial stability of Contractor or any Subcontractor; or (ii) a claim or written allegation of fraud against Contractor or, to the extent Contractor is aware, any Subcontractor by a governmental or public entity arising out of their business dealings with governmental or public entities. The Contractor shall disclose in writing to the Contract Administrator any litigation, investigation, arbitration or other proceeding (collectively, "Proceeding") within 30 days of Contractor learning of its occurrence. Details of settlements that are prevented from disclosure by the terms of the settlement may be annotated. Information provided to the State from Contractor's publicly filed documents referencing its material litigation shall be deemed to satisfy the requirements of this Section.



If any Proceeding disclosed to the State under this Section, or of which the State otherwise becomes aware, during the term of this Contract would cause a reasonable party to be concerned about:

- (a) the ability of Contractor (or a Subcontractor) to continue to perform this Contract according to its terms and conditions, or
- (b) whether Contractor (or a Subcontractor) in performing Services for the State is engaged in conduct which is similar in nature to conduct alleged in the Proceeding, which conduct would constitute a breach of this Contract or a violation of Michigan law, regulations or public policy, then the Contractor must provide the State all reasonable assurances requested by the State to demonstrate that:
 - (1) Contractor and its Subcontractors will be able to continue to perform this Contract and any Statements of Work according to its terms and conditions, and
 - (2) Contractor and its Subcontractors have not and will not engage in conduct in performing the Services which is similar in nature to the conduct alleged in the Proceeding.
- (c) If (a) or (b) of this section are applicable, then Contractor shall make the following notifications in writing:
 - (1) Within 30 days of Contractor becoming aware that a change in its ownership or officers has occurred, or is certain to occur, or a change that could result in changes in the valuation of its capitalized assets in the accounting records, Contractor must notify DTMB Procurement.
 - (2) Contractor shall also notify DTMB Procurement within 30 days whenever changes to asset valuations or any other cost changes have occurred or are certain to occur as a result of a change in ownership or officers.
 - (3) Contractor shall also notify DTMB Purchase Operations within 30 days whenever changes to company affiliations occur.

2.232 CALL CENTER DISCLOSURE

Contractor and/or all Subcontractors involved in the performance of this Contract providing call or contact center services to the State shall disclose the location of its call or contact center services to inbound callers. Failure to disclose this information is a material breach of this Contract.

2.233 BANKRUPTCY

The State may, without prejudice to any other right or remedy, terminate this Contract, in whole or in part, and, at its option, may take possession of the "Work in Process" and finish the Works in Process by whatever appropriate method the State may deem expedient if:

- (a) The Contractor files for protection under the bankruptcy laws;
- (b) An involuntary petition is filed against the Contractor and not removed within 30 days;
- (c) The Contractor becomes insolvent or if a receiver is appointed due to the Contractor's insolvency;
- (d) The Contractor makes a general assignment for the benefit of creditors; or
- (e) The Contractor or its affiliates are unable to provide reasonable assurances that the Contractor or its affiliates can deliver the services under this Contract.

2.240 Performance

2.241 TIME OF PERFORMANCE

- (a) Contractor shall use commercially reasonable efforts to provide the resources necessary to complete all Services and Deliverables according to the time schedules contained in the Statements of Work and other Exhibits governing the work, and with professional quality.
- (b) Without limiting the generality of **Section 2.241**, Contractor shall notify the State in a timely manner upon becoming aware of any circumstances that may reasonably be expected to jeopardize the timely and successful completion of any Deliverables/Services on the scheduled due dates in the latest State-approved delivery schedule and must inform the State of the projected actual delivery date.
- (c) If the Contractor believes that a delay in performance by the State has caused or will cause the Contractor to be unable to perform its obligations according to specified Contract time periods, the Contractor must notify the State in a timely manner and must use commercially reasonable efforts to perform its obligations according to the Contract time periods notwithstanding the State's failure. Contractor will not be in default for a delay in performance to the extent the delay is caused by the State.



2.242 SERVICE LEVEL AGREEMENT (SLA)

- (a) In the event an SLA is identified in a Statement of Work and is specifically identified as such, then it will be completed with the following operational considerations:
 - (1) SLAs will not be calculated for individual Incidents where any event of Excusable Failure has been determined; Incident means any interruption in Services.
 - (2) SLAs will not be calculated for individual Incidents where loss of service is planned and where the State has received prior notification or coordination.
 - (3) SLAs will not apply if the applicable Incident could have been prevented through planning proposed by Contractor and not implemented at the request of the State. To invoke this consideration, complete documentation relevant to the denied planning proposal must be presented to substantiate the proposal.
 - (4) Time period measurements will be based on the time Incidents are received by the Contractor and the time that the State receives notification of resolution based on 24x7x365 time period, except that the time period measurement will be suspended based on the following:
 - (i) Time period(s) will not apply where Contractor does not have access to a physical State Location and where access to the State Location is necessary for problem identification and resolution.
 - (ii) Time period(s) will not apply where Contractor needs to obtain timely and accurate information or appropriate feedback and is unable to obtain timely and accurate information or appropriate feedback from the State.
- (b) Chronic Failure for any Service(s) will be defined as three unscheduled outage(s) or interruption(s) on any individual Service for the same reason or cause or if the same reason or cause was reasonably discoverable in the first instance over a rolling 30 day period. Chronic Failure will result in the State's option to terminate the effected individual Service(s) and procure them from a different vendor for the chronic location(s) with Contractor to pay the difference in charges for up to three additional months. The termination of the Service will not affect any tiered pricing levels.
- (c) Root Cause Analysis will be performed on any Business Critical outage(s) or outage(s) on Services when requested by the Contract Administrator. Contractor will provide its analysis within two weeks of outage(s) and provide a recommendation for resolution.
- (d) All decimals must be rounded to two decimal places with five and greater rounding up and four and less rounding down unless otherwise specified.

2.243 RESERVED - LIQUIDATED DAMAGES

2.244 EXCUSABLE FAILURE

Neither party will be liable for any default, damage or delay in the performance of its obligations under the Contract to the extent the default, damage or delay is caused by government regulations or requirements (executive, legislative, judicial, military or otherwise), power failure, electrical surges or current fluctuations, lightning, earthquake, war, water or other forces of nature or acts of God, delays or failures of transportation, equipment shortages, suppliers' failures, or acts or omissions of common carriers, fire; riots, civil disorders; strikes or other labor disputes, embargoes; injunctions (provided the injunction was not issued as a result of any fault or negligence of the party seeking to have its default or delay excused); or any other cause beyond the reasonable control of a party; provided the non-performing party and its Subcontractors are without fault in causing the default or delay, and the default or delay could not have been prevented by reasonable precautions and cannot reasonably be circumvented by the non-performing party through the use of alternate sources, workaround plans or other means, including disaster recovery plans.

If a party does not perform its contractual obligations for any of the reasons listed above, the non-performing party will be excused from any further performance of its affected obligation(s) for as long as the circumstances prevail. But the party must use commercially reasonable efforts to recommence performance whenever and to whatever extent possible without delay. A party must promptly notify the other party in writing immediately after the excusable failure occurs, and also when it abates or ends.

If any of the above-enumerated circumstances substantially prevent, hinder, or delay the Contractor's performance of the Services/provision of Deliverables for more than 10 Business Days, and the State determines that performance is not likely to be resumed within a period of time that is satisfactory to the State



in its reasonable discretion, then at the State's option: (a) the State may procure the affected Services/Deliverables from an alternate source, and the State is not be liable for payment for the unperformed Services/ Deliverables not provided under the Contract for so long as the delay in performance continues; (b) the State may terminate any portion of the Contract so affected and the charges payable will be equitably adjusted to reflect those Services/Deliverables terminated; or (c) the State may terminate the affected Statement of Work without liability to Contractor as of a date specified by the State in a written notice of termination to the Contractor, except to the extent that the State must pay for Services/Deliverables provided through the date of termination.

The Contractor will not have the right to any additional payments from the State as a result of any Excusable Failure occurrence or to payments for Services not rendered/Deliverables not provided as a result of the Excusable Failure condition. Defaults or delays in performance by Contractor which are caused by acts or omissions of its Subcontractors will not relieve Contractor of its obligations under the Contract except to the extent that a Subcontractor is itself subject to an Excusable Failure condition described above and Contractor cannot reasonably circumvent the effect of the Subcontractor's default or delay in performance through the use of alternate sources, workaround plans or other means.

2.250 Approval of Deliverables

2.251 DELIVERY OF DELIVERABLES

A list of the Deliverables to be prepared and delivered by Contractor including, for each Deliverable, the scheduled delivery date and a designation of whether the Deliverable is a document ("Written Deliverable") or a Work Product relating to the Software (a "Custom Software Deliverable") is included in the Contract. All Deliverables shall be completed and delivered for State review and written approval and, where applicable, installed in accordance with the State-approved delivery schedule and any other applicable terms and conditions of this Contract.

Prior to delivering any Deliverable to the State, Contractor will first perform all required quality assurance activities, and, in the case of Custom Software Deliverables, System Testing to verify that the Deliverable is complete and in conformance with its specifications. Before delivering a Deliverable to the State, Contractor shall certify to the State that (1) it has performed such quality assurance activities, (2) it has performed any applicable testing, (3) it has corrected all material deficiencies discovered during such quality assurance activities and testing, (4) the Deliverable is in a suitable state of readiness for the State's review and approval, and (5) the Deliverable/Service has all critical security patches/updates applied.

In discharging its obligations under this Section, Contractor shall be at all times (except where the parties agree otherwise in writing) in compliance with Level 3 of the Software Engineering Institute's Capability Maturity Model for Software ("CMM Level 3") or its material equivalent.

2.252 CONTRACTOR SYSTEM TESTING

Contractor will be responsible for System Testing each Custom Software Deliverable in Contractor's development environment prior to turning over the Custom Software Deliverable to the State for User Acceptance Testing and approval. The State shall provide an appropriate test environment for such System Testing. Contractor's System Testing shall include the following, at a minimum, plus any other testing required by CMM Level 3 (or its material equivalent) or Contractor's system development methodology:

Contractor will be responsible for performing Unit Testing and incremental Integration Testing of the components of each Custom Software Deliverable.

Contractor's System Testing will also include Integration Testing of each Custom Software Deliverable to ensure proper inter-operation with all prior software Deliverables, interfaces and other components that are intended to inter-operate with such Custom Software Deliverable, and will include Regression Testing, volume and stress testing to ensure that the Custom Software Deliverables are able to meet the State's projected growth in the number and size of transactions to be processed by the Application and number of users, as such projections are set forth in the applicable Statement of Work.



Contractor's System Testing will also include Business Function Testing and Technical Testing of each Application in a simulated production environment. Business Function Testing will include testing of full work streams that flow through the Application as the Application will be incorporated within the State's computing environment. The State shall participate in and provide support for the Business Function Testing to the extent reasonably requested by Contractor. Within ten (10) days before the commencement of Business Function Testing pursuant to this Section, Contractor shall provide the State for State review and written approval Contractor's test plan for Business Function Testing.

Within five (5) Business Days following the completion of System Testing pursuant to this **Section**, Contractor shall provide to the State a testing matrix establishing that testing for each condition identified in the System Testing plans has been conducted and successfully concluded. To the extent that testing occurs on State premises, the State shall be entitled to observe or otherwise participate in testing under this Section as the State may elect.

2.253 APPROVAL OF DELIVERABLES, IN GENERAL

All Deliverables (Written Deliverables and Custom Software Deliverables) require formal written approval by the State, in accordance with the following procedures. Formal approval by the State requires that the Deliverable be confirmed in writing by the State to meet its specifications set forth in the applicable Statement of Work, which, in the case of Custom Software Deliverables, will include the successful completion of State User Acceptance Testing, to be led by the State with the support and assistance of Contractor. The parties acknowledge that the approval process set forth herein will be facilitated by ongoing consultation between the parties, visibility of interim and intermediate Deliverables and collaboration on key decisions.

The State's obligation to comply with any State Review Period is conditioned on the timely delivery of Deliverables being reviewed. If Contractor fails to provide a Deliverable to the State in a timely manner, the State will nevertheless use commercially reasonable efforts to complete its review or testing within the applicable State Review Period.

Before commencement of its review or testing of a Deliverable, the State may inspect the Deliverable to confirm that all components of the Deliverable (e.g., software, associated documentation, and other materials) have been delivered. If the State determines that the Deliverable is incomplete, the State may refuse delivery of the Deliverable without performing any further inspection or testing of the Deliverable. Otherwise, the review period will be deemed to have started on the day the State receives the Deliverable and the applicable certification by Contractor in accordance with this Section.

The State will approve in writing a Deliverable upon confirming that it conforms to and, in the case of a Custom Software Deliverable, performs in accordance with, its specifications without material deficiency. The State may, but shall not be required to, conditionally approve in writing a Deliverable that contains material deficiencies if the State elects to permit Contractor to rectify them post-approval. In any case, Contractor will be responsible for working diligently to correct within a reasonable time at Contractor's expense all deficiencies in the Deliverable that remain outstanding at the time of State approval.

If, after three (3) opportunities (the original and two repeat efforts), Contractor is unable to correct all deficiencies preventing State approval of a Deliverable, (i) the State may demand that Contractor refund any fees paid for the deliverable at issue and terminate the Contract in whole or in part or (ii) the State may terminate this Contract for default, either in whole or in part by notice to Contractor (and without the need to afford Contractor any further opportunity to cure), or (iii) Contractor may refund any fees paid for the deliverable or services at issue and terminate the Contract. Notwithstanding the foregoing, the State shall not use, as a basis for exercising its termination rights under this Section, deficiencies discovered in a repeat State Review Period that could reasonably have been discovered during a prior State Review Period.

The State, at any time and in its own discretion, may halt the UAT or approval process if such process reveals deficiencies in or problems with a Deliverable in a sufficient quantity or of a sufficient severity as to make the continuation of such process unproductive or unworkable. In such case, the State may notify Contractor of the issues discovered under UAT, and if necessary, return the applicable Deliverable to Contractor for correction



and re-delivery prior to resuming the review or UAT process and, in that event, Contractor will correct the deficiencies in such Deliverable in accordance with the Contract, as the case may be.

Approval in writing of a Deliverable by the State shall be provisional; that is, such approval shall not preclude the State from later identifying deficiencies in, and declining to accept, a subsequent Deliverable based on or which incorporates or inter-operates with an approved Deliverable, to the extent that the results of subsequent review or testing indicate the existence of deficiencies in the subsequent Deliverable, or if the Application of which the subsequent Deliverable is a component otherwise fails to be accepted pursuant to **Section 2.080**.

2.254 PROCESS FOR APPROVAL OF WRITTEN DELIVERABLES

The State Review Period for Written Deliverables will be the number of days set forth in the applicable Statement of Work following delivery of the final version of the Written Deliverable (failing which the State Review Period, by default, shall be five (5) Business Days for Written Deliverables of one hundred (100) pages or less and ten (10) Business Days for Written Deliverables of more than one hundred (100) pages). The duration of the State Review Periods will be doubled if the State has not had an opportunity to review an interim draft of the Written Deliverable prior to its submission to the State. The State agrees to notify Contractor in writing by the end of the State Review Period either stating that the Written Deliverable is approved in the form delivered by Contractor or describing any deficiencies that shall be corrected prior to approval of the Written Deliverable (or at the State's election, subsequent to approval of the Written Deliverable). If the State delivers to Contractor a notice of deficiencies, Contractor will correct the described deficiencies and within five (5) Business Days resubmit the Deliverable in a form that shows all revisions made to the original version delivered to the State. Contractor's correction efforts will be made at no additional charge. Upon receipt of a corrected Written Deliverable from Contractor, the State will have a reasonable additional period of time, not to exceed the length of the original State Review Period, to review the corrected Written Deliverable to confirm that the identified deficiencies have been corrected.

2.255 PROCESS FOR APPROVAL OF CUSTOM SOFTWARE DELIVERABLES

The State will conduct UAT of each Custom Software Deliverable in accordance with the following procedures to determine whether it meets the criteria for State approval – i.e., whether it conforms to and performs in accordance with its specifications without material deficiencies.

Within thirty (30) days (or such other number of days as the parties may agree to in writing) prior to Contractor's delivery of any Custom Software Deliverable to the State for approval, Contractor shall provide to the State a set of proposed test plans, including test cases, scripts, data and expected outcomes, for the State's use (which the State may supplement in its own discretion) in conducting UAT of the Custom Software Deliverable. Contractor, upon request by the State, shall provide the State with reasonable assistance and support during the UAT process.

For the Custom Software Deliverables listed in an attachment, the State Review Period for conducting UAT will be as indicated in the attachment. For any other Custom Software Deliverables not listed in an attachment, the State Review Period shall be the number of days agreed in writing by the parties (failing which it shall be forty-five (45) days by default). The State Review Period for each Custom Software Deliverable will begin when Contractor has delivered the Custom Software Deliverable to the State accompanied by the certification required by this **Section** and the State's inspection of the Deliverable has confirmed that all components of it have been delivered.

The State's UAT will consist of executing test scripts from the proposed testing submitted by Contractor, but may also include any additional testing deemed appropriate by the State. If the State determines during the UAT that the Custom Software Deliverable contains any deficiencies, the State will notify Contractor of the deficiency by making an entry in an incident reporting system available to both Contractor and the State. Contractor will modify promptly the Custom Software Deliverable to correct the reported deficiencies, conduct appropriate System Testing (including, where applicable, Regression Testing) to confirm the proper correction of the deficiencies and re-deliver the corrected version to the State for re-testing in UAT. Contractor will coordinate the re-delivery of corrected versions of Custom Software Deliverables with the State so as not to disrupt the State's UAT process. The State will promptly re-test the corrected version of the Software Deliverable after receiving it from Contractor.



Within three (3) business days after the end of the State Review Period, the State will give Contractor a written notice indicating the State's approval or rejection of the Custom Software Deliverable according to the criteria and process set out in this **Section**.

2.256 FINAL ACCEPTANCE

"Final Acceptance" for each phase shall be considered to occur when the Deliverables to be delivered have been approved by the State and have been operating in production without any deficiency for thirty (30) consecutive days. The State in its sole discretion shall determine if and when to approve moving the solution to production for each rollout.

Final Acceptance of the project will occur after acceptance of all phases defined within the Statement of Work.

2.260 Ownership

2.261 OWNERSHIP OF WORK PRODUCT

The State owns all Deliverables, as they are work made for hire by the Contractor for the State, that are Written Deliverables that (i) are specific to Customer's unique requirements and (ii) do not contain any Confidential Information or intellectual property of Contractor. The State owns all United States and international copyrights, trademarks, patents or other proprietary rights in the Deliverables described in the preceding sentence.

Other than as set forth in the preceding paragraph, ownership of all Work Product and Deliverables will remain with Contractor or its licensors at all times. Contractor grants the State a nonexclusive, nontransferable, non-assignable, royalty-free license to use the Work Product and Deliverables only with the Software with which the Work Product operates and only for as long as the State maintains a license for such Software.

2.262 VESTING OF RIGHTS

With the sole exception of any preexisting licensed works, the Contractor assigns, and upon creation of each Written Deliverable automatically assigns, to the State, ownership of all United States and international copyrights, trademarks, patents, or other proprietary rights in each and every Written Deliverable, whether or not registered by the Contractor, insofar as any the Written Deliverable, by operation of law, may not be considered work made for hire by the Contractor for the State. From time to time upon the State's request, the Contractor must confirm the assignment by execution and delivery of the assignments, confirmations of assignment, or other written instruments as the State may request. The State may obtain and hold in its own name all copyright, trademark, and patent registrations and other evidence of rights that may be available for such Written Deliverables.

2.263 RIGHTS IN DATA

The State is the owner of all data made available by the State to the Contractor or its agents, Subcontractors or representatives under the Contract. The Contractor will not use the State's data for any purpose other than providing the Services, nor will any part of the State's data be disclosed, sold, assigned, leased or otherwise disposed of to the general public or to specific third parties or commercially exploited by or on behalf of the Contractor. No employees of the Contractor, other than those on a strictly need-to-know basis, have access to the State's data. Contractor will not possess or assert any lien or other right against the State's data. Without limiting the generality of this Section, the Contractor must only use personally identifiable information as strictly necessary to provide the Services and must disclose the information only to its employees who have a strict need-to-know the information. The Contractor must comply at all times with all laws and regulations applicable to the personally identifiable information.

The State is the owner of all State-specific data under the Contract. The State may use the data provided by the Contractor for any purpose. The State will not possess or assert any lien or other right against the Contractor's data. Without limiting the generality of this Section, the State may use personally identifiable information only as strictly necessary to utilize the Services and must disclose the information only to its employees who have a strict need to know the information, except as provided by law. The State must comply at all times with all laws and regulations applicable to the personally identifiable information. Other material developed and provided to the State remains the State's sole and exclusive property.



2.264 OWNERSHIP OF MATERIALS

The State and the Contractor will continue to own their respective proprietary technologies developed before entering into the Contract. Any hardware bought through the Contractor by the State, and paid for by the State, will be owned by the State. Any software licensed through the Contractor and sold to the State, will be licensed directly to the State.

2.270 State Standards

2.271 EXISTING TECHNOLOGY STANDARDS

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>.

2.272 ACCEPTABLE USE POLICY

To the extent that Contractor has access to the State computer system, Contractor must comply with the State's Acceptable Use Policy, see http://www.michigan.gov/documents/dmb/1460.00_184733_7.pdf. All Contractor employees must be required, in writing, to agree to the State's Acceptable Use Policy before accessing the State system. The State reserves the right to terminate Contractor's access to the State system if a violation occurs.

2.273 SYSTEMS CHANGES

Contractor is not responsible for and not authorized to make changes to any State systems without written authorization from the Project Manager. Any changes Contractor makes to State systems with the State's approval must be done according to applicable State procedures, including security, access and configuration management procedures.

2.280 Extended Purchasing

2.281 MIDEAL (MICHIGAN DELIVERY EXTENDED AGREEMENTS LOCALLY)

Public Act 431 of 1984 permits DTMB to provide purchasing services to any city, village, county, township, school district, intermediate school district, non-profit hospital, institution of higher education, community, or junior college. A current listing of approved program members is available at: www.michigan.gov/buymichiganfirst. Unless otherwise stated, the Contractor must ensure that the non-state agency is an authorized purchaser before extending the Contract pricing.

The Contractor will supply Contract Services and equipment to these local governmental agencies at the established State of Michigan contract prices and terms to the extent applicable and where available. The Contractor must send its invoices to, and pay the local unit of government, on a direct and individual basis.

To the extent that authorized local units of government purchase quantities of Services and/or equipment under this Contract, the quantities of Services and/or equipment purchased will be included in determining the appropriate rate wherever tiered pricing based on quantity is provided.

Please Visit MiDEAL at www.michigan.gov/buymichiganfirst under MiDEAL.

Estimated requirements for authorized local units of government are not included in the quantities shown in this Contract.

2.282 RESERVED - STATE EMPLOYEE PURCHASES

2.290 Environmental Provision

In the event the Contractor provides products other than software or related services, the following sections apply.

2.291 ENVIRONMENTAL PROVISION

Energy Efficiency Purchasing Policy: The State seeks wherever possible to purchase energy efficient products. This includes giving preference to U.S. Environmental Protection Agency (EPA) certified 'Energy Star' products for any category of products for which EPA has established Energy Star certification. For other



purchases, the State may include energy efficiency as one of the priority factors to consider when choosing among comparable products.

Environmental Purchasing Policy: The State of Michigan is committed to encouraging the use of products and services that impact the environment less than competing products. The State is accomplishing this by including environmental considerations in purchasing decisions, while remaining fiscally responsible, to promote practices that improve worker health, conserve natural resources, and prevent pollution. Environmental components that are to be considered include: recycled content and recyclables; energy efficiency; and the presence of undesirable materials in the products, especially those toxic chemicals which are persistent and bioaccumulative. The Contractor should be able to supply products containing recycled and environmentally preferable materials that meet performance requirements and is encouraged to offer such products throughout the duration of this Contract. Information on any relevant third party certification (such as Green Seal, Energy Star, etc.) should also be provided.

Hazardous Materials: For the purposes of this Section, "Hazardous Materials" is a generic term used to describe asbestos, ACBMs, PCBs, petroleum products, construction materials including paint thinners, solvents, gasoline, oil, and any other material the manufacture, use, treatment, storage, transportation or disposal of which is regulated by the federal, state or local laws governing the protection of the public health, natural resources or the environment. This includes, but is not limited to, materials the as batteries and circuit packs, and other materials that are regulated as (1) "Hazardous Materials" under the Hazardous Materials Transportation Act, (2) "chemical hazards" under the Occupational Safety and Health Administration standards, (3) "chemical substances or mixtures" under the Toxic Substances Control Act, (4) "pesticides" under the Federal Insecticide Fungicide and Rodenticide Act, and (5) "hazardous wastes" as defined or listed under the Resource Conservation and Recovery Act.

- (a) The Contractor shall use, handle, store, dispose of, process, transport and transfer any material considered a Hazardous Material according to all federal, State and local laws. The State shall provide a safe and suitable environment for performance of Contractor's Work. Before the commencement of Work, the State shall advise the Contractor of the presence at the work site of any Hazardous Material to the extent that the State is aware of the Hazardous Material. If the Contractor encounters material reasonably believed to be a Hazardous Material and which may present a substantial danger, the Contractor shall immediately stop all affected Work, notify the State in writing about the conditions encountered, and take appropriate health and safety precautions.
- (b) Upon receipt of a written notice, the State will investigate the conditions. If (a) the material is a Hazardous Material that may present a substantial danger, and (b) the Hazardous Material was not brought to the site by the Contractor, or does not result in whole or in part from any violation by the Contractor of any laws covering the use, handling, storage, disposal of, processing, transport and transfer of Hazardous Materials, the State shall order a suspension of Work in writing. The State shall proceed to have the Hazardous Material removed or rendered harmless. In the alternative, the State shall terminate the affected Work for the State's convenience.
- (c) Once the Hazardous Material has been removed or rendered harmless by the State, the Contractor shall resume Work as directed in writing by the State. Any determination by the Michigan Department of Community Health or the Michigan Department of Environmental Quality that the Hazardous Material has either been removed or rendered harmless is binding upon the State and Contractor for the purposes of resuming the Work. If any incident with Hazardous Material results in delay not reasonable anticipatable under the circumstances and which is attributable to the State, the applicable SLAs for the affected Work will not be counted in a time as mutually agreed by the parties.
- (d) If the Hazardous Material was brought to the site by the Contractor, or results in whole or in part from any violation by the Contractor of any laws covering the use, handling, storage, disposal of, processing, transport and transfer of Hazardous Material, or from any other act or omission within the control of the Contractor, the Contractor shall bear its proportionate share of the delay and costs involved in cleaning up the site and removing and rendering harmless the Hazardous Material according to Applicable Laws to the condition approved by applicable regulatory agency(ies).



Labeling: Michigan has a Consumer Products Rule pertaining to labeling of certain products containing volatile organic compounds. For specific details visit http://www.michigan.gov/deq/0,1607,7-135-3310_4108-173523--,00.html

Refrigeration and Air Conditioning: The Contractor shall comply with the applicable requirements of Sections 608 and 609 of the Clean Air Act (42 U.S.C. 7671g and 7671h) as each or both apply to this contract.

Environmental Performance: Waste Reduction Program - Contractor shall establish a program to promote cost-effective waste reduction in all operations and facilities covered by this contract. The Contractor's programs shall comply with applicable Federal, State, and local requirements, specifically including Section 6002 of the Resource Conservation and Recovery Act (42 U.S.C. 6962, et seq.).

2.300 Deliverables

Upon the State's payment of mutually agreeable fees therefor, Contractor agrees to provide the professional services described in any Statement of Work attached hereto and made a part hereof ("Services") including, if applicable any deliverables described in the Statement of Work ("Deliverables") and a limited license to any Deliverables consisting of computer code, documentation or other materials included in any Deliverables and delivered by Contractor in connection with the Services ("Work Product").

2.301 SOFTWARE

A list of the items of related software the State is required to purchase for executing the Contract is attached in Appendix B, Table 2. The list includes all software required to complete the Contract and make the Deliverables operable; if any additional software is required in order for the Deliverables to meet the requirements of this Contract, such software shall be provided to the State by Contractor at no additional charge (except where agreed upon and specified in a Statement of Work or Contract Change Notice). The attachment also identifies certain items of software to be provided by the State.

2.302 RESERVED - HARDWARE

2.303 RESERVED - EQUIPMENT TO BE NEW

2.304 RESERVED - EQUIPMENT TO BE NEW AND PROHIBITED PRODUCTS

2.310 Software Warranties

2.311 PERFORMANCE WARRANTY

Warranty applicable to Software is set forth in Appendix G hereto.

2.312 NO SURREPTITIOUS CODE WARRANTY

The Contractor represents and warrants that no copy of licensed Software provided to the State contains or will contain any Self-Help Code or any Unauthorized Code as defined below. This warranty is referred to in this Contract as the "No Surreptitious Code Warranty."

As used in this Contract, "Self-Help Code" means any back door, time bomb, drop dead device, or other software routine designed to disable a computer program automatically with the passage of time or under the positive control of a person other than the licensee of the software. Self-Help Code does not include Software routines in a computer program, if any, designed to permit an owner of the computer program (or other person acting by authority of the owner) to obtain access to a licensee's computer system(s) (e.g. remote access via modem) for purposes of maintenance or technical support. Contractor and State agree that SAS' Product Authorization Codes are necessary for use of the Software and are not a violation of this Section. Following the applicable annual license period, SAS's Product Authorization Code will continue to operate for a period of ninety (90) days and includes automatic notices to prompt the State to renew their software license.



As used in this Contract, "Unauthorized Code" means any virus, Trojan horse, spyware, worm or other Software routines or components designed to permit unauthorized access to disable, erase, or otherwise harm software, equipment, or data; or to perform any other such actions. The term Unauthorized Code does not include Self-Help Code. Unauthorized Code does not include Software routines in a computer program, if any, designed to permit an owner of the computer program (or other person acting by authority of the owner) to obtain access to a licensee's computer system(s) (e.g. remote access via modem) for purposes of maintenance or technical support.

In addition, Contractor will use up-to-date commercial virus detection software to detect and remove any viruses from any Software prior to delivering it to the State.

2.313 CALENDAR WARRANTY

The Contractor represents and warrants that all Software for which the Contractor either sells or licenses to the State of Michigan and used by the State prior to, during or after the calendar year 2000, includes or shall include, at no added cost to the State, design and performance so the State shall not experience software abnormality and/or the generation of incorrect results from the software, due to date oriented processing, in the operation of the business of the State of Michigan.

The software design, to insure calendar year rollover compatibility, shall include, but is not limited to: data structures (databases, data files, etc.) that provide 4-digit date century; stored data that contain date century recognition, including, but not limited to, data stored in databases and hardware device internal system dates; calculations and program logic (e.g., sort algorithms, calendar generation, event recognition, and all processing actions that use or produce date values) that accommodates same century and multi-century formulas and date values; interfaces that supply data to and receive data from other systems or organizations that prevent non-compliant dates and data from entering any State system; user interfaces (i.e., screens, reports, etc.) that accurately show 4 digit years; and assurance that the year 2000 shall be correctly treated as a leap year within all calculation and calendar logic.

2.314 THIRD-PARTY SOFTWARE WARRANTY

The Contractor represents and warrants that it will disclose the use or incorporation of any third-party software into the Deliverables that require separate licensing from the Software. At the time of Delivery, the Contractor shall provide in writing the name and use of such Third-party Software, including information regarding the Contractor's authorization to include and utilize such software.

2.315 PHYSICAL MEDIA WARRANTY

Contractor represents and warrants that each licensed copy of the Software provided by the Contractor is free from physical defects in the media that tangibly embodies the copy. This warranty does not apply to defects discovered more than (30) thirty days after that date of Final Acceptance of the Software by the State. This warranty does not apply to defects arising from acts of Excusable Failure. If the Contractor breaches this warranty, then the State shall be entitled to replacement of the non-compliant copy by Contractor, at Contractor's expense (including shipping and handling).

2.320 Software Licensing

A list of the items of SAS Institute Inc. software ("Software") the State is required to license for executing the Contract is attached in the Supplement in Appendix G. The terms and conditions governing the Software and the State's license of such Software are set forth in Appendix G hereto, and, with regard to Software, such terms will take precedence over the terms set forth elsewhere in this Contract.

2.321 CROSS-LICENSE, DELIVERABLES ONLY, LICENSE TO CONTRACTOR

The State grants to the Contractor, the royalty-free, world-wide, non-exclusive right and license under any Deliverable now or in the future owned by the State, or with respect to which the State has a right to grant such rights or licenses, to the extent required by the Contractor to market the Deliverables and exercise its full rights in the Deliverables, including, without limitation, the right to make, use and sell products and services based on or incorporating such Deliverables.

**2.322 CROSS-LICENSE, DELIVERABLES AND DERIVATIVE WORK, LICENSE TO CONTRACTOR**

The State grants to the Contractor, the royalty-free, world-wide, non-exclusive right and license under any Deliverable and/or Derivative Work now or in the future owned by the State, or with respect to which the State has a right to grant such rights or licenses, to the extent required by the Contractor to market the Deliverables and/or Derivative Work and exercise its full rights in the Deliverables and/or Derivative Work, including, without limitation, the right to make, use and sell products and services based on or incorporating such Deliverables and/or Derivative Work.

2.323 RESERVED - LICENSE BACK TO THE STATE**2.324 RESERVED - LICENSE RETAINED BY CONTRACTOR****2.325 RESERVED - PRE-EXISTING MATERIALS FOR CUSTOM SOFTWARE DELIVERABLES****2.330 RESERVED - Source Code Escrow**



Glossary

Days	Means calendar days unless otherwise specified.
24x7x365	Means 24 hours a day, seven days a week, and 365 days a year (including the 366th day in a leap year).
Additional Service	Means any Services/Deliverables within the scope of the Contract, but not specifically provided under any Statement of Work, that once added will result in the need to provide the Bidder with additional consideration.
Agency	State of Michigan Unemployment Insurance Agency, Department of Energy, Labor and Economic Growth
Audit Period	See Section 2.110
Base Period	<p>The four consecutive calendar quarters used in determining an individual's eligibility for unemployment insurance. The period is the first four of the last five completed calendar quarters immediately preceding the first day of an individual's benefit year. The way the base period is measured doesn't count the claimant's most recent employment. Depending on when the claim is filed, almost six months of work might not be included in the base period. NOTE- MI has standard and alternate base periods AND Alternate Earnings Qualifier.</p> <ul style="list-style-type: none"> • Standard Base Period: The first 4 of the last 5 completed calendar quarters before the first day of the individual's benefit year. If a claimant cannot qualify for benefits using the standard base period, then the wage paid in the alternate base period are considered. • Alternate Earnings Qualifier: If the worker does not qualify for unemployment insurance benefits using the standard base period calculations the UIA applies the following alternate earnings qualifier: wages in at least 2 quarters and wages in the entire base period of at least 20 times the state average weekly wage. • Alternate Base Period: The last 4 completed calendar quarters before the first day of an individual's benefit year. It is used only if an individual has insufficient wages to establish a benefit year using the standard base period.
BCS	Bureau of Commercial Services
Blanket Purchase Order	An alternate term for Contract as used in the States computer system.
Business Critical	Any function identified in any Statement of Work as Business Critical.
Business Day	Whether capitalized or not, shall mean any day other than a Saturday, Sunday or State-recognized legal holiday (as identified in the Collective Bargaining Agreement for State employees) from 8:00am EST through 5:00pm EST unless otherwise stated. Any date not qualified as business will be calendar day.
BYE	The Benefit Year Ending date (BYE) is the date a claimant's unemployment insurance claim ends and they can no longer collect benefits on that claim.
CAMS	Case Audit Management System
Chronic Failure	Defined in any applicable Service Level Agreements.
Clean Data	<p>A data extract delivered to the contractor/SAS that is representative and identical to the source system it was extracted from. Source system fields, tables, and subsets based on timeframe will be defined during the requirements gathering and definition phase. Examples of dirty data include:</p> <ul style="list-style-type: none"> - Truncated fields or Otherwise Incomplete data - Invalid Dates or Codes - Outdated data - Incorrect data associated with a field - Extract layout does not match the data layout provided with the extract
Data Mining	Process of discovering new patterns from large data sets involving methods from statistics, artificial intelligence and database management. The actual data mining task is the automatic or semi-automatic analysis of large quantities of data in order to extract previously unknown interesting patterns such as groups of data records (cluster analysis), unusual records (anomaly detection) and dependencies (association rule mining).
RESERVED	Section is not applicable or included in this Contract. This is used as a placeholder to maintain consistent numbering.
Deliverable	Physical goods and/or commodities as required or identified by a Statement of Work



DHS	Department of Human Services
DTMB	Michigan Department of Technology, Management and Budget
Environmentally preferable products	A product or service that has a lesser or reduced effect on human health and the environment when compared with competing products or services that serve the same purpose. Such products or services may include, but are not limited to, those that contain recycled content, minimize waste, conserve energy or water, and reduce the amount of toxics either disposed of or consumed.
Excusable Failure	See Section 2.244.
FACTS	Fraudulent Automated Case Tracking System
FAP	Food Assistance Program
FEE	Front End Eligibility System
Hazardous material	Any material defined as hazardous under the latest version of federal Emergency Planning and Community Right-to-Know Act of 1986 (including revisions adopted during the term of the Contract).
Incident	Any interruption in Services.
ITB	A generic term used to describe an Invitation to Bid. The ITB serves as the document for transmitting the RFP to potential bidders
Key Personnel	Any Personnel designated in Article 1 as Key Personnel.
New Work	Any Services/Deliverables outside the scope of the Contract and not specifically provided under any Statement of Work, that once added will result in the need to provide the Bidder with additional consideration.
DTMB	Michigan Department of Technology, Management and Budget
MIDAS	The Michigan Integrated Data Automated System – the FAST Enterprises LLC proprietary commercial-off-the-shelf (COTS) solution for implementation for the state of Michigan UI benefit and tax functionality.
OIG	Office of the Inspector General
Ozone-depleting substance	Any substance the Environmental Protection Agency designates in 40 CFR part 82 as: (1) Class I, including, but not limited to, chlorofluorocarbons, halons, carbon tetrachloride, and methyl chloroform; or (2) Class II, including, but not limited to, hydro chlorofluorocarbons
Post-Consumer Waste	Any product generated by a business or consumer which has served its intended end use, and which has been separated or diverted from solid waste for the purpose of recycling into a usable commodity or product, and which does not include post-industrial waste.
Post-Industrial Waste	Industrial by-products that would otherwise go to disposal and wastes generated after completion of a manufacturing process, but do not include internally generated scrap commonly returned to industrial or manufacturing processes.
Predictive Modeling	Recognize patterns in data; process by which a model is created to best predict the probability of an outcome. Models can use one or more classifiers in trying to determine the probability of a set of a data belonging to another set.
Recycling	The series of activities by which materials that are no longer useful to the generator are collected, sorted, processed, and converted into raw materials and used in the production of new products. This definition excludes the use of these materials as a fuel substitute or for energy production.
Reuse	Using a product or component of municipal solid waste in its original form more than once.
RFP	Request for Proposal designed to solicit proposals for services
Runbook	A routine consolidation/summary of the procedures and operations which the administrator of the system or automation carries out/executes.
Scenario	In connection with fraudulent activity, a scenario is (i) deliberate deception, trickery, or cheating intended to gain an advantage, or (ii) an inappropriate act or omission by person(s) with control over or access to government resources involving the government not receiving reasonable value in connection with government funded activities.
Separating Employer	An individual's most recent employer immediately prior to filing an unemployment claim.
Services	Any function performed for the benefit of the State.
SOM	State of Michigan
Source reduction	Any practice that reduces the amount of any hazardous substance, pollutant, or contaminant entering any waste stream or otherwise released into the environment prior to recycling, energy recovery, treatment, or disposal.
State Location	Any physical location where the State performs work. State Location may include state-owned, leased, or rented space.



Subcontractor	A company Bidder delegates performance of a portion of the Services to, but does not include independent Bidders engaged by Bidder solely in a staff augmentation role.
Unauthorized Removal	Bidder's removal of Key Personnel without the prior written consent of the State.
Waste prevention	Source reduction and reuse, but not recycling.
Waste reduction and Pollution prevention	The practice of minimizing the generation of waste at the source and, when wastes cannot be prevented, utilizing environmentally sound on-site or off-site reuse and recycling. The term includes equipment or technology modifications, process or procedure modifications, product reformulation or redesign, and raw material substitutions. Waste treatment, control, management, and disposal are not considered pollution prevention, per the definitions under Part 143, Waste Minimization, of the Natural Resources and Environmental Protection Act (NREPA), 1994 PA 451, as amended.
Work in Progress	A Deliverable that has been partially prepared, but has not been presented to the State for Approval.
Work Product	Refers to any data compilations, reports, and other media, materials, or other objects or works of authorship created or produced by the Bidder as a result of an in furtherance of performing the services required by this Contract.



Appendices

RESERVED - Appendix A.....Project Manager Resume Summary Template



Appendix B. Breakdown of Hardware and Related Software

The Contract has provided the following recommendation of Hardware to meet the processing requirements of their solution for the initial implementation (UIA and FAP). **The State recognizes that the configuration will change following the completion the Project Initiation and Planning Phase described in Section 1.104.1.**

Item	Brand	Size	Model # and Description
Server	Sun	12 core, 72 GB 6 core, 48 GB 2 core, 4 GB	(4) Sun SPARC Enterprise M5000 server (3) SPARC T4-2 server (1) Sun Fire X4270 M2 ATO server
Storage	Sun	SAN storage local storage	(4) 3000 GB 10000 rpm 2.5-inch SAS HDD with bracket (12) One 600 GB 10000 rpm 2.5-inch SAS-2 HDD (2) 300 GB 15000 rpm 3.5-inch SAS HDD
Etc.	Various	See details in Appendix C Example specs are provided below	See details in example specs below
Total			

The State will purchase Hardware from existing State Contracts.

1. Hardware

2. Related Software

Software Component License	Product Name and Version
Report writers	Not Applicable
Requirement analysis tools	Not Applicable
Design tools	Not Applicable
Development environment tools	Not Applicable
Testing tools (such as issues tracking, defect tracking, load/stress testing, configuration management.)	Not Applicable
Other system utilities	Not Applicable
Server software	See Below Sub items 1,2,3,4
Any other software (list)	Not Applicable



Third party server software components and their associated reference links follow.

1) SAS® 9.3 Support for Java Development Kits

<http://support.sas.com/resources/thirdpartysupport/v93/jdks.html>

SAS 9.3 TS1M2

SAS 9.3 TS1M2			
Platform	Java Version	Link	Notes
Windows 64-bit on x86-64	1.6.0_30	Oracle	SAS 9.3 supports JRockit as an alternative JDK for WebLogic. Customers with an Oracle support contract can obtain this JDK by logging into their Oracle support account and clicking the Patches and Updates link.
	JRockit 6 Update 24 R28.1.3 (Only if using WebLogic)		
Solaris 64-bit on SPARC	1.6.0_30	Oracle	Installation of the 64-bit JDK for Solaris requires installation of the 32-bit JDK first. See Oracle's installation instructions for more detail. SAS 9.3 supports JRockit as an alternative JDK for WebLogic. Customers with an Oracle support contract can obtain this JDK by logging into their Oracle support account and clicking the Patches and Updates link.
	JRockit 6 Update 24 R28.1.3 (Only if using WebLogic)		
Solaris 64-bit on x86-64	1.6.0_30	Oracle	Installation of the 64-bit JDK for Solaris requires installation of the 32-bit JDK first. See Oracle's installation instructions for more detail.
AIX	6.0.0.215 Java 6 SR8 FP1 64-bit	IBM	
HP-UX Itanium	6.0.13	HP	
Linux 64-bit x86-64	1.6.0_30	Oracle	SAS 9.3 supports JRockit as an alternative JDK for WebLogic. Customers with an Oracle support contract can get this JDK by logging into their Oracle support account and clicking the Patches and Updates link.
	JRockit 6 Update 24 R28.1.3 (Only if using WebLogic)		
z/OS	Java 6 31-bit SDK	IBM	



2) Application Server Support (3 options described below)

- A. JBoss Application Server Support for SAS® 9.3
- B. IBM WebSphere Application Server Support for SAS® 9.3
- C. Oracle WebLogic Server Support for SAS® 9.3

2A. JBoss Application Server Support for SAS® 9.3

<http://support.sas.com/resources/thirdpartysupport/v93/appservers/jbossw.html>

Product	Platform	Version	Link	Notes
JBoss Application Server (64-bit)	Linux on x64 (x86-64) (Red Hat Enterprise Linux 5, 6; SUSE Linux Enterprise Server 10, 11)			
	Solaris on SPARC (Solaris 10)			Download a binary file by using the Download link or contact Red Hat .
	AIX on Power (AIX 6.1 and 7.1)	JBoss AS 4.2.3.GA*	Download	Note: You must use a supported version of JDK 1.6 with SAS 9.3, as documented in SAS 9.3 Support for Java Development Kits .
	AIX 7.1	JBoss EAP 4.3	or	Before you run the SAS® Deployment Wizard to install SAS software and configure JBoss, review the JBoss Application Server documentation for SAS 9.3 .
	HP/UX on Itanium (HP-UX 11.31)	JBoss AS 5.1.0.GA	contact Red Hat	Note: If you use JBoss AS 4.2.3.GA in SAS 9.3 Revision 11w29, the SAS Deployment Wizard presents a warning that says you are not using the recommended version. You can ignore that warning.
	Solaris 10 x64 (x86-64) (Solaris 10)	JBoss EAP 5.1.1**		Note: If you use JBoss EAP 5.1.1 prior to SAS 9.3 Revision 11w45, the SAS Deployment Wizard presents a warning that says you are not using the recommended version. You can ignore that warning.
	Windows x64 (x86-64) (Windows Server 2003 x64) (Windows Server 2008 x64) (Windows Server 2008 R2 x64)			



2B. IBM WebSphere Application Server Support for SAS® 9.3

<http://support.sas.com/resources/thirdpartysupport/v93/appservers/webspheresw.html>

SAS 9.3 TS1M2

SAS 9.3 TS1M2				
Product	Platform	Version	Link	Notes
IBM WebSphere Application Server (64-bit)	Linux on x64 (x86-64) (Red Hat Enterprise Linux 5, Novell SuSE Linux Enterprise Server 10 and 11)	7.0.0.13 8.0.0.2	Contact IBM	<p>To contact an IBM representative or to place an order for WebSphere, see the IBM Application Infrastructure page. You can reach a representative by calling the toll-free telephone number under We're here to help in the right pane.</p> <p>You must review and follow the instructions in the section "WebSphere Application Server Fix Packs" (below this table) to obtain and apply the required fix pack from IBM.</p> <p>Before you run the SAS® Deployment Wizard to install SAS software and configure IBM WebSphere, review the IBM WebSphere Application Server Documentation for SAS 9.3.</p>
	Solaris on SPARC (Solaris 10) AIX on Power AIX 6.1 and 7.1 (64-bit) with recommended maintenance packages Solaris 10 x64 (x86-64) (Solaris 10) Windows x64 (x86-64) (Windows Server 2003 x64) (Windows Server 2008 x64) (Windows Server 2008 R2 x64)			
	Linux on x64 (x86-64) (Red Hat Enterprise Linux 6)	7.0.0.15 8.0.0.2		



SAS 9.3 TS1M0 and TS1M1

SAS 9.3 TS1M0 and TS1M1				
Product	Platform	Version	Link	Notes
IBM WebSphere Application Server (64-bit)	Linux on x64 (x86-64) (Red Hat Enterprise Linux 5, Novell SuSE Linux Enterprise Server 10 and 11)	7.0.0.13	Contact IBM	<p>To contact an IBM representative or to place an order for WebSphere, see the IBM Application Infrastructure page. You can reach a representative by calling the toll-free telephone number under We're here to help in the right pane.</p> <p>You must review and follow the instructions in the section "WebSphere Application Server Fix Packs" (below this table) to obtain and apply the required fix pack from IBM.</p> <p>Before you run the SAS® Deployment Wizard to install SAS software and configure IBM WebSphere, review the IBM WebSphere Application Server Documentation for SAS 9.3.</p>
	Solaris on SPARC (Solaris 10) AIX on Power AIX 6.1 and 7.1 (64-bit) with recommended maintenance packages Solaris 10 x64 (x86-64) (Solaris 10) Windows x64 (x86-64) (Windows Server 2003 x64) (Windows Server 2008 x64) (Windows Server 2008 R2 x64)			
	Linux on x64 (x86-64) (Red Hat Enterprise Linux 6)	7.0.0.15		



2C. Oracle WebLogic Server Support for SAS® 9.3

<http://support.sas.com/resources/thirdparty-support/v93/appservers/weblogicsw.html>

Product	Platform	Version	Link	Notes
Oracle WebLogic Server (64-bit)	<p>Linux on x84 (x86-64) (Red Hat Enterprise Linux 5, 6; SUSE Linux Enterprise Server 10, 11)</p> <p>Solaris on SPARC (Solaris 10)</p> <p>AIX on Power (AIX 6.1, 7.1) Note: AIX 7.1 is only supported by WebLogic 10.3.4 and later.</p> <p>HP/UX on Itanium (HP-UX 11.31)</p> <p>Solaris 10 x84 (x86-64) (Solaris 10)</p> <p>Windows x84 (x86-64) (Windows Server 2003 x84) (Windows Server 2008 x84) (Windows Server 2008 R2 x84)</p>	10.3	Contact Oracle	<p>The operating system and the version of WebLogic Server determines the JDK that is required. WebLogic Server supports JDKs from multiple vendors. Java Software Development Kits lists these vendor-specific JDK requirements and identifies the supported platforms for WebLogic.</p> <p>Before you run the SAS® Deployment Wizard to install SAS software and configure Oracle WebLogic, review the Oracle WebLogic Server Documentation for SAS 9.3.</p> <p>For instructions about how to obtain and apply WebLogic Server patches, see Obtaining and Applying Patches for Oracle WebLogic Server 9.x and Later.[™] October 10, 2011</p> <p>Required patches for WebLogic Server 10.3.0</p> <ul style="list-style-type: none"> • Patch ID: 6F8A • Patch ID: CJ4W • Patch ID: IQXV • Patch ID: T552 • Patch ID: 79YU • Patch ID: ETR7 • Patch ID: SYCB • Patch ID: GB3R <p>Required patches for WebLogic Server 10.3.1</p> <ul style="list-style-type: none"> • Patch ID: BR4K • Patch ID: UQJZ • Patch ID: 36RE <p>Required patches for WebLogic Server 10.3.2</p> <ul style="list-style-type: none"> • Patch ID: YQHC • Patch ID: JKDI • Patch ID: W6PT <p>Required patches for WebLogic Server 10.3.3</p> <ul style="list-style-type: none"> • Patch ID: MLHC • Patch ID: 81UZ <p>Required patches for WebLogic Server 10.3.4</p> <ul style="list-style-type: none"> • No patches are required. <p>Required patches for WebLogic Server 10.3.5</p> <ul style="list-style-type: none"> • Patch ID: 6BLB <p>Required patches for WebLogic Server 10.3.6</p> <ul style="list-style-type: none"> • No patches are required.



3) Junit for SAS® 9.3 Support for Additional Software Products

http://support.sas.com/resources/thirdpartysupport/v93/othersw.html#tab_junit

Platform	Version	Link
All SAS 9.3 Supported Platforms	4.8.1	Download

4) SAS® Social Network Analysis Server / SAS® Fraud Framework Supported Databases (4 options described below)

Database	Link
A. Oracle Database 11g Release 2 Documentation Library	http://www.oracle.com/pls/db112/homepage
B. MySQL 5.0 Reference Manual	http://dev.mysql.com/doc/refman/5.0/en/
C. IBM Support Portal - DB2 for Linux, UNIX, and Windows	http://www-947.ibm.com/support/entry/portal/Documentation/Software/Information_Management/DB2_for_Linux,_UNIX_and_Windows
D. Microsoft SQL Server Library	http://technet.microsoft.com/en-us/library/bb545450.aspx



Appendix C. Payment Schedule

SUMMARY TOTAL CONTRACT COST:

Table Number	Table Description	
Table 1	Work and Deliverables Services and Software Payment Schedule	\$4,210,658
Table 2	Warranty, Maintenance and Support	\$1,366,533
Table 3	Contingency Fund - Task 1.104.10	\$430,500
Estimate Contract Value		\$6,007,691

Table 1 - Column Definitions:

Task	The reference to the task number identified in the Contract.
Project Milestone	The description of the Task as outlined in the Contract.
Services Accrual	The amount of Services Payments withheld until the completion and acceptance of both FAP and UIA Implementations.
Services Payment	The amount paid upon completion and acceptance of both FAP and UIA Implementations.
Licensing Cost	The portion of total software license that will be paid the sooner of the Invoice Date or the completion of the Project Milestone.

Table 1 – Work and Deliverables Services and Software Payment Schedule

Task	Project Milestones	Services Accrual	Services Payment	Licensing Cost (Invoice Date)
	Contract Execution			\$700,000 (Contract Execution)
1	Initiation and Planning			
1.1	Project Planning			
1.2	General Timeline			
1.3	Confirm Infrastructure			
1.4	Product Installation			
	Initiation and Planning Complete	\$162,360	\$0	\$150,000 (2/28/2013)
2	Phase 1 FAP Requirements & Design			
2.1	Requirements Definition			
2.2	Functional Design			
3	Phase 1 FAP Construction & Testing			
3.1	Construction and Testing Plan			
3.2	Data Preparation			
3.3	Configure FAP Fraud Detection Analysis Scenarios			
3.4	Integrations			
3.5	Transition and Operations Planning			
3.6	System Testing			
3.7	User Acceptance Testing			
	Phase 1 FAP Construction & Testing Complete			\$500,000 (5/31/2013)
4	Phase 1 FAP Implementation			



Task	Project Milestones	Services Accrual	Services Payment	Licensing Cost (Invoice Date)
4.1	Production Cutover			
4.2	Installation Testing			
4.3	Post Implementation Evaluation Report			
	Phase 1 FAP Implementation Acceptance (Year 1 of Warranty begins following Acceptance of Phase 1 FAP or Phase 2 UIA, whichever comes first) For purposes of licensing, this is the Anniversary Date.	\$421,080	\$200,000	\$500,000 (7/31/2013)
5	Phase 2 UIA Requirements & Design			
5.1	Requirements Definition			
5.2	Functional Design			
	Phase 2 UIA Functional Design Approved			\$150,000 (6/30/2013)
6	Phase 2 UIA Construction & Testing			
6.1	Construction and Testing Plan			
6.2	Data Preparation			
6.3	Configure UIA Benefit and Tax Fraud Detection Analysis Scenarios			
6.4	Integrations			
6.5	Transition and Operations Planning			
6.6	System Testing			
6.7	User Acceptance Testing			
	Phase 2 UIA Construction & Testing Complete			\$500,000 (8/30/2013)
7	Phase 2 UIA Implementation			
7.1	Production Cutover			
7.2	Installation Testing			
7.3	Post Implementation Evaluation Report			
	Phase 2 UIA Implementation Acceptance	\$567,358	\$ 950,798	\$559,860 (9/30/2013)
	Total Services and Software Payments		\$1,150,798	\$3,059,860

Notes:

1. Quick Start: Upon request from the State, the Contractor will implement its 'Quick Start Methodology' at no additional cost to the State. The State will host the Quick Start.
2. The Contractor will provide the Michigan Enterprise Fraud Detection System which is an Enterprise License.
 - a. The Michigan Enterprise Fraud Detection System is comprised of the following SAS offerings: SAS Fraud Framework for Government, DataFlux Data Management Server and Studio Enrichment, and DataFlux DataPack (DF) – US Address Verification. Includes two modules, UIA Benefits Overpayments and FAP (SNAP) Fraud Detection. Up to five (5) SAS Access Engine licenses and the associated services to implement them. Three authorized agencies at this time are Unemployment Insurance Agency, Department of Human Services, and The Office of Inspector General. Includes 40 Fraud Framework clients, not concurrent,



and five (5) DF Client users, not concurrent and an unlimited number of Investigative Workbench clients (web-based GUI). Additional clients, fraud modules and expansion of use to other agencies are available from SAS for additional fees

- b. License Costs will be paid as defined in the Licensing Cost Column in Table 1. Invoice will be due on the dates listed in the Licensing Cost column of Table 1.
- c. Contractor shall extend to the State of Michigan 2012 pricing on all future fraud modules and licenses purchased within 18 months of signing the contract. Further, Contractor will negotiate and provide pricing and project timelines upon the State's request following conveyance of appropriate specifications. Licenses and Fraud modules currently available include the following:
 - Medicaid Fraud – to include eligibility and pre-payment detection.
 - Tax Fraud – To include income tax, business tax, retail sales tax as a result of "Zapper Technology," property/homestead tax, tax credit fraud due to identity theft, cigarette tax evasion, and hard liquor tax evasion, etc.
 - Workers' Compensation Fraud – To include employee misclassification, premium evasion, claims, and medical providers.
 - Social Service Program Fraud – To include TANF, WIC, child care services, Work First, and housing and heating.
 - Grant and Contract Fraud – To include human services, economic development, education, disaster assistance and manipulation of bidding or collusion.

Table 2 – Warranty, Maintenance and Support

Task	Warranty, Maintenance and Support Activities	Cost
8.1	Warranty (One Year) Complete Begins with Phase I FAP or Phase 2 UIA Implementation Acceptance (whichever occurs first)	\$ Included in first year software costs
9.1	Maintenance and Support (Support Year 1) Complete	\$ Included in first year software costs
9.1	Maintenance and Support (Support Year 2) Complete	\$673,169
9.1	Maintenance and Support (Support Year 3) Complete	\$693,364
	Total for Support years 1-3.	\$1,366,533

Table 2b –Maintenance and Support for Optional Years

Task	Warranty, Maintenance and Support Activities Option Years	Services Accrual
9.1	Optional Maintenance and Support (Support Year 4) Complete	\$714,164
9.1	Maintenance and Support (Support Year 5) Complete	\$735,589
9.1	Maintenance and Support	\$757,657



Task	Warranty, Maintenance and Support Activities Option Years	Services Accrual
	(Support Year 6) Complete	
9.1	Maintenance and Support (Support Year 7) Complete	\$780,387
9.1	Maintenance and Support (Support Year 8) Complete	\$803,798

Notes:

1. Warranty: Includes Costs for One (1) Year of Warranty as Described in Section 1.104.8. Note that Year 1 of Warranty begins following Acceptance of either Phase 1 or Phase 2, whichever occurs first.
2. Maintenance and Support: Payment for Support Year 2 is made upon the end of the Contract Warranty Period identified in Section 1.104.8. Thereafter, each Maintenance and Support payment will be invoiced on an annual basis.

Table 3 – Contingency Fund - Task 1.104.10

Contractor Staffing Category	Firm Fixed Hourly Rate
Senior Project Manager	\$200
Tech Lead	\$225
Analytical Lead	\$225
Developer	\$225
Analyst	\$225
Tester	\$200
SAS Admin	\$200
SSOIT	\$200
Documentation	\$200
Reserved Contingency Fund	\$430,500

Notes:

1. Hourly rates provided are firm, fixed rates for the duration of the contract. Travel and other expenses will not be reimbursed.
2. The State will utilize the firm fixed fully loaded hourly rates detailed above for each staff that will be used as fixed rates for responses to separate statements of work.
3. The State intends to establish funding for additional enhancements. Actual funding for enhancements will occur on a yearly basis, and there is no guarantee as to the level of funding, if any, available to the project.
4. This funding may also be utilized towards additional software licensing, software services or other related matters.

Table 4 – Additional (Optional) Training Tools



The Contractor has provided the following list of computer-based or web-based training tools available to the State and all associated optional costs. These are additional training tools outside of those required in 1.104 of the Contract.

Data Integration Developer

Training Tool	Type (CBT or WBT)	Cost (\$)
SAS Programming 1: Essentials This course is the entry point to learning SAS programming and is a prerequisite to many other SAS courses. Duration: 3 days	self-paced e-Learning	3 EPTO units or \$1,500/person
SAS SQL 1: Essentials This course teaches you how to process SAS data using Structured Query Language (SQL). Duration: 2 days	<u>Public Training (Detroit)</u> Also available as self-paced e-Learning	2.4 EPTO units or \$1,200/person
SAS Macro Language 1: Essentials This course focuses on the components of the SAS macro facility and how to design, write, and debug macro systems. Emphasis is placed on understanding how programs with macro code are processed. Duration: 2 days	<u>Public Training (Detroit)</u> Also available as self-paced e-Learning	2.4 EPTO units or \$1,200/person
SAS Data Integration Studio: Fast Track This intensive training course provides accelerated learning for those students who will register sources and targets; create and deploy jobs; work with transformations; set up change management; work with slowly changing dimensions; and the scheduling of jobs. This course is for individuals who are comfortable with learning large amounts of information in a short period of time. The SAS Data Integration Studio 1: Essentials and SAS Data Integration Studio 2: Additional Topics courses are available to provide the same type of information in a much more detailed approach over a longer period of time. Duration: 5 days	<u>Public Training</u>	7.5 EPTO units or \$3,750/person

Business User

Training Tool	Type (CBT or WBT)	Cost (\$)
SAS Business Intelligence Reporting 1: Essentials This course teaches how to access reports and	<u>Public Training</u>	2.4 EPTO units or \$1,200/person



analyze data using several of the business user applications in the platform for SAS Business Analytics. Duration: 2 days		
SAS Business Intelligence Reporting 2: Additional Topics This course expands on the knowledge learned in the SAS Business Intelligence Reporting 1: Essentials course and provides additional information for using several of the business user applications in the platform for SAS Business Analytics. Duration: 2 days	<u>Public Training</u>	2.4 EPTO units or \$1,200/person
SAS Enterprise Guide 1: Querying and Reporting - Recommended This course is for users who do not have SAS programming experience but need to access, manage, and summarize data from different sources, and present results in tables and graphs. This course focuses on using the menu-driven tasks in SAS Enterprise Guide, the point-and-click interface to SAS, to create queries and reports. It does not address writing SAS code or statistical concepts. Duration: 2 days	<u>Public Training</u> Also available as self-paced e-Learning	2.0 EPTO units or \$1,000/person

Statistical Analyst

Training Tool	Type (CBT or WBT)	Cost (\$)
Applied Analytics Using SAS Enterprise Miner This course covers the skills required to assemble analysis flow diagrams using the rich tool set of SAS Enterprise Miner for both pattern discovery (segmentation, association, and sequence analyses) and predictive modeling (decision tree, regression, and neural network models). Duration: 3 days	<u>Public Training</u> Also available as self-paced e-Learning	4.5 EPTO units or \$2,250/person
SAS Enterprise Guide 1: Querying and Reporting - Recommended This course is for users who do not have SAS programming experience but need to access, manage, and summarize data from different sources, and present results in tables and graphs. This course	<u>Public Training</u> Also available as self-paced e-Learning	2.0 EPTO units or \$1,000/person



focuses on using the menu-driven tasks in SAS Enterprise Guide, the point-and-click interface to SAS, to create queries and reports. It does not address writing SAS code or statistical concepts.

Duration: 2 days

Investigator

Training Tool	Type (CBT or WBT)	Cost (\$)
SAS Fraud Framework: Using the Social Network Analysis Interface This customized course provides you with the knowledge and skills needed to use the Investigator User Interface, a component of SAS Fraud Framework. The course covers identifying individuals associated with fraud, researching the data related to the individuals, and exploring the social network of individuals. Duration: 1 day	<u>On-site only (Detroit)</u> Allow 90 days for customization and scheduling	\$3,120 course fee plus \$9,000 customization fee for up to 15 people

Platform Administrator

Training Tool	Type (CBT or WBT)	Cost (\$)
SAS Platform Administration: Getting Started - Recommended This course provides an overview of the platform for SAS Business Analytics from a platform administrator's perspective. Duration: 1 day	<u>Self-paced e-Learning only</u>	1.5 EPTO units or \$750/person
SAS Platform Administration 1: Essentials - Recommended This course provides students with the essential knowledge to perform the job functions of a SAS platform administrator. Duration: 3 days	<u>Public Training</u>	4.5 EPTO units or \$2,250/person

Data Quality Steward

Training Tool	Type (CBT or WBT)	Cost (\$)
---------------	----------------------	-----------



DataFlux dfPower Studio Overview Recommended This course is designed for Data Quality Stewards who need an overview of the DataFlux dfPower Studio version 8.2. Duration: 3 days	Public Training	3.6 EPTO units or \$1,800/person
--	-----------------	----------------------------------

BI Content Developer

Training Tool	Type (CBT or WBT)	Cost (\$)
Creating Business Intelligence for Your Organization: Fast Track Recommended This intensive training course provides accelerated learning for those students who will build reports, analyses, and dashboards for consumption by business users and other information consumers in their organization. This course is for individuals who are comfortable with learning large amounts of information in a short period of time. The Creating Business Intelligence for Your Organization 1: Essentials and Creating Business Intelligence for Your Organization 2: Additional Topics courses are available to provide the same type of information in a much more detailed approach over a longer period of time. Duration: 5 days	Public Training	7.5 EPTO units or \$3,750/person
Designing, Tuning, and Maintaining SAS OLAP Cubes Recommended This course teaches students how to use the SAS OLAP environment to build, tune, and maintain multidimensional cubes. Duration: 3 days	Public Training	4.5 EPTO units or \$2,250/person

Notes

Courses offered in Detroit are indicated in the pricing column.

All courses are also available privately on-site at a higher rate plus expenses.

All fees include specific pricing for State of Michigan and are valid through March 31, 2014.

Enterprise Professional Training Offer

Contractor has developed a program that enables the State to purchase training units in advance and apply those units to a variety of training services, often with significant discounts. The pricing and number of units required for the training services varies.



EPTO units	Prices for State of Michigan
60	\$22,300
120	\$44,000
240	\$85,200

***Units may be purchased in any quantity**



RESERVED - APPENDIX D. PRELIMINARY PROJECT PLAN

RESERVED - APPENDIX E. ORGANIZATION CHART AND STAFFING RESOURCE TABLE

RESERVED - APPENDIX F. MANDATORY MINIMUM REQUIREMENTS



Appendix G. Master License Agreement

The Contractor has provided their Master License Agreement as Appendix G.

If there are any conflicts between the terms of Appendix G and the terms in Article 2, Article 2 will take precedence.

Master License Agreement

For purposes of this Master License Agreement ("MLA"), Contractor is referred to as "SAS" and the State is referred to as "Customer." This MLA and its Supplement (collectively, "Agreement") govern Customer's license of Software listed above and any related user documentation and is an attachment to, and made a part of the Contract.

1. License Grant; Authorized Use; Purpose. SAS grants Customer a nonexclusive, nontransferable and nonassignable license to use the Software for the Purpose with designated operating systems under the Agreement. Except as otherwise provided in the Agreement, the Software may be accessed only by Customer's employees and on site contractors ("Users") doing work in the United States solely for the following State of Michigan governmental agencies: Unemployment Insurance Agency, Department of Human Services and the Office of Inspector General. The license is an annual license renewed at the mutual agreement of the parties. Renewal is accomplished by SAS sending an invoice for the applicable Software license renewal fees and Customer paying the invoice. "Purpose" means use by three (3) authorized State of Michigan agencies (Unemployment Insurance Agency, Department of Human Services, and The Office of Inspector General) to provide data integration, analytics and reporting capabilities solely to support fraud and improper payments detection, investigation and prevention efforts within Customer's UIA and SNAP programs.

1.1 Territory; Report Access. Customer may install and use the Software (a) within the United States ("Territory"); (b) on a portable computer in countries outside the Territory for up to three (3) months of an annual license period; and (c) in a manner allowing any party in or outside the Territory limited access to Software applications to view reports showing results of Customer's analysis of Customer's data ("Reports"). Customer may allow this limited Report viewing via the internet, Customer's intranet or terminal emulation sessions.

1.2. Other Uses of the Software.

SAS grants no usage rights beyond those specifically listed herein. By way of example, the following uses are prohibited unless specifically set forth in a written amendment to the Agreement: (a) installation or use outside the Territory; (b) use for the benefit of a third party in exchange for compensation; (c) use in application or data service provision, outsourcing, time-sharing, data or information technology management, or other similar arrangements; (d) use to process third party data; or (e) allowing any party other than Users to use, edit, modify, or otherwise access underlying Software, or to perform free form programming with the Software.

2. Authorized Hardware. Customer shall install the Software only on hardware authorized and listed in the Supplement ("Authorized Hardware"). Software is licensed for use on server hardware, listed in the Supplement and located on Customer's premises that Customer identifies to SAS by type and CPU number.

3. Fees. License fees for the Software are set forth in the Contract.

4. Product Authorization Code. Customer may allow Users to access only Software licensed to Customer for which Customer receives a Product Authorization Code. Customer shall not allow Users to install or attempt to use other products contained on media received from SAS. The "Product Authorization Code" is a component of the Software that enables the Software to operate for the applicable license period. At each new license period, or if required as a result of changes in Authorized Hardware or Software, Customer must apply a new Product Authorization Code to keep the Software operating. SAS is not required to provide the Product Authorization Code if Customer is in breach of the Agreement or has not paid any undisputed amounts due under the Agreement. SAS is not liable for damages caused by the resulting Software interruption. Customer may allow only Users to access the Product Authorization Code. Customer acknowledges and agrees that the Product Authorization Code is SAS' Confidential Information under the Contract.

5. Copying. Customer may copy the Software only for (a) disaster recovery and back-up purposes, and (b) installation of personal computer Software authorized hereunder. All copies remain the property of SAS. Customer may deliver a copy of the Software to a disaster recovery contractor to perform temporary disaster recovery work for Customer. Customer shall give SAS the name and address of the disaster recovery contractor before delivery. The identical copyright notices and any other proprietary rights notices found on the original Software media must be reproduced on all copies authorized under this Section.

6. Title; Source Code. Title to the Software and its documentation remains with SAS and its licensors at all times. Copyright notices and other proprietary rights notices in the Software shall not be deleted or modified. The Agreement does not transfer any ownership rights. Source code from which the Software object code is derived ("Source Code") is not being provided and is a trade secret of SAS and



SAS' licensors to which access is not authorized. Neither Customer nor any other User shall reverse engineer, reverse assemble or decompile the Software or in any way attempt to recreate the Source Code, except and only to the extent applicable laws specifically prohibit such restriction.

7. Technical Support. During the term of the Software license, SAS will use reasonable efforts, either by telephone or in writing, to help Customer solve specific problems with installation or use of the Software within the Territory. It may not be possible for SAS to solve all problems or correct all errors in the Software. From time to time, SAS may make available, and Customer agrees to use reasonable efforts to install, new releases, updates and corrective code. During ongoing Software development, SAS may add, change or delete individual components or functionality in new releases. Such Software modifications shall be subject to the terms of the Agreement. If Customer chooses not to install the most current release of the Software, the level of technical support may diminish over time.

8. Payment.

8.1 Invoices. Customer will pay the Software license fees set forth in the payment schedule of the Contract as specified in the Contract. Payment terms for all invoices are as set forth in the payment schedule set forth in the Contract. License fees do not include taxes. SAS will use reasonable efforts to include all taxes applicable to Customer on the relevant invoice and Customer agrees to pay such taxes to SAS; however, Customer is responsible for taxes on its licensing of the Software. Customer is not responsible for taxes based on SAS' income. Except as otherwise allowed in the Agreement, refunds are not available after the Product Authorization Code has been provided.

9. Limited Warranties and Representations.

9.1 Warranties by SAS; Remedies.

9.1.1 SAS warrants that it has the right to license the Software to Customer. The exclusive remedy for breach of this warranty is set forth in Section 11 (Indemnification).

9.1.2 SAS warrants that each production release of the Software shall substantially conform to its documentation including any updates thereto, and the Software and the media on which it is installed shall be free of software viruses when received by Customer. SAS also provides the warranties set forth in Section 2.312 and 2.313 of the Contract with respect to the Software. As the exclusive remedy for breach of these warranties, SAS, at its option, shall: (a) repair the Software; (b) replace the Software; or (c) terminate the Software license and refund the fees paid for the Software at issue during the then-current license period.

9.2 Warranty Disclaimers. SAS AND ITS LICENSORS DISCLAIM ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, OR ARISING AS A RESULT OF CUSTOM OR USAGE IN THE TRADE OR BY COURSE OF DEALING. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, SAS AND ITS LICENSORS DO NOT WARRANT OR REPRESENT THAT THE SOFTWARE WILL RESULT IN COMPLIANCE, FULFILLMENT OR CONFORMITY WITH THE

LAWS, RULES, REGULATIONS, REQUIREMENTS OR GUIDELINES OF ANY GOVERNMENTAL AGENCY. SAS' LICENSORS PROVIDE THEIR SOFTWARE "AS IS." NOTHING IN THIS SUBSECTION NEGATES THE EXPRESS WARRANTIES SAS PROVIDES IN THE AGREEMENT.

9.3 Representations by Customer. Customer represents it shall (a) implement procedures to verify accuracy of data input and output while using the Software, and (b) inform all parties authorized to use the Software of the relevant terms of the Agreement and any related user documentation, and be responsible for their adherence to such terms. Customer agrees that the Software and Services, in and of themselves, will not ensure compliance with laws.

10. Exclusions of Damages; Limitation of Liability.

10.1 The exclusions of damages and limitations of liability set forth in Section 2.220 of the Contract apply to the Software. **SAS' LICENSORS ARE NOT LIABLE FOR SPECIAL, INCIDENTAL, INDIRECT, CONSEQUENTIAL, PUNITIVE, OR RELIANCE DAMAGES (ARISING IN TORT, CONTRACT OR OTHERWISE), EVEN IF THEY HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. SAS' LICENSORS ARE NOT LIABLE FOR ANY CLAIM AGAINST THE CUSTOMER BY A THIRD PARTY RELATING TO USE OF THE SOFTWARE. SAS' LICENSORS ARE NOT LIABLE FOR DIRECT DAMAGES (ARISING IN TORT, CONTRACT OR OTHERWISE) AND DISCLAIM ANY LIABILITY CONNECTED WITH USE OF THE SOFTWARE. THE PARTIES MAKE THESE EXCLUSIONS IN CONSIDERATION OF THE FEES PAID AND LICENSES GRANTED UNDER THE AGREEMENT.**

11. Indemnification. SAS' indemnification obligations with respect to the Software are as set forth in Section 2.140 of the Contract.

12. Termination; Expiration. The termination provisions set forth in Section 2.150 and 2.160 of the Contract apply to this Agreement. Upon termination or expiration of each Software license hereunder, or when a User, Related Entity or disaster recovery contractor is no longer authorized to access the Software, Customer agrees to reclaim, delete, and destroy the Software at issue, along with any related user documentation.

13. Governing Law; Export and Import Restrictions. Section 2.211 of the Contract identifies the governing law applicable to this Agreement. SAS hereby notifies Customer that United States export laws and regulations apply to the Software. Both parties agree to comply with these and other applicable export and import laws and regulations. The parties expressly agree to exclude from the Agreement the United Nations Convention on Contracts for the International Sale of Goods.

14. General.

14.1 Severability. If a court of competent jurisdiction finds any part unenforceable, that part is excluded, but the remainder of the Agreement stays in full force and effect.

14.2 No Waiver. Failure to require compliance with a part of the Agreement is not a waiver of that part. Nothing in this subsection waives any remedy



either party may have under the Agreement at law, in equity, or otherwise.

14.3 Non-assignment. The provisions of Section 2.029 of the Contract apply to this Agreement.

14.4 Audit. Upon fifteen (15) business days' notice to Customer, SAS will have the right to conduct an on-site audit during Customer's normal business hours to verify compliance with the terms and conditions of the Agreement. Customer shall cooperate with SAS by: (a) making applicable records available; (b) providing copies of the records requested; and (c) directing all agents to cooperate. If the audit reveals that Customer owes additional license fees, Customer shall pay the amounts owed and SAS' reasonable expenses in conducting the audit.

14.5 Injunctive Relief. The provisions of Section 2.193 of the Contract apply to this Agreement.

15. Complete Agreement; Modifications. The Agreement and invoices arising under it are the parties' complete and exclusive statement relating to their subject matter. Modifications must be in writing, signed by both parties, and specifically reference the Agreement.



Supplement Number 1 ("Supplement")

to Master License Agreement ("MLA")

					FOR SAS USE ONLY		
Software and Subcomponents ¹		Applicable Pricing Metric, Number of Authorized Units ²	Operating System ³	Authorized Hardware (CPU/Server Manufacturer, Model type/Serial No.) ³	Initial Fees ⁴ (in above Currency Type)	License Beginning Date	Anniversary Date
Software:	Michigan Enterprise Fraud Detection Solution*	Solution Test and Development	To be defined by Customer in writing to SAS	To be defined by Customer in writing to SAS	As set forth in Contract	31DEC12	See Appendix C, Table 1, Section 4.3
Subcomponents:	SAS Fraud Framework Analytics Personal Client	PC Use (40)	WNDW	N/A			
	JMP Pro	PC Use (40)	WX6	N/A			
	SAS Text Miner Language Support for English	Solution Test and Development	To be defined by Customer in writing to SAS	N/A			
	SAS/ACCESS Interface to [to be determined]	Solution Test and Development	To be defined by Customer in writing to SAS	N/A			
	SAS/ACCESS Interface to [to be determined]	Solution Test and Development	To be defined by Customer in writing to SAS	N/A			
	SAS/ACCESS Interface to [to be determined]	Solution Test and Development	To be defined by Customer in writing to SAS	N/A			
	SAS/ACCESS Interface to [to be determined]	Solution Test and Development	To be defined by Customer in writing to SAS	N/A			
	SAS/ACCESS Interface to [to be determined]	Solution Test and Development	To be defined by Customer in writing to SAS	N/A			
	SAS Metadata Bridge for [to be determined]	Solution Test and Development	To be defined by Customer in writing to SAS	N/A			
	DataFlux Data Management Platform for	PC Use (5)	WNDW	N/A			

	SAS						
	DataFlux Data Management Studio Profile	PC Use (5)	WNDW	N/A			
	DataFlux Data Management Studio Entity Resolution	PC Use (5)	WNDW	N/A			
	DataFlux Data Management Studio Integration	PC Use (5)	WNDW	N/A			
	DataFlux Data Management Studio Quality	PC Use (5)	WNDW	N/A			
	DataFlux Data Management Studio Quality	PC Use (5)	WNDW	N/A			
	DataFlux Data Management Studio Quality	PC Use (5)	WNDW	N/A			
	DataFlux Data Management Studio Quality	PC Use (5)	WNDW	N/A			
Software:	DataFlux Data Management Server Enrichment	Capacity Based	To be defined by Customer in writing to SAS	To be defined by Customer in writing to SAS	As set forth in Contract	31DEC12	
Software:	DataFlux Data Management Studio Enrichment	PC Use (1)	WNDW	N/A	As set forth in Contract	31DEC12	
Software:	DataFlux DataPack for US Address Verification	Site License; Enrichment Data Use Terms	To be defined by Customer in writing to SAS	To be defined by Customer in writing to SAS	As set forth in Contract	31DEC12	



- ¹ Pricing metrics, operating systems and/or Authorized Hardware for subcomponents which differ from that of the Software with which they are associated are listed in the column that corresponds to the applicable subcomponent. Unless otherwise noted, subcomponents listed here are included in the Software license fee for the Software product with which they are licensed or provided.
- ² The pricing metric is used to derive license fees; for example, but without limitation, Capacity Based, Total Users, PC Use, etc. as described on page 2 of this Supplement. Certain pricing metrics contain additional terms that pertain to Customer's use of the Software.
- ³ Customer must provide Operating System and Authorized Hardware information to SAS prior to shipment of Software.
- ⁴ Unless otherwise described in this Supplement, these are the first year license fees for the Software.
- *This solution is made up of SAS Fraud Framework for Government and the other Software products listed above.

License of Software. This Supplement is an attachment to the MLA (collectively, "Agreement").

Pricing Metrics. The pricing metrics described herein apply to the Software and any Software subcomponents. For the avoidance of doubt, only those pricing metrics listed on page 1 apply to the Software and Software subcomponents licensed hereunder.

Capacity Based - the Software license fee is based on the total processing power of the Authorized Hardware on which the Software is installed. With respect to server hardware, processing power includes each processor on each chip. With respect to mainframe hardware, processing power is based on Millions of Instructions Per Second ("MIPS").

Solution Test and Development - In addition to the license for the production version of the Software, the license granted hereunder also authorizes a single configured installation of the Software in both a test environment and a development environment. Customer may use the Software installed in the test environment solely for the purpose of testing the Software and Software applications and code prior to installation in Customer's production environment ("Test Environment"). Customer may use the Software installed in the development environment solely for the purposes of developing and creating applications and code with the Software for use in Customer's internal production environment ("Development Environment"). Customer must identify in writing the Authorized Hardware for the Test Environment and the Development Environment. The operating system for the Test Environment and the Development Environment must be the same as the operating system for the production Software. The Test Environment and Development Environment shall be used only for the test and development purposes described above and shall at no time be used for production purposes or as a fail-over system. The license to use the Software in the Test Environment and Development Environment shall automatically terminate upon termination of Customer's license for the Software.

Enrichment Data Use Terms - All data necessary to use the Software (collectively, the "Enrichment Data") is licensed to Customer on an annual, non-exclusive, revocable basis. SAS makes no representation or warranty as to the availability of updates to the Enrichment Data. Notwithstanding anything to the contrary contained herein, the license for all or any part of the Enrichment Data is subject to termination by SAS on thirty (30) days prior written notice to Customer in the event SAS' licensor terminates the license for such Enrichment Data ("Enrichment Data Termination"). In the event of an Enrichment Data Termination, Customer must (i) terminate its use of, and delete and destroy, the affected Enrichment Data on or before the date provided by SAS in such written notice and (ii) upon request from SAS, provide SAS with a certification of the deletion and destruction of the affected Enrichment Data signed by an authorized officer of Customer. In the event of an Enrichment Data Termination, provided Customer has complied with its obligations hereunder, SAS will refund to Customer a prorated portion of the license fees paid by Customer for the then-current term for the affected Enrichment Data. In such event, Customer may also terminate the license for the DataFlux Data Management Studio Enrichment software and SAS will refund to Customer a prorated portion of the license fee paid by Customer for that Software for the then-current annual license period. The Enrichment Data may be used only in conjunction with, and under the same terms and conditions as, the corresponding Enrichment Software. Customer must terminate its use of, and delete and destroy, all Enrichment Data if the license therefor is not renewed for any reason. THE SOFTWARE MAY CONTAIN OR PROVIDE ACCESS TO DATA LICENSED TO SAS BY THIRD PARTY VENDORS ("THIRD PARTY DATA") AND PROVIDE ACCESS TO SERVICES AND DATA PROVIDED BY THIRD PARTIES (COLLECTIVELY, "THIRD PARTY SERVICES"). THIRD PARTY DATA, THIRD PARTY SERVICES, AND ACCESS THERETO ARE PROVIDED TO CUSTOMER "AS IS" WITHOUT ANY WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT, OR ARISING AS A RESULT OF CUSTOM OR USAGE IN THE TRADE OR BY COURSE OF DEALING. SAS DISCLAIMS ANY WARRANTY AS TO (A) THE CONTINUED CERTIFICATION OF THE SOFTWARE BY ANY THIRD PARTY OR (B) THE CONTINUED AVAILABILITY OF ANY DISCOUNT PROVIDED FROM USE OF THE SOFTWARE. SAS DISCLAIMS ANY AND ALL LIABILITY IN CONNECTION WITH CUSTOMER'S USE OF THE THIRD PARTY DATA AND THIRD PARTY SERVICES. THE DISCLAIMERS HEREIN DO NOT APPLY TO ANY THIRD PARTY SOFTWARE ACTUALLY EMBEDDED WITHIN THE SOFTWARE, BUT APPLY IN ALL RESPECTS TO ANY DATA SUPPLIED WITH, CONTAINED IN, OR ACCESSED THROUGH THE SOFTWARE. THE PROVISIONS OF THIS PRICING METRIC SHALL TAKE PRECEDENCE OVER ANY CONFLICTING TERMS IN THIS AGREEMENT.

Site License - Customer's use of the Software is dependent upon Customer's licensing the DataFlux Data Management Studio Enrichment Software identified above ("Prerequisite Software"). Customer may install the Software on, and/or access the Software from, any Authorized Hardware, located at a single physical site, for which Customer has licensed the Prerequisite Software.

PC Use - the Software license fee is based on the greater of either (i) the total number of Users authorized to access the Software or (ii) the total number of personal computers on which the Software will be installed and available for processing on the designated operating system.



Subcomponent Installations. Some Software consists of subcomponents which may be used only in connection with a single Software configuration. When the Software requires installation of subcomponents on more than one hardware tier, the server-tier subcomponents may be installed only on the Authorized Hardware listed on page 1 of this Supplement. If authorized by SAS, however, some server-tier subcomponents also may be installed on separate hardware. Where the license fee is based on hardware capacity, then the separate hardware must have the same or lower classification as the Authorized Hardware. Software or subcomponents licensed to SAS by third parties may only be installed once.



Appendix H. Optional Medicaid Functional Requirements and Pricing

Optional Pricing for Medicaid Phase

Task	Project Stages	Estimated Hours	Amount
	Medicaid Phase Work and Deliverables Services Complete (New Phase through BAFO) Milestone Payment	4139	\$1,110,650
	Medicaid Fraud Software License – 2012 Pricing This provides licenses for an additional 20 Fraud Framework clients (power user).	N/A	\$1,912,365
	Maintenance and Support (Support Year 1) Complete Milestone Payment	N/A	\$ Included in first year software costs
	Maintenance and Support (Support Year 2) Complete Milestone Payment	N/A	\$420,721
	Maintenance and Support (Support Year 3) Complete Milestone Payment	N/A	\$433,342
	Total		\$3,877,078



1.104 II.C: Functional Requirements – Medicaid

- The first column (“Contract Ref. #”) of the Medicaid functional requirements document below contains the functional requirement number (i.e. 2-12) from the Contract that serves as the basis for the development of each Medicaid requirement, where applicable, or “New” if the Medicaid requirement does not have a reference requirement in the Contract.
- The Functional Requirements – Medicaid document contains the entire list of Medicaid requirements and does not affect any of the UI or FAP requirements provided in the Contract in Section 1.104 II.B.

The Medicaid Functional requirements identify what the fraud detection system must do to enable performance of work tasks and any applicable service levels.

The Contractor has responded whether or not their proposed solution complies with each requirement by checking *the box that applies to each requirement in the columns labeled: **Yes**, **Yes with Modifications**, or **No**.*

- a. **Yes** – *is defined as the Contractor’s solution complies with all aspects of the requirement and is currently a standard feature.*
 - *In the **comment box** the Contractor may provide comments and descriptions on compliance, but are not required to.*
- b. **Yes with Modification** – *is defined as the solution does not currently comply with the requirement but the Contractor can modify the solution through configuration, programming or source code changes which, in the Contractor’s opinion, would result in their solution reaching full compliance with a requirement. If a modification is required to the solution, fill in the column with **A**, **B** or **C** as defined below:*
 - A.** *Configuration required to comply with the requirement*
 - B.** *Programming required to comply with the requirement*
 - C.** *Source code change required to comply with the requirement*
 - *In the **comment box** the Contractor has described the modification that will be made and how it will comply with the requirement. All such modifications are considered to be part of the solution being proposed and included in the Appendix H Medicaid Pricing.*
- c. **No** – *is defined as the Contractor’s proposed solution does not comply with all aspects of the requirement.*
 - *In the **comment box** the Contractor has described the impact of not meeting the requirement.*



Contract Ref. #	Medicaid Functional Requirement		Yes	Yes, with Modification (A, B or C)	No	Comments
1. Fraud Functions: General						
1-1	1-1	The system must identify and report attempted fraud by individuals and groups using predictive analytics based on information derived from the DTMB Data Warehouse.		X, B		The SAS Fraud Framework employs a hybrid approach to detecting and preventing fraud, waste, and abuse by employing business rules, anomaly detection, predictive modeling and social network analysis. The framework will enable these methods to operate on the DTMB Data Warehouse data.
1-2	1-2	The system must analyze and identify possible characteristics of Medicaid program fraud perpetrated by Medicaid providers using predictive analytics.		X, B		The SAS Fraud Framework employs a hybrid approach to detecting and preventing fraud, waste, and abuse by employing business rules, anomaly detection, predictive modeling and social network analysis. The analysis identifies characteristics that may indicate fraud on all entities, including Medicaid providers..
1-3	1-3	The system must analyze and identify possible characteristics of Medicaid, UI and PA fraud perpetrated by State staff using predictive analytics.		X, B		The SAS Fraud Framework employs a hybrid approach to detecting and preventing fraud, waste, and abuse by employing business rules, anomaly detection, predictive modeling and social network analysis. The analysis identifies characteristics that may indicate fraud on all entities, including agency staff members.
1-6	1-4	The system must identify the potential individual and organized fraud using predictive analytics in the Medicaid program where an individual could mean either a Medicaid beneficiary or a Medicaid provider.		X, B		The SAS Fraud Framework employs a hybrid approach to detecting and preventing fraud, waste, and abuse by employing business rules, anomaly detection, predictive modeling and social network analysis. This enables us to identify fraud by individual entities (beneficiaries and providers) as well as organized, collusive fraud rings in Medicaid programs.
1-7	1-5	The system must analyze and identify possible characteristics of Medicaid fraud perpetrated by beneficiaries using predictive analytics.		X, B		The SAS Fraud Framework employs a hybrid approach to detecting and preventing fraud, waste, and abuse by employing business rules, anomaly detection, predictive modeling and social network analysis. The analysis identifies characteristics that may indicate fraud on all entities, including fraud perpetrated by beneficiaries.

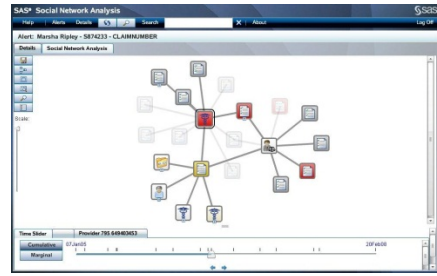


Contract Ref. #	Medicaid Functional Requirement		Yes	Yes, with Modification (A, B or C)	No	Comments
2. Fraud Functions: Medicaid Beneficiaries						
2-1	2-1	The system must verify information from a Medicaid beneficiary, UI claimant, and PA recipient.		X, B		The system can be configured to compare and verify information the state has about a claimant or recipient and flag discrepancies. A weighted score representing the associated risk with such a scenario can also be generated and used in conjunction with other indicators.
2-3	2-2	The system must be flexible enough to allow for analysis and reporting that can be performed on an ad hoc /on demand basis.		X, A		Ad hoc / on demand analysis and reporting is supplied by default. While the strength of the systems lies in the multiple, weighted scoring , execution of the a deployed detection analytic test can be enabled for individual execution.
2-4	2-3	Data Analysis: The system must use data analytics to analyze accumulated data from the DTMB Data Warehouse to verify information from a Medicaid beneficiary, UI claimant, and/or PA recipient and utilize data analytics to detect potential patterns of fraud.		X, B		The SAS Fraud Framework employs a hybrid approach to detecting and preventing fraud, waste, and abuse by employing business rules, anomaly detection, predictive modeling and social network analysis. The framework will enable these methods to operate on the DTMB Data Warehouse data for information verification and fraud detection.
2-5	2-4	User ID pattern: The system must identify user IDs that are the same or have slight variations, e.g. ABC123, ABC1234.	X			The SAS Fraud Framework employs sophisticated data quality, data matching, and entity resolution capabilities that allow for the identification of entities with slight variations, including individuals, companies and addresses.
2-6	2-5	State ID pattern: The system must analyze Medicaid beneficiaries according to their State ID and/or State Driver License for valid patterns.	X			The SAS Fraud Framework employs sophisticated data quality capabilities that allow for the identification and analysis of patterns in data field, including SSN, State ID, phone number, and Driver License.
2-7	2-6	The system must analyze Medicaid beneficiaries, UI claimants, and PA benefit recipients against the SSA disability database to identify potential fraudulent Medicaid applications/ redeterminations, UI claims and PA applications/redeterminations.		X, A		The system can be configured to compare and verify available third-party information the state has access to, including SSA disability data to flag potential discrepancies related to application and eligibility redeterminations. A weighted score representing the associated risk with such a scenario can also be generated and used in conjunction with other indicators.
2-8	2-7	Birthday pattern: The system must analyze UI claimants, Medicaid beneficiaries, and PA recipients according to their birth date and detect patterns of claims using the same birthday over a period of time.		X, B		The system can be configured to analyze birth data across entities and time in order to identify claims using the same, or slightly different birthday over time.



Contract Ref. #	Medicaid Functional Requirement		Yes	Yes, with Modification (A, B or C)	No	Comments
2-9	2-8	Address patterns: The system must analyze Medicaid beneficiaries, UI claimant, and PA recipient address discrepancies detected from external data sources.		X, B		The system can be configured to compare and verify available external data sources the State has access to and flag potential discrepancies related to address or slightly different addresses. A weighted score representing the associated risk with such a scenario can also be generated and used in conjunction with other indicators.
2-11	2-9	Repeated IP address: The system must identify multiple Medicaid applications/ redeterminations, UI claims and PA applications/ redeterminations originating within a user-defined time period from the same IP address (e.g. UI claims are filed within a week; PA redeterminations can be within 30 days).		X, B		The system can be configured to analyze IP addresses across entities and time in order to identify claims and eligibility redeterminations using the same IP addresses. A weighted score representing the associated risk with such a scenario can also be generated and used in conjunction with other indicators.
2-12	2-10	Prior detection: The system must identify Medicaid beneficiaries, UI claimants and PA recipients with a prior history of fraud detection.		X, A		The system can be configured to identify claimants, employers, recipients or other entities of interest with a prior history of fraud, as well as score the associated risk of such activity.
2-13	2-11	Incarceration: The system must verify information from a Medicaid beneficiary, UI claimant and PA recipient against incarceration records/data.		X, A		The system can be configured to compare and verify available external data sources the state has access to, including incarceration/corrections data, to flag potential cross-matches, as well as score the associated risk of such cross-matches.



Contract Ref. #	Medicaid Functional Requirement		Yes	Yes, with Modification (A, B or C)	No	Comments
2-14	2-12	Social network pattern: The system must utilize Web services to detect patterns in social networks to identify fraud in Medicaid, public assistance and unemployment insurance.		X, B		<p>The system can be configured to detect collusive patterns of fraud by linking entities on relevant data attributes for a more complete picture of potentially fraudulent activity at the network level as well as the entity level. This capability has been deployed to our labor and public assistance customers, as well as government healthcare.</p> <p>SAS Fraud Framework inherently leverages specific web services for alert and network generation. Web services can be called and leveraged as part of detection or make detection routines/models available via a web service as necessary.</p> <p>The diagram below is an example of a social network, or linkage graph of a medical provider, created by linking the provider to other providers and hospitals through patients that have filed claims as well as demographic information about the providers, facilities and patients in question.</p> 
2-18	2-13	Close-to-beneficiary address: The system must analyze related Medicaid claims based on the purified street address.		X, B		<p>The system can be configured to analyze beneficiary addresses and distances between them or any other geographic point. A weighted score representing the associated risk with such a scenario can also be generated and used in conjunction with other indicators.</p>
2-25	2-14	The system must provide the ability for end users to restrict analysis scenario results to Medicaid claims filed within the user-specified range of dates.		X, B		<p>The system can be configured to allow end users to filter scenario results to any desired parameters. A weighted score representing the associated risk with such a scenario can also be generated and used in conjunction with other indicators.</p>
2-29	2-15	High volume of claims: The system must analyze unusually high volumes of claims by Medicaid beneficiaries.		X, A		<p>The system can be configured to identify and analyze such activity. A weighted score representing the associated risk with such a scenario can also be generated and used in conjunction with other indicators.</p>



Contract Ref. #	Medicaid Functional Requirement		Yes	Yes, with Modification (A, B or C)	No	Comments
2-30	2-16	The system must provide a user-definable parameter to set the value for unusually high volumes of billable health care service usage by Medicaid beneficiaries.		X, A		The system can accept user-defined parameters and set thresholds for the specified scenario to be alerted.
2-35	2-17	Time period between transactions pattern: The system must detect and analyze Medicaid beneficiary transactions which occur within a user-defined time period.		X, B		The system can be configured to identify and analyze such activity. The system can accept user-defined parameters and set thresholds for the specified scenario to be alerted. A weighted score representing the associated risk with such a scenario can also be generated and used in conjunction with other indicators.
2-36	2-18	The system must provide a user-definable parameter to set the time period between transactions by a Medicaid beneficiary.		X, B		The system can accept user-defined parameters and set thresholds for the specified scenario to be alerted.
2-39	2-19	Medicaid beneficiaries, public assistance recipients and UI claimants: The system must analyze Medicaid beneficiaries, PA recipients and UI claimants to identify potential fraud across programs.		X, B		The system can be configured to compare and verify across data sources the state has access to, including UI, PA and Medicaid data, to flag potential cross-matches, as well as score the associated risk of such cross-matches.
3. Fraud Functions: Medicaid Providers						
5-1	3-1	The system must verify information from a Medicaid provider.		X, B		The system can be configured to compare and verify against available data sources the state has access to flag potential discrepancies. A weighted score representing the associated risk with such a scenario can also be generated and used in conjunction with other indicators.
5-2	3-2	High volume of Medicaid provider payments: The system must analyze unusually high volumes of payments to Medicaid providers.		X, A		The system can be configured to identify and analyze such activity. Payment activity can be compared across groups or individuals where those that are anomalous or are outliers are flagged. A weighted score representing the associated risk with such a scenario can also be generated and used in conjunction with other indicators.
5-3	3-3	The system must provide a user-definable parameter to set the value for unusually high volumes of payments to Medicaid providers.		X,A		The system can accept user-defined parameters and set thresholds for the specified scenario to be alerted.

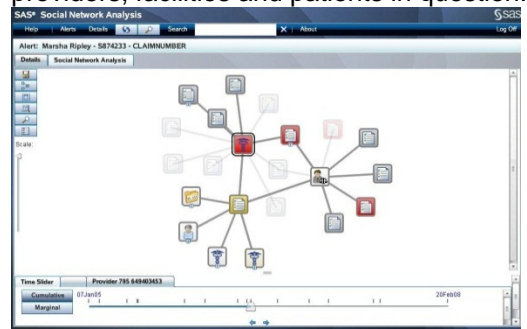


Contract Ref. #	Medicaid Functional Requirement		Yes	Yes, with Modification (A, B or C)	No	Comments
5-4	3-4	Multiple payments for a single beneficiary: The system must analyze multiple reimbursements for a single Medicaid beneficiary within a configurable time frame.		X, A		The system can be configured to identify and analyze such activity. The system can accept user-defined parameters and set thresholds for the specified scenario to be alerted. A weighted score representing the associated risk with such a scenario can also be generated and used in conjunction with other indicators.
5-5	3-5	Even dollar transactions: The system must detect patterns of even dollar transactions for a Medicaid provider.		X, B		The system can be configured to identify and analyze such activity. A weighted score representing the associated risk with such a scenario can also be generated and used in conjunction with other indicators.
5-8	3-6	Off-hours transactions: The system must detect and analyze off-hour transactions for Medicaid providers where 'off-hours' is a configurable time frame.		X, B		The system can be configured to identify and analyze such activity. The system can accept user-defined parameters and set thresholds for the specified scenario to be alerted. A weighted score representing the associated risk with such a scenario can also be generated and used in conjunction with other indicators.
5-9	3-7	Time period between transactions pattern: The system must detect and analyze Medicaid provider transactions which occur within a user-defined time period.		X, B		The system can be configured to identify and analyze such activity. The system can accept user-defined parameters and set thresholds for the specified scenario to be alerted. A weighted score representing the associated risk with such a scenario can also be generated and used in conjunction with other indicators.
5-10	3-8	The system must provide a user-definable parameter to set the time period between transactions by a Medicaid provider.		X, A		The system can accept user-defined parameters and set thresholds for the specified scenario to be alerted.
5-11	3-9	Exceeded threshold amount transactions: The system must analyze transaction amounts which have exceeded a user-defined threshold amount for transactions by a Medicaid provider.		X, A		The system can be configured to identify and analyze such activity. The system can accept user-defined parameters and set thresholds for the specified scenario to be alerted. A weighted score representing the associated risk with such a scenario can also be generated and used in conjunction with other indicators.
5-12	3-10	The system must provide user-defined parameters to set the threshold amount for the Exceeded threshold amount by a Medicaid provider.		X, B		The system can accept user-defined parameters and set thresholds for the specified scenario to be alerted.



Contract Ref. #	Medicaid Functional Requirement		Yes	Yes, with Modification (A, B or C)	No	Comments
5-14	3-11	Prior detection: The system must identify Medicaid providers with a prior history of fraud detection.		X, B		The system can be configured to identify providers or other entities of interest with a prior history of fraud, waste, and abuse, A weighted score representing the associated risk with such a scenario can also be generated and used in conjunction with other indicators.
3-2	3-12	Fictitious Medicaid provider: The system must analyze variations of provider names, addresses, type of services performed, dates of services performed, phone numbers, how the claim or provider application/redetermination was filed (Internet or phone), etc., to identify fictitious providers.		X, B		The system can be configured to identify and analyze such activity. The SAS Fraud Framework employs sophisticated data quality, data matching, and entity resolution capabilities that allow for the identification of entities with slight variations, including individuals, companies and addresses. A weighted score representing the associated risk with such a scenario can also be generated and used in conjunction with other indicators.
3-3	3-13	Abandoned building pattern: The system must analyze Medicaid claims, applications/ determinations and provider accounts to detect providers who have registered an address which is designated as abandoned.		X,B		The system can be configured to identify and analyze such activity. The SAS Fraud Framework employs data verification capabilities to identified deliverable addresses. If a data source of abandoned addresses is available, the analysis can be enabled. A weighted score representing the associated risk with such a scenario can also be generated and used in conjunction with other indicators.
3-4	3-14	Terminated building pattern: The system must analyze Medicaid claims, applications/ redeterminations and provider accounts to detect providers who have registered an address for a building which is no longer valid.		X, B		The system can be configured to identify and analyze such activity. The SAS Fraud Framework employs data verification capabilities to identified deliverable addresses which can point to a terminated building scenario. A weighted score representing the associated risk with such a scenario can also be generated and used in conjunction with other indicators.
3-7	3-15	Data analysis: The system must analyze accumulated data to detect Medicaid provider fraud.		X, A		The system relies on accumulated data to employ the hybrid approach of business rules, anomaly detection, predictive modeling and link analysis to detect provider fraud.
3-8	3-16	High percentage of claims: The system must identify Medicaid providers that have a high percentage of Medicaid claims filed in relation to the size of their client base.		X, A		The system can be configured to identify and analyze such activity. A weighted score representing the associated risk with such a scenario can also be generated and used in conjunction with other indicators.



Contract Ref. #	Medicaid Functional Requirement		Yes	Yes, with Modification (A, B or C)	No	Comments
3-19	3-17	Repeated IP address for registration: The system must identify multiple Medicaid provider registrations within a given a specified time period originating from the same IP address.		X, B		The system can be configured to analyze IP addresses across entities and time in order to identify registrations using the same IP addresses. A weighted score representing the associated risk with such a scenario can also be generated and used in conjunction with other indicators.
2-14	3-18	Social network pattern: The system must utilize Web services to detect patterns in social networks to identify fraud for Medicaid providers.		X, B		<p>The system can be configured to detect collusive patterns of fraud by linking entities on relevant data attributes for a more complete picture of potentially fraudulent activity at the network level as well as the entity level. This capability has been deployed to our labor and public assistance customers, as well as government healthcare.</p> <p>SAS Fraud Framework inherently leverages specific web services for alert and network generation. Web services can be called and leveraged as part of detection or make detection routines/models available via a web service as necessary.</p> <p>The diagram below is an example of a social network, or linkage graph of a medical provider, created by linking the provider to other providers and hospitals through patients that have filed claims as well as demographic information about the providers, facilities and patients in question.</p> 
2-13	3-19	Incarceration: The system must verify information from Medicaid providers against incarceration records/data.		X,A		The system can be configured to compare and verify available external data sources the state has access to, including incarceration/corrections data, to flag potential cross-matches, as well as score the associated risk of such cross-matches.



Contract Ref. #	Medicaid Functional Requirement		Yes	Yes, with Modification (A, B or C)	No	Comments
New	3-20	Provider ID: The system must identify any ID associated with Medicaid providers that are the same or have slight variations, e.g. ABC123, ABC1234.		X, B		The SAS Fraud Framework employs sophisticated data quality, data matching, and entity resolution capabilities that allow for the identification of entities with slight variations, including IDs, individuals, companies and addresses.
Fraud Functions: Internal Staff						
4-1	4-1	The system must identify internal fraud by employees or contractors of the state of Michigan including those with access to Medicaid, unemployment insurance and /or public assistance agencies and systems.		X, B		The SAS Fraud Framework employs a hybrid approach to detecting and preventing fraud, waste, and abuse by employing business rules, anomaly detection, predictive modeling and social network analysis. The analysis identifies characteristics that may indicate fraud on all entities, including agency employees and staff.
4-2	4-2	Data analysis: The system must use data analytics to analyze accumulated data to detect internal fraud committed by state employees.		X, B		The system relies on accumulated data to employ the hybrid approach of business rules, anomaly detection, predictive modeling and link analysis to detect fraud, waste, and abuse committed by agency employees.
4-3	4-3	IP Addresses: The system must analyze the source of the IP Address to identify continued Medicaid claims, UI claims and ongoing PA benefits originating from a state agency.		X, B		The system can be configured to analyze IP addresses across entities and time in order to identify claims and benefits originating from the same IP addresses. A weighted score representing the associated risk with such a scenario can also be generated and used in conjunction with other indicators.
4-4	4-4	Employee address cross match: The system must cross match combinations of Medicaid Claims, UI Claims and PA applications/ redeterminations against the employee addresses to identify employees who claim Medicaid benefits, UI benefits, PA benefits and model payments while still employed by the State.		X, B		The system can be configured to identify and analyze such activity. Data can be cross-matched against employee addresses in order to flag addresses, or similar addresses of State employees that may be receiving benefits. A weighted score representing the associated risk with such a scenario can also be generated and used in conjunction with other indicators.
4-5	4-5	Employee filing as beneficiary: The system must cross match the Medicaid claims against the State payroll records to identify employees who claim Medicaid benefits while still employed by the State.		X, A		The system can be configured to identify and analyze such activity. Data can be cross-matched against employee records in order to flag names or addresses of State employees that may be receiving benefits. A weighted score representing the associated risk with such a scenario can also be generated and used in conjunction with other indicators.



Contract Ref. #	Medicaid Functional Requirement		Yes	Yes, with Modification (A, B or C)	No	Comments
4-7	4-6	Repeated employee involvement on Medicaid claims processing: The system must analyze unusually high volumes of claims processing by a particular employee.		X, B		The system can be configured to identify and analyze such activity. Processing activity can be compared across groups or individuals where those that are anomalous or are outliers are flagged. A weighted score representing the associated risk with such a scenario can also be generated and used in conjunction with other indicators.
4-9	4-7	Staff involvement for high number of claims: The system must identify repeated involvement by a particular agency employee on Medicaid provider accounts with a high number of claims.		X, B		The system can be configured to identify and analyze such activity. Claim activity can be compared across groups or individuals where those that are anomalous or are outliers are flagged. A weighted score representing the associated risk with such a scenario can also be generated and used in conjunction with other indicators.
4-10	4-8	Employee filing as Medicaid provider: The system must cross match Medicaid provider claims against the State payroll records to identify employees who submit claims for payments while still employed by the state.		X, B		The system can be configured to identify and analyze such activity. Data can be cross-matched against employee information in order to flag State employees that may be receiving benefits. A weighted score representing the associated risk with such a scenario can also be generated and used in conjunction with other indicators.
4-11	4-9	Repeated employee involvement on Medicaid applications: The system must analyze unusually high volumes of opening and/or processing changes to Medicaid applications and ongoing cases by a particular state employee relative to the office average.		X, B		The system can be configured to identify and analyze such activity. Application activity can be compared across groups or individuals where those that are anomalous or are outliers are flagged. A weighted score representing the associated risk with such a scenario can also be generated and used in conjunction with other indicators.



Contract Ref. #	Medicaid Functional Requirement		Yes	Yes, with Modification (A, B or C)	No	Comments
Fraud Functions: Medicaid Specific						
New	5-1	The system must be able to employ Michigan specific fraud algorithms and algorithms used by CMS, HHS OIG and other state Medicaid programs or other health insurance providers and be kept up-to-date with emerging fraud trends and best practices.		X,B		The SAS Fraud Framework employs a hybrid approach to detecting and preventing fraud, waste, and abuse by employing business rules, anomaly detection, predictive modeling and social network analysis. While the solution provides SAS-designed algorithms tuned for Michigan data, other algorithms (Michigan, state, federal) not included in the solution can be deployed
New	5-2	The system must be able to identify over-utilization and under-utilization of Medicaid services.		X, B		The system can be configured to identify and analyze such activity. Utilization can be compared across groups or individuals where those that are anomalous or are outliers are flagged. A weighted score representing the associated risk with such a scenario can also be generated and used in conjunction with other indicators.
New	5-3	The system must be able to generate Medicaid provider, or provider group profiles for rendering, billing, referring and prescribing providers.		X, B		The system can be configured to create entity profiles. A weighted score representing the associated risk with such a scenario can also be generated and used in conjunction with other indicators.
New	5-4	The system must be able to apply or suppress rules based on Medicaid beneficiary, provider, or managed care organization (e.g. exclude individuals from exception processing).		X, B		The system allows for suppression of alerts on flagged entities. Various suppression rules can be configured to fit the agency's process.
New	5-5	The system must analyze any combination across Medicaid provider types and claim types down to the procedure code; diagnosis code, national drug codes (NDC), Diagnosis Related Groupings (DRGs) level and other user-defined parameters.		X, B		The system can be configured to analyze any combination of available data attributes including user defined attributes. A weighted score representing the associated risk with such analysis can also be generated and used in conjunction with other indicators.
New	5-6	Exception processing: the system must be able to provide an established set of exception processing criteria and automatically flag and report occurrences.		X, B		The system can be configured to accommodate specific exception criteria as well as flag and report on these exceptions.



Contract Ref. #	Medicaid Functional Requirement		Yes	Yes, with Modification (A, B or C)	No	Comments
New	5-7	The system must be able to identify significant spikes and dips in Medicaid services by provider(s) and beneficiaries and identify other types of significant aberrant trends by selected date ranges.		X, B		The system can be configured to identify and analyze such activity. Services provided or consumed are monitored over time where those that are anomalous or are outliers are flagged. A weighted score representing the associated risk with such a scenario can also be generated and used in conjunction with other indicators.
New	5-8	The system must be able to identify improbable Medicaid service/procedure frequencies and/or quantities utilizing the National Correct Coding Initiative (NCCI) and medically unlikely events (MUE) code sets as a guide.		X, B		The system identifies improbable and anomalous service/procedure frequencies and quantities based on various sources, including NCCI and MUE.
New	5-9	The system must be able to provide unduplicated count of Medicaid beneficiaries, providers, and services at any level of user-defined summarization.		X, A		The SAS Fraud Framework solution provides the capability for end users to create, customize and modify reports and dashboards. Data elements collected, stored and analyzed can be made available for canned or ad hoc reporting.
New	5-10	The system must allow users to link to Medicaid provider data and/or access to the provider's specific claim details that were identified by a query.		X, B		The system provides drill-down access to the supporting detail data related to an alerted entity. This includes provider, beneficiary and claim detail.
New	5-11	The system must be able to rank Medicaid providers, prescribers, beneficiaries, and procedure or diagnosis codes based on user-defined parameters for provider type, provider specialty, and claim type combinations.		X, B		Detection scenarios generate a weighted score representing the associated risk is used to rank the desired entities. Users are able to sort and filter these ranked lists on the desired parameters
New	5-12	The system must allow the user to query the data to select, compare, and report data for both Medicaid fee for service (FFS) and Medicaid managed care organization (MCO) delivery systems, to include any: Element or combination of elements in the data; Claim types or combination of claim types; Provider types or combination of provider types; and Provider specialties or combination of provider specialties		X, A		The SAS Fraud Framework solution provides the capability for end users to create, customize and modify reports and dashboards. Data elements collected, stored and analyzed can be made available for canned or ad hoc reporting with the parameters arithmetic operations stated.



Contract Ref. #	Medicaid Functional Requirement		Yes	Yes, with Modification (A, B or C)	No	Comments
New	5-13	<p>Medicaid reporting: following the completion of fraud analysis queries and scenarios, the system must be able to sort and rank reports with user-defined criteria such as:</p> <p>Sort or select by procedure code, diagnosis code, NDC, DRG, provider, prescriber, or beneficiary;</p> <p>Report across all provider and beneficiary service types;</p> <p>Specify arithmetic, algebraic, and statistical calculations (e.g. subtotals, totals, percentages, ratios, percentiles, selections by less than, equal to or greater than criteria, unduplicated counts, rates, and frequency distributions);</p> <p>Focus reports based on day or date, maximum visits, location, zip code, multiple addresses;</p> <p>Report on beneficiary activity by day or date for provider in one or multiple locations</p>		X, A		The SAS Fraud Framework solution provides the capability for end users to create, customize and modify reports and dashboards. Data elements collected, stored and analyzed can be made available for canned or ad hoc reporting with the parameters arithmetic operations stated.
New	5-14	The system must allow profiling of provider billing practices and the review of beneficiary utilization of medical and pharmacy services.		X, B		The SAS Fraud Framework solution provides the capability for end users to create, customize and modify reports and dashboards. Data elements collected, stored and analyzed for fraud detection are available for canned or ad hoc reporting.
New	5-15	The system must analyze and test paid claims data (fee for service and encounter) to identify possible improper payments.	X			The system will analyze and test all paid claims data.
New	5-16	Excluded Medicaid Providers: the system must verify Medicaid providers do not exist in the List of Excluded Individuals/Entities (LEIE), Medicaid and Children's Health Insurance State Information Sharing System (MCSIS) and other such databases listing all providers prohibited from participating in the Medicaid and Medicare programs.		X, B		The system can be configured to compare and verify available state and third-party information the state has access to, including excluded providers to flag potential discrepancies related to banned providers. A weighted score representing the associated risk with such a scenario can also be generated and used in conjunction with other indicators.



Contract Ref. #	Medicaid Functional Requirement		Yes	Yes, with Modification (A, B or C)	No	Comments
New	5-17	Deceased: the system must be able to compare death certificate data and SSA records with the beneficiary eligibility file and the provider file to prevent improper payments and flag beneficiaries and providers that are deceased and still enrolled or have claims and/or dates of service after date of death.		X, B		The system can be configured to compare and verify available state and third-party information the state has access to, including death and SSA data to flag potential discrepancies related to improper payments. A weighted score representing the associated risk with such a scenario can also be generated and used in conjunction with other indicators.
New	5-18	Access to PARIS: the system must access PARIS, a federal program used to verify that Medicaid beneficiaries enrolled in the state's program are not enrolled in other states' programs.		X, B		The system can be configured to compare and verify available state and third-party information the state has access to, including federal enrollment data to flag potential discrepancies related to improper payments. A weighted score representing the associated risk with such a scenario can also be generated and used in conjunction with other indicators.
New	5-19	Profiling algorithms: the system must be able to develop profiling algorithms for both Medicaid providers and beneficiaries.		X, B		The systems profiling algorithms can be configured for both providers and beneficiaries. Additionally, new algorithms can be developed and deployed.
New	5-20	The system must be able to identify and report on prior authorization and program exceptions.		X, B		The system can be configured to compare and verify available state and third-party information the state has access to, including prior authorization and program exceptions. A weighted score representing the associated risk with such a scenario can also be generated and used in conjunction with other indicators.
New	5-21	The system must be able to provide user-specified classifications as well as the following Medicaid group classifications: family members as well as aid categories treatment modalities tax identification number or other Medicaid provider reference file information program code and level of care		X, B		Ad hoc/on demand analysis and reporting is supplied by default providing users the ability to specify multiple classifications when slicing and dicing data.



Contract Ref. #	Medicaid Functional Requirement		Yes	Yes, with Modification (A, B or C)	No	Comments
New	5-22	The system must be able to link family members in analyzing Medicaid beneficiary fraud.		X, B		The system can be configured to detect collusive patterns of fraud by linking entities on relevant and available data attributes for a more complete picture of potentially fraudulent activity at the network level as well as the entity level. This social network analysis component is used as part of the hybrid-approach to detect fraud.
New	5-23	The system must be able to link Medicaid providers and/or beneficiaries within and across geographic areas.		X, B		The system can be configured to detect collusive patterns of fraud by linking entities on relevant and available data attributes for a more complete picture of potentially fraudulent activity at the network level as well as the entity level. This social network analysis component is used as part of the hybrid-approach to detect fraud.
New	5-24	The system must identify other insurance carriers with respect to third party liability to ensure Medicaid remains the payer of last resort.		X, B		The System can be configured to compare the Medicaid eligibility and claims data with other outside data sources, such as Medicare information and state employee health plan eligibility, to determine if there is third party liability.
New	5-25	The system must allow for creating and storing report schedules by various date spans (e.g. calendar year, state fiscal year, federal fiscal year, etc.)	X			The SAS Fraud Framework solution provides the capability for end users to create, customize and modify reports and dashboards. These reports can be scheduled to generate at various times with various reporting date spans.
New	5-26	Gender specific: the system must be able to identify Medicaid claims where gender specific requirements are incorrect.		X, A		The system can be configured to identify and analyze such activity. Violated gender requirements can be identified via the business rules in the hybrid approach. A weighted score representing the associated risk with such a scenario can also be generated and used in conjunction with other indicators.
New	5-27	Duplicate check: the system must be able to identify repeated claim submissions for paid, denied and suspended claims with duplicate beneficiary ID number, dates, and procedure codes.		X, A		The system can be configured to identify and analyze such activity. Duplicates over the specified attributes can be identified via the business rules in the hybrid approach. A weighted score representing the associated risk with such a scenario can also be generated and used in conjunction with other indicators.



Contract Ref. #	Medicaid Functional Requirement		Yes	Yes, with Modification (A, B or C)	No	Comments
New	5-28	The system must be able to use supervised methods of data mining such as neural networks, decision trees, and logistic regression using Medicaid Fraud Control Unit (MFCU) referrals, LEIE, MCSIS etc. as dependent variables.		X, B		The SAS Fraud Framework employs a hybrid approach to detecting and preventing fraud, waste, and abuse by employing business rules, anomaly detection, predictive modeling and social network analysis. The predictive modeling component includes the listed supervised methods and can be configured for a number of dependent variables. These are used in conjunction with the other techniques to create a composite fraud-risk score.
New	5-29	The system must be able to use non supervised methods of data mining such as clustering.		X, B		The SAS Fraud Framework employs a hybrid approach to detecting and preventing fraud, waste, and abuse by employing business rules, anomaly detection, predictive modeling and social network analysis. The approach includes unsupervised methods, including clustering, used in conjunction with the other techniques to create composite fraud-risk score.
	General System Functionality					
6-1	6-1	Pattern Analysis: The system must use data analytics to detect patterns from disparate data sources in the DTMB Data Warehouse that could point to fraudulent activity.		X, B		The SAS Fraud Framework employs a hybrid approach to detecting and preventing fraud, waste, and abuse by employing business rules, anomaly detection, predictive modeling and social network analysis. The capabilities used collectively create a sophisticated detection engine that flags potentially fraudulent activity from any data sources ingested.
6-2	6-2	The system must identify known techniques for identity theft and organized fraud and include future enhancements when improvements are made in identification techniques to identity theft.		X, B		The SAS Fraud Framework employs a hybrid approach to detecting and preventing fraud, waste, and abuse by employing business rules, anomaly detection, predictive modeling and social network analysis. A library of program-specific detection methods around UI, PA, Medicaid and other areas such as Tax and Revenue is part of the solution for detecting opportunistic and organized fraud.



Contract Ref. #	Medicaid Functional Requirement		Yes	Yes, with Modification (A, B or C)	No	Comments
6-3	6-3	The system must provide pre-configured data analytics patterns which have been proven to identity theft and organized fraud.		X, B		The SAS Fraud Framework employs a hybrid approach to detecting and preventing fraud, waste, and abuse by employing business rules, anomaly detection, predictive modeling and social network analysis. A library of program-specific detection methods around UI, PA, Medicaid and other areas such as Tax and Revenue is part of the solution for detecting opportunistic and organized fraud.
6-4	6-4	Data Navigation: The system must provide the ability for the end user to navigate the result set included in a given audit and/or analysis.		X, A		The SAS Fraud Framework provides an Alert Management interface allowing users to navigate and drill down on results sets flagged by the detection processes.
6-5	6-5	The system must provide the drill down techniques that allow information to be filtered and sorted in varying levels of detail by the end user.		X, A		The SAS Fraud Framework provides an Alert Management interface allowing users to navigate and drill down on results sets flagged by the detection processes. Filtering and sorting of result sets is configurable.
6-6	6-6	Data Filtering: The system must provide the ability for the end user to select the level of data filtering to decrease or increase the result set included in a given audit and/or analysis.		X, A		The SAS Fraud Framework provides an Alert Management interface allowing users to navigate and drill down on results sets flagged by the detection processes. Filtering and sorting of result sets is configurable.
6-7	6-7	Technical Knowledge Requirements: The system must provide the ability for end users to configure and execute analysis scenarios without knowledge of query languages (e.g. SQL).			X	The SAS Fraud Framework provides an Alert Administration interface that allows users to configure and deploy scenarios. While many scenarios do not require knowledge of SQL, some scenarios do require this knowledge.
6-8	6-8	The system must provide the ability for end users to configure and execute analysis scenarios without assistance from the Information Technology department.		X, A		The SAS Fraud Framework provides an Alert Administration interface that allows users to create, configure and deploy scenarios without the assistance of the IT department.
6-9	6-9	The system must provide the ability to configure and execute analysis scenarios without requiring the end user to have knowledge of the underlying data sources and structures.			X	The SAS Fraud Framework provides an Alert Administration interface that allows users to configure and deploy scenarios. While many scenarios do not require knowledge of underlying data sources, some scenarios do require this knowledge.
6-10	6-10	The system must be deployable with only minimal assistance and support of the Information Technology department.	X			The installation and configuration can be performed by SAS, thus minimizing the resources required from the Information Technology department.



Contract Ref. #	Medicaid Functional Requirement		Yes	Yes, with Modification (A, B or C)	No	Comments
6-11	6-11	Create analysis scenarios: The system must provide the ability for end users to create ad hoc and scheduled analysis scenarios for simple and complex queries where the end user has knowledge of the underlying data sources and data structure.		X, B		The SAS Fraud Framework provides an Alert Administration interface that allows users to configure and deploy scenarios in batch (scheduled). Ad hoc scenarios can also be created, vetted and saved with web-based and thin-client analysis tools.
6-12	6-12	Saving analysis scenarios: The system must provide the ability for end users to save ad hoc analysis scenarios for future reuse.	X			The SAS Fraud Framework provides an Alert Administration interface that allows users to configure and deploy scenarios in batch (scheduled). Ad hoc scenarios can also be created, vetted and saved with web-based and thin-client analysis tools for future use and deployment.
6-13	6-13	Modify analysis scenarios: The system must provide the ability for end users to modify ad hoc analysis scenarios and re-save for future reuse.	X			The SAS Fraud Framework provides an Alert Administration interface that allows users to create, configure and deploy scenarios in batch (scheduled). Ad hoc scenarios can also be created, vetted, modified and saved with web-based and thin-client analysis tools for future use and deployment.
6-14	6-14	Saving results: The system must provide the ability for the end user to save the result set of an audit and/or analysis for future reference.	X			Result sets of individual audits can be saved for future reference.
6-15	6-15	The system must provide the ability for the end user to save the result set of an audit and/or analysis in common output formats (e.g. Word, Excel, flat file).	X			Result sets of individual audits can be saved for future reference and output in common formats including MS Office formats, PDF, and flat files.
6-16	6-16	The system must provide the ability for the end user to export the result set of an audit and/or analysis in common output formats.	X			Result sets of individual audits can be saved for future reference and output in common formats including MS Office formats, PDF, and flat files.
6-17	6-17	Modify result set: The system must provide the ability for the end user to modify the analysis scenario result set based on a refresh of existing analysis scenarios as they are developed.	X			Ad hoc scenarios can also be created, vetted, modified and saved with web-based and thin-client analysis tools. Users can modify the scenarios and refresh results sets as they are developed and/or modified.
6-18	6-18	Analysis scenario execution: The system must provide the ability for the end user to execute both ad hoc and saved analysis scenarios.	X			Users can modify ad hoc and saved scenarios and refresh results sets as they are developed and/or modified.



Contract Ref. #	Medicaid Functional Requirement		Yes	Yes, with Modification (A, B or C)	No	Comments
6-19	6-19	The system must provide the ability for the end user to execute an analysis scenario immediately.	X			Users can modify ad hoc and saved scenarios and refresh results sets immediately.
6-20	6-20	The system must provide the ability for the end user to schedule the execution of analysis scenarios as a batch process.		X, B		The SAS Fraud Framework provides an Alert Administration interface that allows users to configure and deploy scenarios in batch (scheduled).
6-21	6-21	The system must provide the ability for the end user to modify the parameters of an existing analysis scenario.		X, B		The SAS Fraud Framework provides an Alert Administration interface that allows users to create, configure and deploy scenarios as well as modify existing scenarios.
6-22	6-22	The system must provide predefined analysis scenario parameters. (E.g. previous month, previous quarter, etc.)		X, B		The SAS Fraud Framework provides existing parameters related to the applicable analysis. Pre-defined parameters can be used as-is or modified by end users.
6-23	6-23	Scoring framework: The system must provide the ability to assign a probability/weighting to the patterns that make up a potential fraud case.		X, B		The SAS Fraud Framework employs a hybrid approach to detecting and preventing fraud, waste, and abuse by employing business rules, anomaly detection, predictive modeling and social network analysis. Each of the multiple outputs of these techniques provides a weighted input to an overall fraud risk score that helps prioritize cases as well as reduce the false positives.
6-24	6-24	The system must provide the ability to assign a probability/ weighting based on the likelihood of fraud applying user definable criteria (I.e. length of time a person has had an overpayment).		X, B		The SAS Fraud Framework employs a hybrid approach to detecting and preventing fraud, waste, and abuse by employing business rules, anomaly detection, predictive modeling and social network analysis. Each of the multiple outputs of these techniques provides a weighted input to an overall fraud risk score that helps prioritize cases as well as reduce the false positives.
6-25	6-25	The system must provide the ability for end users to define the criteria used for probability/ weighting of the potential fraud characteristics.		X, A		The SAS Fraud Framework employs a hybrid approach to detecting and preventing fraud, waste, and abuse by employing business rules, anomaly detection, predictive modeling and social network analysis. Each of the multiple outputs of these techniques provides a weighted input to an overall fraud risk score that helps prioritize cases as well as reduce the false positives. The weighting of each component is configurable by an end user.



Contract Ref. #	Medicaid Functional Requirement		Yes	Yes, with Modification (A, B or C)	No	Comments
6-26	6-26	The system must aggregate scores of detected patterns when creating a fraud detection work item for a Medicaid beneficiary, UI claimant, PA recipient, internal staff, employer, Medicaid provider and provider/retailer.		X, B		The SAS Fraud Framework employs a hybrid approach to detecting and preventing fraud, waste, and abuse by employing business rules, anomaly detection, predictive modeling and social network analysis. Each of the multiple outputs of these techniques provides a weighted input to an overall fraud risk score that helps prioritize cases as well as reduce the false positives. The weighting of each component is configurable by an end user.
6-27	6-27	The system must provide the ability for end users to modify the scoring of the analysis scenario.		X, B		The SAS Fraud Framework employs a hybrid approach to detecting and preventing fraud by employing business rules, anomaly detection, predictive modeling and social network analysis. Each of the multiple outputs of these techniques provides a weighted input to an overall fraud risk score that helps prioritize cases as well as reduce the false positives. The weighting of each component is configurable by an end user.
6-28	6-28	The system must provide the ability for users based on their security role to adjust the scoring of a generated result set within cross-agency data.		X, A		The SAS Fraud Framework provides the ability to use logic to adjust the scoring of a generated result set, but this capability should be restricted to appropriate users.
6-29	6-29	The system must provide the ability for end users to score individual cases that could result in an overpayment.		X, B		The SAS Fraud Framework provides the ability for end users to score individual cases that could result in an overpayment.
6-30	6-30	The system must provide the ability for end users to score individual cases for possible identity theft.		X, B		The SAS Fraud Framework provides the ability for end users to score individual cases for possible identity theft.
6-31	6-31	The system must provide the ability for end users to score individual cases for possible internal staff fraud.		X, B		The SAS Fraud Framework provides the ability for end users to score individual cases for possible internal staff fraud.
6-32	6-32	The system must combine and adjust the score of an existing work item based on the weight of new and existing patterns detected for Medicaid beneficiaries, UI claimants, PA recipients, internal staff, employers, Medicaid providers and providers/ retailers.		X, B		The SAS Fraud Framework provides the ability for score adjustment based on the weights of other patterns.



Contract Ref. #	Medicaid Functional Requirement		Yes	Yes, with Modification (A, B or C)	No	Comments
6-33	6-33	The system must provide the ability for end users to designate Opt-in and Opt-out lists for rules scoring.		X, B		The SAS Fraud Framework provides the ability to create and maintain such lists for rules scoring.
6-34	6-34	Reporting: The system must provide a pre-configured report and dashboard library.			X	While the system has interfaces to view the alerted entities and associated detail data, no pre-configured reports or dashboards are provide. The solution deployments typically include report specification and creation specific for each state and agency. The creation of these reports and dashboards has been scoped as part of the implementation and will be tailored specifically to the unique needs of the State.
6-35	6-35	The system must provide pre-configured dashboards and reports for different user roles.			X	While the system has interfaces to view the alerted entities and associated detail data, no pre-configured reports or dashboards are provided. The solution deployments typically include report specification and creation specific for each state and agency. Groups and users can be denied or granted access to the generated reports. The creation of these reports and dashboards has been scoped as part of the implementation and will be tailored specifically to the unique needs of the State.
6-36	6-36	The system must provide the ability for end users to customize and modify existing reports and dashboards.	X			The SAS Fraud Framework solution provides the capability for end users to create, customize and modify reports and dashboards that are deployed, provided the user or group has authorization to do so.
6-37	6-37	The system must provide Key Performance Indicators for management staff.	X			The SAS Fraud Framework solution provides the capability for end users to create, customize and modify reports and dashboards that are deployed, including any Key Performance Indicators that the State specifies (including operational metrics).
6-38	6-38	The system must provide the ability for end users to create new reports and dashboards.	X			The SAS Fraud Framework solution provides the capability for end users to create, customize and modify reports and dashboards.
6-39	6-39	The system must provide the ability for end users to create new reports and dashboards by modifying existing reports and dashboards.	X			The SAS Fraud Framework solution provides the capability for end users to create, customize and modify reports and dashboards.



Contract Ref. #	Medicaid Functional Requirement		Yes	Yes, with Modification (A, B or C)	No	Comments
6-40	6-40	The system must provide the ability for the end user to review and enter data on the outcome of a case to improve the efficiency of future analysis scenario results.		X, B		The SAS Fraud Framework provides the capability to capture outcomes and results related to the alerts that are generated for the purpose of fine tuning the detection mechanisms in a “Learn and Improve”, thus improving detection and reducing false positives.
6-41	6-41	Performance: The system must execute ad hoc analysis scenarios in seconds or minutes, rather than hours.	X			The system can be configured and architected to meet the desired response times indicated by the State.
6-42	6-42	The system must execute scheduled analysis scenarios as a batch process which is assumed to take longer to generate than ad hoc analysis scenarios.	X			The SAS Fraud Framework solution provides batch-processing capabilities.
6-43	6-43	Data Sources: The system must utilize data from the DTMB Data Warehouse which contains data from multiple agencies.		X, A		The SAS Fraud Framework can be configured to leverage many data sources, including data from the DTMB Warehouse.
6-44	6-44	The system must use data analytics to detect patterns on data in the DTMB Data Warehouse (i.e. not against production data systems) that might reveal an organized attempt to defraud the state Medicaid, UI and PA systems.		X, B		The SAS Fraud Framework employs a hybrid approach to detecting and preventing fraud, wastes, and abuse by employing business rules, anomaly detection, predictive modeling and social network analysis. Each of the multiple outputs of these techniques provides a weighted input to an overall fraud risk score that helps reveal attempts to defraud the State. This can be performed on DTMD Data Warehouse data.
6-45	6-45	The system must interface analysis scenario results with agency systems used for fraud investigation based on the priority/scoring of the potential fraud case (e.g. high, medium or low risk).		X, A		The SAS Fraud Framework employs a hybrid approach to detecting and preventing fraud by employing business rules, anomaly detection, predictive modeling and social network analysis. Each of the multiple outputs of these techniques provides a weighted input to an overall fraud risk score that can be sorted in order to prioritize the case. Prioritization parameters are configurable.



Contract Ref. #	Medicaid Functional Requirement		Yes	Yes, with Modification (A, B or C)	No	Comments
6-46	6-46	The system must provide users the ability to update the analysis scenario results based on the outcome of a fraud investigation.		X, B		<p>The SAS Fraud Framework provides the ability to strengthen models by using investigative outcomes through an iterative approach.</p> <p>This is called our alert feedback loop. Detection techniques and rules can be created/updated to account for past/prior known outcomes for specific entities. Scenarios can be updated and the results would be applied the next time the alert generation process is executed.</p>
6-53	6-47	The system must utilize web services to integrate with LexisNexis.		X, B		The SAS Fraud Framework can consume or deploy web services for the purposes of integrating with other systems, including LexisNexis.
New	6-48	The system must interface with the CHAMPS system for Medicaid beneficiary fraud cases.		X, B		The SAS Fraud Framework can employ multiple technology methods to interface with the CHAMPS system.