



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 2

to

Contract Number 071B3200030

CONTRACTOR	OCCUPATIONAL RESEARCH AND ASS
	124 Elm Street
	Big Rapids, MI 49307
	Steven Clark
	231-796-2822
	sclark@orainc.com
	*****1703

STATE	Program Manager		MDE
	Contract Administrator	Malu Natarajan	DTMB
		(517) 284-7044	
		hatchd@michigan.gov	

CONTRACT SUMMARY				
CTE HOSTING, MAINTENANCE & SUPPORT				
INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE	
November 16, 2012	November 15, 2015	5 - 1 Year	November 15, 2016	
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 type="checkbox"/> Yes <input checked="" type="checkbox"/> No	
MINIMUM DELIVERY REQUIREMENTS				
N/A				
DESCRIPTION OF CHANGE NOTICE				
OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
<input checked="" type="checkbox"/>	1 Year	<input type="checkbox"/>		November 15, 2017
CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE		
\$178,984.00	\$57,528.00	\$236,512.00		
DESCRIPTION				
Effective 8/16/2016, the state exercises the second option year at the rate of \$ 57,528.00 per original cost tables. 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. 1
 to
CONTRACT NO. 071B3200030
 between
THE STATE OF MICHIGAN
 and

NAME & ADDRESS OF CONTRACTOR	PRIMARY CONTACT	EMAIL
Occupational Research and Assessment, Inc. 124 Elm Street Big Rapids, MI 49307	Dr. Steven Clark, PhD	sclark@orainc.com
	PHONE	CONTRACTOR'S TAX ID NO. (LAST FOUR DIGITS ONLY)
	(231) 796-2822	1703

STATE CONTACTS	AGENCY	NAME	PHONE	EMAIL
PROGRAM MANAGER / CCI				
CONTRACT ADMINISTRATOR	DTMB	Jarrod Barron	(517) 284-7045	Barronj1@michigan.gov

CONTRACT SUMMARY			
DESCRIPTION: CTE Hosting, Maintenance and Support			
INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW
November 16, 2012	November 15, 2015	5, one year	November 15, 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 type="checkbox"/> Yes <input checked="" 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	<input type="checkbox"/>		November 15, 2016
CURRENT VALUE		VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE	
\$169,395.00		\$9,589.00	\$178,984.00	

DESCRIPTION: Effective 8/26/2015, the State exercises the first option year at the rate of \$57,528.00 per the original cost tables, utilizing \$47,939.00 of existing contract funds and adding 9,589.00, for continuing maintenance and support. Remaining contract balance after amendment: \$6,400.00 per original Cost Tables 1a, 1b and 3). All other pricing, terms, and conditions remain the same. Per contractor and agency agreement and the approval of DTMB Procurement.

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. 071B3200030
 between
 THE STATE OF MICHIGAN
 and**

NAME & ADDRESS OF CONTRACTOR:	PRIMARY CONTACT	EMAIL
Occupational Research and Assessment, Inc. 124 Elm Street Big Rapids, MI 49307	Dr. Steven Clark, PhD	sclark@orainc.com
	TELEPHONE	CONTRACTOR #, MAIL CODE
	(231) 796-2822	

STATE CONTACTS	AGENCY	NAME	PHONE	EMAIL
CONTRACT COMPLIANCE INSPECTOR:				
BUYER:	DTMB	Reid Sisson	517-241-1638	sissonr@michigan.gov

CONTRACT SUMMARY:			
DESCRIPTION: Descriptive Contract Title (Not always the same language as provided in MAIN)			
CTE Hosting, Maintenance and Support			
INITIAL TERM	EFFECTIVE DATE	INITIAL EXPIRATION DATE	AVAILABLE OPTIONS
3 years	November 16, 2012	November 15, 2015	5, one year
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 type="checkbox"/> YES <input checked="" type="checkbox"/> NO
MINIMUM DELIVERY REQUIREMENTS:			
N/A			
MISCELLANEOUS INFORMATION:			
N/A			
ESTIMATED CONTRACT VALUE AT TIME OF EXECUTION:			\$169,395.00

THIS IS NOT AN ORDER: This Contract Agreement is awarded on the basis of our inquiry bearing the solicitation #REQ 084R2200157. Orders for delivery will be issued directly by the Department of Technology, Management & Budget through the issuance of a Purchase Order Form.

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. 071B3200030
 between
THE STATE OF MICHIGAN
 and

NAME & ADDRESS OF CONTRACTOR:	PRIMARY CONTACT	EMAIL
Occupational Research and Assessment, Inc. 124 Elm Street Big Rapids, MI 49307	Dr. Steven Clark, PhD	sclark@orainc.com
	TELEPHONE	CONTRACTOR #, MAIL CODE
	(231) 796-2822	

STATE CONTACTS	AGENCY	NAME	PHONE	EMAIL
CONTRACT COMPLIANCE INSPECTOR:				
BUYER:	DTMB	Reid Sisson	517-241-1638	sissonr@michigan.gov

CONTRACT SUMMARY:			
DESCRIPTION: Descriptive Contract Title (Not always the same language as provided in MAIN)			
CTE Hosting, Maintenance and Support			
INITIAL TERM	EFFECTIVE DATE	INITIAL EXPIRATION DATE	AVAILABLE OPTIONS
3 years	November 16, 2012	November 15, 2015	5, one year
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 type="checkbox"/> YES <input checked="" type="checkbox"/> NO
MINIMUM DELIVERY REQUIREMENTS:			
N/A			
MISCELLANEOUS INFORMATION:			
N/A			
ESTIMATED CONTRACT VALUE AT TIME OF EXECUTION:			\$169,395.00

THIS IS NOT AN ORDER: This Contract Agreement is awarded on the basis of our inquiry bearing the solicitation #REQ 084R2200157. 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 #:071B3200030

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



Table of Contents

DTMB Procurement 4

Article 1 – Statement of Work (SOW) 11

1.000 Project Identification 11

 1.001 Project Request 11

 1.002 Background 11

1.100 Scope of Work and Deliverables 11

 1.101 In Scope 11

 1.102 Out of Scope 12

 1.103 Environment 12

 1.103 Part A - Enterprise IT Policies, Standards, and Procedures: 12

 1.103 Part C - DTMB IT eMichigan Web Development Standard Tools: 13

 1.103 Part D - The State Unified Information Technology Environment (SUITE): 13

 1.103 Part E – EA Solution Assessment 13

 1.104 Work And Deliverables 15

 1.104 Part A: Services To Be Provided 15

1.200 Roles and Responsibilities 17

 1.201 Contractor Staff, Roles, and Responsibilities 17

 1.202 State Staff, Roles, and Responsibilities 19

 1.203 RESERVED - Other Roles And Responsibilities 20

1.300 Project Plan 20

 1.301 Project Plan Management 20

 1.302 Reports 21

1.400 Project Management 22

 1.401 Issue Management 22

 1.402 Risk Management 23

 1.403 Change Management 23

1.500 Acceptance 23

 1.501 Criteria 23

 1.502 Final Acceptance 24

1.600 Compensation and Payment 24

 1.601 Compensation And Payment 24

 1.602 RESERVED - Holdback 25

2.000 Contract Structure and Term 26

 2.001 Contract Term 26

 2.002 Options to Renew 26

 2.003 Legal Effect 26

 2.004 Attachments, Exhibits and Appendices 26

 2.005 Ordering 26

 2.006 Order of Precedence 26

 2.007 Headings 26

 2.008 Form, Function & Utility 27

 2.009 Reformation and Severability 27



- 2.010 Consents and Approvals.....27
 - 2.011 No Waiver of Default27
 - 2.012 Survival27
- 2.020 Contract Administration27
 - 2.021 Issuing Office27
 - 2.022 Contract Compliance Inspector27
 - 2.023 RESERVED28
 - 2.024 Change Requests28
 - 2.025 Notices29
 - 2.026 Binding Commitments29
 - 2.027 Relationship of the Parties29
 - 2.028 Covenant of Good Faith29
 - 2.029 Assignments.....29
- 2.030 General Provisions30
 - 2.031 Media Releases30
 - 2.032 Contract Distribution.....30
 - 2.033 Permits30
 - 2.034 Website Incorporation30
 - 2.035 Future Bidding Preclusion30
 - 2.036 Freedom of Information.....30
 - 2.037 Disaster Recovery.....30
- 2.040 Financial Provisions.....31
 - 2.041 Fixed Prices for Services/Deliverables.....31
 - 2.042 Adjustments for Reductions in Scope of Services/Deliverables.....31
 - 2.043 Services/Deliverables Covered31
 - 2.044 Invoicing and Payment – In General31
 - 2.045 Pro-ration31
 - 2.046 Antitrust Assignment31
 - 2.047 Final Payment31
 - 2.048 Electronic Payment Requirement.....32
- 2.050 Taxes32
 - 2.051 Employment Taxes32
 - 2.052 Sales and Use Taxes32
- 2.060 Contract Management32
 - 2.061 Contractor Personnel Qualifications.....32
 - 2.062 Contractor Key Personnel.....32
 - 2.063 Re-assignment of Personnel at the State’s Request33
 - 2.064 Contractor Personnel Location.....33
 - 2.065 Contractor Identification33
 - 2.066 Cooperation with Third Parties33
 - 2.067 Contract Management Responsibilities.....33
 - 2.068 Contractor Return of State Equipment/Resources.....34
- 2.070 Subcontracting by Contractor34



- 2.071 Contractor full Responsibility.....34
- 2.072 State Consent to delegation.....34
- 2.073 Subcontractor bound to Contract34
- 2.074 Flow Down34
- 2.075 Competitive Selection35
- 2.080 State Responsibilities35
 - 2.081 Equipment.....35
 - 2.082 Facilities35
- 2.090 Security.....35
 - 2.091 Background Checks35
 - 2.092 Security Breach Notification35
 - 2.093 PCI DATA Security Requirements35
- 2.100 Confidentiality36
 - 2.101 Confidentiality.....36
 - 2.102 Protection and Destruction of Confidential Information.....36
 - 2.103 Exclusions37
 - 2.104 No Implied Rights.....37
 - 2.105 Respective Obligations37
- 2.110 Records and Inspections37
 - 2.111 Inspection of Work Performed.....37
 - 2.112 Examination of Records37
 - 2.113 Retention of Records37
 - 2.114 Audit Resolution38
 - 2.115 Errors38
- 2.120 Warranties38
 - 2.121 Warranties and Representations.....38
 - 2.122 Warranty of Merchantability - RESERVED39
 - 2.123 Warranty of Fitness for a Particular Purpose - RESERVED39
 - 2.124 Warranty of Title - RESERVED39
 - 2.125 Equipment Warranty - RESERVED39
 - 2.126 Equipment to be New - RESERVED39
 - 2.127 Prohibited Products - RESERVED39
 - 2.128 Consequences for Breach.....39
- 2.130 Insurance39
 - 2.131 Liability Insurance39
 - 2.132 Subcontractor Insurance Coverage41
 - 2.133 Certificates of Insurance and Other Requirements41
- 2.140 Indemnification.....42
 - 2.141 General Indemnification42
 - 2.142 Code Indemnification42
 - 2.143 Employee Indemnification42
 - 2.144 Patent/Copyright Infringement Indemnification42
 - 2.145 Continuation of Indemnification Obligations.....43



- 2.146 Indemnification Procedures..... 43
- 2.150 Termination/Cancellation 44
 - 2.151 Notice and Right to Cure..... 44
 - 2.152 Termination for Cause..... 44
 - 2.153 Termination for Convenience 44
 - 2.154 Termination for Non-Appropriation..... 44
 - 2.155 Termination for Criminal Conviction 45
 - 2.156 Termination for Approvals Rescinded 45
 - 2.157 Rights and Obligations upon Termination 45
 - 2.158 Reservation of Rights..... 46
- 2.160 Termination by Contractor 46
 - 2.161 Termination by Contractor..... 46
- 2.170 Transition Responsibilities 46
 - 2.171 Contractor Transition Responsibilities..... 46
 - 2.172 Contractor Personnel Transition 46
 - 2.173 Contractor Information Transition..... 46
 - 2.174 Contractor Software Transition 46
 - 2.175 Transition Payments 47
 - 2.176 State Transition Responsibilities 47
- 2.180 Stop Work 47
 - 2.181 Stop Work Orders 47
 - 2.182 Cancellation or Expiration of Stop Work Order 47
 - 2.183 Allowance of Contractor Costs..... 47
- 2.190 Dispute Resolution..... 47
 - 2.191 In General 47
 - 2.192 Informal Dispute Resolution 48
 - 2.193 Injunctive Relief..... 48
 - 2.194 Continued Performance 48
- 2.200 Federal and State Contract Requirements 48
 - 2.201 Nondiscrimination..... 48
 - 2.202 Unfair Labor Practices..... 49
 - 2.203 Workplace Safety and Discriminatory Harassment..... 49
 - 2.204 Prevailing Wage – RESERVED/NA 49
- 2.210 Governing Law..... 49
 - 2.211 Governing Law 49
 - 2.212 Compliance with Laws 49
 - 2.213 Jurisdiction 49
- 2.220 Limitation of Liability 49
 - 2.221 Limitation of Liability..... 49
- 2.230 Disclosure Responsibilities 49
 - 2.231 Disclosure of Litigation 49
 - 2.232 Call Center Disclosure 50
 - 2.233 Bankruptcy 50



- 2.240 Performance51
 - 2.241 Time of Performance.....51
 - 2.242 Service Level Agreement (SLA).....51
 - 2.243 Liquidated Damages51
 - 2.244 Excusable Failure.....52
- 2.250 Approval of Deliverables.....53
 - 2.251 Delivery of Deliverables53
 - 2.252 Contractor System Testing.....53
 - 2.253 Approval of Deliverables, In General54
 - 2.254 Process for Approval of Written Deliverables.....55
 - 2.255 Process for Approval of Software Deliverables55
 - 2.256 Final Acceptance.....55
- 2.260 Ownership.....56
 - 2.261 Ownership of Work Product by State56
 - 2.262 Vesting of Rights56
 - 2.263 Rights in Data.....56
 - 2.264 Ownership of Materials56
- 2.270 State Standards56
 - 2.272 Acceptable Use Policy56
 - 2.273 Systems Changes57
- 2.280 Extended Purchasing.....57
 - 2.281 MiDEAL (Michigan Delivery Extended Agreements Locally - RESERVED.....57
 - 2.282 RESERVED - State Employee Purchases.....57
- 2.290 Environmental Provision - RESERVED/NA57
- 2.300 Deliverables57
 - 2.301 Software57
 - 2.302 RESERVED - Hardware.....57
- 2.310 Software Warranties57
 - 2.311 Performance Warranty57
 - 2.312 No Surreptitious Code Warranty57
 - 2.313 Calendar Warranty58
 - 2.314 Third-party Software Warranty58
 - 2.315 Physical Media Warranty58
- 2.320 Software Licensing58
 - 2.321 RESERVED - Cross-License, Deliverables Only, License to Contractor.....58
 - 2.322 RESERVED - Cross-License, Deliverables and Derivative Work, License to Contractor.....58
 - 2.323 RESERVED - License Back to the State58
 - 2.324 RESERVED - License Retained by Contractor.....58
 - 2.325 Pre-existing Materials for Software Deliverables58
- 2.330 Source Code Escrow59
 - 2.331 Definition59
 - 2.332 Delivery of Source Code into Escrow.....59
 - 2.333 Delivery of New Source Code into Escrow59



- 2.334 Verification59
- 2.335 Escrow Fees59
- 2.336 Release Events59
- 2.337 Release Event Procedures59
- 2.338 License.....60
- 2.339 Derivative Works60
- Glossary.....61
- Appendix A – Business/Technical Requirements63
- Appendix B – Forms for Specified Deliverables for Section 1.104 A.2: EA Solution Assessment and DIT0-170 Security Assessment66
- 1.0 Introduction79**
 - 1.1 Resource Roles and Responsibilities.....79**
- 2.0 Current Status79**
- 3.0 SEM Initiation and Planning Stage79**
 - 3.1 Purpose79**
 - 3.2 Laws, Regulations, DTMB and/or Agency Security Policies, Standards and Procedures80**
 - 3.3 Data classification80**
 - 3.4 System and Information Security Level (Low, Moderate, High)81**
- 4.0 SEM IT Business/Security Requirements Stage81**
- 5.0 & 6.0 SEM Functional and System Design Stage82**
 - 5.1/6.1 Describe the function of the system/application and the information processed for each server utilized in this project.82**
 - 5.2/6.2 Other Systems or Applications serviced by this hardware82**
 - 5.3/6.3 Hardware this system/application will be utilizing83**
 - 5.4/6.4 Security Control Groups Implemented in the Project83**
 - 5.5/6.5 Infrastructure/Network Diagram87**
 - 5.6/6.6 Data Flow Diagram88**
- 7.0 SEM Construction Stage89**
- 8.0 SEM Testing Stage.....89**
- 9.0 SEM Implementation Stage89**
 - 9.1 Security Analysis (To be completed by MCS Security Liaison)89**
 - 9.2 Sponsors and Stakeholders90**
 - 9.3 Approvals90**
- Appendix A - System and Information Security Level Matrix.....91**
- Appendix B - System Security Control Requirements93**
- Appendix C – Acronyms104**
- Appendix D - Laws, Regulations, DTMB and/or Agency Security Policies, Standards & Procedures ...105**
- Appendix E - Security Analysis (To be completed by MCS Security Liaison).....107**
- Appendix D - Personnel Resume Template118
- Appendix E – Preliminary Project Plan129
- Appendix F – Federal and State Assurances and Certifications130
- Appendix G - Cost Tables.....136



Article 1 – Statement of Work (SOW)

1.000 Project Identification

1.001 Project Request

The State of Michigan (State), through the Department of Technology, Management and Budget (DTMB) in partnership with the Michigan Department of Education (MDE), Office of Career and Technical Education (OCTE) has issued this Contract to host, maintain, support and provide future enhancements for the already existing the “Michigan CTE Navigator” (NAVIGATOR) web-based software application.

This RFP contemplates a very aggressive project to assume hosting of the NAVIGATOR system and data in production **by January 2, 2013.**

NAVIGATOR allows Michigan Career and Technical Education (CTE) professionals to access and use Michigan CTE program standards for local curriculum development and to show alignment to state and national standards.

1.002 Background

NAVIGATOR for Michigan's Career and Technical Education community (State/Regional/Local Administrators, and Instructors) provides real-time access to Michigan's state-approved CTE program standards, which is necessary for educational decision-making, management and ultimately student achievement. This comprehensive, statewide web-based system is user-friendly and instructor-driven and can be used for managing the technical standards, career cluster content, segments, resource content, and academic alignment results for all of Michigan's CTE program areas. NAVIGATOR was developed by a vendor as part of a grant from OCTE in 2006 in response to federal requirements, as a system for validating statewide curriculum standards delivery. The system (design, code, scripts and all associated technical documents) and the domain name are the property of the State and currently being hosted, maintained and supported by the vendor. The current grant will expire on December 31, 2012

NAVIGATOR was developed using Ruby on Rails (RoR), PHP, Django, Python, HTML, JavaScript, Adobe Photoshop CS3, Adobe Flash CS4, Adobe Connect and MySQL. It is currently hosted on a single virtual dedicated (Cloud) server that runs Ubuntu (Linux), Apache 2.x, MySQL 5.x, postfix (for emails). There are approximately 2500 users with 120 visits per day and 30,000 page views per year. The current MySQL database size of Navigator is 104 MB and the disk space being used is 1.3 GB. Based on the current trends, the database is expected to grow by 20 to 50 MB per year.

1.100 Scope of Work and Deliverables

General

The State has made significant investment in a number of enterprise, shared solutions or services (see Article 1, Section 1.103, Environment). All information, data, software source code, and documentation are the sole property of the State and shall not be sold or made available to any person or entity without the written authorization of the State.

1.101 In Scope

The Contractor will be responsible for :

- Application Hosting and Data Storage
 - Database backup and disaster recovery;
- System Documentation
- Maintenance and support (technical and help desk) –
 - (1) Break-fix Maintenance and update of the software source code;
 - (2) application of necessary software and security patches as and when needed;



- Future enhancements – Contractor will be responsible for making changes to the existing functionality or adding new functionality based on the changing business needs.

A detailed description of the services and deliverables that the Contractor will provide is described in Article 1, Section 1.104, Work and Deliverables supported by Appendix A.

The State reserves the right to add additional services to the Contract according to its best interests.

1.102 Out of Scope

The bidder proposal shall not include:

- Purchase, maintain, and/or support technology not directly assigned to the Solution

1.103 Environment

The hosting environment should meet or exceed the requirements identified in section 1.103 Part A and Part B; Appendix A of this RFP. State data center standards in quality and performance (see below). 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).

Contractors are advised that the State has methods, policies, standards and procedures that have been developed over the years. Contractors who desire to perform work for the State are advised the State requires this work to conform to established and published methods, policies, standards, and procedures. Contractors are expected to provide proposals that conform to State IT policies and standards. All services and products provided as a result of this RFP must comply with all applicable State IT policies and standards. Contractor is required to review all applicable links provided below and state compliance in their response. These policies and procedures are available as follow:

1.103 Part A - Enterprise IT Policies, Standards, and Procedures:

1. The State maintains and secures the IT Enterprise by applying change in measured and controlled processes which are documented and published.
2. In the event an exception to the standards is desired, this request must be submitted with justification in writing to the assigned contract manager or DTMB Project Manager. The State must approve these requests and agree to the changes in writing before work has begun.

The Michigan Administrative Guide to State Government:

http://www.michigan.gov/dmb/0,1607,7-150-9131_9347---,00.html

- State Policy 1335.00: Information Technology Access Control
- State Policy 1340.00: Information Technology Information Security
- State Policy 1345.00: Information Technology Network and Infrastructure

The State's security environment leverages:

- Data base security
- Secured Socket Layers
- Database encryption to protect selected data elements

All State and contractual employees are required to have an application level login and password to access system functions. Any contract employee that accesses the system functions must adhere to all State security policies. For example each contract employee must use his/her individual account with password-no shared accounts or passwords, authorizations with least privileges based on need-to-know basis. Any additional State/OCTE specific security requirements are stated in Appendix A – Business/Technical Requirements.



In the event the Contractor or an individual representing the Contractor is granted access to State IT resources, this individual acknowledges and agrees to the State's acceptable use policy;

http://www.michigan.gov/documents/dmb/1460.00_184733_7.pdf

1.103 Part C - DTMB IT eMichigan Web Development Standard Tools:

The State web presence is show cased at www.michigan.gov and the State desires to leverage this synergy to provide a common look and feel to those who visit State web sites. As part of the enhancements of the NAVIGATOR, the selected Contractor will be responsible for updating the current NAVIGATOR site to comply with the eMichigan look and feel standards

View eMichigan Web Development Standards

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

1.103 Part D - The State Unified Information Technology Environment (SUITE):

SUITE is a methodology which includes standards, forms and templates for project management and systems engineering; see <http://www.michigan.gov/suite>.

- The Contractor shall conform to SUITE and adopt said processes and templates in performance of the project.
- The Contractor shall be familiar with SUITE in order to assist the DTMB Project Manager in completing required documentation and satisfying other SUITE requirements.

1.103 Part E – EA Solution Assessment

The Contractor will work with the State to finalize the EA Solution Assessment following award.

1.103 Part F - NAVIGATOR's current technical environment

HARDWARE

Operating system	Ubuntu Linux or comparable Linux distribution
Processor	Quad-Core AMD Opteron(tm) Processor 2374 HE, 4 cores
Real memory	4 GB
Virtual memory	8 GB
Disk Space	150 GB
Network Up Speed	100 Mbps

SOFTWARE

Apache 2	2.2.12
MySQL	5.1.37
Ruby	1.8.7
RubyGems	1.3.5
ImageMagick	6.5.1-0
Sendmail	8.14.3 (postfix can also be used instead of sendmail)

GEMS

fastercsv	1.5.0
passenger	2.2.9
rails	2.0.2
roo	1.2.3
spreadsheet	0.6.5.2
will_paginate	2.3.12



HOW MCCTE NAVIGATOR WORKS

What is in NAVIGATOR?

- **Programs** – Provides CTE programs within the state of Michigan with the capability of listing their programs by Cluster and Classification of Instructional Programs (CIP). Available for each CIP is a list of the minimum standards (Foundation, Pathway, MI Technical and MI Career and Employability Standards). In this section the teacher has the capability of adding resources that they would use to deliver the standards (images, documents, presentations and lesson plans). Gap analysis documents are available in Excel and on line. Included is a CIP self-review, in which the electronic program files for state approved program may be provided for monitoring purposes.
- **Reports** – There are three sets of reports available to be printed or exported into Excel. The reports are by Curriculum, Segment and Academic Alignment. Each report can be done by state, PSN or program.
- **Schools** – List of schools with addresses and phone numbers that deliver state approved CTE programs in Michigan
- **MI Merit and Common Core** – Alignment of CTE Curriculum to Content expectations for Mathematics (Math 7, Math 8, Algebra 1, Algebra 2, Geometry, Statistics and Probability and Pre-calculus), Science (Earth Science, Biology, Chemistry & Physics), and Language Arts as identified by the Michigan Department of Education. We anticipate addition of the Science Common Core standards during the 2012-13 year.

Levels of users: In NAVIGATOR there are several levels of users. They are; Career Education Planning District (CEPD) Administrator, Operating Building Administrator, CTE District Consultants/CTE Directors/Supervisors, and CTE Teachers. Each level has different user capability. Refer to the User Roles & Responsibilities document available on <http://navigator.mccte-fsu.org/>.

User Roles and Responsibilities

CEPD Administrators

- Activated by: OCTE gives the updated CEPD Administrator list to MCCTE Navigator administration team so they can send emails out to start the updating process.
- Definition: Each CEPD has one person identified as the CEPD Administrator.
- Rights: Authorized to activate operating building administrators and/or teachers and CTE district consultants, CTE directors/supervisors, view all Program Serial Number (PSN) related content for their buildings, generate reports at state and PSN levels, and view all teacher level support material within their authorized PSN.
- Special options: If the CEPD administrator is also the Operating Building Administrator they can identify this when they update their profile data. Then they will have the rights of the Operating Building Administrator.

Operating Building Administrator

- Activated by: CEPD Administrator
- Definition: In Navigator each building can only have ONE building administrator or principal. The person who is assigned to the building where the CTE program is operating.
- Rights: Authorized to activate CTE teachers, CTE District Consultants/CTE Directors/Supervisors and any additional building administrators that have CTE responsibilities. They can also view all PSN related content, will receive communication from MCCTE-FSU and MDE related to teacher participation and other notifications, generate reports at state and PSN levels, and view all teacher level support material within their authorized PSN.

CTE Teachers

- Activated by: Operating Building Administrator
- Definition: Teachers that are teaching in a state-approved CTE program as identified by a PSN.
- Rights : Perform PSN academic alignment, generate reports at state and PSN levels, input lesson plans, documents, images, and presentations at their PSN level, organize standards into custom



courses using the “Courses” feature in the “Programs” link, customize segment content as applied to their PSN and complete their gap analysis.

CTE District Consultants/CTE Directors/Supervisors (including academic support personnel)

- Activated by: Operating Building Administrator
- Rights: They assist teachers in academic alignment; can view all PSNs within the assigned district and their standards; personnel in this level are not authorized to activate teachers; will not receive communications regarding teacher participation or+ other notifications.

Activation process:

This process begins with the CEPD Administrators in August or September of each year and automatically cascades to the Operating Building Administrators and then to CTE Teachers and other end users of NAVIGATOR. Teachers may experience a few days of inactive status while their CEPD Administrator works with their Operating Building Administrator to update the data for this year.

1.103 Part G – Federal and State Assurances and Certifications

The Michigan Department of Education receives funding through United State federal grants that may be applied to fund the NAVIGATOR System. In addition to the State’s terms and conditions detailed in Article 2, this places specific legal requirements on both the State and any vendors who receive compensation for providing services to the System.

Please see Appendix F – Federal and State Assurances and Certifications for the list of applicable assurances and certifications.

1.104 Work And Deliverables

The awarded bidder shall in fulfillment of work, provide staff, equipment, and otherwise do all things necessary to complete all deliverables and associated tasks in order to meet the terms and conditions of the Contract.

1.104 Part A: Services To Be Provided

The NAVIGATOR system is currently operational. The Contractor will be responsible for setting up all necessary server hardware and software; database required for hosting the system; and installing the currently working application on the contractor’s server(s); Transition to hosting, maintenance and support services under this Contract will be effective January 2, 2013.

Part A Section 1: Data Storage Reconfiguration

Contractor will do all things necessary to reconfigure the NAVIGATOR System so that Data shall not to reside outside of the Continental United States, inclusive of configuration, policy development, testing, documentation and implementation. Contractor will complete this reconfiguration by December 14, 2012.

Part A Section 2: Solution Documentation

Contractor will collaborate with State IT Staff, and State IT Staff will assist Contractor, to complete the following documents:

1. A completed EA Solution Assessment. Please see Appendix B for the Solution Assessment template. It will be the State’s responsibility to gain final approvals of the EA Solution Assessment through its internal review processes. As part of deliverables for future enhancements, the Contract may be required to provide updated information for these forms. Any remediation to the NAVIGATOR system resulting from review will be addressed through formal change management.
2. A DIT-0170 Security Assessment: Contractor will fill out and provide the Security Assessment to the State. Please see Appendix B for the template. It will be the State’s responsibility to gain final approvals of the Security Assessment through its internal review processes. As part of deliverables for future enhancements, the Contract may be required to provide updated information for these forms. Any remediation to the NAVIGATOR system resulting from review will be addressed through formal change management.

Contractor’s collaboration in completing the above documents is not expected to exceed 40 billable hours.



1.104 Part A Section 3: Hosting Solution

The State requires for the contractor that was awarded this contract through this RFP to have the NAVIGATOR system be fully operational with all the existing data and functionality available to the users by no later than January 2, 2013.

The NAVIGATOR system will be hosted in a commercially managed data center with 98% uptime where users of the system can access the system 24X7X365 over the internet. The NAVIGATOR System will have to be:

- Hosted in a secured and stable data center that has
 - o Redundant power supply
 - o Bandwidth that can handle System traffic. The current system has 2,500 users, average 120 daily visits, with 30,000 yearly page-views. The system needs to be able to handle traffic spikes and incremental growth over time.
 - o Managed Backup

The proposed solution may consist of either physical and/or virtual servers.

The State's prefers the solution be is hosted on a dedicated server. Shared servers may be considered if the NAVIGATOR system is co-hosted only with other applications that have equivalent or more stringent security requirements.

The Solution must be hosted on hardware covered under manufacturer warranty.

To prevent security breaches, Contractor must update all necessary patches in a timely manner to all the software's used to successfully run the Navigator system that will include but not limited to the Operating system, Database etc.

Hardware refreshes shall not impact System performance or user access.

- System must be available 24x7x365, except for mutually agreed scheduled maintenance

1.104 Part A Section 4: Maintenance, Technical and Help Desk Support

In the day to day operation of the system it is anticipated the system will require maintenance and it is also anticipated that questions will surface from the users of the system. Contractor shall provide software break-fix maintenance for the NAVIGATOR Application to ensure the software continues to run error-free. Additionally, Contractor shall provide technical and help desk support for NAVIGATOR System users during the normal business hours (8 a.m. to 5 p.m. EST), for the following:

- all NAVIGATOR system related issues
- all issues related to network connectivity
- problems and complaints about accessing the functionality of the system

The Contractor's help desk will field both technical and functional system questions related to the Navigator system and general project , and will respond within 24 hours of receipt via phone or email. The Contractor shall provide Technical Support and Help Desk staff knowledgeable of the NAVIGATOR system who are located in the United States. It will be Contractor's responsibility to train their staff.

The Contractor shall provide a toll-free help desk telephone number for reporting all system related issues, for which the Contractor shall bear the cost. There shall be no limit to the number of calls that can be placed to the help desk. The help desk shall be staffed adequately to handle all questions and complaints. Call hold-times will not exceed three minutes. Answering machine service shall be available when help desk is not able to respond after three minutes of hold-time. All calls will be returned within 15 minutes. The Contractor shall staff the Help Desk with experienced personnel that can answer "how to" questions about the application. Merely answering the phone and assigning a case number to a problem does not meet this requirement.



1.104 Part A Section 5 - Future enhancements

The State anticipates requests for new functionality and/or changes to the existing system throughout the contract period. 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. Pricing is provided in Appendix D.

The State will provide the details of the changes that need to be made to the system and it is Contractors responsibility to analyze and provide a proposal (Change request) with an estimate and a level of effort required to make such changes. The proposal must include details of the actual tasks that will be completed, estimated number of hours for each task, number of technical resources that will be used to develop, test and implement the changes and their hourly rate and the total cost for implementing those changes. All proposals will have to be approved by the State before the work can begin. Any changes to the agreed upon functionality will have to go through a Change Management process. All requested changes will be developed and tested before deploying into the production environment. Contractor to provide these services using a fixed cost.

The Contractor shall provide updates of the NAVIGATOR manuals as a deliverable when an approved enhancement is made. All manuals shall be approved by the State.

1.104 Part B.1: System Requirements

As part of Contractor's implementation, hosting, and maintenance of the NAVIGATOR system Contractor shall meet the requirements detailed in Appendix A: Business and Technical Requirements

1.104 Part B. 2: System Security

Contractor shall be responsible for the secure hosting and operation of the NAVIGATOR system. Contractor shall be responsible for all breaches of security of sensitive data, including Personal Information and Personal Identifiable Information that resides on the NAVIGATOR system, per the terms of the State's security policies and of the Michigan Identity Theft Protection Act (Act 452 of 2004, as amended).

1.200 Roles and Responsibilities

1.201 Contractor Staff, Roles, and Responsibilities

A. Contractor Staff

The Contractor will provide sufficient staffing to provide the requested services and meet all requirements under this Contract. The Contractor shall be responsible for the continuous training of its staff. The Contractor shall train its staff and update their manuals in a timely manner so the staff remains competent and knowledgeable in order to provide a high quality service to the State and its customers.

The Contractor will identify a Single Point of Contact (SPOC). The duties of the SPOC shall include, but not be limited to:

- supporting the management of the Contract,
- facilitating dispute resolution, and
- advising the State of performance under the terms and conditions of the Contract.

The State reserves the right to require a change in the current SPOC if the assigned SPOC is not, in the opinion of the State, adequately serving the needs of the State.

Key Personnel: All Key Personnel may be subject to the State's interview and approval process. Any key staff substitution must have the prior approval of the State. The State has identified the following as key personnel for this project. Bidders may propose one person for no more than two key positions.

- Project Manager: Dr. Steven Clark, PhD
- Lead Developer: Kavan Story



The Contractor will provide a Project Manager 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:

- Manage all defined Contractor responsibilities in this Scope of Services.
- Manage Contractor's subcontractors, if any
- Develop the project plan and schedule, and update as needed
- Serve as the point person for all project issues
- Coordinate and oversee the day-to-day project activities of the project team
- Assess and report project feedback and status
- Escalate project issues, project risks, and other concerns
- Review all project deliverables and provide feedback
- Proactively propose/suggest options and alternatives for consideration
- Utilize change control procedures
- Prepare project documents and materials
- Manage and report on the project's budget

Project Manager Requirements

1. 7+ years of recent IT project management experience managing large scale application development and implementation projects.
2. 3+ years of experience working on projects involving interfacing with the State of Michigan or that of a similar state-level system.
3. Experience in structured development process using a formal Project Management Methodology and formal Development Methodology.
4. Certification as a Project Management Professional (PMP) is a plus

The Contractor's Lead Developer responsibilities include, at a minimum:

- Analyzing, coding, testing, trouble shooting and implementing the changes requested.
- Day-to-day maintenance and management of the application code and database
- Performance tuning
- Documentation

Lead Developer Requirements

1. 5+ years of experience working on projects involving interfacing with a hosting environment
2. 5+ years of experience in analyzing, developing, testing, trouble shooting and maintaining a web based application.
3. 2+ years of experience in Ruby on Rails (RoR), JavaScript and MySQL, Linux, Apache 2.x, MySQL 5.x, postfix (for emails).

The Contractor shall complete and include the Staffing Plan Matrix (see Appendix E). This indicates by role, how many persons would be involved in each phase. This will also identify if persons are dedicated to the project and, if not, approximate percentage by phase.

The Contractor will provide sufficient qualified staffing to satisfy the deliverables of this Statement of Work.

B. On Site Work Requirements

1. Location of Work

At a minimum the Contractor must be onsite during project kickoff, requirements gathering for future enhancements, and training. On-site work may include but are not limited to the following locations:

- Lansing Michigan



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.
 - d. Travel time will not be reimbursed.
4. Security and Background Check Requirements:

See 2.091 for Security and Background Check Requirements.

1.202 State Staff, Roles, and Responsibilities

The State will provide the following resources only on as needed basis for the Contractor’s use on this project:

- Conference room for business requirements gathering meetings and monthly/quarterly project status update meetings
- Access to copier

The State project team will consist of Subject Matter Experts (SME’s), and Agency project manager:

Subject Matter Experts

The Executive Subject Matter Experts representing the business units involved will provide the vision and functionality needed for future. They shall be available on an as needed basis. The Executive SME’s will be empowered to:

- Resolve project issues in a timely manner
- Review project plan, status, and issues
- Resolve deviations from project plan
- Provide acceptance sign-off
- Utilize change control procedures
- Ensure timely availability of State resources
- Make key implementation decisions, as identified by the Contractor’s project manager, within 48-hours of their expected decision date.

State Project Manager- (Agency)

The State will provide a Project Manager who will be responsible for coordinating with the Contractor in determining the project needs. The State’s Project Manager will provide the following services:

- Provide State facilities, as needed
- Coordinate the State resources necessary for the project
- Facilitate coordination between various external contractors
- Facilitate communication between different State departments/divisions
- Provide acceptance and sign-off of deliverable/milestone
- Review and sign-off on invoices after the Agency Project Manager approves
- Resolve project issues



- Escalate outstanding/high priority issues
- Utilize change control procedures
- Conduct regular and ongoing review of the project to confirm that it meets original objectives and requirements
- Document and archive all important project decisions
- Arrange, schedule and facilitate State staff attendance at all project meetings.

Name	Agency/Division	Title
Glenna Zollinger-Russell	OCTE	Agency Project Manager
Maria Thomas	DTMB	IT Project Manager

DTMB will provide a Contract Administrator whose duties shall include, but not be limited to, supporting the management of the Contract.

1.203 RESERVED - Other Roles And Responsibilities

1.300 Project Plan

1.301 Project Plan Management

Project Planning

Contractor will provide a Project Work Breakdown Structure for all services to the State other than for hosting (see Section 1.104 Part A Section 1) and maintenance(see Section 1.104 Part A Section 3), including necessary time frames and deliverables for the various stages of the project and the responsibilities and obligations of both the Contractor and the State.

1. Project Work Breakdown Structures will include the following:
 - MS Project schedule
 - Internal milestones
 - Task durations
 - Deliverable target dates and critical paths
 - Project approach / Statement of Work
 - Scope statement with a description of the deliverables to be provided under this contract
 - Assumptions and exclusions
 - Critical success factors
 - Initial resource plan with anticipated resources by organization, role, and responsibility
 - Initial risk plan
 - Initial communication plan
 - Anticipated hardware, materials, and supplies to be provided by the State in meeting the target dates established in the Preliminary Project Plan

See Section 1.500 for acceptance criteria.

Orientation Meeting

If requested by the State, within 7 calendar days from execution of the Contract, the Contractor will be required to attend an orientation meeting to discuss the content and procedures of the Contract. The meeting will be held in Lansing, Michigan, at a date and time mutually acceptable to the State and the Contractor. The State shall bear no cost for the time and travel of the Contractor for attendance at the meeting.



Performance Review Meetings

The Contractor shall attend monthly or quarterly meetings (see 1.302 Steering Committee) to review the Contractor's performance under the Contract. The monthly or quarterly meetings will be held in 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

1. The Contractor will carry out this project under the direction and control of DTMB.
2. Within 7 business days of the execution of the Contract, the Contractor will submit the project plan to the State project manager(s) for final approval. This project plan must be in agreement with Article 1, Section 1.104 Work and Deliverables, and must include the following:
 - a. The Contractor's project organizational structure.
 - b. The Contractor's staffing table with names and title of personnel assigned to the project. This must be in agreement with staffing of accepted proposal. Necessary substitutions due to change of employment status and other unforeseen circumstances may only be made with prior approval of the State.
 - c. The project work breakdown structure (WBS) showing sub-projects, activities and tasks, and resources required and allocated to each.
3. The Contractor will manage the project in accordance with the State Unified Information Technology Environment (SUITE) methodology, which includes standards for project management, systems engineering, and associated forms and templates which is available at "<http://www.michigan.gov/suite>".
 - a. Contractor will use an automated tool for planning, monitoring, and tracking the Contract's progress and the level of effort of any Contractor personnel spent performing Services under the Contract. The tool shall have the capability to produce:
 - Staffing tables with names of personnel assigned to Contract tasks.
 - Project plans showing tasks, subtasks, deliverables, and the resources required and allocated to each (including detailed plans for all Services to be performed within the next 30 calendar days, updated weekly or biweekly as directed by the State PM).
 - Updates must include actual time spent on each task and a revised estimate to complete.
 - Graphs showing critical events, dependencies and decision points during the course of the Contract.
 - b. Any tool(s) used by Contractor for such purposes must produce information of a type and in a manner and format that will support reporting in compliance with the State standards.

1.302 Reports

Project Reporting:

As part of the initial migration and for future enhancements, a bi-weekly Project status report is required from the Contractor to the State Project Manager on the topics of status, schedule, risks, issues, impediments, deliverables, change control, and accomplishments, beginning upon execution of the Contract for the duration of the contract unless otherwise agreed to.

Reporting topics will include but not limited to the following items.

- Project Status
- Planned % Complete
- Actual % complete
- Current SUITE stage
- Planned SUITE stage
- Planned Start Date
- Planned Finish Date



- Planned Hours
- Actual Start
- Actual Finish
- Actual Hours
- On Target for Completion (Y/N)
- New Forecast Completion Date
- # of Defects Identified
- # of Defects Resolved
- Pending Change Requests under the subheadings Corrective Actions and Enhancements
- Help desk issues
- Team Changes

Hosting and Maintenance Reporting:

Upon successful implementation and go-live of the NAVIGATOR System, Contractor will provide the following:

1. Inventory Report: The Contractor will provide a semi-annual inventory report for all hardware and software supplied by the Contractor, used to support and host the NAVIGATOR system.
2. Disaster Recovery Plan Test Report: The Contractor will provide an annual report detailing the execution of the System's disaster recovery plan and testing of the Disaster Recovery Environment, including all issues encountered, interruptions to service, and identified remediations.
3. Help Desk Call Log: The Contractor shall maintain a log of all calls made to the helpdesk, which shall be updated a minimum of daily. The Contractor will fully document the complaints and problems reported. The log shall record the actions that were taken to resolve the issue and the date such issue was resolved. The log shall be available online to the State staff to track the status of the issues.
4. System Usage and Maintenance Report: The Contractor will provide a monthly report detailing Network and bandwidth issues if any.
5. Maintenance Report: The Contractor will provide a monthly report detailing scheduled maintenance for the upcoming month, and also all maintenance events, both scheduled and unscheduled, for the previous month. Contractor shall also calculate and report their adherence to Service Level Agreements.

1.400 Project Management

1.401 Issue Management

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

The Contractor shall maintain an issue log in an agreed upon format, to document and track issues relating to the provision of services under this Contract. The Contractor shall communicate the status of issues to the State's Project Manager weekly, as required or agreed and the status must contain the following minimum elements:

- Description of issue
- Status
- Date reported
- Resolution deadline
- Date resolved
- Project impact (viz. schedule, resources)
- Priority
- Assigned To
- Related risk
- Notes



The State will escalate issues for resolution as follows:

- Level 1 – Business leads / Subject matter experts
- Level 2 – Project Managers / Project Leadership Team
- Level 3 – Executive Team

1.402 Risk Management

A risk is an unknown circumstance or event that, if it occurs, may have a positive or negative impact on the project. If the unknown becomes known or the event occurs, a risk may escalate to become an issue.

The Contractor is responsible for establishing a risk management plan including the identification and recording of risk items, prioritization of risks, definition of mitigation strategies, monitoring of risk items, and periodic risk assessment reviews with the State.

The Contractor will submit an initial risk management plan to the State for approval within seven (7) business days from execution of the contract. The risk management plan will be in accordance with the State's PMM methodology. The Contractor shall communicate the status of risks to the State's Project Manager weekly, as required or agreed and the status must contain the following minimum elements:

- Risk
- Status
- Date documented
- Controlled
- Impact
- Description
- Trigger Event
- Mitigation
- Likely Project Phase
- Owner

The Contractor is responsible for identification of risks throughout the life cycle of the project. Mitigating and/or eliminating risks will be the responsibility of the assigned party.

1.403 Change Management

Change management is defined as the process to communicate, assess, monitor, and control changes to system resources and processes. The State employs change management at the Project level and in its administration of the Contracts.

The Contractor must employ change management procedures to handle requests which impact schedule or resources and such things as "out-of-scope" requests or enhancements. Change requests must be submitted to the Project Manager and shall be approved by the State in writing before they are implemented. DTMB Procurement will issue an addendum to the Contract, via a Contract Change Notice if the Change request is approved.

1.500 Acceptance

1.501 Criteria

The Contractor will provide notice to the DTMB Project Manager when a deliverable is complete. The DTMB Project Manager in conjunction with the Agency Project Manager will evaluate the deliverable in order to determine if it satisfies the requirements of the RFP with an adequate level of quality. The Contractor will be provided written notice of approval or rejection within ten (10) business days of the receipt of notice.



In the event the work and/or deliverable is not accepted by the DTMB Project Manager, the State will respond to the Contractor with written notice describing the deficiencies using a corrective action plan listing tasks with associated completion dates. The Contractor has five (5) business days to respond to the notice indicating agreement to the terms unless an alternate Solution is agreed by both parties. Upon completion, State will have ten (10) business days to accept and approve the revised deliverable(s).

1.502 Final Acceptance

“Final Acceptance” shall be considered to occur when the Solution to be delivered has been approved by the State and has been operating in production without any material deficiency for fourteen (14) consecutive days. If the State elects to defer putting the Solution into live production for its own reasons, not based on concerns about outstanding material deficiencies in the Deliverable, the State shall nevertheless grant Final Acceptance of the Project.

1.600 Compensation and Payment

1.601 Compensation And Payment

A. Method of Payment

Hosting (Section 1.104 A.3) and maintenance (Section 1.104 A.4) services will be paid on firm, fixed monthly basis. Rates shall not increase over the term of the Contract. Payment for hosting and maintenance shall not commence prior to January 2, 2013.

Data Storage Reconfiguration (Section 1.104 A.1) and Solution Documentation (Section 1.104 A.2) will be paid on a T&M hourly rate.

Project services for future enhancements (Section 1.104A.5) will be paid on a **firm, fixed-price deliverable-basis**. Payment for future enhancements will be determined within the individual project’s Statements of Work, based on the number of estimated hours and the Contractor’s not-to-exceed hourly rates detailed in Appendix G Table 3: Block of Hours for Future Enhancements.

Please see the Costs Table(s) in **Appendix G** (attached)

B. Travel

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

C. Out-of-Pocket Expenses

Contractor out-of-pocket expenses are not separately reimbursable by the State.

D. Statements of Work and Issuance of Purchase Orders for Future Projects

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



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.

E. Invoicing

Contractor will submit properly itemized invoices to

DTMB – Financial Services
Accounts Payable
P.O. Box 30026
Lansing, MI 48909
or

DTMB-Accounts-Payable@michigan.gov

Invoices must provide and itemize, as applicable:

- Contract number;
- Purchase Order number
- Contractor name, address, phone number, and Federal Tax Identification Number;
- Description of any commodities/hardware, including quantity ordered;
- Date(s) of delivery and/or date(s) of installation and set up;
- Price for each item, or Contractor's list price for each item and applicable discounts;
- Number of each item provided with extension subtotal amounts
- Net invoice price for each item;
- Shipping costs;
- Other applicable charges;
- Total invoice price; and
- Payment terms, including any available prompt payment discount.

Incorrect or incomplete invoices will be returned to Contractor for correction and reissue.

1.602 RESERVED - Holdback



ARTICLE TWO

2.000 Contract Structure and Term

2.001 Contract Term

This Contract is for a period of three (3) years beginning November 15, 2012 through November 1, 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 five (5) additional one (1)-year periods.

2.03 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 Attachments, Exhibits and Appendices

All Attachments, Exhibits and Appendices affixed to any and all Statement(s) of Work, or appended to or 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, Attachments, Exhibits and Appendices, 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. 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 Department of Natural Resources (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:

Reid Sisson, Procurement
Department of Technology, Management and Budget
Mason Bldg, 2nd Floor
PO Box 30026
Lansing, MI 48909
Email: SissonR@michigan.gov
Phone: 517-241-1638

2.022 Contract Compliance Inspector

The Director 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 for this Contract is:

Maria Thomas, Application Manager,
DTMB Agency Services - MDE
Hannah Building
608 West Allegan St
Lansing, MI 48909



2.023 RESERVED

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 Services/Deliverables that are outside the scope of the Contractor's responsibilities under the Contract ("New Work"), 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 Amendment Labor Rates 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.

(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
PO Box 30026
530 West Allegan
Lansing, Michigan 48909

Contractor: See Contract Cover Page

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.

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.

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 Contractor 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 Attachment, Exhibit, or Appendix) 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 Attachment, Exhibit, or Appendix) the prices for all Services/Deliverables, equipment and commodities 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 individual, the number of hours of Services performed during the billing period, the billable skill/labor category for such person 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 Director of Procurement, 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, less any penalty cost charges accrued by those dates. As a general policy statements shall be forwarded to the designated representative by the 15th day of the following month.

2.045 Pro-ration

To the extent there are Services that are to be paid for on a monthly basis, the cost of such Services shall be pro-rated for any partial month.

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, including the taxes.

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.
- (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 10 business days before redeploying non-Key Personnel, who are dedicated to 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 Attachment, Exhibit, or Appendix.

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 the Contractor's personnel before they may have access to State facilities and systems. 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. Contractor will pay for all costs associated with ensuring their staff meets these requirements.

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/dtmb> . 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

Contractors with access to credit/debit card cardholder data must adhere to the Payment Card Industry (PCI) Data Security requirements. Contractor agrees that they are responsible for security of cardholder data in their possession. Contractor agrees that data can ONLY be used for assisting the State in completing a transaction, supporting a loyalty program, supporting the State, providing fraud control services, or for other uses specifically required by law.



Contractor agrees to provide business continuity in the event of a major disruption, disaster or failure.

The Contractor shall contact the Department of Technology, Management and Budget, Financial Services immediately to advise them of any breaches in security where card data has been compromised. In the event of a security intrusion, the Contractor agrees the Payment Card Industry representative, or a Payment Card Industry approved third party, shall be provided with full cooperation and access to conduct a thorough security review. The review will validate compliance with the Payment Card Industry Data Security Standard for protecting cardholder data.

Contractor agrees to properly dispose sensitive cardholder data when no longer needed. The Contractor shall continue to treat cardholder data as confidential upon contract termination.

The Contractor shall provide the Department of Technology, Management and Budget, Financial Services documentation showing PCI Data Security certification has been achieved. The Contractor shall advise the Department of Technology, Management and Budget, Financial Services of all failures to comply with the PCI Data Security Requirements. Failures include, but are not limited to system scans and self-assessment questionnaires. The Contractor shall provide a time line for corrective action not to exceed 6 months from the time of notification of breach.

In the event the State incurs charges as a result of a breach by the Contractor, the Contractor will reimburse the State.

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 reasonably 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 20 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 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.

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.
- (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.
- (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 Bidder for the purpose of restricting competition; the prices quoted were not knowingly disclosed by Contractor to any other Bidder; 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.

- 2.122 Warranty of Merchantability - RESERVED
- 2.123 Warranty of Fitness for a Particular Purpose - RESERVED
- 2.124 Warranty of Title - RESERVED
- 2.125 Equipment Warranty - RESERVED
- 2.126 Equipment to be New - RESERVED
- 2.127 Prohibited Products - RESERVED
- 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.

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.

All insurance coverage provided relative to this Contract/Purchase Order is PRIMARY and NON-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/LARA

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 INSUREDS 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 INSUREDS 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. Cyber-Liability Insurance with the following minimum limits:
\$1,000,000 Per Occurrence

Additional Requirements:

The Contractor must list the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents as additional insureds. The Contractor also agrees to provide evidence that insurance policies contain a waiver of subrogation by the insurance company.

- 6. 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 fifty thousand dollars (\$50,000.00).
- 7. 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.
- 8. 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.
- 9. 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 “accord” 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 Provider. All Certificate(s) must contain a provision indicating that coverage afforded under the policies SHALL NOT BE CANCELLED, MATERIALLY CHANGED, OR NOT RENEWED without 30 days prior written notice, except for 10 days for non-payment of premium, having been given to the Director of DTMB Procurement, Department of Technology, Management and Budget. The notice must include the Contract or Purchase Order number affected. Before the Contract is signed, and not less than 20 days before the insurance expiration date 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 or procure similar insurance coverage from another company or companies. 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), 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 piece of equipment, software, commodity or service supplied by the Contractor or its subcontractors, or the operation of the equipment, software, commodity or service, or the use or reproduction of any documentation provided with the equipment, software, commodity or service 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 equipment, software, commodity, or service, 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 equipment, software, commodity or service or, if the option is not reasonably available to the Contractor, (ii) replace or modify to the State's satisfaction the same with equipment, software, commodity or service 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.

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) equipment developed based on written specifications of the State; (ii) use of the equipment in a configuration other than implemented or approved in writing by the Contractor, including, but not limited to, any modification of the equipment by the State; or (iii) the combination, operation, or use of the equipment with equipment 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 10 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. 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 relating 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 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 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. All completed or partially completed Deliverables prepared by Contractor under this Contract, at the option of the State, becomes the State's property, and Contractor is entitled to receive equitable fair compensation for the Deliverables. 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, or (iii) does not cure the breach within the time period specified in a written notice of breach. But the Contractor must discharge its obligations under **Section 2.160** before it terminates the Contract.

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 reasonable period of time that in no event will exceed one hundred and eighty (180) 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 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 asset management 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, the Contract price, or both, and the Contract shall be modified, in writing, accordingly, if: (a) the Stop Work Order results in an increase in the time required for, or in Contractor's costs properly allocable 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 the Director of Procurement, 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 Director of Procurement, DTMB, 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, to preserve a superior position with respect to other creditors, or under Section 2.193.

(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 – RESERVED/NA

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 convenience or otherwise. Contractor agrees to appoint agents in the State of Michigan to receive service of process.

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 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 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) 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.

Contractor will fix appropriate notices or labels on the Work in Process to indicate ownership by the State. To the extent reasonably possible, materials and Work in Process shall be stored separately from other stock and marked conspicuously with labels indicating ownership by the State.



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 Attachment, Exhibit, or Appendix governing the work, and with professional quality.

(b) Without limiting the generality of **Section 2.241**, the Contractor shall notify the State in a timely manner pursuant to the SLA 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 impact and risk to projected actual delivery date.

(c) If the Contractor believes 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. The 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) SLAs as described in Appendix C will consider the following.

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 agreed, planned, and the State has received prior notification.
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 the State receives notification of resolution based on 24x7x365 time period. Time period measurement may be suspended based on the following:
 - a. The Contractor does not have access to a physical State Location and where access to the State Location is necessary for problem identification and resolution.
 - b. The 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 outage(s) as prescribed by the SLA or when requested by the Contract Administrator. The Contractor will provide its analysis as prescribed by the SLA or within two weeks of the 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 Liquidated Damages

The parties acknowledge that late or improper completion of the Work will cause loss and damage to the State, and that it would be impracticable and extremely difficult to fix the actual damage sustained by the State as a result. Therefore, Contractor and the State agree that if there is late or improper completion of the Work and the State does not elect to exercise its rights under Section 2.152, the State is entitled to collect liquidated damages in the amount of \$1,000.00 and an additional \$100.00 per day for each day Contractor fails to remedy the late or improper completion of the Work.



Unauthorized Removal of any Key Personnel

It is acknowledged that an Unauthorized Removal will interfere with the timely and proper completion of the Contract, to the loss and damage of the State, and that it would be impracticable and extremely difficult to fix the actual damage sustained by the State as a result of any Unauthorized Removal. Therefore, Contractor and the State agree that in the case of any Unauthorized Removal in respect of which the State does not elect to exercise its rights under Section 2.152, the State may assess liquidated damages against Contractor as specified below.

For the Unauthorized Removal of any Key Personnel designated in the applicable Statement of Work, the liquidated damages amount is \$25,000.00 per individual if the Contractor identifies a replacement approved by the State under Section 2.060 and assigns the replacement to the Project to shadow the Key Personnel who is leaving for a period of at least 30 days before the Key Personnel's removal.

If Contractor fails to assign a replacement to shadow the removed Key Personnel for at least 30 days, in addition to the \$25,000.00 liquidated damages for an Unauthorized Removal, Contractor must pay the amount of \$833.33 per day for each day of the 30 day shadow period that the replacement Key Personnel does not shadow the removed Key Personnel, up to \$25,000.00 maximum per individual. The total liquidated damages that may be assessed per Unauthorized Removal and failure to provide 30 days of shadowing must not exceed \$50,000.00 per individual.

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 one or more of the following.

- government regulations or requirements (executive, legislative, judicial, military or otherwise)
- failures of commercial transportation, equipment shortages, suppliers' failures, or acts or omissions of common carriers
- 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)
- strikes, labor disputes, embargoes, riots, or civil disorders
- cause deemed beyond the reasonable control of the party provided the non-performing party and its Subcontractors are
 - without fault in causing the default or delay
 - the default or delay could not have been prevented by reasonable precautions
 - the default or delay could not have been reasonably circumvented by the non-performing party through the use of alternate sources or workaround plans

Disasters such as power failure, electrical surges or current fluctuations, lightning, earthquake, fire, water or other forces of nature or acts of God should be mitigated with a planned response documented in the disaster plan.

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

Deliverables will be prepared and delivered as planned and documented in the project plan. Changes in deliverables which impact quality, requirements, and/or schedule will be managed by the State's change control process.

Prior to delivering any Deliverable to the State, Contractor will first perform all required quality assurance activities, and, in the case of 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 the State's project management SUITE mythology.

2.252 Contractor System Testing

Contractor will be responsible for testing each Software Deliverable in Contractor's development environment prior to turning over the Software Deliverable to the State for User Acceptance Testing and approval. Contractor's System Testing shall include the following, at a minimum, plus any other testing required by CMM Level 3 or Contractor's system development methodology:

Contractor will be responsible for performing Unit Testing and incremental Integration Testing of the components of each Software Deliverable.

Contractor's System Testing will also include Integration Testing of each Software Deliverable to ensure proper inter-operation with all prior software Deliverables, interfaces and other components that are intended to inter-operate with such Software Deliverable, and will include Regression Testing, volume and stress testing to ensure that the 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 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, which, in the case of 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 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, the State may: (i) demand that Contractor cure the failure and give Contractor additional time to cure the failure at the sole expense of Contractor; or (ii) keep this Contract in force and do, either itself or through other parties, whatever Contractor has failed to do, in which event Contractor shall bear any excess expenditure incurred by the State in so doing beyond the contract price for such Deliverable and will pay the State an additional sum equal to ten percent (10%) of such excess expenditure to cover the State's general expenses without the need to furnish proof in substantiation of such general expenses; or (iii) 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). 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 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 Software Deliverables

The State will conduct UAT of each 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 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 Software Deliverable. Contractor, upon request by the State, shall provide the State with reasonable assistance and support during the UAT process.

For the Software Deliverables listed in an attachment, the State Review Period for conducting UAT will be as indicated in the attachment. For any other 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 Software Deliverable will begin when Contractor has delivered the 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 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 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 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 Software Deliverable according to the criteria and process set out in this **Section**.

2.256 Final Acceptance

"Final Acceptance" shall be considered to occur when the Solution to be delivered has been approved by the State and has been operating in production without any material deficiency for fourteen (14) consecutive days. If the State elects to defer putting the Solution into live production for its own reasons, not based on concerns



about outstanding material deficiencies in the Deliverable, the State shall nevertheless grant Final Acceptance of the Project.

2.260 Ownership

2.261 Ownership of Work Product by State

The State owns all Deliverables, as they are work made for hire by the Contractor for the State. The State owns all United States and international copyrights, trademarks, patents or other proprietary rights in the Deliverables.

2.262 Vesting of Rights

With the sole exception of any preexisting licensed works identified in the SOW, the Contractor assigns, and upon creation of each Deliverable automatically assigns, to the State, ownership of all United States and international copyrights, trademarks, patents, or other proprietary rights in each and every Deliverable, whether or not registered by the Contractor, insofar as any the 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 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 - Please refer to Section 1.103.-

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://michigan.gov/cybersecurity/0,1607,7-217-34395_34476---,00.html 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 - RESERVED)

2.282 RESERVED - State Employee Purchases

2.290 Environmental Provision - *RESERVED/NA*

2.300 Deliverables

2.301 Software

A list of the items of software the State is required to purchase for executing the Contract is attached. 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

2.310 Software Warranties

2.311 Performance Warranty

The Contractor represents and warrants that Deliverables, after Final Acceptance, will perform and operate in compliance with the requirements and other standards of performance contained in this Contract (including all descriptions, specifications and drawings made a part of the Contract) for the duration of the Contract. In the event of a breach of this warranty, Contractor will promptly correct the affected Deliverable(s) at no charge to the State.

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.

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. At the time of Delivery, the Contractor shall provide in writing the name and use of any Third-party Software, including information regarding the Contractor's authorization to include and utilize such software. The notice shall include a copy of any ownership agreement or license that authorizes the Contractor to use the Third-party 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 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

2.321 RESERVED - Cross-License, Deliverables Only, License to Contractor

2.322 RESERVED - Cross-License, Deliverables and Derivative Work, License to Contractor

2.323 RESERVED - License Back to the State

2.324 RESERVED - License Retained by Contractor

2.325 Pre-existing Materials for Software Deliverables

Neither Contractor nor any of its Subcontractors shall incorporate any preexisting materials (including Standard Software) into Custom Software Deliverables or use any pre-existing materials to produce Custom Software Deliverables if such pre-existing materials will be needed by the State in order to use the Custom Software Deliverables unless (i) such pre-existing materials and their owners are identified to the State in writing and (ii) such pre-existing materials are either readily commercially available products for which Contractor or its Subcontractor, as the case may be, has obtained a license (in form and substance approved by the State) in the name of the State, or are materials that Contractor or its Subcontractor, as the case may be, has the right to license to the State and has licensed to the State on terms and conditions approved by the State prior to using such pre-existing materials to perform the Services.



2.330 Source Code Escrow

2.331 Definition

“Source Code Escrow Package” shall mean:

- (a) A complete copy in machine-readable form of the source code and executable code of the Licensed Software, including any updates or new releases of the product;
- (b) A complete copy of any existing design documentation and user documentation, including any updates or revisions; and/or
- (c) Complete instructions for compiling and linking every part of the source code into executable code for purposes of enabling verification of the completeness of the source code as provided below. Such instructions shall include precise identification of all compilers, library packages, and linkers used to generate executable code.

2.332 Delivery of Source Code into Escrow

Contractor shall deliver a Source Code Escrow Package to the Escrow Agent, pursuant to the Escrow Contract, which shall be entered into on commercially reasonable terms subject to the provisions of this Contract within (30) thirty days of the execution of this Contract.

2.333 Delivery of New Source Code into Escrow

If at any time during the term of this Contract, the Contractor provides a maintenance release or upgrade version of the Licensed Software, Contractor shall within ten (10) days deposit with the Escrow Agent, in accordance with the Escrow Contract, a Source Code Escrow Package for the maintenance release or upgrade version, and provide the State with notice of the delivery.

2.334 Verification

The State reserves the right at any time, but not more than once a year, either itself or through a third party contractor, upon thirty (30) days written notice, to seek verification of the Source Code Escrow Package.

2.335 Escrow Fees

The Contractor will pay all fees and expenses charged by the Escrow Agent.

2.336 Release Events

The Source Code Escrow Package may be released from escrow to the State, temporarily or permanently, upon the occurrence of one or more of the following:

- (a) The Contractor becomes insolvent, makes a general assignment for the benefit of creditors, files a voluntary petition of bankruptcy, suffers or permits the appointment of a receiver for its business or assets, becomes subject to any proceeding under bankruptcy or insolvency law, whether domestic or foreign;
- (b) The Contractor has wound up or liquidated its business voluntarily or otherwise and the State has reason to believe that such events will cause the Contractor to fail to meet its warranties and maintenance obligations in the foreseeable future;
- (c) The Contractor voluntarily or otherwise discontinues support of the provided products or fails to support the products in accordance with its maintenance obligations and warranties.

2.337 Release Event Procedures

If the State desires to obtain the Source Code Escrow Package from the Escrow Agent upon the occurrence of an Event in this **Section**, then:

- (a) The State shall comply with all procedures in the Escrow Contract;



(b) The State shall maintain all materials and information comprising the Source Code Escrow Package in confidence in accordance with this Contract;

(c) If the release is a temporary one, then the State shall promptly return all released materials to Contractor when the circumstances leading to the release are no longer in effect.

2.338 License

Upon release from the Escrow Agent pursuant to an event described in this Section, the Contractor automatically grants the State a non-exclusive, irrevocable license to use, reproduce, modify, maintain, support, update, have made, and create Derivative Works. Further, the State shall have the right to use the Source Code Escrow Package in order to maintain and support the Licensed Software so that it can be used by the State as set forth in this Contract.

2.339 Derivative Works

Any Derivative Works to the source code released from escrow that are made by or on behalf of the State shall be the sole property of the State. The State acknowledges that its ownership rights are limited solely to the Derivative Works and do not include any ownership rights in the underlying source code.

Bidder shall check only 1 box below, and identify exception(s) in regard to Article 2	
<input type="checkbox"/>	I have reviewed Article 2 agree with no exceptions.
<input type="checkbox"/>	<p>I have reviewed Article 2 and have identified all exceptions per the instructions below.</p> <p>I have identified all exceptions and revisions to Article 2 as track changes. I understand this could impact the State’s ability to award a contract to my firm by considering my proposal, and furthermore the State reserves the right to deduct as much as ten (10) points from my technical score for any exception or revision to Article 2. Furthermore, I understand that, if the State awards to my firm, and if the State and my firm cannot reach agreement on all excepted or revised Article 2 Terms and Conditions within five (5) business days of Notice of Recommendation, then the State reserves the right, at its sole discretion, to rescind the Award and to re-award to the next-most qualified bidder.</p>

Bidder shall provide a statement that a Certificate of Insurance will be provided as a condition of award has been included (referenced in Section 2.133).

Bidder Response:	
-------------------------	--



Glossary

#	Term	Definition
1.	24x7x365	A service that will be present regardless of current time or day. Specifically, 24 hours a day, seven days a week, 365 days a year including the 366th day in a leap year.
2.	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 Contractor with additional consideration.
3.	Audit Period	See Section 2.110
4.	Blanket Purchase Order	An alternate term for Contract as used in the State's computer system
5.	Business Critical	Any function identified in any Statement of Work as Business Critical.
6.	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.
7.	CEPD	Career Education Planning District
8.	Chronic Failure	See Section 2.240
9.	CTE	Career and Technical Education
10.	Data Center	A facility used to house computer systems and associated components, such as telecommunications and storage systems. It generally includes redundant or backup power supplies, redundant data communications connections, environmental controls (e.g., air conditioning, fire suppression) and security devices.
11.	Deleted/NA	Section is not applicable or included in this RFP. This is used as a placeholder to maintain consistent numbering.
12.	MDE	Michigan Department of Education
13.	OCTE	Office of Career and Technical Education
14.	DTMB	Department of Technology, Management and Budget
15.	Excusable Failure	See Section 2.244.
16.	Fiscal Year	October 1 through September 30 of the following calendar year.
17.	Incident	See SLA.
18.	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	See Article 1
19.	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 Contractor with additional consideration.
20.	PSN	Program Serial Number
21.	Reserved	Section is not applicable or included in this RFP. This is used as a placeholder to maintain consistent numbering.
22.	RFP	Request for Proposal designed to solicit proposals for services.
23.	Services	Any function performed for the benefit of the State.
24.	State	State of Michigan
25.	State Location	Any physical location where the State performs work. State Location may include state-owned, leased, or rented space.
26.	Subcontractor	A company Contractor delegates performance of a portion of the Services to, but does not include independent contractors engaged by Contractor solely in a staff augmentation role.
27.	SUITE	The State Unified Information Technology Environment. See Article 1, Section 1, Subsection 103.
28.	Unauthorized Removal	Contractor's removal of Key Personnel without the prior written consent of the State.



29.	Work in Progress	A Deliverable that has been partially prepared, but has not been presented to the State for Approval.
30.	Work Product	Refers to any data compilations, reports, and other media, materials, or other objects or works of authorship created or produced by the Contractor as a result of an in furtherance of performing the services required by this Contract.



Appendix A – Business/Technical Requirements

Your proposal must indicate ALL requirements were evaluated by responding in the column titled “Y/M/N” as follows.

1. **Yes** - abbreviated with the letter “Y”. “Y” is defined as the proposed solution complies with all aspects of the requirement as written.
 - In the event the response is “Y”, the bidder does not have to provide comments in the box, but may do so if they wish.

2. **Yes with Modifications** – abbreviated with the letter “M”. “M” is defined as the proposed solution does not comply with all aspects of the requirement as written but the Bidder agrees to modify the solution by adding additional resources, configure current resources, and/or perform custom programming (source code modifications) which will result in the solution reaching full compliance.
 - In the event the response is “M”, the bidder must describe in the comments column the proposed modification(s), how the modification(s) will satisfy the requirement.

3. **No** - abbreviated with the letter “N”. “N” is defined as the Bidder’s proposed solution does not comply with all aspects of the requirement as written and Bidder will not modify their solution to achieve full compliance with the requirement as written. **If you are not able to meet all aspects of the requirement as written you must indicate “N”.**
 - In the event the response is “N”, the bidder must describe in the comments column how not achieving this requirement will be mitigated in the Solution.

Bidder COMMENTS should be brief and relevant.



#	Requirement	Y/M/N
1	General Solution	
2	Contractor shall host and maintain the NAVIGATOR system 7x24x365 at operability, except for scheduled maintenance agreed upon with the State.	Y
3	Contractor shall host and maintain the system with an uptime of 98%, except for scheduled maintenance agreed upon with the State.	Y
4	The Contractor shall be responsible for installation and support of all software necessary for the operation of NAVIGATOR.	Y
5	The Contractor shall be responsible for the procurement, installation and support of all hardware necessary for the operation of NAVIGATOR	Y
6	The Contractor shall be responsible for the procurement, installation and support of the operating system, database and associated software related to NAVIGATOR. The Contractor shall not be responsible for maintaining State owned systems that use the NAVIGATOR application.	Y
7	The Contractor shall provide direct support (technical and help desk) to all end users identified in section 1.004 of this RFP.	Y
8	The Contractor will be responsible for updating the current NAVIGATOR site to comply with the eMichigan look and feel standards	Y
9	The system shall use a single centralized database	
10	The Contractor shall proactively update the application to remain current with latest browser versions of Internet Explorer, Mozilla Firefox, Safari and Chrome	Y
11	Telecom - Hardware - Software	
12	The Contractor shall pay the cost of providing, maintaining and repairing all systems.	Y
13	Telecom	
14	The Contractor shall provide a toll-free telephone number or a toll free number for Technical Support and Help Desk.	Y
15	Hardware	
16	The Contractor shall provide, own and support all hardware necessary for the setup and operation of the NAVIGATOR system.	Y
17	The Contractor shall be responsible for ongoing system configuration, performance tuning and maintenance activities.	Y
18	The Contractor shall be responsible for capacity management including timely forewarning if the growth exceeds capacity limitations.	Y
19	The Contractor shall be responsible for disk space management including archival, restoration, space management, and performance monitoring.	Y
20	The Contractor shall be responsible for application database management to ensure integrity and optimal performance of the database.	Y
21	The Contractor shall be responsible for server performance and system response time. The system shall be able to support 1.5x the peak number of concurrent users in order to provide sufficient capacity for growth. The system shall also support 1.25x the peak transaction volume in order to provide sufficient capacity for growth.	Y
22	Contractor shall host the Solution on hardware, covered under manufacturer warranty.	Y
23	Contractor shall conduct hosting hardware refreshes so as not to impact System performance or user access.	Y
23	Software	
25	The Contractor shall be responsible for installation and support of application software, operating system and all related software necessary to run the NAVIGATOR system.	Y
26	The Contractor shall provide at their expense any and all licenses needed for the operation of the NAVIGATOR.	Y
27	Contractor must update all necessary software patches in a timely manner for all software used to successfully run the Navigator system that will include but not limited to the Operating system,	Y



	Database etc.	
28	Data Access – Retention - Migration	
29	Data Access	
30	The Contractor shall provide the State admin read-only access to all the tables and views on the production database server upon the State's request.	Y
31	Data Retention	
32	The Contractor shall not purge data from the production database unless requested by the State.	Y
33	Data Conversion	
34	Contractor will be responsible for uploading the System data to the target environment database	Y
35	Disaster Recovery	
36	The Contractor shall provide with a disaster recovery plan and environment for server hosting facilities and the NAVIGATOR system, including application and database servers.	Y
37	System Backup and Recovery	
38	The Contractor shall provide for full backup of the NAVIGATOR System including database, application and web servers.	Y
39	The production servers shall be backed fully on a weekly basis and incrementally on a daily basis. Backup data shall be retained for at least 30 days or as required by OCTE.	Y
40	The system shall have the ability to allow for continued use of the system during backup.	Y
41	The system shall use transactional log files to provide point-in-time recovery of data to the last completed transaction.	Y
42	Upon failure, the contractor shall ensure that complete system is restored to its previous operational status within (4) hours after initiation of recovery process.	Y
43	The Contractor shall maintain secure, off-site backup of the data and application.	Y
44	Technical Support and Help Desk	
45	Call hold-times will not exceed three minutes.	Y
46	Answering machine service shall be available when help desk is not able to respond after three minutes of hold-time.	Y
	All calls will be returned within 15 minutes.	
47	Hosting Center	
48	The hosting sites shall have a physical environment plan including but not limited to UPS protection, backup power, temperature control, LAN, WAN and phone.	Y
49	Security	
50	Contractor shall protect the network from unauthorized or improper access by using firewall and intruder detection software.	Y
51	The Contractor's Network Administration shall monitor, log and report all intrusion attempts.	Y
52	The Vendor shall provide controlled access to the physical site.	Y
53	Technical Support and Help Desk	
54	The Contractor shall maintain a log of all calls made to the helpdesk and fully document the complaints and problems reported.	Y
55	Contractor will update the log immediately, at the date and time an end-user places the call to the Help Desk.	Y
56	Reporting Issues to OCTE	
57	The contractor shall report all operational issues and system failures to the State's project managers within two hours or as required by OCTE. Examples include equipment failures, delays due to unexpected overloads etc.	Y



Appendix B – Forms for Specified Deliverables for Section 1.104 A.2: EA Solution Assessment and DIT0-170 Security Assessment

Bidders are not required to complete the EA Solution Assessment with their proposal response. Bidders shall review Appendix B and be prepared to work with the State to finalize the EA Solution Assessment following award.

<input type="checkbox"/>	Bidder Response: I have reviewed Appendix B and will work with the State to finalize the EA Solution Assessment and the DIT-0170 Security Assessment following award.
--------------------------	---

Enterprise Architecture Solution Assessment	
Contact Info & Purpose (vendor version)	
The purpose of the EA Solution Assessment is to document architectural details of proposed IT solutions in order to determine compatibility with the overall SOM architecture. MDIT/SOM activities which require an Assessment include: the purchase of new licenses, contracting for software development services, purchase of new software components, installation of new software components, the purchase of new hardware components or the use of MDIT staff resources on any project beyond the design phase. All vendor proposals and new contracts must be accompanied by an Assessment, documenting the architectural details of the proposed solution. Vendor should complete all areas except where indicated.	
Vendor Version 2.3	
Solution/Project Name	<i>Central Reservation System</i>
RFP Name/Number	<i><SOM complete></i>
Date Submitted	<i><SOM complete></i>
Vendor Name	<i><vendor complete></i>
Vendor City and State	<i><vendor complete></i>
Vendor Phone No.	<i><vendor complete></i>
Vendor email	<i><vendor complete></i>
A brief description of the proposed solution and business purpose/process. <i>(please keep the description brief)</i>	The contractor will provide equipment and services resulting in the successful deployment of the new Campground Reservation System in identified State Parks, Harbors, OCTE offices, and commercial data center. The resulting Solution will enhance OCTE productivity and result in a high level of customer satisfaction.
Additional description of the solution and business purpose. <i>(please expand the row as much as needed)</i>	<i><vendor complete></i>



Select all that apply ✓ (vendor complete)	Enterprise Architecture Solution Assessment	
	Architecture Overview (vendor version)	
	<i>Vendor: the technologies listed below are standards used by the State of Michigan. Utilization of existing technology for new solutions is encouraged. Check the left column if the technology can be used with the solution being proposed. Add comments as needed.</i>	
1	Server/Application Hosting	Comments
	Internally Hosted	
	Externally Hosted	
	Internally & Externally Hosted	
2	User Interface Type	Comments (e.g. version or release)
	Browser	
	Citrix	
	Client	
	Mobile Browser	
	Mobile Client	
	Terminal	
	Other (explain =>)	
3	Supported Browsers (internet)	Comments
	Internet Explorer 6.x (intranet)	
	Firefox 3.0.x (internet)	
	Chrome 3.0 (internet)	
	Safari 4.x (internet)	
	Other (explain =>)	
4	Data Exchange Interface	Comments (e.g. version or release)
	EDI (industry protocol)	
	Flat File (private protocol)	
	Web Service	
	XML	
	Other (explain =>)	
5	System Access	Comments
	Internal (SOM)	
	External (public)	
	External (authorized)	
	Mixed (internal-external)	
6	User Access	Comments
	Internet	
	Intranet	
	Local Government (LGNet)	
	Public facing internet	
	Kiosk terminal	
	Vendor Net	
	VPN	
	Other (explain =>)	
7	Data Classification	Comments
	Non-sensitive	
	Sensitive w/ personal ID info	
	Sensitive w/ no personal ID info	
	Not classified	
	Other (explain =>)	
8	PCI-DSS Compliance Needed?	Comments
	Yes	
	No	



Enterprise Architecture Solution Assessment		
Architecture Overview (vendor version)		
Select all that apply ✓ (vendor complete)	<i>Vendor: the technologies listed below are standards used by the State of Michigan. Utilization of existing technology for new solutions is encouraged. Check the left column if the technology can be used with the solution being proposed. Add comments as needed.</i>	
1	Server/Application Hosting	Comments
	Internally Hosted	
	Externally Hosted	
	Internally & Externally Hosted	
2	User Interface Type	Comments (e.g. version or release)
	Browser	
	Citrix	
	Client	
	Mobile Browser	
	Mobile Client	
	Terminal	
	Other (explain =>)	
3	Supported Browsers (internet)	Comments
	Internet Explorer 6.x (intranet)	
	Firefox 3.0.x (internet)	
	Chrome 3.0 (internet)	
	Safari 4.x (internet)	
	Other (explain =>)	
4	Data Exchange Interface	Comments (e.g. version or release)
	EDI (industry protocol)	
	Flat File (private protocol)	
	Web Service	
	XML	
	Other (explain =>)	
5	System Access	Comments
	Internal (SOM)	
	External (public)	
	External (authorized)	
	Mixed (internal-external)	
6	User Access	Comments
	Internet	
	Intranet	
	Local Government (LGNet)	
	Public facing internet	
	Kiosk terminal	
	Vendor Net	
	VPN	
	Other (explain =>)	
9	Data Audit Trail Implementation	Comments
	Application Code	
	Database Audit Files	
	Database Triggers	
	Stored Procedures	
	Other (explain =>)	
10	IT Services (Centers of Excellence)	Comments
	x86 Virtualization	



Enterprise Architecture Solution Assessment		
Architecture Overview (vendor version)		
Select all that apply ✓ (vendor complete)	<i>Vendor: the technologies listed below are standards used by the State of Michigan. Utilization of existing technology for new solutions is encouraged. Check the left column if the technology can be used with the solution being proposed. Add comments as needed.</i>	
	1	Server/Application Hosting
	Internally Hosted	
	Externally Hosted	
	Internally & Externally Hosted	
2	User Interface Type	Comments (e.g. version or release)
	Browser	
	Citrix	
	Client	
	Mobile Browser	
	Mobile Client	
	Terminal	
	Other (explain =>)	
3	Supported Browsers (internet)	Comments
	Internet Explorer 6.x (intranet)	
	Firefox 3.0.x (internet)	
	Chrome 3.0 (internet)	
	Safari 4.x (internet)	
	Other (explain =>)	
4	Data Exchange Interface	Comments (e.g. version or release)
	EDI (industry protocol)	
	Flat File (private protocol)	
	Web Service	
	XML	
	Other (explain =>)	
5	System Access	Comments
	Internal (SOM)	
	External (public)	
	External (authorized)	
	Mixed (internal-external)	
6	User Access	Comments
	Internet	
	Intranet	
	Local Government (LGNet)	
	Public facing internet	
	Kiosk terminal	
	Vendor Net	
	VPN	
	Other (explain =>)	
	Address Verification	
	Business Objects Reporting	
	Digital Electronic Gateway (DEG)	
	Extract Transform Load (ETL)	
	Citrix Virtualization	
11	Enterprise Data Storage	Comments
	SAN	
	CAS / NAS	
	Internal Disk	



Enterprise Architecture Solution Assessment		
Architecture Overview (vendor version)		
Select all that apply ✓ (vendor complete)	<i>Vendor: the technologies listed below are standards used by the State of Michigan. Utilization of existing technology for new solutions is encouraged. Check the left column if the technology can be used with the solution being proposed. Add comments as needed.</i>	
1	Server/Application Hosting	Comments
	Internally Hosted	
	Externally Hosted	
	Internally & Externally Hosted	
2	User Interface Type	Comments (e.g. version or release)
	Browser	
	Citrix	
	Client	
	Mobile Browser	
	Mobile Client	
	Terminal	
	Other (explain =>)	
3	Supported Browsers (internet)	Comments
	Internet Explorer 6.x (intranet)	
	Firefox 3.0.x (internet)	
	Chrome 3.0 (internet)	
	Safari 4.x (internet)	
	Other (explain =>)	
4	Data Exchange Interface	Comments (e.g. version or release)
	EDI (industry protocol)	
	Flat File (private protocol)	
	Web Service	
	XML	
	Other (explain =>)	
5	System Access	Comments
	Internal (SOM)	
	External (public)	
	External (authorized)	
	Mixed (internal-external)	
6	User Access	Comments
	Internet	
	Intranet	
	Local Government (LGNet)	
	Public facing internet	
	Kiosk terminal	
	Vendor Net	
	VPN	
	Other (explain =>)	
	Other (explain =>)	
12	Database (RDBMS)	Comments
	MS SQL Server 2008	
	MySQL 5.1	
	Oracle 11g	
	TeraData A28V2R6.2 / 12.0	
	Other (explain =>)	

(continued)



Select all that apply ✓ (vendor complete)	Enterprise Architecture Solution Assessment	
	Architecture Overview (continued)	
	<i>Vendor: the technologies listed below are standards used by the State of Michigan. Utilization of existing technology for new solutions is encouraged. Check the left column if the technology can be used with the solution being proposed. Add comments as needed.</i>	
13	Database Modeling Tools	Comments
	Erwin 7.x	
	MSSQL Server Mgmt Studio (match db)	
	MySQL Workbench (match db)	
	Oracle Designer (match db)	
	TeraData Utilities (match db)	
	Other (explain =>)	
14	Development Framework	Comments
	.NET Framework 3.5	
	Java J2EE 5.x	
	Other (explain =>)	
15	Development Platform	Comments
	Eclipse 3.x	
	Hibernate 3.x	
	IBM Websphere Integration Dev 6.1 & 6.2	
	Microsoft SilverLight Expression 2.x	
	Microsoft Team Foundation System 2008	
	Microsoft Visual Studio 2008	
	Oracle JDeveloper 11g	
	Spring 2.5	
	Struts 2.x	
	XML Spy 2010	
	Other (explain =>)	
16	Development Language	Comments
	ASP .NET 2008	
	CSS Level 2	
	Microsoft C#	
	Microsoft VB.Net	
	Java	
	JavaScript	
	JDK 6.x	
	PHP 5.2	
	Other (explain =>)	
17	Markup languages	Comments
	HTML 4 & 5	
	XML Schema 1.1	
	XSLT 2.0	
	XHTML 2.0	
18	Presentation (Web) Server	Comments
	Apache HTTPD 2.2.x	
	IBM Websphere IHS 6.1	
	Microsoft IIS 7.0	
	Other (explain =>)	
19	Application Server	Comments
	.NET Framework 3.5	



	IBM WebSphere 6.1	
	JBoss 5.x	
	Oracle C4J	
	Other (Explain)	
20	HW Platform	Comments
	Dell	
	HP	
	Sun	
	Unisys Mainframe	
	x86 Virtualization	
	Other (explain =>)	
21	Server OS	Comments
	Linux Redhat Enterprise Server 5.x	
	Linux SUSE Enterprise 10.x	
	Microsoft Windows 2008	
	Unix HPUX 11i v3	
	Unix Sun Solaris 10.x	
	VMWare vSphere 4	
	Other (explain =>)	
22	Document Management	Comments
	EMC Documentum 6.5 & 7.0	
	FileNet Content Services 5.4	
	FileNet Document Mgmt P8	
	HP Trim	
	PaperPort 10	
	MS SharePoint Server 2007 EE	
	Other (explain =>)	
23	Centralized Printing	Comments
	DMB consolidated print center	
	Other (explain =>)	
24	Testing Tools	Comments
	Junit 4.x	
	LoadRunner 9.x	
	Microsoft Team Foundation System	
	Quick Test Pro 10.x	
	Selenium 1.x	
	Other (explain =>)	
25	Identity Management (network)	Comments
	Active Directory 2008	
	Other (explain =>)	
26	Identity Management (application)	Comments
	IBM Tivoli SSO (TIM-TAM)	
	Novell e-Dir 8.8.x	
	Other (explain =>)	
27	Project Management	Comments
	Clarity 12.0	
	MS Project 2007	
	Other (explain =>)	

(continued)



Select all that apply ✓ (vendor complete)	Enterprise Architecture Solution Assessment	
	Architecture Overview (continued)	
	<i>Vendor: the technologies listed below are standards used by the State of Michigan. Utilization of existing technology for new solutions is encouraged. Check the left column if the technology can be used with the solution being proposed. Add comments as needed.</i>	
28	Requirements Gathering	Comments
	Compuware Optimal Trace 5.x	
	Microsoft Office	
	Microsoft Visio	
	SUITE/SEM templates	
	Rational Requisite Pro 7.1	
	Serena Dimensions 2009 R1.x	
	Other (explain =>)	
29	Design Tools	Comments
	Microsoft Visio	
	MSSQL Server Mgmt Studio (match db)	
	Rational Rose 7.0	
	Serena Prototype Composer 2009 R1.x	
	Other (explain =>)	
30	Version Control	Comments
	Microsoft Team Foundation System	
	Serena Dimensions (PVCS Mgr) 2009 R1.x	
	Subversion 1.6	
	Other (explain =>)	
31	Message Queuing	Comments
	Apache Active MQ 5.3	
	IBM Websphere MQ 6.x, 7.x	
	Other (explain =>)	
32	Business Integration	Comments
	JBoss SOA 4.3	
	Websphere Message Broker 6.x	
	Other (explain =>)	
33	Database Tools	Comments
	DBArtisan 8.6, 8.7	
	Infosphere Information Svr v8.1.x	
	MSSQL Server Mgmt Studio (match db)	
	MySQL Workbench (match db)	
	Oracle Developer Suite (match db)	
	Oracle Enterprise Manager (match db)	
	Oracle SQL Developer (match db)	
	Rapid SQL 7.6 & 7.7	
	TeraData Utilities (match db)	
	Toad 9.x & 10.x	
	Other (explain =>)	
34	Reporting Tools	Comments
	ActivePDF 2009	
	ActiveReports 4.0	
	Crystal Reports XI R2, 2008	
	Crystal Xcelsius 2008	
	Crystal Reports for Eclipse 2.x	



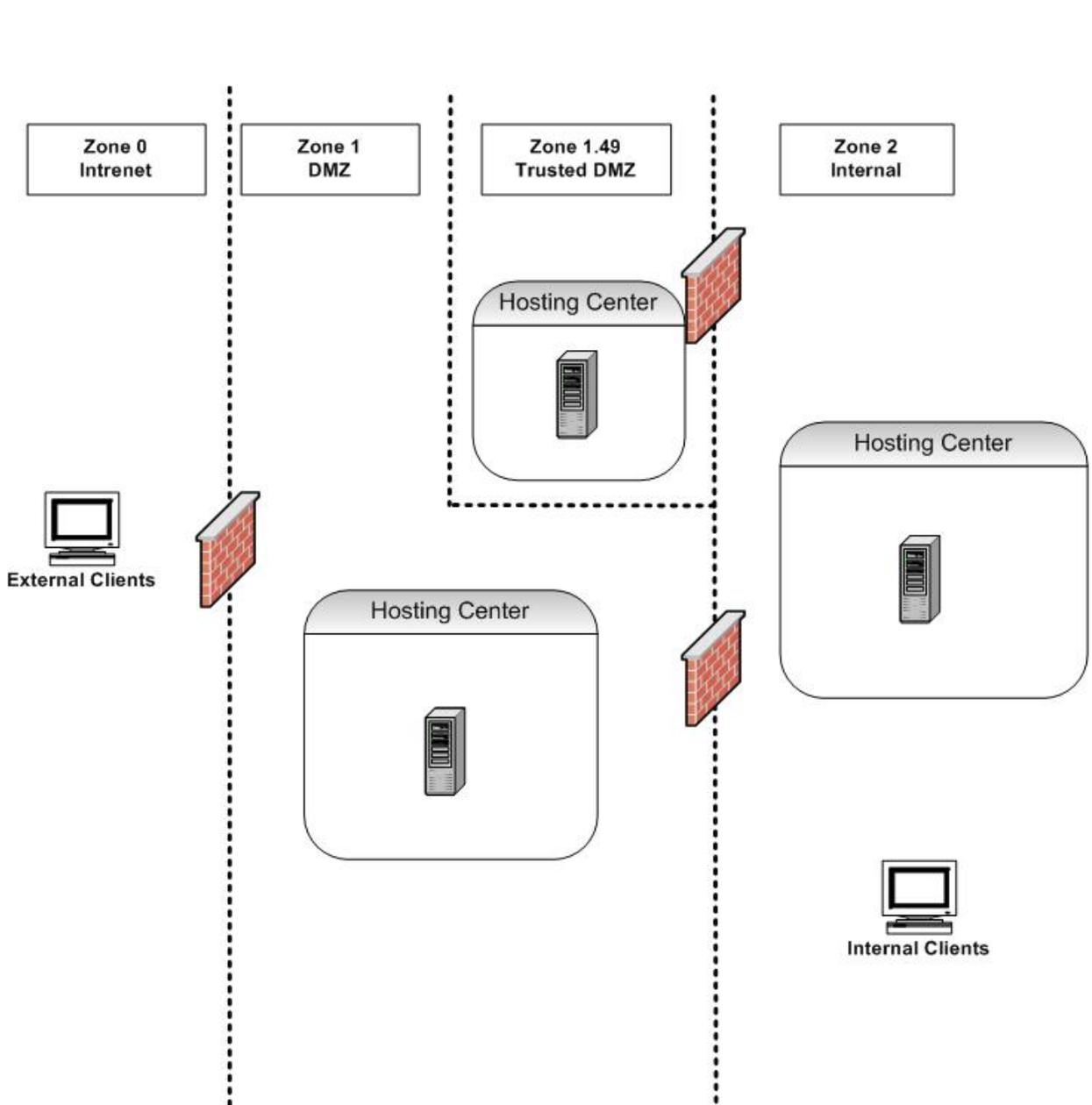
	MSSQL Reporting Services (match db)	
	Oracle Reports (match db)	
	Other (explain =>)	
35	End-User Tools	Comments
	Business Objects (BO) XI R2, 3.x	
	Oracle Discoverer (match db)	
	Other (explain =>)	
36	Deployment Tools	Comments
	Microsoft Team Foundation System 2008	
	Serena Dimensions CM Mover 2009, 2.3	
	Other (explain =>)	
(continued)		
37	Build Tools	Comments
	Apache Ant 1.7.1	
	Apache Maven 2.1.x	
	Microsoft Team Foundation System 2008	
	Serena Dimensions CM Builder 2009 R1.x	
	Other (explain =>)	
38	Job Schedulers	Comments
	BL/Sched 5.2	
	OpCon XPS 4.x.x	
	Tidal Enterprise Scheduler 5.3.1 & 6.0	
	UC4 Global 5.0	
	UC4 Op Mgr 6.0 & 8.0	
	Other (explain =>)	
39	GIS Technologies	Comments
	ArcIMS 9.3	
	ArcGIS Server 9.3	
	ArcSDE 9.3	
	Erdas ADE Rel. 2	
	ER Mapper Image Server 7.2	
	Oracle Spatial (match db)	
	Oracle MapView (match db)	
	Other (explain =>)	
40	Issue & Defect Tracking	Comments
	Bugzilla 3.2.5 & 3.4.2	
	Clear Quest Chg Mgmt Suite 7.5	
	Microsoft Team Foundation System 2008	
	Serena Mashup Composer 2009 R1.x	
	Other (describe =>)	



Enterprise Architecture Solution Assessment

Server/Network Diagram (vendor version)

Diagrams are useful to illustrate the interaction of technologies. The "Server/Network Diagram" is intended to allow the EA (Enterprise Architecture) Core Team to understand the relationship between the system components. Below is an example illustrating the network components deemed necessary. Vendors may use their own format so long as adequate information is conveyed.



State of Michigan Network Diagram Example
 Network example only
 To be completed by vendor



STATE OF MICHIGAN



Department or Agency
Title of Application

Technology, Management and Budget
Project Security Plan & Assessment

Prepared by:
Date:

	Initiation & Planning	Requirements Definition	Functional Design	System Design	Construction	Testing	Implementation	Operations/Maintenance	Disposal
Lifecycle Stage	<input type="checkbox"/>								

MCS USE ONLY			
C	I	A	Total Score



Table of Contents

- o
- o
- [1.0 Introduction](#) 79
 - [1.1 Resource Roles and Responsibilities](#) 79
- [2.0 Current Status](#) 79
- [3.0 SEM Initiation and Planning Stage](#) 79
 - [3.1 Purpose](#) 79
 - [3.2 Laws, Regulations, DTMB and/or Agency Security Policies, Standards and Procedures](#) 80
 - [3.3 Data classification](#) 80
 - [3.4 System and Information Security Level \(Low, Moderate, High\)](#) 81
- [4.0 SEM IT Business/Security Requirements Stage](#) 81
- [5.0 & 6.0 SEM Functional and System Design Stage](#) 82
 - [5.1/6.1 Describe the function of the system/application and the information processed for each server utilized in this project.](#) 82
 - [5.2/6.2 Other Systems or Applications serviced by this hardware](#) 82
 - [5.3/6.3 Hardware this system/application will be utilizing](#) 83
 - [5.4/6.4 Security Control Groups Implemented in the Project](#) 83
 - [5.5/6.5 Infrastructure/Network Diagram](#) 87
 - [5.6/6.6 Data Flow Diagram](#) 88
- [7.0 SEM Construction Stage](#) 89
- [8.0 SEM Testing Stage](#) 89
- [9.0 SEM Implementation Stage](#) 89
 - [9.1 Security Analysis \(To be completed by MCS Security Liaison\)](#) 89
 - [9.2 Sponsors and Stakeholders](#) 90
 - [9.3 Approvals](#) 90
- [Appendix A - System and Information Security Level Matrix](#) 91
- [Appendix B - System Security Control Requirements](#) 93
- [Appendix C – Acronyms](#) 104
- [Appendix D - Laws, Regulations, DTMB and/or Agency Security Policies, Standards & Procedures](#) 105
- [Appendix E - Security Analysis \(To be completed by MCS Security Liaison\)](#) 107



o

Revision History

o

Name	Date	Reason for Change	Version



o

1.0 Introduction

o Including security early in the life cycle of a project will usually result in less expensive and more effective security than adding it to an operational system. This document presents a guide for incorporating security into the Systems Engineering Methodology (SEM) of the State Unified Information Technology Environment (SUITE) Model. This document will help agencies select and acquire cost-effective security controls by explaining how to include information system security requirements within the appropriate stages of the SEM.

o SEM includes the following stages: Initiation & Planning, Requirements Definition, Functional Design, System Design, Construction, Technical Testing, and Implementation. Each of these stages identifies minimum security needed to effectively incorporate security into a system during its development.

o This document serves as documentation of the structured process of planning adequate, cost-effective security protection for a system. This document contains detailed technical information about the system, its security requirements, and the controls implemented to provide protection against its risks and vulnerabilities. This document, at a minimum, is marked, and should be handled and controlled as a sensitive document. This document is submitted to obtain a formal security sign off from the sponsors. The lack of sign-off may prevent the security elements of this project from proceeding to production.

o

o

1.1 Resource Roles and Responsibilities

o

Insert Matrix

o

"Click HERE and Type"

o

o

Or

o Completed DIT Form PMM-02, Project Charter

2.0 Current Status

This section documents the current status of the software/project. If the application is new and has never existed before, this section can be skipped.

o

"Click HERE and Type"

o

o

3.0 SEM Initiation and Planning Stage

o This is the first stage in the SEM lifecycle of the project. This stage involves the establishment of a need for a new system or enhancements to an existing system, the data that is being collected or handled, and which policies or standards need to be addressed in the design phase. This stage will also classify the data handled by the project based on Federal NIST Guidelines.

o

o

3.1 Purpose

o

This section documents the purpose of the application/project, including the business problem to be solved or reason for changes that need to be made to the current status of the application/project.

o



○
"Click HERE and Type"

-
-

3.2 Laws, Regulations, DTMB and/or Agency Security Policies, Standards and Procedures

○
○ The State of Michigan information is a valuable asset that must be protected from unauthorized disclosure, modification, use, or destruction. Prudent steps must be taken to ensure that its integrity, confidentiality, and availability are not compromised. Laws, regulations, policies, standards and procedures have been developed to provide a secure environment for developing, implementing, and supporting information technology and systems. The system must comply with all applicable laws, both state and federal, and any additional regulations and guidelines established by the agency or DTMB. Below is a list of some of the applicable laws, regulations, policies, standards and procedures many systems must comply with. This is not an all-inclusive list and short explanations are supplied in Appendix D:

- Identity Theft Protection Act (Senate Bill No. 309), Public Act 566 of 2006, amending Act 452 of 2004
- Social Security Number Privacy Act (Senate Bill No. 795, Public Act 454 of Public Acts 2004)
- 1305 SOM Enterprise Information Technology Policy
- 1310.03 Active Directory Password Standard
- 1315.00 Policy for Storage of Sensitive Information on Mobile Devices & Portable Media
- 1315.10 Standard for Electronic Data Encryption
- 1325 Information Technology Security Awareness Policy
- 1335 Information Technology Access Control Policy
- 1340 Information Technology Information Security Policy
- 1345 Information Technology Network and Infrastructure Policy
- 1350.11 Security Operational Guidelines for Servers
- 1350.20 Authorization Access to Data Sources
- 1350.40 Access Control Criteria for Data Sources
- 1350.90 Secure Disposal of Installed & Removable Digital Media
- 1355 Project Management Methodology Policy
- 1360 Systems Engineering Methodology Policy
- 1390 Information Technology Continuity of Business Policy
- 1410.21 Procurement and Usage of State Wireless Devices – Usage of PDAs, Blackberrys, phones, and pagers
- 1420.00 Wireless – Usage and deployment of wireless LANs and equipment.

○
○
"Click HERE and Type"

-
-

3.3 Data classification

-



Does this project collect Social Security Numbers, Drivers License Numbers, Credit Card Numbers, or other potentially sensitive information?

"Click HERE and Type"

Does the hardware supporting this project also support other projects that handle sensitive information?

"Click HERE and Type"

3.4 System and Information Security Level (Low, Moderate, High)

-
- The System and Information Security Level Matrix (see Appendix A for guidelines pertaining to data classification) is used to determine the overall security level categorization of your information, application, and the interconnectivity of other systems used by your application. This categorization will determine the appropriate security controls that need to be implemented. Your Security Liaison can assist you.
-
- (This system categorization is based on FIPS Publication 199 and NIST 800-60 ver. 2.0)
-

Category	Application/Data (Classification of data handled by this project/application)	Systems* (Classification of data handled by other applications that are also installed on this server hardware)	Overall Security Level
Confidentiality			
Integrity			
Availability			

-
- Based on the System and Information Security Level Matrix, the "Overall Security Level" categorization of your application system has been rated a "Enter Overall Security Level rating" level in regards to Confidentiality, Integrity, and Availability risk.
-

* This rating is based on the most sensitive information.

4.0 SEM IT Business/Security Requirements Stage

-
- The primary goal of this stage is to identify the security requirements for the project. These security requirements become the initial baseline for product design and a reference for determining whether the completed product performs as the system owner requested and expected. All system security requirements, (e.g., software, hardware, performance, functional, infrastructure, etc.) should be evaluated and included in the requirements gathering process.
-

-
- NIST Special Publication 800-53 was selected as a baseline of minimum security controls to protect the system, information, and apply tailoring guidance as necessary. These detailed security controls are contained in Appendix B of this document.
-



- The required security controls for your application are based on the previous section’s Data Classification (Section 3.3)/System and Information Categorization (Section 3.4) “Overall Security Level” (Low, Moderate, High).
- If your application is determined to be “**Low**”, you need only to implement the controls in the Low columns of Appendix B.
- If your application is determined to be “**Moderate**”, you must implement all controls in the Low and Moderate columns of Appendix B.
- If your application is determined to be “**High**”, you must implement all controls in the Low, Moderate, and High columns of Appendix B.
- The detailed NIST security controls in Appendix B are rolled together into higher level groups and for speed of documentation these security control groups can be checked off as the project design proceeds through the Functional & System Design Stages (Stage 5 & 6) and the appropriate SUITE SEM templates are completed.
- If SEM templates are completed and on file with the project manager, place a check mark in the associated box for that template indicating the documentation for that security group in the DIT-0170 can be obtained from those templates and it need not be duplicated here.
- Any control groups not implemented may be flagged as a risk by the Security Liaison in the final Risk Analysis Section (Section 9) and additional controls may be recommended before implementation.

"Click **HERE** and Type"

-
-
-

5.0 & 6.0 SEM Functional and System Design Stage

- During this stage, the overall structure of the product is defined from a Functional & System viewpoint. The Functional & System design describes the logical system flow, data organization, system inputs and outputs, processing rules, operational characteristics of the product from the user’s point of view and documents that the Security Control Groups have been implemented in the design.

-
-

5.1/6.1 Describe the function of the system/application and the information processed for each server utilized in this project.

- *List each server name and then describe how each server will be utilized in the project.*

-
-

"Click **HERE** and Type"

-
-

- Completed SEM-501 (Functional Design Document)

-
-

5.2/6.2 Other Systems or Applications serviced by this hardware

-

- Other Information Security Assessments (DIT-0170) are reviewed and updated for other systems or applications serviced by this same hardware (Section 3.2 & 3.3) to now include this project’s information.



5.3/6.3 Hardware this system/application will be utilizing

- Solutions Engineering form for hosting the hardware is completed

5.4/6.4 Security Control Groups Implemented in the Project

Check the Security Control Groups being implemented for this project to provide for the protection of the Agency's assets. These Security Control Groups are a high level representation of the most critical of the detailed Security Controls that are listed in Appendix B. The detailed controls should be reviewed to ensure that each control within the group is implemented in accordance with the Overall Security Level of this application/project.

- **Access Control:** *(See Appendix B for individual control details.)*

Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

- Process in place for management of accounts which includes separation of duties.
- Follows M1 guidelines including unique IDs for every user.
- Utilizes Role based controls and least privilege.

- **Awareness & Training:** *(See Appendix B for individual control details.)*

Organizations must: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

- Personnel and system users receive appropriate security training
- Completed SEM-0703 (Training Plan) and included Security and Awareness training
- Completed SEM-0704 (Training Checklist)

- **Audit & Accountability:** *(See Appendix B for individual control details.)*

Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

- System generated audit logs are written, stored securely, and they are reviewed regularly.

- **Certification, Accreditation, & Security Assessments:** *See Appendix B for individual control details.)*

Organizations must: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information



systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

- o Completed DIT-0170 is reviewed by the Office of Cyber Security, and the Agency approves the information system security assessment before full implementation.

- o **Configuration Management:** (See Appendix B for individual control details.)

Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems

- o Hardware and Software are listed in CMDB and follow the hardening and change control process.
- o Completed SEM-0302 (Software Configuration Management Plan)

- o **Continuity Planning/Disaster Recovery:** (See Appendix B for individual control details.)

Organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

- o Business Continuity Plan is in place
- o Business Application Criticality Request (DIT-0208) completed if appropriate
- o Disaster Recovery Plan is in place
- o Backups of system are performed and stored in off site location
- o Backups are tested for restore capability
- o Business Continuity Plan and Disaster Recovery Plan are tested.

- o **Identification & Authentication:** (See Appendix B for individual control details.)

Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

- o Unique identification of user is accomplished through use of passwords, tokens, or biometrics following M1 guidelines
- o Authentication system meets requirements of applicable laws, policies, and standards

- o **Incident Response:** (See Appendix B for individual control details.)

Organizations must: (i) establish an operational incident handling capability for all components and data of organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.

- o Organization has a documented incident response process per above



○ **Maintenance:** (See Appendix B for individual control details.)

Organizations must: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

- Completed SEM-0301 Maintenance Plan
- Only authorized personnel are allowed to perform maintenance
- Change control process is utilized for all maintenance

○ **Media Protection:** (See Appendix B for individual control details.)

Organizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.

- Only authorized users have access to information either printed or electronic
- Media is sanitized and disposed of in accordance with DTMB policies
- Sensitive (PII) information is stored and transported in encrypted form

○ **Physical & Environmental Protection:** (See Appendix B for individual control details.)

Organizations must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

- System is located in Lake Superior, Lake Ontario, or Traverse Bay Hosting Center
- Completed SEM DIT-0184 (Infrastructure Service Request)

○ **Planning:** (See Appendix B for individual control details.)

Organizations must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the ethical rules of behavior for individuals accessing the information systems.

- Information Security Assessment (DIT-0170) is regularly reviewed and updated
- Contractors have signed Non-disclosure Agreement (DIT-0049) before access is allowed
- Users have signed End User Computing Agreement (DIT-0929) before access is allowed

○ **Personnel Security:** (See Appendix B for individual control details.)

Organizations must: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.



- Background checks (DIT-0021) have been performed where appropriate
- SLAs are signed before allowing Inter-agency access
- Non-Disclosure Contractor Security Agreements (DIT-0928) have been completed and signed where appropriate

○ **Risk Assessment:** *(See Appendix B for individual control details.)*

Organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

- Information Security Risk Assessment (DIT-0170) is completed
- Security Scans are regularly performed and vulnerabilities are mitigated

○ **System & Services Acquisition:** *(See Appendix B for individual control details.)*

Organizations must: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

- SUITE systems life cycle is used to procure, develop, and manage systems

○ **System & Communications Protection:** *(See Appendix B for individual control details.)*

Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

- System has inactivity time out
- System Communications are encrypted when appropriate

○ **System and Information Integrity:** *(See Appendix B for individual control details.)*

Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

- System employs malicious code protection techniques (i.e., SQL Injection)
- System restricts data input to authorized personnel only

○ **Vendor, contractor & third party:** *(See Appendix B for individual control details.)*

- Remote access is secured through VPN
- Security agreements are signed, maintained and reviewed yearly



- - **Infrastructure/Network:** *(See Appendix B for individual control details.)*
 - Enterprise Architecture solution assessment is completed
 - Network diagram is approved (email from Liaison) by Cyber Security based on DTMB network security standards
 - Exceptions completed and approved for deviation to network standards or PCI compliance

-
-

5.5/6.5 Infrastructure/Network Diagram

○
 The network diagram depicts the way that the data is transported on the network equipment from one device to the next without regard to the physical interconnections of the devices.

○
Network diagram must be approved (email from Liaison) by Cyber Security based on DTMB network security standards

○
 Furnish network diagram detailing infrastructure features

- Include:*
- Specify name and location of the system/application*
 - Servers/IP Addresses*
 - Services*
 - Database Names*
 - Load Balances*
 - Ports and Protocols*
 - Encrypted Communication*
 - Communication port numbers*

"Click [HERE](#) and create / paste your diagram"

-



5.6/6.6 Data Flow Diagram

○ Describe data process flow of the application from system input to system output.

- Furnish diagram
- Describe interface and how it is accomplished
- Identify data flow
- Type of data
- Direction of flow

"Click HERE and paste diagram"

○
○
○ **Or**

- Completed SEM-0604 (System Design Document)
- Completed SEM-0605 (System Design Checklist)

○ If a completed SEM-0604 and SEM-0605 are on file with the project, Section **5.6/6.6 Data Flow Diagram** can be check marked above and completion of the DIT-0170 document can proceed to Section **7.0 SEM Construction Stage**.



7.0 SEM Construction Stage

-
- In this stage, confirmation that sensitive data or data under conversion is handled and protected correctly based on classification.
-
- ○ Completed SEM-0701 (Transition Plan)
- ○ Completed SEM-0601 (Conversion Plan)

8.0 SEM Testing Stage

-
- In this stage, security controls are tested to determine whether the sensitive data or data under conversion is handled and protected based on classification.
-
- *Is there a test plan?*

"Click HERE and Type"

-
-
- *Are roles and responsibilities tested?*

"Click HERE and Type"

-
-
- *Is there separation of duties implemented?*

"Click HERE and Type"

-
-
- ○ Completed SEM-0602 (Test Plan)

9.0 SEM Implementation Stage

-
- In this stage, Qualys scans are performed, security training is performed and security controls are validated. A final security analysis is provided, identifying residual risks of which DTMB and the agency approve.
-
- *Every PCI vulnerability must be covered by one of three scenarios*
 1. *Remediated by patch or version.*
 2. *False Positive (documented, submitted to MCS, and approved).*
 3. *Exception Request (documented, submitted to TRB, and approved).*

9.1 Security Analysis (To be completed by MCS Security Liaison)

-
- *See Appendix E.*



-
-

9.2 Sponsors and Stakeholders

-
-

"Click HERE and Type"

-
-

9.3 Approvals

-

By signing below, I certify that I have read and acknowledge all sections of this document and each residual risk and recommended control (Appendix E) contained in Section 9. My signature indicates that the Agency has accepted each residual risk if the corresponding recommended control is not implemented.

-
-

○ **Approved** ○ **Date:** ○
 by: _____
 ○ (Project Manager) ○

By signing below, I certify that I have read and acknowledge Sections 2, 3, 4, 5.4/6.4, 9, and each residual risk and recommended control contained in Appendix E of this document. My signature indicates that the Agency accepts each residual risk if the corresponding recommended control is not implemented.

○ **Approved** ○ **Date:** ○
 by: _____
 ○ (Business Owner) ○

By signing below, I certify that I have read and acknowledge all sections of this document and each residual risk and recommended control (Appendix E) contained in Section 9. My signature indicates that the Agency has accepted each residual risk if the corresponding recommended control is not implemented.

○ **Approved** ○ **Date:** ○
 by: _____
 ○ (Client Service Director) ○

By signing below, Office of Cyber Security believes that all information and sections of this document are accurate and complete to the best of the information provided. Each residual risk and recommended control (Appendix E) contained in Section 9 has been reviewed and the Agency has accepted each residual risk if the corresponding recommended control is not implemented.

○ **Approved** ○ **Date:** ○
 by: _____
 ○ (Office of Cyber Security) ○



Appendix A - System and Information Security Level Matrix

Security Objective	Potential Impact		
	Low	Moderate	High
<p>Confidentiality:</p> <p>Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.</p>	<p>The unauthorized disclosure of information would have limited adverse effect on State of Michigan operations, assets, or individuals.</p> <p>Example(s):</p> <ul style="list-style-type: none"> ○ Public Information ○ Information available via Freedom of Information Act 	<p>The unauthorized disclosure of information would have a serious adverse effect on State of Michigan operations, assets, or individuals.</p> <p>Example(s):</p> <ul style="list-style-type: none"> ○ Personal information affecting an individual's privacy (e.g. an individual's medical information; driver's license number; social security number; banking information, etc...) 	<p>The unauthorized disclosure of information would have a severe or catastrophic adverse effect on State of Michigan operations, assets, or individuals.</p> <p>Example(s):</p> <ul style="list-style-type: none"> ○ Highly sensitive information that may affect human life or safety (e.g. under cover investigation information; confidential response plans for emergencies) ○ Information that if released would violate State or Federal Law ○ Significant amount of privacy information (e.g. thousands of individuals credit card numbers; social security numbers; banking information; medical information, etc...)
<p>Integrity:</p> <p>Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.</p>	<p>The unauthorized modification or destruction of information would have limited adverse effect on State of Michigan operations, assets, or individuals.</p>	<p>The unauthorized modification or destruction of information would have a serious adverse effect on State of Michigan operations, assets, or individuals.</p>	<p>The unauthorized modification or destruction of information would have a severe or catastrophic adverse effect on State of Michigan operations, assets, or individuals.</p> <p>Example(s):</p> <ul style="list-style-type: none"> ○ Information that could affect human life or safety (e.g. criminal history; warrant/arrest data; active investigation information; child protection services information) ○ Information that could severely affect public confidence (e.g. modification of voter registration or voting results; tax information; lottery drawings) <p>Information that may affect national security (e.g. birth certificates; emergency response plans and procedures; risk assessments and vulnerability information)</p>



	Low	Moderate	High
<p>Availability:</p> <p>Ensuring timely and reliable access to and use of information and systems.</p>	<p>The disruption of access to or use of information or an information system would have limited adverse effect on State of Michigan operations, assets, or individuals.</p>	<p>The disruption of access to or use of information or an information system would have a serious adverse effect on State of Michigan operations, assets, or individuals.</p> <p>Example(s):</p> <ul style="list-style-type: none"> ○ Information or information system that if not available, would seriously affect the public's trust of the State (e.g. unemployment applications; Secretary of State applications; OTIS) ○ Information or information system that if not available, could seriously affect the State financially (e.g. large revenue generating applications;) 	<p>The disruption of access to or use of information or an information system would have a severe or catastrophic adverse effect on State of Michigan operations, assets, or individuals.</p> <p>Example(s):</p> <ul style="list-style-type: none"> ○ Information or information system that if not available, could affect human life or safety (e.g. LEIN; prisoner tracking systems; emergency response systems) ○ Information or information system that if not available, would severely affect the public's trust of the State (e.g. welfare checks; food stamps; voter registration) ○ Information or information system that if not available, could severely affect the State financially (e.g. Tax systems;)

○



Appendix B - System Security Control Requirements

NIST 800-53 Control Name	Security Classification		
	Low	Moderate	High
<p>Access Control (AC)</p> <ul style="list-style-type: none"> ○ Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise. 	<ul style="list-style-type: none"> ● Access Control Policy & Procedure documented, reviewed and updated (AC-1) ● Management of accounts (AC-2) ● Comply with DTMB and Agency policies and procedures ● A unique user ID and password is required for access (AC-3) ● Tighten default settings to prevent unauthorized access ● Disable inactive accounts ● Terminate temporary and emergency accounts ● The system automatically locks an account until released by an administrator when five unsuccessful attempts is exceeded (AC-7) ● Remote Server Access is authenticated using 2-factors and/or VPN ● System displays an approved message of use restrictions before granting access. (AC-8) ● Review audit records (e.g., user activity logs) on a regular basis. (AC-13) ● Remote access is controlled. (AC-17) ● Inter-agency access is controlled. (AC-20) ● Separation of Duties ● Security Disclosure and Acceptable Use Agreements signed, maintained and reviewed on a yearly basis 	<p>All Low plus the following:</p> <ul style="list-style-type: none"> ● Automatically terminate temporary and emergency accounts ● Automatically disable inactive accounts ● Role based access controls must be applied to databases, applications, or computer hosts that contain protected information. (AC-4) ● Firewall rules, Access Control Lists. (AC-4) ● Separation of Duties through assigned access authorizations. (AC-5) ● Initiate session lock after period of inactivity. (AC-11) ● Initiate disconnect on remote connection after period of inactivity. (AC-12) ● Access is deleted no later than day-end of the user's last day if the separation is friendly, or immediately if the separation is unfriendly ● Least Privilege – Access restrictive set of rights/privileges or accesses needed. (AC-6) ● Ensure that access to security functions (hardware, software, and firmware) and information is restricted to authorized personnel ● Authentication and encryption is used to protect wireless access ● Mobile devices that access the system are scanned for malicious code, updated virus protection software, scan for critical software updates and patches. (AC-19) 	<p>All Low and Moderate plus the following:</p> <ul style="list-style-type: none"> ● Auditing of account creation, modification, disabling and termination ● Review audit records (e.g., user activity logs) on a daily basis ● Removable hard drives or cryptography to protect information residing on portable and mobile devices ● System limits the number of concurrent sessions. (AC-10) ● Automated marking of outputs to identify special handling. (AC-15) ● Transmitted minimum 128-bit encryption



NIST 800-53 Control Name	Security Classification		
	Low	Moderate	High
<p>Awareness & Training (AT)</p> <ul style="list-style-type: none"> ○ Organizations must: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities. 	<ul style="list-style-type: none"> ● A documented security awareness and training policy and procedure developed and distributed to all employees. (AT-1) ● System users receive security awareness training prior to authorizing access. (AT-2) ● Personnel who have significant system security roles or responsibilities receive appropriate security training based on that role. (AT-3) ● Document and monitor individual security training activities. (AT-4) ● All employees have a signed security agreement in their personnel file upon hire and renewed yearly ● Background check upon hire and security exit interview upon termination (retire, transfers, terminations, etc.) ● Acceptable Use Policy 	<p>All Low plus the following:</p> <ul style="list-style-type: none"> ● Information disclosure and confidentiality statements, are posted throughout the facility 	<p>All Low & Moderate plus the following:</p>
<p>Audit & Accountability (AU)</p> <ul style="list-style-type: none"> ○ Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions. 	<ul style="list-style-type: none"> ● A documented audit and accountability policy (AU-1) ● System generates Audit Records for Agency/DIT defined events. (AU-2) ● Audit record should contain: data and time of the event, subject identity, type of event, how data changed, where the event occurred, and the outcome of the event. (AU-3) (AU-8) ● Sufficient audit storage capacity should allocated. (AU-4) ● System alerts if audit log generation fails. (AU-5) ● System protects audit information from unauthorized access. (AU-9) 	<p>All Low plus the following:</p> <ul style="list-style-type: none"> ● Audit record should be reviewed on a regular basis. (AU-6) ● Audit logs are stored for sufficient period of time. (AU-7) (AU-11) 	<p>All Low & Moderate plus the following:</p> <ul style="list-style-type: none"> ● Audit record should be reviewed on a daily basis ● System automatically processes audit records for events of interest. (AU-7(1))



NIST 800-53 Control Name	Security Classification		
	Low	Moderate	High
<p>Certification & Accreditation (CA)</p> <ul style="list-style-type: none"> ○ Organizations must: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls. 	<ul style="list-style-type: none"> ● A documented security assessment policy and procedure that is consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance and distributed to all employees. (CA-1) ● Organization conducts an assessment of the security controls in all their information systems to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome. (CA-2) ● Organization formally authorizes all connections from other information systems and carefully considers the risks that may be introduced. (CA-3) ● Organization conducts an assessment of the security controls in all their information systems to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome and this assessment is reviewed by the Office of Cyber Security. (CA-4) ● Organization develops and updates a plan of action and milestones for information systems to correct deficiencies noted during the assessment of security controls and to reduce or eliminate known vulnerabilities in the systems. (CA-5) ● Organization formally authorizes and approves the information system security assessment before full implementation. (CA-6) ● Organization monitors the security controls in the 	<p>All Low plus the following:</p>	<p>All Low & Moderate plus the following:</p>



NIST 800-53 Control Name	Security Classification		
	Low	Moderate	High
	information system on an ongoing basis. (CA-7)		
<p>Configuration Management (CM)</p> <ul style="list-style-type: none"> o Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems 	<ul style="list-style-type: none"> • A documented configuration management policy that addresses purpose scope, roles, responsibilities, and procedures, developed and distributed to all employees. (CM-1) • Organization develops, documents, and maintains current baseline configuration of system. (CM-2) • Organization develops, documents, and maintains mandatory security configuration settings of system. (CM-6) • System components are documented with relevant ownership information. (CM-8) 	<p>All Low plus the following:</p> <ul style="list-style-type: none"> • Define the mechanism by which changes to applications, network, infrastructure or other IT components are planned, communicated, authorized, documented, tested, and coordinated.(CM-3)(CM-5) • System changes are monitored and security impact analyses are performed to determine the effects of the changes. (CM-4) • Organization configures system to provide only essential capabilities based on functions, ports, protocols, and/or services. (CM-7) 	<p>All Low & Moderate plus the following:</p>
<p>Continuity Planning (CP)</p> <ul style="list-style-type: none"> o Organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations. 	<ul style="list-style-type: none"> • A documented Continuity Planning policy that addresses purpose scope, roles, responsibilities, and procedures, developed and distributed to all employees. (CP-1) • Develop, implement, and periodically review a continuity plan that addresses roles & responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure, (CP-2) • Review Continuity Plan periodically and revise the plan based on system or personnel changes. (CP-5) • Backups of user-level and system-level information stored at appropriately secured location. (CP-9) • Mechanisms with 	<p>All Low plus the following:</p> <ul style="list-style-type: none"> • Train personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training. (CP-3) • Test the contingency plan at least annually and initiate necessary corrective actions. (CP-4) • Backups of user-level and system-level information is stored at alternate storage site and is geographically separated from the primary storage site. (CP-6) • Alternate processing site identified and agreements in place. (CP-7) • Alternate site telecommunications are identified and agreements in 	<p>All Low & Moderate plus the following:</p>



NIST 800-53 Control Name	Security Classification		
	Low	Moderate	High
	procedures are in place to allow full system recovery and reconstitution to fully secure state. (CP-10)	place. (CP-8)	
<p>Identification & Authentication (IA)</p> <ul style="list-style-type: none"> o Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. 	<ul style="list-style-type: none"> ● Identification and Authentication Policy & Procedure documented, reviewed and updated (IA-1) ● Unique Authentication of a user's identity is accomplished through the use of passwords, tokens, biometrics. (IA-2) ● Management of accounts (IA-4) ● Authentication information (e.g., password or PIN) must never be disclosed to another user or shared among users. (IA-5) ● Authentication information feedback to user is obscured (e.g., asterisks in password field). (IA-6) ● Authentication systems employs methods that meet requirements of applicable laws, Exec Orders, policies, and standards. (IA-7) 	<p>All Low plus the following:</p> <ul style="list-style-type: none"> ● Identify and authenticate devices (e.g., MAC, TCP/IP, etc.) (IA-3) 	<p>All Low & Moderate plus the following:</p> <ul style="list-style-type: none"> ● Authentication of a user's identity is accomplished through the use of multifactor passwords, tokens, or biometrics. (IA-2)
<p>Incident Response (IR)</p> <ul style="list-style-type: none"> o Organizations must: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities. 	<ul style="list-style-type: none"> ● Documented and implemented Incident Response Policy & Procedure. (IR-1) ● Incident handling form for consistent, repeatable process for monitoring and reporting when dealing with incidents. (IR-4) (IR-5) (IR-6) ● Incident response resource identified to assist users in handling and reporting incidents. (IR-7) 	<p>All Low plus the following:</p> <ul style="list-style-type: none"> ● Personnel trained in their incident response roles and responsibilities at least annually. (IR-2) ● Incident response testing at least annually (IR-3) 	<p>All Low and Moderate plus the following:</p>



NIST 800-53 Control Name	Security Classification		
	Low	Moderate	High
<p>Maintenance (MA)</p> <ul style="list-style-type: none"> Organizations must: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance. 	<ul style="list-style-type: none"> A documented Maintenance policy that addresses purpose scope, roles, responsibilities, and procedures, developed and distributed to all employees. (MA-1) Agency schedules, performs, documents, and reviews records of preventative and regular maintenance. (MA-2) Agency authorizes, monitors, and controls any remote maintenance. (MA-4) Agency allows only authorized personnel to perform maintenance. (MA-5) 	<p>All Low plus the following:</p> <ul style="list-style-type: none"> Agency approves, controls, and monitors the use of maintenance tools. (MA-3) Agency obtains maintenance support in a timely manner. (MA-6) 	<p>All Low and Moderate plus the following:</p>
<p>Media Protection (MP)</p> <ul style="list-style-type: none"> Organizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse. 	<ul style="list-style-type: none"> A documented Media Protection policy that addresses purpose scope, roles, responsibilities, and procedures, developed and distributed to all employees. (MP-1) Agency ensures that only authorized users have access to information in any media, printed or digital. (MP-2) Media is sanitized and disposed of based on DTMB and Agency policies and procedures. (MP-6) 	<p>All Low plus the following:</p> <ul style="list-style-type: none"> Track, document and verify media destruction and disposal actions Paper and digital media is stored in a secure storage area and audit of access attempts and access granted is documented. (MP-4) Agency restricts the pickup, receipt, transfer, and delivery of media to authorized personnel. (MP-5) 	<p>All Low and Moderate plus the following:</p> <ul style="list-style-type: none"> Agency affixes external labels to removeable media and output indicating distribution restrictions, handling caveats and applicable security markings. (MP-3) Digital media stored at a minimum of 128-bit encryption
<p>Physical & Environmental (PE)</p> <ul style="list-style-type: none"> Organizations must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for 	<ul style="list-style-type: none"> A documented Physical and Environmental protection policy that addresses purpose scope, roles, responsibilities, and procedures, developed and distributed to all employees. (PE-1) Agency develops and keeps current a list of personnel with authorized access to facilities. (PE-2) Agency controls all physical access points to facilities. (PE-3) Agency monitors physical 	<p>All Low plus the following:</p> <ul style="list-style-type: none"> Agency controls physical access to system devices that display output. (PE-5) Agency protects power equipment from damage and destruction. (PE-9) Agency provides remote emergency shutoff. (PE-10) Agency provides short term uninterruptible power supply for systems. (PE-11) 	<p>All Low and Moderate plus the following:</p> <ul style="list-style-type: none"> Agency controls physical access to system transmission lines within facilities. (PE-4)



NIST 800-53 Control Name	Security Classification		
	Low	Moderate	High
information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.	<p>access to systems to detect and respond to security incidents. (PE-6)</p> <ul style="list-style-type: none"> • Agency controls physical access to systems by authenticating visitors before allowing access to facilities. (PE-7) • Agency maintains visitor access records for facilities. (PE-8) • Agency employs and maintains automatic emergency lighting. (PE-12) • Agency employs and maintains fire suppression and detection systems. (PE-13) • Agency employs and maintains temperature and humidity levels within the facilities. (PE-14) • Agency employs water damage and detection systems in facilities. (PE-15) • Agency controls, documents, and authorizes all delivery and removal of systems and related items entering and exiting the facilities. (PE-16) 	<ul style="list-style-type: none"> • Agency maintains appropriate security controls for telecommuting or communications from alternate worksites. (PE-17) • Agency locates systems within facilities to minimize potential damage or unauthorized access. (PE-18) 	
<p>Planning (PL)</p> <ul style="list-style-type: none"> ○ Organizations must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems. 	<ul style="list-style-type: none"> • A documented Security Plan policy that addresses purpose scope, roles, responsibilities, and procedures, developed and distributed to all employees. (PL-1) • Agency develops, implements, and regularly reviews an Security Plan. (PL-2) (PL-3) • Agency establishes an End User Computing agreement describing roles and responsibilities and expected behavior. Document is read, understood, and a signed copy is retained before authorizing access. (PL-4) 	<p>All Low plus the following:</p> <ul style="list-style-type: none"> • Agency organizes and plans security related activities, assessments, maintenance, audits,.... (PL-6) 	<p>All Low and Moderate plus the following:</p>



NIST 800-53 Control Name	Security Classification		
	Low	Moderate	High
	<ul style="list-style-type: none"> Agency conducts a privacy assessment of system. (PL-5) 		
<p>Personnel Security (PS)</p> <ul style="list-style-type: none"> Organizations must: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures. 	<ul style="list-style-type: none"> A documented Personnel Security policy that addresses purpose scope, roles, responsibilities, and procedures, developed and distributed to all employees. (PS-1) Agency heads shall designate every competitive service position within the agency at a high, moderate, or low risk level as determined by the position's potential for adverse impact to the efficiency and integrity of the service. (PS-2) Agency screens individuals requiring access before authorizing access. (PS-3) Agency conducts exit interviews upon termination of employees and terminates access to systems. (PS-4) Agency reviews system and facility access upon reassignment of personnel. (PS-5) Agency completes signed inter-agency access agreements before authorizing system access. (PS-6) Agency establishes security requirements for third party vendors and monitors their compliance. (PS-7) Agency employs a formal sanction process for security non-compliance. (PS-8) 	All Low plus the following:	All Low and Moderate plus the following:
<p>Risk Assessment (RA)</p> <p>Organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation),</p>	<ul style="list-style-type: none"> A documented Risk Assessment policy that addresses purpose scope, roles, responsibilities, and procedures, developed and distributed to all employees. (RA-1) Agency categorizes their 	All Low plus the following:	All Low and Moderate plus the following:



NIST 800-53 Control Name	Security Classification		
	Low	Moderate	High
organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.	<p>information in accordance with applicable laws, orders, and policies. (RA-2)</p> <ul style="list-style-type: none"> Agency has a risk assessment done for systems, to identify magnitude of harm from breach, use, disclosure, modification, or destruction. (RA-3) Agency updates the risk assessment or whenever majors changes are performed. (RA-4) Agency regularly scans for vulnerabilities in the system. (RA-5) 		
<p>System & Services Acquisition (SA)</p> <ul style="list-style-type: none"> Organizations must: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization. 	<ul style="list-style-type: none"> A documented Systems and Services Acquisition policy that addresses purpose scope, roles, responsibilities, and procedures, developed and distributed to all employees. (SA-1) Agency performs and allocates capital resources for Security. (SA-2) Agency manages systems using SUITE. (SA-3) Agency includes security requirements in contracts. (SA-4) Agency adequately documents systems. (SA-5) Agency complies with software usage policies. (SA-6) Agency enforces policies governing software installation by users. (SA-7) Agency requires that external providers of systems employ adequate security controls. (SA-9) 	<p>All Low plus the following:</p> <ul style="list-style-type: none"> Agency utilizes security engineering principles in system designs. (SA-8) Agency requires that system developers create security test and evaluation plans. (SA-11) 	<p>All Low and Moderate plus the following:</p> <ul style="list-style-type: none"> Agency requires that system developers create and implement configuration management plans. (SA-10)
System & Communications Protection (SC)	<ul style="list-style-type: none"> A documented Systems and Communication Protection policy that addresses purpose scope, 	<p>All Low plus the following:</p> <ul style="list-style-type: none"> Agency separates user functionality from system 	<p>All Low and Moderate plus the following:</p> <ul style="list-style-type: none"> Agency separates security



NIST 800-53 Control Name	Security Classification		
	Low	Moderate	High
<p>o Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.</p>	<p>roles, responsibilities, and procedures, developed and distributed to all employees. (SC-1)</p> <ul style="list-style-type: none"> • System protects against denial of service attacks. (SC-5) • System monitors and controls communications at all boundaries. (SC-7) • System protects the integrity and availability of public information. (SC-14) 	<p>management. (SC-2)</p> <ul style="list-style-type: none"> • System prevents unauthorized information transfer via shared systems. (SC-4) • System protects the integrity of transmitted information. (SC-8) • System protects the confidentiality of the transmitted information. (SC-9) • System terminates a network connection at end of session or inactivity timeout. (SC-10) • System prohibits remote activation of video or audio conferencing. (SC-15) • Agency utilizes public key certificates from an approved provider. (SC-17) • Agency restricts and manages mobile code technologies, ie. Java, ActiveX, Flash, ... (SC-18) • Agency restricts and manages voice over IP systems. (SC-19) • Agency restricts and manages fault tolerant Domain Name Systems (DNS). (SC-20) (SC-22) • System provides communication protection at the session level when session level protection is needed, ie. SOA, ... (SC-23) 	<p>functions from non-security functions. (SC-3)</p>
<p>System & Information Integrity (SI)</p> <p>o Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations</p>	<ul style="list-style-type: none"> • A documented Systems and Information Integrity policy that addresses purpose scope, roles, responsibilities, and procedures, developed and distributed to all employees. (SI-1) • Agency identifies, reports, and corrects information system flaws. (SI-2) • Agency implements malicious code protection and 	<p>All Low plus the following:</p> <ul style="list-style-type: none"> • Agency employs tools to monitor system attacks and unauthorized usage. (SI-4) • System has spam protection. (SI-8) • System restricts data input to authorized personnel only. (SI-9) • System checks information 	<p>All Low and Moderate plus the following:</p> <ul style="list-style-type: none"> • System verifies correct operation of security functions. (SI-6) • System detects and protects against unauthorized software and information changes. (SI-7)



NIST 800-53 Control Name	Security Classification		
	Low	Moderate	High
within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.	techniques. (SI-3) <ul style="list-style-type: none"> Agency receives system security alerts and advisories and reissues them to appropriate personnel for action. (SI-5) 	for accuracy, completeness, validity, and authenticity. (SI-10) <ul style="list-style-type: none"> System identifies and handles error without providing information that could be used for exploitation. (SI-11) Agency handles and retains outputs from systems in accordance with laws, orders, directives, and policies. (SI-12) 	
Vendor, contractor & third party	<ul style="list-style-type: none"> Adherence to DTMB and Agency security policies Security Agreements signed, maintained and reviewed yearly Remote Access must be secured through the use of VPN, authentication, and access control lists Monitor and audit contractor activities Contractor software and equipment installed and configured to operate securely; virus protection and other SOM security procedures Eliminate physical and electronic access on the same day the contract ends 	All Low plus the following: <ul style="list-style-type: none"> No self-assessment Required to implement controls that meet or exceed the State of Michigan's established security controls. Must provide the State with identified or established vendor policies or a third party independent audit (e.g.: SAS70) and/or certification of their hosting facility to verify identified or established policies are in place to protect the State's confidential and sensitive data. 	All Low and Moderate plus the following:
Infrastructure/Network	<ul style="list-style-type: none"> Virus protection mechanisms Virus protection mechanisms updated whenever new releases are available All publicly available host resources shall be placed in the DMZ All servers must pass a vulnerability scan Defined firewall rules prohibiting access and restricting traffic 	All Low plus the following: <ul style="list-style-type: none"> Hosted in trusted environment All servers must have standardized security logging enabled 	All Low and Moderate plus the following: <ul style="list-style-type: none"> Hosted in protected environment



Appendix C – Acronyms

ACH	Automated Clearing House
CAC	Customer Assistance Center
CEPAS	Centralized Electronic Payment Authorization System
CI	Configuration Item
CMDB	Configuration Management Data Base
DLN	Driver's License Number
DOB	Date of Birth
DMZ	DeMilitarized Zone
ECB	Enterprise Change Board
EFT	Electronic Funds Transfer
ESB	Enterprise Service Bus
ETRB	Executive Technical Review Board
FDGS	First Data Government Solutions
FEIN	Federal Employer Identification Number
FTP	File Transfer Protocol
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICHAT	Internet Criminal History Access Tool
IMAC	Install, Move, Add, Change
J2EE	Java 2 Enterprise Edition
JSP	Java Server Pages
LCB	Local Change Board
MEDC	Michigan Economic Development Corporation
DTMB	Michigan Department of Technology, Management and Budget
MIME	Multipurpose Internet Mail Extensions
OneStop	MIBusinessOneStop
MCS	Michigan Office of Cyber Security
PC	Personal Computer
PDF	Portable Document Format
QA	Quality Assurance
RAID	Redundant Array of Independent Disks
RFC	Request for Change
RTN	Routing Transit Number
SAN	Storage Area Network
SBTCD	Small Business Technical Data Center
SEM	Systems Engineering Methodology
SMC	Service Management Center
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SoM	State of Michigan
SRDF	Symmetrix Remote Data Facility
SSL	Secure Socket Layer
SSN	Social Security Number
SSO	Single Sign-On
SUITE	State Unified Information Technology Environment
TDE	Transparent Data Encryption
TIM/TAM	Tivoli Identity Manager/Tivoli Access Manager
TCP/IP	Transmission Control Protocol/Internet Protocol
TRB	Technical Review Board
UAT	User Acceptance Testing
XML	Extensible Markup Language



Appendix D - Laws, Regulations, DTMB and/or Agency Security Policies, Standards & Procedures

Identity Theft Protection Act (Senate Bill No. 309), Public Act 566 of 2006, amending Act 452 of 2004 - *A person shall not obtain or possess personal identifying information of another person. If a security breach is determined, notification of the breach must be communicated in reasonable time. DTMB has published breach notification procedures*

Social Security Number Privacy Act (Senate Bill No. 795, Public Act 454 of Public Acts 2004) - *A person shall not publicly display, use, or print all or more than 4 sequential digits of another persons SSN. Any use of SSN must use an encrypted manner and in accordance with the acts restrictions.*

1305 SOM Enterprise Information Technology Policy – *Generic policy which designates DTMB as the Agency to control technology and its implementation in a secure manner.*

1310.03 Active Directory Password Standard – *Requirements for length, complexity, age, and lockout for system passwords.*

1315.00 Policy for Storage of Sensitive Information on Mobile Devices & Portable Media – *All information classified as sensitive must be encrypted to be stored, transported, or written to any mobile device or media.*

1315.10 Standard for Electronic Data Encryption – *All information classified as sensitive must utilize minimum 128 bit encryption in storage (at rest) and 128 bit encryption in transmission over internal or external networks.*

1325 Information Technology Security Awareness Policy – *Designates that security awareness shall be performed and it is the responsibility of Agency Directors in conjunction with the State CISO to ensure delivery.*

1335 Information Technology Access Control Policy – *Requires systems to control Authentication, Authorization, and Accountability in order to provide for separation of duties and least privilege and documentation of system usage..*

1340 Information Technology Information Security Policy – *Due diligence must be performed in securing SOM information in respect to Confidentiality, Integrity, and Availability by all employees and trusted partners based on the classification of the information.*

1345 Information Technology Network and Infrastructure Policy – *It is the sole responsibility of DTMB to design and implement a technical infrastructure to deliver IT services for Agency business requirements.*

1350.11 Security Operational Guidelines for Servers – *General guidelines for installation, configuration, operation and maintenance of SOM servers including roles and responsibilities to minimize security risks.*

1350.20 Authorization Access to Data Sources – *Each user shall have a unique user Id.*

1350.40 Access Control Criteria for Data Sources – *Each user will be assigned a user Id based on least privilege and these Ids will be periodically reviewed and audited.*

1350.90 Secure Disposal of Installed & Removable Digital Media – *Identifies proper procedures and standards to be used to dispose of hardware which contains SOM information.*



1355 Project Management Methodology Policy – *DTMB and its client agencies are required to follow the Project Management Methodology for all IT-based initiatives.*

1360 Systems Engineering Methodology Policy – *DTMB and its client agencies are System Engineering Methodology for all new initiatives as well as enhancement and maintenance of existing systems.*

○

1390 Information Technology Continuity of Business Planning Policy – *Each Agency will ensure a Business Continuity Plan is developed and to identify and provide funding to support Disaster Recovery for essential critical business operations.*

1410.21 Procurement and Usage of State Wireless Devices – *Usage of PDAs, Blackberrys, phones, and pagers*

○

1420.00 Wireless – *Usage and deployment of wireless LANs and equipment.*



○

Appendix E - Security Analysis *(To be completed by MCS Security Liaison)*

○ The Office of Cyber Security believes that the recommended additional controls listed in the analysis below, will additionally reduce the security risk to the public, maintain the SOM's business objectives to protect the public, and are relevant and responsive to the threats identified and therefore, strongly recommend that these controls be incorporated into your system in a deliberate and timely manner.

○

The Office of Cyber Security makes no warranty that the threats/vulnerabilities or recommended controls identified in the Security Analysis are all inclusive.



Threats / Vulnerabilities	Risks if a control is not implemented	Controls Currently Implemented in the Project (See Section 5.4/6.4)	Probability (H, M, L)*	Impact (H,M,L)*	Recommended Additional Controls
Password sharing	<p>Persons could gain unauthorized access to sensitive information or system.</p> <p>Non-repudiation can no longer be achieved</p>				<p>1350.20</p> <p>Security Awareness Training Program "MOST"</p>
Carelessly stored passwords	<p>Passwords could be stolen and used for unauthorized access to sensitive data or system</p>				<p>Store passwords encrypted</p> <p>Security Awareness Training Program</p>
Lose/forget password for network access or application	<p>Denial of Service for users.</p> <p>Unable to perform maintenance resulting in persons gaining unauthorized access to sensitive data or system.</p>				<p>Password locked in secure fireproof cabinet in secure location with only individual need-to-know access.</p> <p>Two or more security questions.</p> <p>Lock out after 5 invalid attempts</p>
Password effectiveness	<p>Passwords could easily be guessed and used for unauthorized access to sensitive data or system</p>				<p>Adherence to Michigan 1 password policy.</p> <p>Security Awareness Training Program</p>
Shoulder surfing	<p>Passwords could be obtained and used for unauthorized access to sensitive data or system.</p> <p>Sensitive data could be viewed by unauthorized individuals.</p>				<p>Passwords masked when displayed.</p> <p>Security Awareness Training Program</p>
Social engineering (i.e. phone, email, web site, in person)	<p>Hacker persuades staff to provide information that would enable them to gain access to SOM resources and sensitive data</p>				<p>Security Awareness Training Program</p>



Threats / Vulnerabilities	Risks if a control is not implemented	Controls Currently Implemented in the Project (See Section 5.4/6.4)	Probability (H, M, L)*	Impact (H,M,L)*	Recommended Additional Controls
Unauthorized access to sensitive/personal/confidential information	Data is stolen resulting in identity theft. Financial Impact				Documented process for reviewing logs on a daily basis. Access Management process and procedures Security Agreements signed and maintained
Unauthorized modifications made to sensitive/personal/confidential information	Data is rendered useless. Credibility damage, legal ramifications of falsification of data.				Documented process for reviewing logs on a daily basis. Access Management process and procedures Change Management Process and Procedures Configuration management process and procedures Separation of Duties Least Privilege Security Agreements signed and maintained.
Intercepted transmission of sensitive/personal/confidential information via Internet	Data is captured when transmitted via Internet resulting in unauthorized access of sensitive/personal/confidential data.				1315.10 Encrypt data end to end during transmission Documented process for reviewing logs on a daily basis
Intercepted transmission of sensitive/personal/confidential information via LMAN	Data is captured when transmitted between web application and database resulting in unauthorized access of sensitive/personal/confidential data.				1315.10 Encryption to secure personal data at the application level Documented process for reviewing logs on a daily basis.
Use of insecure protocols for transmission of sensitive/personal/confidential data	Penetration of system resulting in compromise of data.				1315.10 Encrypt data in database



Threats / Vulnerabilities	Risks if a control is not implemented	Controls Currently Implemented in the Project (See Section 5.4/6.4)	Probability (H, M, L)*	Impact (H,M,L)*	Recommended Additional Controls
Intentional or inadvertent exposure of sensitive / personal / confidential data to the internet or other inappropriate networks	Data is altered resulting in identity theft. Violating State & Federal Laws Fraud				1315.10 Database in secured zone Data encrypted during session Encrypt data in database
Information leakage or inappropriate disclosure of sensitive/personal/confidential data	Identity Theft Fraud Legal ramifications				Security / Disclosure agreements signed and maintained. Security Awareness Training Program
Installing unauthorized software	Could install a virus that will affect system and could spread to rest of network. May be coded illegally, which could subject the agency to penalties. Vulnerable to security flaws (not kept updated) Could contain spy ware that will capture sensitive data to unauthorized users.				Software License validation Security Awareness Training Program
Loss, or theft of, sensitive/personal/confidential data on mobile devices (i.e. USB drives, laptops, PDAs, etc.)	Mobile device being compromised and sensitive data obtained by unauthorized user(s). Bad publicity, or damaging and costly litigation				1315.10
Not keeping operating systems, databases, and other software patched	Attacker could exploit vulnerabilities and take control of the system.				1350.11 Automated patch management process documented, tested, and followed.



Threats / Vulnerabilities	Risks if a control is not implemented	Controls Currently Implemented in the Project (See Section 5.4/6.4)	Probability (H, M, L)*	Impact (H,M,L)*	Recommended Additional Controls
Lack of Server Hardening	Unauthorized users may be able to obtain sensitive information about system resources, such as a list of all accounts or shared resources, registry permission settings, and make modifications to the registry				1350.11 Adherence to Michigan 1 password policy.
Elevation of Privileges or Excessive Access Rights	Users having elevated privileges could obtain root privileges to sabotage system and gain access to sensitive/personal/confidential data				1350.40
Users leaving desktops unlocked while unattended	Individual impersonating the user logged in can read all assets residing on the client machine and travel over the network to gain access to sensitive information and SOM resources				1410.88 Adherence to Michigan 1 policy.
Improper Separation of Duties	One individual having complete control of a process from start to finish leading to costly errors or fraud				1350.40
Lack of knowledge of vendor's security controls	Vendor capable of intentional/unintentional misuse of system without Agency knowledge				Documented security controls of vendor SAS70 from Vendor
Sensitive/personal/confidential data being stored without strong encryption	Unauthorized access to sensitive/personal/confidential data resulting in corruption or destruction of data				1315.10
Discarding of media that contains sensitive/personal/confidential data	Output containing sensitive/personal/confidential data improperly disposed of could lead to unauthorized access				1350.90



Threats / Vulnerabilities	Risks if a control is not implemented	Controls Currently Implemented in the Project (See Section 5.4/6.4)	Probability (H, M, L)*	Impact (H,M,L)*	Recommended Additional Controls
Lack of system/application /network logging	Malicious user gains unauthorized access to system and modifies data without being detected or misuses resources of the system/application/ network				1350.11
Easy-to-crack NetBIOS passwords being used on the network making it easy for hackers to traverse the network	Unauthorized users can launch brute force password attacks and other intrusive attacks to gain access to the network				Firewall Rules – specific ports identified Documented Incident Response process and procedure
Malicious Attacks	<p>Data could be rendered useless.</p> <p>Data could be discreetly modified or deleted</p> <p>Data could be inaccessible</p> <p>Persons could gain unauthorized access to sensitive data.</p> <p>Consume bandwidth causing systems to slow down or become unusable</p>				<p>Automated patch management process documented, tested, and followed.</p> <p>Anti-Virus</p> <p>Security Awareness Training Program</p> <p>Access Control Policy</p> <p>Quality Assurance Process</p> <p>Change Management Process</p> <p>Configuration Management Process</p> <p>Code review walk-through</p>
Buffer overflow	A malicious user can cause a breach in system security causing damage to data, modifications to data and disclosure of data				<p>Quality Assurance Process</p> <p>Code reviews performed to ensure that all parameters are validated.</p> <p>Documented Change Control Process to ensure that appropriate security is maintained over application program code files.</p>



Threats / Vulnerabilities	Risks if a control is not implemented	Controls Currently Implemented in the Project (See Section 5.4/6.4)	Probability (H, M, L)*	Impact (H,M,L)*	Recommended Additional Controls
Malicious Program Code	Malicious programs and code injected into application code in order to gain unauthorized access to sensitive data and resources				Quality Assurance Process Code reviews performed to ensure that all parameters are validated. Documented Change Control Process to ensure that appropriate security is maintained over application program code files.
Denial of Service (DoS) caused by flooding with a large number or requests	Malicious user can compromise the availability of the application and disable services. Crash or ungraceful degradation of the system				Firewall Rules – specific ports identified Utilized Intrusion Detection Software tools to continuously monitor servers. Load Balancing Documented Incident Response process and procedure
Sniffing	Data packets are captured and decoded to collect information such as passwords or infrastructure configurations				Firewall Rules – specific ports identified Utilized Intrusion Detection software tools to continuously monitor servers Documented Incident Response process and procedure
Scanning	Penetration of system enabling an intruder to access the network's unsecured ports				Firewall Rules – specific ports identified Utilized Intrusion Detection software tools to continuously monitor servers Documented Incident Response process and procedure
Spoofing	Compromise or destruction of state systems				1350.11 Firewall Rules – specific ports identified Application level security



Threats / Vulnerabilities	Risks if a control is not implemented	Controls Currently Implemented in the Project (See Section 5.4/6.4)	Probability (H, M, L)*	Impact (H,M,L)*	Recommended Additional Controls
Wireless broadcasting of sensitive/personal/confidential data in an insecure manner	An attacker uses a wireless network to launch an attack and gains unauthorized access				1420.00
Wireless access point spoofing	An attacker uses a wireless network to launch an attack and gains unauthorized access				1420.00
Wireless systems using WEP or less security	An attacker uses a wireless network to launch an attack and gains unauthorized access				1420.00
Logs stored in insecure location	Malicious user modifies logs to 'cover their tracks'				Encrypt log data Logs stored on other network devices (IE: SAN, NAS, etc.)
Logs store confidential data such as passwords	<p>Malicious user accesses logs containing confidential data and sabotages network or gains unauthorized access to sensitive data</p> <p>Legal exposure from security breaches and costly network downtime.</p>				Encrypt log data Documented process for reviewing logs on a daily basis.
Back doors to network (i.e. dial-in modems, wireless access points, etc.)	<p>Unauthorized users can log into the system undetected, execute unauthorized commands and leave the system vulnerable to other unauthorized users.</p> <p>Malicious users may use the system to access other systems and perform a coordinated DoS attack.</p>				Firewall Rules – specific rules identified Utilized Intrusion Detection Software tools to continuously monitor servers. Document Incident Response process and procedure



Threats / Vulnerabilities	Risks if a control is not implemented	Controls Currently Implemented in the Project (See Section 5.4/6.4)	Probability (H, M, L)*	Impact (H,M,L)*	Recommended Additional Controls
Network devices and servers remotely administered with insecure protocols	Direct access to SOM resources resulting in intrusion or unauthorized access to personal data.				1410.21 1410.22 1410.24
Devices being connected to the network that may be infected with viruses (e.g. contractor laptops)	Unauthorized access to sensitive/ personal/ confidential data. Port/segment blocking due to the spreading of a virus System down time, lost productivity.				DIT-0155 Foreign Device Network Connection Request
Remote users that may have infected computers, connecting to the network	Unauthorized access to sensitive/ personal/ confidential data. Port/segment blocking due to the spreading of a virus System down time, lost productivity.				DIT-0155 Foreign Device Network Connection Request
Physical damage to facility and/or equipment caused by storm, tornado, vandalism, accident, etc.	Information unavailable Loss of service to public System down time, lost productivity				Business Continuity Plan and disaster Recovery Plan documented, tested and implemented
Equipment failure/malfunction	Information unavailable System down time, lost productivity				Business Continuity Plan and disaster Recovery Plan documented, tested and implemented.

-
- * - The Probability and Impact are based on the Agency's existing controls.
-



Appendix C - Staffing Plan Matrix and Organization Chart

STAFFING PLAN MATRIX

For each role and phase, list the estimated number of persons and estimated percent dedicated to the project. Some roles may have some people fully dedicated and others not within the same phase. For example, you could have in Section 3 (Architect/Design the new System), 5 Developers at 100% and 5 Developers at 50%. You may add rows as required for other roles critical to delivery of the “development project” or “ongoing support.” Entries herein shall be consistent with information provided in Appendix D for Key Personnel as to their percentage allocation to the project.

Though the bidder may add rows, they shall not add or remove columns.

Phase And Role	S1 Initiation and Planning	S2 Hosting	S3 Day-to-day Maintenance	S4 Technical Support	S5 Help Desk Support
Project Manger					
Lead Developer					
<i>List all other non-key positions...</i>					



Organization Chart

The bidder shall provide an organizational chart indicating lines of authority for all personnel involved in performance of this Contract. 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.

**Appendix D - Personnel Resume Template**

Resumes are required for key persons. They are not representative resumes but specific individuals committed to this project. No less than 2 references are required for each of the Key Personnel outlined below:

RESUME 1 – PROJECT MANAGER
RESUME 2 – LEAD DEVELOPER

References are not required for other roles, but may be provided for the following 2 required Key Personnel Resumes.

Do not modify the form; unless notes indicate this is allowed.



RESUME 1

Proposed Resource Name	
Proposed Role	PROJECT MANAGER
Associated With: Indicate if Prime or Subcontractor If Sub, provide Company Name	
Key Personnel: Yes or No	YES
Dedicated to Project? Yes or No	

Approximate Percentage of Resources Time Allocated to Project by State (For example if this resource is split 50/50 during a specific stage between this project and another they should indicated 50% for the stage in the table below)						
S1 Initiation and Planning	S2 Requirements Definition	S3 Architect/Design the new System	S4 Install, Configure, Modify Solution	S5 Training / User Acceptance Testing	S6 Implementation	Post Implementation Operations

Verification of Necessary Skills			
Required Skill	Met (Y or N)	Client Name and Project Name	Start & End Month/Year MM/YY-MM/YY
7+ years of recent IT project management experience managing large scale application development and implementation projects.			
3+ years of experience working on projects involving interfacing with the State of Michigan or that of a similar state-level system.			
Experience in structured development process using a formal Project Management Methodology and formal Development Methodology.			
Certification as a Project Management Professional (PMP) is a plus			

Chronological resume using the table below

Start Date		End Date	
Client Name			
Project Name			
Employer (at time)			
Project Role/Tile			
Brief Description of Duties			

Note: Repeat this table as necessary



Education

University or College Name	City, State/Province Degree, Program
University or College Name	City, State/Province Degree, Program

Note: Add rows if necessary

Relevant Professional or Technical Training

Course Name Topic Date (MM/YY)
Course Name Topic Date (MM/YY)

Note: Add rows if necessary

Relevant Certifications/Affiliations

Name Topic/Description Date Completed
Name Topic/Description Date Completed

Note: Add rows if necessary

References

Name of Client Company and Department
Name of Your Employer
Start and End Date (MM/YY- MM/YY)
Brief description of Project
Relevancy to this Project
Contact Name
Contact Phone Number
Contact Role on the Project

Note 1: References should be for performing the same role as proposed for this project

Note 2: Relevancy factors include but not limited to: similar dollar value, similar headcount under your control, similar duration, similar effort (modification of COTS or custom development), and/or similar client

Note 3: Repeat table no less than 2 references



RESUME 2

RESUME 1

Proposed Resource Name	Steven Clark, PhD
Proposed Role	PROJECT MANAGER/SYSTEM ARCHITECT
Associated With: Indicate if Prime or Subcontractor If Sub, provide Company Name	ORA
Key Personnel: Yes or No	Yes
Dedicated to Project? Yes or No	Yes

Approximate Percentage of Resources Time Allocated to Project by State

(For example if this resource is split 50/50 during a specific stage between this project and another they should indicated 50% for the stage in the table below)

S1 Initiation and Planning	S2 Requirements Definition	S3 Architect/Design the new System	S4 Install, Configure, Modify Solution	S5 Training / User Acceptance Testing	S6 Implementation	Post Implementation Operations
10%	10%	50%	0%	10%	10%	10%

Verification of Necessary Skills

Required Skill	Met (Y or N)	Client Name and Project Name	Start & End Month/Year MM/YY-MM/YY
7+ years of recent IT project management experience managing large scale application development and implementation projects.	Y	MichCon Gas Planner IT CDC SUIDI National Registry USDOJ NamUs CTE Navigator (R&D) NAME I&A Program	2000-2006 2004-2008 2007-2012 2007-2012 2008-2012
3+ years of experience working on projects involving interfacing with the State of Michigan or that of a similar state-level system.	Y	MDILog <>MI State Registrar MDILog<>Michigan Gift of Life NamUsMP<>NamUsUP	2010-2012 2010-2012 2007-2010
Experience in structured development process using a formal Project Management Methodology and formal Development Methodology.	Y	All above	1987-Present
Certification as a Project Management Professional (PMP) is a plus	N	N/A	



Chronological resume using the table below

Start Date	2010	End Date	Present
Client Name	University of North Texas (UNT)		
Project Name	National Missing and Unidentified Persons System (NamUs)		
Employer (at time)	National Institute of Justice (NIJ) US Department of Justice		
Project Role/Tile	National System Administrator/System Design		
Brief Description of Duties	Direct improvements to NamUs-MP and NamUs-UP Systems		

Start Date	2007	End Date	2010
Client Name	National Forensic Science and Technology Center (NFSTC)		
Project Name	National Missing and Unidentified Persons System (NamUs)		
Employer (at time)	National Institute of Justice (NIJ) US Department of Justice		
Project Role/Tile	Project Director/System Administrator		
Brief Description of Duties	Direct the development and National deployment and use of the NamUs system.		

Start Date	2006	End Date	2010
Client Name	U.S. Department of Justice		
Project Name	National NamUs Training Academies		
Employer (at time)	National Institute of Justice (NIJ)		
Project Role/Tile	Project Director		
Brief Description of Duties	Design curriculum and materials for five national training academies involving: Law Enforcement, Medical Examiners, Death Investigators, Forensic Specialists, and Victim Advocates.		

Start Date	2004	End Date	2008
Client Name	Centers for Disease Control and Prevention (CDC)		
Project Name	Sudden Infant Death Investigation System (SUIDI)		
Employer (at time)	Center for Maternal Health		
Project Role/Tile	Project Director		
Brief Description of Duties	Design curriculum and materials for five national training academies involving: Law Enforcement, Medical Examiners, Death Investigators, University Professors, and Victims.		

Note: Repeat this table as necessary

Education	
University or College Name City, State/Province Degree, Program	Central Michigan University Mt. Pleasant, MI BAA - Industrial Supervision and Management
University or College Name City, State/Province Degree, Program	Eastern Michigan University Ypsilanti, MI Secondary Education MA - Industrial Technology
University or College Name City, State/Province Degree, Program	Michigan State University East Lansing, MI PhD - Curriculum and Instruction Counseling and Educational Psychology



Relevant Certifications/Affiliations	
Name Topic/Description Date Completed	American Psychological Association (Member)
Name Topic/Description Date Completed	

References	
Name of Client Company and Department	Ferris State University College of Education
Name of Your Employer	FSU
Start and End Date (MM/YY-MM/YY)	07/06-Present
Brief description of Project	Develop web-based state-wide CTE curriculum standards validation system for administrators, teachers, employers. This system allows Michigan's CTE community easy access to state-approved program standards and local program data.
Relevancy to this Project	Web system upgrades, management and administration.
Contact Name	Katherine Manley, EdD
Contact Phone Number	Project Director
Contact Role on the Project	231-591-2726

References	
Name of Client Company and Department	National Association of Medical Examiners (NAME)
Name of Your Employer	NAME
Start and End Date (MM/YY-MM/YY)	1/00-Present
Brief description of Project	Administer and maintain three national data systems for the Association (Inspection and Accreditation Online System, National Death Registry, Pediatric Death Registry).
Relevancy to this Project	Web system design, upgrades, management and administration.
Contact Name	Randy Hanzlick, MD
Contact Phone Number	404-730-4407
Contact Role on the Project	Data Committee Chairperson

References	
Name of Client Company and Department	University of Michigan Department of Forensic Pathology
Name of Your Employer	Washtenaw County Department of Public Health
Start and End Date (MM/YY-MM/YY)	1/10-Present
Brief description of Project	Administer and maintain the medical examiner case management system (MDILog.com).
Relevancy to this Project	Web system upgrades, management and administration.
Contact Name	Jeffrey Jentzen, MD, PhD
Contact Phone Number	Clinical Professor/Medical Examiner
Contact Role on the Project	734-936-7045



References	
Name of Client Company and Department	Center for Human Identification
Name of Your Employer	University of North Texas (UNT)
Start and End Date (MM/YY- MM/YY)	10/10-Present
Brief description of Project	Administer and maintain three national data systems for the NIJ/USDOJ (NamUs-MP, NamUs-UP and NamUs-UC).
Relevancy to this Project	Web system upgrades, management and administration.
Contact Name	Arthur Eisenberg (UNT)
Contact Phone Number	Project Director
Contact Role on the Project	817-735-0555

References	
Name of Client Company and Department	National Forensic Science and Technology Center (NFSTC)
Name of Your Employer	National Institute of Justice (NIJ) US Department of Justice (USDOJ)
Start and End Date (MM/YY- MM/YY)	10/07-12/11
Brief description of Project	National administration of web-based registry for unidentified dead and missing persons data system for matching UID cases with missing persons cases nationally.
Relevancy to this Project	Web-based data system design, management and deployment.
Contact Name	Mike O'Berry
Contact Phone Number	727-549-6067
Contact Role on the Project	Program Manager

References	
Name of Client Company and Department	Department of Health and Human Services Maternal and Infant Health Branch
Name of Your Employer	Centers for Disease Control and Prevention (CDC)
Start and End Date (MM/YY- MM/YY)	10/04-12/08
Brief description of Project	Develop national training curriculum and create and run five national training academies for investigators of infant deaths in the US. Create a "beta" national web-based infant death registry data system for surveillance of infant deaths nationally.
Relevancy to this Project	Curriculum development, standards, data system design, management and deployment.
Contact Name	Terry Davis, EdD
Contact Phone Number	770-488-3940
Contact Role on the Project	Program Manager



RESUME 2

Proposed Resource Name	Kavan Story
Proposed Role	LEAD DEVELOPER
Associated With: Indicate if Prime or Subcontractor If Sub, provide Company Name	Occupational Research and Assessment, Inc. (ORA)
Key Personnel: Yes or No	Yes
Dedicated to Project? Yes or No	Yes

Approximate Percentage of Resources Time Allocated to Project by State (For example if this resource is split 50/50 during a specific stage between this project and another they should indicated 50% for the stage in the table below)						
S1 Initiation and Planning	S2 Requirement s Definition	S3 Architect/Desi gn the new System	S4 Install, Configur e, Modify Solution	S5 Training / User Acceptance Testing	S6 Implementatio n	Post Implementati on Operations
10%	10%	20%	30%	10%	10%	10%

Verification of Necessary Skills			
Required Skill	Met (Y or N)	Client Name and Project Name	Start & End Month/Year MM/YY-MM/YY
5+ years' experience working on projects involving interfacing with a hosting environment of complexity to a similar system.	Y	CDC SUIDI National Registry USDOJ NamUs CTE Navigator (R&D)	2005-2008 2007-2012 2007-2012
2+ years of experience in defining the architecture for a widely distributed real time reservation system or equivalent system.	Y	MDILog <> MI State Registrar MDILog <> Michigan Gift of Life NamUs MP <> NamUs UP SOMDI/MOCAC	2010-2012 2010-2012 2007-2010 2010-2012

Chronological resume using the table below

Start Date	2007	End Date	Present
Client Name	FSU		
Project Name	MCCTE Navigator		
Employer (at time)	Occupational Research and Assessment		
Project Role/Title	Developer/Programmer		
Brief Description of Duties	Design and development of the current system, enhancements, and bug fixes; manage server environment; and provide technical support.		

Start Date	2005	End Date	Present
Client Name	NFSC - NFSTC - NIJ (USDOJ)		



Project Name	National Missing and Unidentified Persons System (NamUs)
Employer (at time)	Occupational Research and Assessment
Project Role/Title	Developer/Programmer
Brief Description of Duties	Design and development of a Missing Persons Database (MP), Unidentified Persons Database (UP), and Unclaimed Persons Database (UC) as three separate systems that securely transfer data between each other. Program enhancements, fix bugs, and provide technical support.

Start Date	2005	End Date	Present
Client Name	NAME		
Project Name	National Association of Medical Examiners Data Systems		
Employer (at time)	Occupational Research and Assessment		
Project Role/Title	Developer/Programmer		
Brief Description of Duties	Design and development of multiple data collection systems: <ul style="list-style-type: none"> • Inspection & Accreditation System – Data system to collect information about a medical examiner’s office and keep track of accredited medical examiner offices. • NAME Death Registry – Collects information about specific medical examiner cases and allows members of NAME to search the cases. • Pediatric Toxicology – Collects toxicology information on pediatric cases and stores information in searchable database. 		

Start Date	2005	End Date	Present
Client Name	ORA		
Project Name	TaskScope – Learning Management System		
Employer (at time)	Occupational Research and Assessment		
Project Role/Title	Developer/Programmer		
Brief Description of Duties	Development and programming of a data system to manage members, deploy standardized tests, and track testing progress. Used by multiple organizations. Also maintain the server environment.		

Start Date	2005	End Date	Present
Client Name	Various User Jurisdictions (US Counties)		
Project Name	MDILog		
Employer (at time)	Occupational Research and Assessment		
Project Role/Title	Developer/Programmer		
Brief Description of Duties	Developed and maintain a case management system for Medical Examiner/Coroner offices. Implemented data exchanges with: Michigan Electronic Death Reporting System, Gift of Life Michigan, and NamUs UP. Developed an iPhone App to transfer data from scene to system over cell phone network. Maintain server environment.		

Start Date	2009	End Date	Present
Client Name	Kentucky Department of Public Health		
Project Name	Kentucky Mortality Data Management System (MDMS-KY)		
Employer (at time)	Occupational Research and Assessment		
Project Role/Title	Developer/Programmer		
Brief Description of Duties	Developed a statewide mass fatality data management system for Kentucky. Manage server environment.		

Start Date	2005	End Date	Present
Client Name	Various Projects (see description below)		



Project Name	Online Delphi Data Collection System
Employer (at time)	Occupational Research and Assessment
Project Role/Title	Developer/Programmer
Brief Description of Duties	Developed an online data system to use the Delphi process for surveying subject matter experts about a specific topic and generate reports. Used for a projects with Kentucky Community and Technical College System, Michigan Center for Career and Technical Education, and the International Association of Coroners & Medical Examiners.

Note: Repeat this table as necessary

Education

University or College Name	Ferris State University (BS)
City, State/Province	Big Rapids, MI
Degree, Program	Bachelor of Science, Applied Mathematics / Computer Science

Note: Add rows if necessary

Relevant Professional or Technical Training

Course Name	Object Oriented Programming
Topic	Computer Science
Date (MM/YY)	08/03 – 12/03
Course Name	Scientific Programming with Fortran
Topic	Computer Science
Date (MM/YY)	01/04 – 05/04
Course Name	Data Structures & Algorithms
Topic	Computer Science
Date (MM/YY)	01/05 – 05/05
Course Name	Computational Number Theory and Cryptology
Topic	Computer Science
Date (MM/YY)	01/05 – 05/05
Course Name	Fundamentals of Hardware & Operating System
Topic	Computer Information Systems
Date (MM/YY)	08/05 – 12/05
Course Name	Database Design and Implementation
Topic	Computer Information Systems
Date (MM/YY)	01/06 – 05/06
Course Name	Computer Simulation
Topic	Computer Science
Date (MM/YY)	08/06 – 12/06

Note: Add rows if necessary

Relevant Certifications/Affiliations

Name	
Topic/Description	
Date Completed	
Name	
Topic/Description	
Date Completed	

Note: Add rows if necessary

References

Name of Client	Randy Hanzlick, MD
----------------	--------------------



Company and Department	NAME
Name of Your Employer	ORA
Start and End Date (MM/YY-MM/YY)	2005-Present
Brief description of Project	Various (see above)
Relevancy to this Project	
Contact Name	Randy Hanzlick, MD
Contact Phone Number	
Contact Role on the Project	Project Director

References	
Name of Client	Katherine Manley, EdD
Company and Department	FSU
Name of Your Employer	ORA
Start and End Date (MM/YY-MM/YY)	2005-Present
Brief description of Project	MCCTE Navigator
Relevancy to this Project	
Contact Name	Katherine Manley, EdD
Contact Phone Number	231-591-2726
Contact Role on the Project	Project Director

References	
Name of Client	Emily Craig, PhD
Company and Department	UNT Health Science Center
Name of Your Employer	ORA
Start and End Date (MM/YY-MM/YY)	2008-Present
Brief description of Project	Various projects including MDMS-KY and NamUs (see above)
Relevancy to this Project	
Contact Name	Emily Craig, PhD
Contact Phone Number	859-396-3689
Contact Role on the Project	Project Director (MDMS-KY) Regional System Administrator and Forensic Anthropologist (NamUs)

References	
Name of Client	Jeffery Jentzen, MD, PhD
Company and Department	University of Michigan
Name of Your Employer	ORA
Start and End Date (MM/YY-MM/YY)	2009-Present
Brief description of Project	MDILog – Case management system for Medical Examiner Offices.
Relevancy to this Project	
Contact Name	Jeffery Jentzen, MD
Contact Phone Number	734-615-7173
Contact Role on the Project	Chief Medical Examiner

Note 1: References should be for performing the same role as proposed for this project

Note 2: Relevancy factors include but not limited to: similar dollar value, similar headcount under your control, similar duration, similar effort (modification of COTS or custom development), and/or similar client

Note 3: Repeat table no less than 2 references



Appendix E – Preliminary Project Plan

DELETED/NA



Appendix F – Federal and State Assurances and Certifications

Governing Law

The grant shall in all respects be governed by, and construed in accordance with, the laws of the state of Michigan. By signing this agreement, Grantee consents to personal jurisdiction in the state of Michigan. Any dispute arising herein shall be resolved in the state of Michigan.

Applicable Statutes

The following statutes, rules, and laws are applicable to the performance of this grant; some statutes are reflected in the clauses of this Grant Agreement. This list is NOT exhaustive.

MI Uniform Commercial Code (MIUCC) MCL 440. (All sections unless otherwise altered by agreement)

MI OSHA MCL §§ 408.1001 – 408.1094

Freedom of Information Act (FIOA) MCL §§ 15.231, et seq.

Natural Resources and Environmental Protection Act MCL §§ 324.101, et seq.

MI Consumer Protection Act MCL §§ 445.901 – 445.922

Laws relating to wages, payments of wages, and fringe benefits on state projects MCL §§ 408.551 – 408.558, 408.471 – 408.490, 1965 PA 390.

Department of Civil Service Rules and regulations

Elliot Larsen Civil Rights Act MCL §§ 37.2201, et seq.

Persons with disabilities Civil Rights Act MCL §§ 37.1101, et seq.

MCL §§ 423.321, et seq.

MCL § 18.1264 (law regarding debarment)

Davis-Bacon Act (DBA) 40 USCU § 276(a), et seq.

Contract Work Hours and Safety Standards Act (CWHSSA) 40 USCS § 327, et seq.

Business Opportunity Act for Persons with Disabilities MCL §§ 450.791 – 450.795

Rules and regulations of the Environmental Protection Agency

Internal Revenue Code

Rules and regulations of the Equal Employment Opportunity Commission (EEOC)

The Civil Rights Act of 1964, USCS Chapter 42

Title VII, 42 USCS §§ 2000e et seq.

The Americans with Disabilities Act (ADA), 42 USCS §§ 12101 et seq.

The Age Discrimination in Employment Act of 1967 (ADEA), 29 USCS §§ 621, 623 et seq.

The Old Workers Benefit and Protection Act of 1990 (OWBPA), 29 USCS §§ 626, et seq.

The Family Medical Leave Act of 1993 (FMLA), 29 USC §§ 651 et seq.

The Fair Labor Standards Act (FLSA), 29 USC §§ 201 et seq.

Pollution Prevention Act of 1990 (PPA) 42 U.S.C. §13106

Sherman Act, 15 U.S.C.S. § 1 et seq.

Robinson-Patman Act, 15 U.S.C.S. § 13 et seq.

Clayton Act, 15 U.S.C.S. § 14 et seq.

Certification Regarding Lobbying For Grants And Cooperative Agreements

No federal, appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of a federal agency, a Member of Congress, an officer or employee of Congress, or an employee of a member of Congress in connection with the making of any federal grant, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any federal grant or cooperative agreement. If any funds other than federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a member of Congress, an officer or employee of Congress, or an employee of a member of Congress in connection with this federal grant or cooperative agreement, the undersigned shall complete and submit Standard Form – LL **Disclosure Form to Report Lobbying**, in accordance with its instructions. The undersigned shall require that the language of this certification be included in the awards documents for all subawards at all tiers (including subgrants, contracts under grants



and cooperative agreements, and subcontracts) and that all subrecipients shall certify and disclose accordingly.

Certification Regarding Debarment, Suspension, Ineligibility, and Voluntary Exclusion – Lower Tier Covered Transactions

The prospective lower tier participant certifies, by submission of this proposal, that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participating in this transaction by any federal department or agency. Where the prospective lower tier participant is unable to certify to any of the statements in this certification, such prospective participant shall attach an explanation to this proposal.

Assurance With Section 511 Of The U. S. Department Of Education Appropriation Act of 1990

When issuing statements, press releases, requests for proposals, solicitations, and other documents describing this project, the recipient shall state clearly: 1) the dollar amount of federal funds for the project, 2) the percentage of the total cost of the project that will be financed with federal funds, and 3) the percentage and dollar amount of the total cost of the project that will be financed by nongovernmental sources.

Assurance Concerning Materials Developed with Funds Awarded Under This Grant

The grantee assures that the following statement will be included on any publication or project materials developed with funds awarded under this program, including reports, films, brochures, and flyers: "These materials were developed under a grant awarded by the Michigan Department of Education".

Certification Regarding Nondiscrimination Under Federally and State Assisted Programs

The applicant hereby agrees that it will comply with all federal and Michigan laws and regulations prohibiting discrimination and, in accordance therewith, no person, on the basis of race, color, religion, national origin or ancestry, age, sex, marital status, or handicap, shall be discriminated against, excluded from participation in, denied the benefits of, or otherwise be subjected to discrimination in any program or activity for which it is responsible or for which it receives financial assistance from the U.S. Department of Education or the Michigan Department of Education.

Recipients of federal funds are required to issue notice of nondiscrimination to applicants, participants, beneficiaries and others in a continuous manner. Regulations require that the name or title, address, and telephone number of the employee designated to coordinate compliance efforts be included. A statement of nondiscrimination must be included in all bulletins, announcements, publications, catalogs, applications, agreements, and recruitment materials. Additional forms of notification (publication in newspapers, cable public access, web sites, etc.) may also be used.

(See technical assistance guide for Civil Rights Compliance in Career and Technical Education, Michigan Department of Education, Revised April 2011.)

Certification Regarding Boy Scouts of America Equal Access Act, 20 U.S.C. 7905, 34 CFR Part 108

A state or subgrantee that is a covered entity as defined in Sec. 108.3 of this title shall comply with the non-discrimination requirements of the Boy Scouts of America Equal Access Act, 20 U.S.C. 7905, 34 CFR part 108.

Participation of Nonpublic Schools

The applicant assures that private nonprofit schools have been invited to participate in planning and implementing the activities of this application.

Assurance Regarding Access to Records and Financial Statements

The applicant hereby assures that it will provide the pass-through entity, i.e., the Michigan Department of Education, and auditors with access to the records and financial statements as necessary for the pass-through entity to comply with Section 400 (d) (4) of the U.S. Department of Education Compliance Supplement for A-133.

**Assurance Regarding Compliance with Grant Program Requirements**

The grantee agrees to comply with all applicable requirements of all state statutes, federal laws, executive orders, regulations, policies, and award conditions governing this program. The grantee understands and agrees that if it materially fails to comply with the terms and conditions of the grant award, the Michigan Department of Education may withhold funds otherwise due to the grantee from this grant program, any other federal grant programs or the State School Aid Act of 1979, as amended, until the grantee comes into compliance or the matter has been adjudicated and the amount disallowed has been recaptured (forfeited). The department may withhold up to 100% of any payment based on a monitoring finding, audit finding or pending final report.

Certification Regarding Title II Of The Americans With Disabilities Act (A.D.A.), P. L. 101-336, State and Local Government Services

The Americans with Disabilities Act (ADA) provides comprehensive civil rights protections for individuals with disabilities. Title II of the ADA covers programs, activities, and services of public entities. Title II requires that, "No qualified individual with a disability shall, by reason of such disability be excluded from participation in or be denied the benefits of the services, programs, or activities of a public entity, or be subjected to discrimination by such entity". In accordance with Title II ADA provisions, the applicant has conducted a review of its employment and program/service delivery processes and has developed solutions to correcting barriers identified in the review.

Certification Regarding Title III of the Americans with Disabilities Act (A.D.A.), P.L. 101-336, Public Accommodations And Commercial Facilities

The Americans with Disabilities Act (ADA) provides comprehensive civil rights protections for individuals with disabilities. Title III of the ADA covers public accommodations (private entities that affect commerce, such as museums, libraries, private schools, and day care centers) and only addresses existing facilities and readily achievable barrier removal. In accordance with Title III provisions, the applicant has taken the necessary action to ensure that individuals with a disability are provided full and equal access to the goods, services, facilities, privileges, advantages, or accommodations offered by the applicant. In addition, a Title III entity, upon receiving a grant from the Michigan Department of Education, is required to meet the higher standards (i.e., program accessibility standards) as set forth in Title III of the ADA for the program or service for which they receive a grant.

Certification Regarding Gun-Free Schools - Federal Programs (Section 4141, Part A, Title Iv, NCLB)

The applicant assures that it has, in effect, a policy requiring the expulsion from school for a period of not less than one year of any student who is determined to have brought a weapon to school under the jurisdiction of the agency except such policy may allow the chief administering officer of the agency to modify such expulsion requirements for student on a case-by-case basis. (The term "weapon" means a firearm as such term is defined in Section 92` of Title 18, United States Code.)

The district has adopted, or is in the process of adopting, a policy requiring referral to the criminal or juvenile justice system of any student who brings a firearm or weapon to a school served by the agency.

Audit Requirements

All grant recipients who spend \$500,000 or more in federal funds from one or more sources are required to have an audit performed in compliance with the Single Audit Act (*effective July 1, 2003*).

Further, the applicant hereby assures that it will direct its auditors to provide the Michigan Department of Education access to their audit work papers to upon the request of the Michigan Department of Education.

Assurance Against Trafficking in Persons

The applicant assures that it adopts the requirements in the Code of Federal Regulations at 2 CFR 175 as a condition for this grant. You, as a subrecipient under this award, and your employees may not:

- i. Engage in severe forms of trafficking in persons during the period of time that the award is in effect.
- ii. Procure a commercial sex act during the period of time that the award is in effect.
- iii. Use forced labor in the performance of the award or subawards under the award.



Under this condition, the federal awarding agency may terminate this grant without penalty for any violation of these prohibitions by the grantee, its employees, or its subrecipients.

Assurance Regarding the Prohibition of Text Messaging and Emailing While Driving During Official Federal Grant Business

The applicant assures that it prohibits text messaging and emailing while driving during official grant business. Federal grant recipients, subrecipients, and their grant personnel are prohibited from text messaging while driving a government owned vehicle, or while driving their own privately owned vehicle during official grant business, or from using government supplied electronic equipment to text message or email when driving.

Recipients must comply with these conditions under Executive Order 13513, "Federal Leadership on 'Reducing Text Messaging While Driving'", October 1, 2009.

Certification Regarding Universal Identifier Requirements

The applicant or grant recipient certifies it will meet the requirement for supplying a Data Universal Numbering System (DUNS) number. As a condition of a subrecipient of a federal grant award, you must supply a DUNS number to MDE. No entity may receive a federal subaward without a DUNS number. MDE will not make a subaward to an entity unless that entity has provided its DUNS number.

Assurance Regarding Reporting Subaward Data For Subrecipients

The Federal Funding Accountability and Transparency Act (FFATA) is designed to increase transparency and improve the public's access to federal government information. To this end, FFATA requires that subaward data be reported for all new federal grants funded at \$25,000 or more with an award date on or after October 1, 2010.

An applicant or subrecipient assures that it will timely report data as needed to MDE for the purposes of federal reports for any subaward on a grant awarded by the U. S. Department of Education will be reported for each action or subaward that obligates \$25,000 or more in federal funds that does not include Recovery funds (as defined in section 1512(a)(2) of the American Recovery and Reinvestment Act of 2009, Pub. L. 111-5).

Assurance Concerning Non-Construction Programs

The applicant assures compliance with the following regulations regarding non-construction programs:

1. Has the legal authority to apply for federal assistance, and the institutional, managerial, and financial capability (including funds sufficient to pay the non-federal share of project cost) to ensure proper planning, management, and completion of the project described in this application.
2. Will give the awarding agency, the Comptroller General of the United States, and if appropriate, the state, through any authorized representative, access to and the right to examine all records, books, papers, or documents related to the award, and will establish a proper accounting system in accordance with generally accepted accounting standards or agency directives.
3. Will establish safeguards to prohibit employees from using their positions for a purpose that constitutes or presents the appearance of personal or organizational conflict of interest, or personal gain.
4. Will initiate and complete the work within the applicable time frame after receipt of approval from the awarding agency.
5. Will comply, as applicable, with the provisions of the Hatch Act (5U.S.C. 1501-1508 and 7324-7328) which limit the political activities of employees whose principal employment activities are funded in whole or in part with federal funds.

Certification Regarding Drug-Free Workplace Requirements

The applicant agrees to comply with the Drug-Free Workplace Act of 1988, and implemented at 34 CFR Part 85, Subpart F, for grantees, as defined at 34 CFR Part 85.605 and 85.610. Grantee certifies and agrees that it will provide a drug-free workplace by:



1. Publishing and providing to all of its employees a statement notifying employees that the unlawful manufacture, distribution, dispensing, possession, or use of a controlled substance is prohibited in the vendor's workplace and specifying the actions that will be taken against employees for violations of such prohibition.
2. Establishing a drug-free awareness program to inform employees about: 1) the dangers of drug abuse in the workplace, 2) the vendor's policy of maintaining a drug-free workplace, 3) any available drug counseling, rehabilitation, and employee assistance programs, and 4) the penalties that may be imposed upon an employee for drug abuse violations occurring in the workplace.
3. Notifying all employees in the statement required by subparagraph (1) above that as a condition of continued employment the employee will: 1) abide by the terms of the statement, and 2) notify the employer of any criminal drug statute conviction for a violation occurring in the workplace no later than five days after such conviction.
4. Notifying the granting state agency within 15 days after receiving notice from an employee under subdivision (C)(2) above, or otherwise receiving actual notice of such conviction.
5. Within 30 days after receiving notice under subdivision (C)(2), imposing the proper sanctions as communicated to the employee through the statement required by subparagraph (1).
6. Making a good-faith effort to maintain a drug-free workplace through the implementation of sub paragraphs (1) through (5) above.

Disclosure of Federal Funding in Public Announcements (Public Law 111-8, the Omnibus Appropriations Act, 2009, U.S. Department of Education Appropriation Act)

When issuing statements, press releases, requests for proposals, bid solicitations, and other documents describing projects or programs funded in whole or in part with federal money, the recipient shall clearly state:

1. The percentage of the total cost of the program or project that will be financed with federal money.
2. The dollar amount of federal funds for the project or program.
3. Percentage and dollar amount of the total cost of the project or program that will be financed by nongovernmental sources.

Supplement, Not Supplant

Federal funds received under this Act shall be used to supplement, and not supplant, state or local funds for any activity carried out in delivery of this program.



Assurances/Certifications Signature Page

I/we certify that all federal/state assurances and certifications contained in this continuation proposal will be met during the grant period.

I/we further certify that the information contained in this proposal is accurate, true, and will be supported with documentation for monitoring purposes.

I/we agree with the guidelines related to this program. Any deviations from the approved activities or expenditures will have prior approval from the Office of Career and Technical Education.

Name of Applicant:			
Address:			
Telephone Number:		Fax Number:	
Email Address			
Taxpayer Identification Number (TIN) (for payment purposes):			
Signature of Applicant's Authorized Representative:			
Date:			



Appendix G - Cost Tables

Please refer to Article 1, Section 1.601 Compensation and Payment

Table 1a: Data Storage Reconfiguration: Contractor will reconfigure the NAVIGATOR System so that Data shall not to reside outside of the Continental United States, inclusive of configuration, policy development, testing, documentation and implementation. To be complete by 12.14.2012.

Contractor Resources	Estimated Hours	Not-to-Exceed Hourly Rate	Cost
Steven Clark	8	\$50	\$400
Kavan Story			
Table 1b Total:		Not-to-Exceed Cost:	\$400

Table 1b: Contractor will collaborate with DTMB IT Staff and DTMB IT Staff will assist Contractor to complete the EA Solution Assessment and DIT-0170 IT Security Assessment Documents (Appendix B in the RFP), not to exceed 40 hours of labor

Contractor Resources	Estimated Hours	Not-to-Exceed Hourly Rate	Cost
Steven Clark		\$50	\$2000
Kavan Story			
Table 1b Total:	40		\$2000

Table 2: HOSTING AND MAINTENANCE

	Monthly Fee	Maximum Number of Months starting 1/1/2013 – 10/31/2015	Total
Hosting, per Section 1.101 A.2	\$480	34	\$16,320
Maintenance, per Section 1.101 A.3, including Help Desk Support	\$4,314	34	\$146,675
Table 2 Total:			\$162,995

TABLE 3: RESERVED BANK OF HOURS FOR SUPPLEMENTAL SERVICES, PER SECTION 1.104 A.4

Bidder Staffing Category	Not-to Exceed Hourly Rate	Estimated Hours (3 year total)	Extended Price
Steven Clark	\$50	10	\$500
Jennifer Proctor	\$40	40	\$1600
Steven Clark	\$50	12	\$600
Kavan Story	\$35	20	\$700
Jordan Hendricks	\$30	10	\$300
Jason Metz	\$20	15	\$300
List all others...			
Table 3: Total	N/A	80	\$4000

Notes:

- Hourly rates provided in Table 3 are not-to-exceed rates for the duration of the contract. "Estimated Hours" and "Extended Price" are non-binding. 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.
- The State reserves the right to add money for additional future enhancements as needed.

Contract Total Value on Award	\$169,395.00
--------------------------------------	--------------