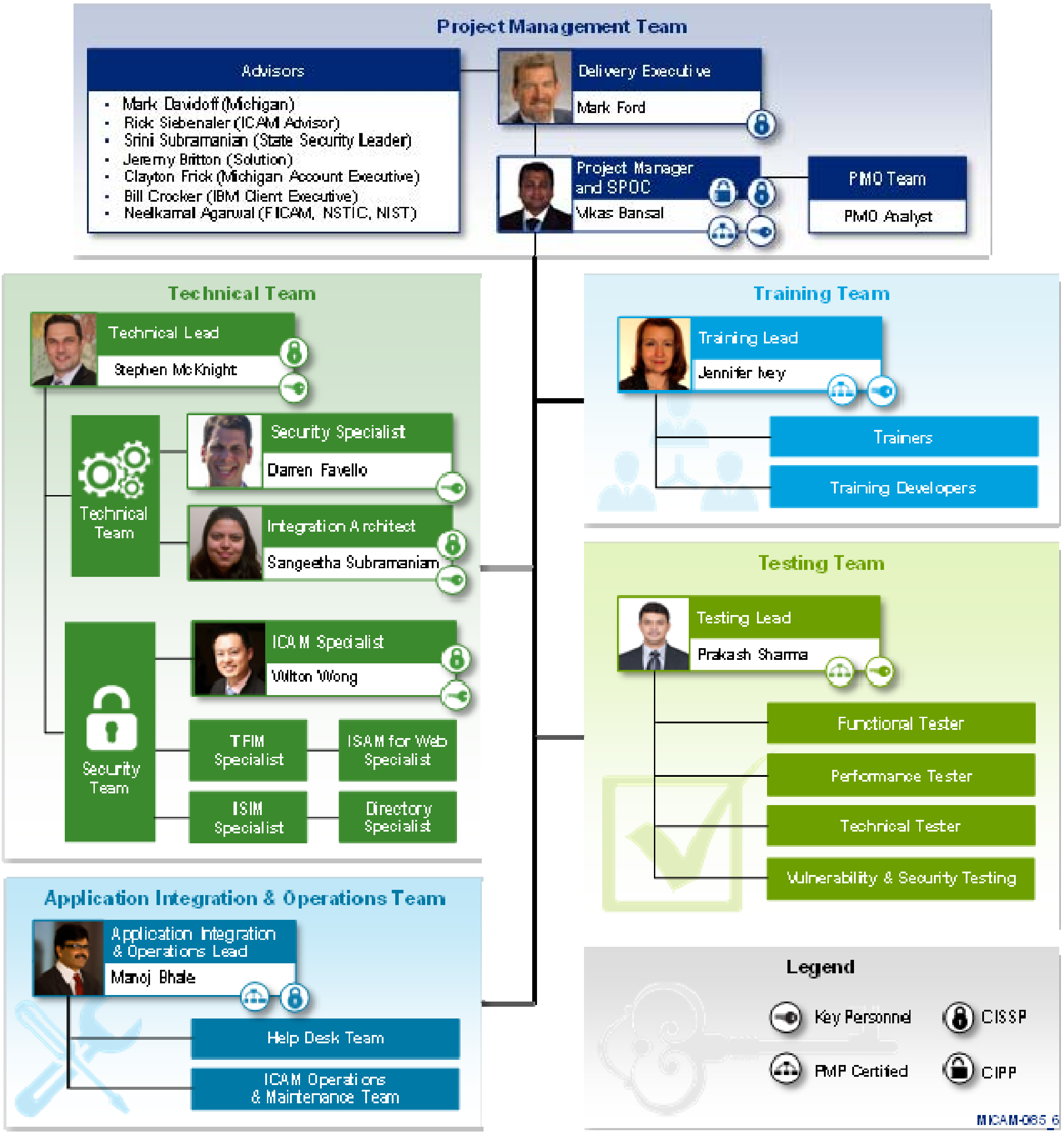
Attachment 1 –Organizational Chart

Deloitte's MICAM Project Team



Project Management Team

Advisors

- Mark Davidoff (Michigan)
- Rick Siebenaler (ICAM Advisor)
- Srini Subramanian (State Security Leader)
- Jeremy Britton (Solution)
- Clayton Frick (Michigan Account Executive)
- Bill Crocker (IBM Client Executive)
- Neelkamal Agarwal (FICAM, NSTIC, NIST)

Delivery Executive
Mark Ford

Project Manager and SPOC
Vikas Bansal

PMO Team
PMO Analyst

Technical Team

Technical Lead
Stephen McKnight

Technical Team

Security Specialist
Darren Favello

Integration Architect
Sangeetha Subramaniam

Security Team

ICAM Specialist
Wilton Wong

TFIM Specialist

ISAM for Web Specialist

ISIM Specialist

Directory Specialist

Training Team

Training Lead
Jennifer Ivey

Trainers

Training Developers

Testing Team

Testing Lead
Prakash Sharma

Functional Tester

Performance Tester

Technical Tester

Vulnerability & Security Testing

Application Integration & Operations Team

Application Integration & Operations Lead
Manoj Bhale

Help Desk Team

ICAM Operations & Maintenance Team

Legend

Key Personnel

CISSP

PMP Certified

CIPP

MICAM-065_6

Appendix A - Breakdown of Hardware and Related Software

Table 1: Hardware

Item	Brand, Model # and Description	Specifications	Cost ($): State will provide from existing Contracts	Comments
Server	Secure-24 VMware Cluster Access for deploying ISIM, ISAM and ISFIM components	Total # of Virtual Machines: 48 Total # of Virtual CPUs: 96 Total Virtual RAM: 416 GB OS: RedHat Linux 6.x		The hardware is sized for Production, QA/Staging, Development, and Sandbox environments in the primary data center and for Production, and QA environments in the secondary data center
Storage	Enterprise Class SAN Storage	Total Storage: 35.7 TB (3.8TB of Bronze Tier, 15.8TB of Silver Tier, 5.1TB of Logs Tier, 11TB of Gold Tier)		The total storage is estimated for Production, , QA/Staging, Development and Sandbox environments in the primary data center and for Production, QA environments in the secondary data center
CD/DVD Backup Device	None	None		
Rack w/ Power Supply	Rack mountable	Redundant Power		
Screen	None	None		
Any other Hardware (list)	Web Gateway Hardware Appliance	v7.0		A total of 10 Web Gateway appliances are estimated for Production, QA/Staging, Development and Sandbox environments in the primary data center and for Production, QA environments in the secondary data center.
		TOTAL	**$**	

Table 2: Related Software

Software Component License	Product Name and Version	# of Licenses	Cost ($): State will provide from existing Contracts	Comments
Report writers	MS Office 2010	Contractor user laptops already include this software. State of Michigan user laptops will need this software for up to 4 users.		We will reuse the State owned software licenses
Requirement analysis tools	MindMap	5 user licenses		No cost and open source software
	MS Visio 2010	Contractor user laptops already include this software. State of Michigan user laptops will need this software for up to 4 users.		We will reuse the State owned software licenses
	MS Office 2010	Contractor user laptops already include this software. State of Michigan user laptops will need this software for 4 users.		We will reuse the State owned software licenses
Design tools	Rational (Rational Modeler for UML 2.1)	IBM Rational Modeler is a free software		No cost
	MS Visio 2010	Contractor user laptops already include this software. State of Michigan user laptops will need this software for up to 4 users.		We will reuse the State owned software licenses
Development environment tools	Eclipse 4.x	Up to 5 user licenses		No cost
	TextPad	Up to 15 user licenses		We will reuse the State owned software licenses
	XML Spy 2010[1] (professional edition)	Up to 2 user licenses		No cost
	Toad 9.x or 10.x[2] (Quest Toad for IBM DB2 LUW (Linux, Unix	Up to 5 user licenses.		We will reuse the State owned software licenses

[1, 2, 3] If the State has software providing comparable capabilities and functionality as provided by these products, we are flexible in utilizing those.

	and Windows – DM))			
	Putty 0.62 (Telnet)	Up to 8 user licenses.		No cost
	WindSCP 4.3.6 (FTP)	Up to 6 user licenses		No cost
Testing tools (such as issues tracking, defect tracking, load/stress testing, configuration management.)	Bugzilla 3.4.2 – Issue and defect Tracking	Up to 8 user licenses for Testers and Developers.		No cost and open source
	Load Runner 11.x – Performance/Stress Testing	Up to the virtual user load determined for MICAM		We will reuse the State owned software licenses
	Concurrent Version Control - Subversion 1.6	Up to 6 user licenses for developers.		No cost and open source
	Accessibility Testing – • JAWS (JAWS 14 professional edition) • Dragon Naturally Speaking Software • Zoom Text[3] (ZoomText Magnifier)	1 user license for Accessibility Testing.		The State will procure the licenses
	IBM Application Vulnerability Scan	1 license		.
	Nessus Network Vulnerability [4]	1 enterprise license (Local installation with initial subscription of 1 year)		The State will procure the licenses
Other system utilities	SSL Certificates – Secure Communication	Depending on State requirements, but minimally 1 SSL Certificates from a globally known Certificate Authority will be needed for Citizens. We envision using self-signed certificates for server to server communication between the MICAM solution components.		The State to generate SSL certificates using State owned Internal certification authority or procure from a third-party CA
Server software	• IBM Security Identity Manager 6.0 (Identity Management Software) • IBM Security Role and Policy Modeler v1.1 • IBM Security Access Manager for Web 7.0	Estimated in processor value units (PVUs)		The State will procure the Software licenses for Production, DR, QA/Staging, Development, and Sandbox environments.

[4] If the State has software providing comparable capabilities and functionality as provided by these products, we are flexible in utilizing those.

	(Access Management Software) • IBM Security Federated Identity Manager 6.2.2 (Federation and Risk based Authentication Software) • IBM Websphere Application Server 7.0 (Middleware Software) • IBM Tivoli Directory Server 6.3 (Directory Server Software) • IBM DB2 9.7 (Database Software) • IBM Tivoli Common Reporting (Reporting Software) • IBM Tivoli Key Lifecycle Manager v2.0.1 (Key lifecycle management tool)			
	Operating System – Linux Redhat Enterprise Server 6.x	48 licenses have been included in our estimate. Secure-24 will provide these for the MICAM for Citizens environment as part of our Mandatory Response		Total number of enterprise servers in Production, DR, QA/Staging, Development and Sandbox environments
	Security Information and Event Management Tool	For MICAM we have included LogRhythm for the infrastructure components (firewall, routers, switches, servers) and Operating Systems (Redhat). This means Secure-24 is providing the infrastructure and licensing for these components in the MICAM solution.		
Any other software (list)	reCAPTCHA			No cost and open source
	Project Management - MS Project 2010	Contractor user laptops already include this software. State of Michigan user laptops will need this software for up to 4 users.		We will reuse the State owned software licenses

	RSA SecurID - Two Factor Authentication Hardware Token	The State will provide the appropriate number of RSA Secure-ID tokens for accessing the MICAM for Worker environment by users and Contractor project and support professionals.		Secure-24 will provide 40 RSA tokens for secure remote access to the MICAM for Citizens environment
	Angel Call Center Management tool (Helpdesk Tool)	None		Included in our pricing cost
	Application Management – Process Manager (Helpdesk Tool)	Up to 20 users included in our response (Intended for users that will be submitting or monitoring MICAM related service requests)		Included in our pricing cost
	MS SharePoint Server 2007 EE (Document Management)	Contractor: up to 15 users		We will reuse the State owned software licenses
	Birt 3.7 (Reporting Tool)	Contractor: 3 users		No cost
		TOTAL	**$**	

Instructions:

1. Bidder must list all hardware components and any necessary related software individually (components above are sample only).
2. Bidder must list all software components individually (components above are sample only).
3. Bidder must include detailed specifications for all proposed software and hardware
4. Bidder must include detailed description of their licensing rules and model

BIDDER RESPONSE:

APPENDIX A: BREAKDOWN OF HARDWARE AND RELATED SOFTWARE

Bidders are to provide additional details needed to fully understand the proposed pricing contained in the cost tables. Please provide response in the text box below.

The following criteria were considered for sizing the hardware and software:

1. Total. No of Users = 4,665,000 (State of Michigan Citizens)
2. Anticipated user arrival rate is 0.5 users per second
3. Web Login rate = 0.9 users per second
4. No. of transactions per second = 1
5. The solution to be deployed on a 3- tier architecture
6. Virtualized environment
7. Maximum CPU utilization of 70 percent
8. Use of a Web Gateway Hardware appliance as a secure proxy

9. SSL Communication
10. The solution is hosted externally by Secure-24

For Mandatory option (i.e., Externally Hosted MICAM for Citizens), Secure-24 will provide:

- High-Quality Data Center Services (Physical Security, Redundant Power, Access Control etc.)
- Required Server, storage, and network hardware
- Secure-24 will provide infrastructure management, monitoring, and support
- Secure-24 will provide Redhat operating system licensing
- Secure-24 will provide OS management, monitoring, and support
- Log tracking provided via LogRhythm
- Secure-24 provided web/application load balancing using F5 GTM and LTM solutions
- Secure-24 will provide change management for environment with ITIL ticketing /workflow tool
- There will be 10 named technical contacts who can contact Secure-24 24x7 – Client will provide Level 1 help desk for End Users
- Two factor authentication with RSA security, 40 key fobs provided
- Highly available Multi-tiered VPN, Firewall, and security infrastructure
- 24x7 Systems Monitoring and Alarming with Incident Management
- Cross connect to MPLS for primary WAN connection and 2Mb VPN for secondary WAN connect
  - Access to 10Mbit Sonet between data centers for replication
  - Daily Backups to Disk at Local Site
  - Prod Data - Daily Incremental, Weekly Full Backups to Disk (13.5TB/Full) - 30 Days Held Onsite, 30 Days Held Offsite
  - Pre-Prod Data - Daily Incremental, Weekly Full Backups to Disk (18.6TB/Full) - 30 Days Held Onsite, No Offsite
  - Production data held onsite for 30 days
  - Pre-production data held onsite for 30 days
- Nightly Offsite Replication of Backups to Disk at Alternate Data Center
  - Production data held offsite for 30 days
- Cross Connect to State of Michigan MPLS Cloud (Primary WAN)
- Internet Bandwidth: "2"Mbit/s "CIR" to 4 ISPs (Burstable to 100Mbit) (Secondary WAN)
- Access to Highly Available Multi-Tiered Firewall and Security Infrastructure
- Access to Core Highly Available Cisco Ethernet Switching Infrastructure
- Access to Highly Available Intrusion Detection/Inspection (IDS/IPS) Infrastructure
- Access to Clustered F5 Load Balancers - LTM and GTM Load Balancers
- Access to 10Gbit/s SONET Connection for Replication
- 24x7 Replication Management and Monitoring
- Annual DR Failover Testing

Other Software Estimation.

For the supporting software listed above, we will reuse the licenses currently owned by the State. If the software license is unavailable then the State will procure the required licenses and make them available for the project.

Appendix B – Cost Table

Table 1: Total 5 Years Cost

No.	Cost Categories	Cost ($)	Comments
Appendix A	Breakdown of Hardware and Related Software Cost (Total of Table 1 and 2 in Appendix A)		State will provide cost from existing State contracts.
Table 2	Work and Deliverables Cost	**$9,905,771.17**	For BAFO purposes, we have considered a cost reduction of **$143,795.** This is a reduction in IBM IAM software licensing cost, and Experian Identity Proofing cost. The estimated cost associated with the inclusion of following software licenses and new requirements is **$382,620** which is an investment by Deloitte & Touche LLP. These additional products and services which Deloitte & Touche LLP is providing to the State reflects no additional cost to the State of Michigan. • IBM Tivoli Key Lifecycle Manager (TKLM) and IBM Tivoli Directory Server software • Deploying one (1) instance of TKLM for certificate management • Integrating the eight (8) Active Directory (AD) forests. Note: Removed software licensing cost for IBM and Experian Identity proofing from table. The State will directly procure IBM IAM software from IBM.
Table 2b	Work and Deliverables Cost/Payment Schedule for Risk-Based Authentication Option		The cost associated with implementing risk based authentication (RBA) for five (5) applications is estimated to be **$350,000**. This cost is not added to the overall cost for the Table 1 (Total 5 Years cost) and is considered as already included in the overall pricing for BAFO.
Table 2c	Work and Deliverables / Captcha Option		The cost associated with implementing CAPTCHA for one (1) use case is estimated to be **$25,000**. This cost is not added to the overall cost for the Table 1 (Total 5 Years cost) and is considered as already included in the overall pricing for BAFO.

Table 3	Recurring Post-Implementation Costs for Maintenance and Support	**$ 6,937,770.84**	
Table 4	Recurring Hosting Costs	**$ 3,798,518.00**	For BAFO purposes, we have included a cost reduction of **$197,280** on the recurring hosting cost, submitted as part of the RFP response.
Table 5	Recurring Operational Services Costs for day to day operations	**$ 2,577,360.00**	For BAFO purposes, we have included a cost reduction of **$201,054** on the Help desk cost, submitted as part of the RFP response.
Table 7	Operational Services Costs for New Integrations	**$ 9,024,253.48**	Considered maximum two hundred (200) new applications to be integrated with MICAM solution (as specified in MICAM Appendix C Migration and Integration Types) from month 19 – 60 of the project.
Table 8, Row I	Experian Identity Proofing	**$360,000.00**	
Table 9	Training and Documentation Cost	**-**	
Table 10	Reserved Bank of Hours for Future Projects Cost	**$ 10,617,500**	We understand it will be at the State of Michigan's direction that these costs will be incurred. We understand this may represent **$0** as it is all optional.
	Total 5 Years Cost	**$ 43,221,173.49**	For BAFO purposes, the total savings to the State is **$1,299,749.00.** It is categorized as: • **$542,129.48** cost reduction on the cost submitted as part of the RFP response This cost reduction is depicted in the overall cost for the Table 1 (Total 5 Years cost). • **$757,619.52** cost for new products and services that we will offer to the State of Michigan at no additional cost. This cost is not added to the overall cost for the Table 1 (Total 5 Years cost) and is considered as already included in the overall pricing for BAFO. **Note:** 1. Updated Table 2 to drop the cost associated with procurement of IBM IAM and Experian Identity proofing software 2. Added Table 8 to reflect software cost for Experian Identity proofing.

Table 2: Work and Deliverables Cost/Payment Schedule

Task	Cost Categories / Milestone	Cost	Holdback (10% of Amount)	Payment Amount (Less 10% Holdback)
	Initiation and Planning	$	$	$
1.1	Project Planning	$ 151,909.80	$ 15,190.98	$ 136,718.82
1.2	General Timeline	$ 37,977.45	$ 3,797.75	$ 34,179.70
1.3	Confirm Infrastructure	$ 230,475.96	$ 23,047.60	$ 207,428.36
Initiation and Planning Total		**$ 420,363.21**	**$ 42,036.33**[1]	**$ 378,326.88**
	Phase 1 MICAM	$	$	$
2.1	Requirements Definition	$ 240,390.30	$ 24,039.03	$ 216,351.27
2.2	Functional Design	$ 240,390.30	$ 24,039.03	$ 216,351.27
3.1	Construction and Testing Plan	$ 240,390.30	$ 24,039.03	$ 216,351.27
3.2	Environment Installation and Plan			
3.2a	Sandbox Environment	$144,234.18	$14,423.42	$129,810.76
3.2b	Development Environment	$144,234.18	$14,423.42	$129,810.76
3.2c	Staging Environment	$192,312.24	$19,231.22	$173,081.02
3.3	System Testing	$ 120,195.15	$ 12,019.52	$ 108,175.63
3.4	Federation Pilot User Acceptance Testing	$216,351.27	$21,635.13	$194,716.14
4.1	Federation Pilot Production Testing	$86,540.51	$8,654.05	$77,886.46
4.2	Federation Pilot Production Cutover	$129,810.76	$12,981.08	$116,829.69
4.4	Federation Pilot Post Implementation Evaluation Report	$ 120,195.15	$ 12,019.52	$ 108,175.63
3.4	Migration Pilot User Acceptance Testing	$216,351.27	$21,635.13	$194,716.14
4.1	Migration Pilot Production Testing	$86,540.51	$8,654.05	$77,886.46
4.2	Migration Pilot Production Cutover	$129,810.76	$12,981.08	$116,829.69
4.4	Migration Pilot Post Implementation Evaluation Report	$ 96,156.12	$ 9,615.61	$ 86,540.51
Phase 1 Total		**$2,403,903.00**	**$ 240,390.31**[2]	**$2,163,512.69**
	Phase 2 Migrations of Existing SSO Applications	$	$	$
	Migrations in Table 6	$ 7,081,504.96[3]	$ 708,150.50[4]	$ 6,373,354.46
Phase 2 Migrations of Existing SSO Applications Total				
			Initiation and Planning Total Cost	**$ 420,363.21**
			Phase 1 Total Cost	**$2,403,903.00**
			Phase 2 Total Cost	**$7,081,504.96**
			GRAND TOTAL	**$9,905,771.17**
Payment on Final Acceptance				

Task	Cost Categories / Milestone	Cost	Holdback (10% of Amount)	Payment Amount (Less 10% Holdback)
Initiation and Planning Holdback				$ 42,036.33
Phase 1 Holdback				$ 240,390.32
Phase 2 Holdback				$ 708,150.50

1. The Holdback amount for Initiation and Planning will be paid to Contractor, in accordance with Section 1.602, on the State's acceptance of all deliverables in the Initiation and Planning phase.
2. The Holdback amount for Phase 1 will be paid to Contractor, in accordance with Section 1.602, on the State's acceptance of all Deliverables in Phase 1.
3. The State will approve payments per application release/bundle migrated to MICAM, less the Holdback amount.
4. The Holdback amount for Phase 2 will be paid to Contractor, in accordance with Section 1.602, on acceptance of all Deliverables in Phase 2.

Table 2b: Work and Deliverables Cost/Payment Schedule for Risk-Based Authentication Option

Task	Cost Categories	Cost Value	Comments, including licensing information
		$	
2b.1	One-time setup fee (includes planning, requirements definition, design, configuration & construction, testing	$ 70,000.00	
2b.2	Software license fees	-	1. Deloitte & Touche LLP has factored the cost for software licenses for the initial contract period in the Table 8 – Licensing cost
2b.3	Implementation Fee	1. $ 280,000.00	2. Considered five (5) applications to be integrated with MICAM for Risk-Based Authentication.
2b.4	Five years Maintenance (include annual fee in Comments field, if applicable) -		
Table 2b Total Cost		**$ 350,000.00**	The costs in this table represent the value of the Risk-Based Authentication solution, which Contractor will provide to the State at no additional charge. These costs are provided here for informational puposes only.

Table 2c: Work and Deliverables / Captcha Option

Task	Cost Categories	Cost	Holdback (10% of Amount)	Payment Amount (Less 10% Holdback)	Comments, including licensing information
		$	$	$	
2c.1	One-time setup fee (includes planning, requirements definition, design, configuration & construction,	$ 25,000.00	$ 2,500.00	$ 22,500.00	

Task	Cost Categories	Cost	Holdback (10% of Amount)	Payment Amount (Less 10% Holdback)	Comments, including licensing information
	testing				
2c.2	Software license fees	-	-	-	The proposed solution leverages reCAPTCHA from Google which is ADA-compliant free service
2c.3	Implementation Fee	-	-	-	The implementation fees is already factored in the One-time set up fee specified in row 2c.1
2c.4	Five years Maintenance (include annual fee in Comments field, if applicable)	-	-	-	
			Table 2c Total Cost	$ 25,000.00	The costs in this table represent the value of the Captcha solution, which Contractor will provide to the State at no additional charge. These costs are provided here for informational puposes only.

Table 3: Recurring Maintenance and Support Cost

No.	Cost Categories	Annual Rate	Years	Cost ($)	Comments
A.	**Annual Maintenance and support rate (Beginning after Phase 2. This table includes optional years; depending upon the GO-Live date)**				1. Consolidated fees provided along with the yearly rate as the resources for Maintenance and Support are ramped up as the project progresses and the number of applications and MICAM users increases.
	Total Recurring Cost	Year 1 (Month 7-12): $ 340,952.04 Year 2: $ 808,888.08 Year 3: $ 1,406,982.72 Year 4: $ 2,043,172.56 Year 5: $ 2,337,775.44	**5**	**$ 6,937,770.84**	

Table 4: Recurring Hosting Cost

No.	Cost Categories	Annual Rate	Years	Cost ($)	Comments
B.	**Hosting rate (Beginning after Phase 2. This table includes optional years; depending upon the GO-Live date)**				1. Considers Hosting Services for externally facing MICAM solution for the initial contract term, i.e., 5 years and one time environment setup cost.
	Total Recurring Cost	One time cost= $ 50,198 Yearly cost = $ 749,664.00	**5**	**$ 3,798,518.00**	

Table 5: Recurring Operational Services Costs for day to day operations

No.	Cost Categories	Annual Rate	Years	Cost ($)	Comments

C.	**Annual Operational Services (Beginning after Phase 2. This table includes optional years; depending upon the GO-Live date)**				1. Consolidated fees provided along with the yearly rate as the resources for Help Desk are ramped up as the project progresses and the number of applications and MICAM user's increases.
	Total Recurring Cost	Year 1 (Month 7-12): $ 239,838.00 Year 2: $ 547,708.00 Year 3: $ 579,164.00 Year 4: $ 613,941.00 Year 5: $ 596,709.00	**5**	**$ 2,577,360.00**	

Table 6: Migrations of Existing SSO Applications Costs

No.	Cost Categories	Number of Applications	Cost ($)	Comments
D.	**IBM Tivoli Identity Manager and Tivoli Access Manager and NetIQ Access Manager and Identity Manager**			Considered maximum one hundred ninety five (195) applications to be migrated to MICAM solution (as specified in MICAM Appendix C Migration and Integration Types) from month 7 – 24 of the project. For planning purposes, we have considered the following number of applications to be migrated from the existing IBM Tivoli, NetIQ, and Microsoft Forefront IDM based solutions. • Type A = 10 applications • Type B = 10 applications • Type C = 150 applications • Type D = 10 applications • Type E = 15 applications **Note**: The estimation of cost by application is provided as a high level budgetary estimate. As mentioned in the assumptions below, these estimates will be reviewed for effort and cost during the planning exercise before migration of the applications identified by the State of Michigan. As applicable, the deviation in initially provided estimates and those determined during planning, before the migration of applications, will be addressed through a change request (CR).
	Type A	< 10	$ 470,137.67	
	Type B	< 10	$ 367,295.05	
	Type C	150 > x > 130	$ 3,305,655.49	
	Type D	<10	$ 734,590.11	
	Type E	<15	$ 2,203,826.64	
	Total Cost	**195**	**$ 7,081,504.96**	

Table 7: Operational Services Costs for New Integrations

No.	*Cost Categories*	*Cost ($)*	*Comments*
E.	***Per Applications Integration flat fee based on Type for 100 Integrations per year***		Considered maximum two hundred (200) new applications to be integrated with MICAM solution (as specified in MICAM Appendix C Migration and Integration
	Type A	$ 1,247,565.51	

	Type B	$ 974,660.55	Types) from month 19 – 60 of the project. For planning purposes, we have considered the following number of applications to be integrated with the proposed MICAM solution. • Type A = 38 applications • Type B = 38 applications • Type C = 38 applications • Type D = 38 applications • Type E = 38 applications • Type F = 4 applications • Type G = 6 applications **Note**: The estimation of cost by application type is provided as a high level budgetary estimate. As mentioned in the assumptions below, these estimates will be reviewed for effort and cost during the planning exercise before integration of applications identified by the State of Michigan. As applicable, the deviation in initially provided estimates and those determined during planning, before the integration of applications, will be addressed through a change request (CR).
	Type C	$ 584,796.33	
	Type D	$ 1,949,321.11	
	Type E	$ 3,898,642.22	
	Type F	$ 61,557.51	
	Type G	$ 307,710.25	
	Total Cost	**$ 9,024,253.48**	

Table 8: Licensing Cost

Per Addendum 8, Bidders may feel free to provide information within the column fields Number of Licensing Units and Per Unit Cost ($) as additional information, if this information is applicable to their solution.

No.	Cost Categories	Number of Licensing Units	Per Unit Cost ($)	Total Cost ($)	Comments
F.	COTS/Application Software Product Licensing (Includes licensing and updates each year)			$ 1,875,291.32	Citizens • 1,000 User Value Units in addition to the 24,500 User Value Units currently licensed by the State of Michigan • 2,500 User Value Units in addition to the 24,500 User Value Units currently licensed by the State of Michigan. • The State will
G.	Internal User Licensing (55,000 estimated number of current Internal Users) (Includes licensing and updates each year) (Including Per Unit Price)	1000	54.16	54,163.34	
H.	External User Licensing (500,000 estimated number of External Users after phase 2) (Includes licensing and updates each year)	2500	54.16	135,408.34	
H.1	IBM DataPower Appliances	6	77,175	$463,048.00	
I.	**Experian Identity Proofing for External Users (estimate 500,000)**			**$360,000.00**	

	Total Licensing Cost			**$ 2,887,911.00**	directly procure software licenses from IBM for the MICAM solution.

Table 9: Training and Documentation Cost

No.	Training and Documentation	Cost ($)	Comments
J.	1) User training		1. Cost related to training and documentation will be determined based on specific training and documentation needs identified by the State of Michigan as the project progresses. This will be addressed through a change request. 2. For planning purposes, we have already considered a total of three (3) sessions of four (4) hours each in every three (3) months period for training the staff identified by the State of Michigan for conducting the User Acceptance Testing (UAT) of the MICAM solution. This cost is already factored in implementation and migration cost during the initial contract period. It is the State of Michigan's responsibility to coordinate with its staff to make them available for these training sessions. These training sessions will be focused on the MICAM solution to help enable State of Michigan staff perform UAT and does not include product related trainings. Deloitte & Touche LLP may provide additional MICAM solution training, IAM product training, or transition services, at the request of the State of Michigan, upon execution of a change request for these activities. 3. The cost associated with the End User communication with respect to application integration and migration roll out, such as frequently asked questions (FAQ), is already factored in our proposed fees. 4. Our operational and maintenance cost estimate is included in the proposed fees.
	2) User training documentation		
	3) Operational management training		
	4) Operational management training documentation		
	5) DBA training		
	6) DBA training documentation		
	7) Others: (List below)		
	Total Cost of Training & Documentation	**$**	

Table 10: Reserved Bank of Hours for Future Projects Costs

No.	Customization or Application Development		Not-to-Exceed Hourly Rate ($)	Total cost ($)	Comments
K.	1. Project Management		$265		1. The estimation of hours by
	2. Business Analysts		$175		

	3. System Analysts		$175		resource is provided as a high level budgetary estimate as the scope and requirements are unknown at this time.
	4. Programmer/Developers		$175		
	5. System/Application Administrators		$175		
	6. Database Administrators		$210		
	7. Q/A Manager		$230		
	8. Security Specialist		$230		
	9. Testers		$175		
	10. Technical Writers		$175		
	11. CM Specialists		$175		
	12. System Architects		$230		
	13. Network Engineer/Administrator		$215		
	14. Software Architects		$230		
	15. Project Assistants		N/A		
	16. Web Developers		$175		
	17. Application Trainers		$175		
	Others: (List below)				
	18. Security lead		$300		
	19. ICAM Specialist		$215		
	20. Operation & Maintenance Staff		$98		
	21. Help Desk Staff		$49		
	Table 10 Total, estimated 50,000 hours			**$ 10617500.00**	

Notes:

1. *Bidder will identify staffing positions that it intends on using during this contract. Bidders must complete and provide "Not-to-Exceed Hourly Rate" for the duration of the contract.*
2. *Not-to-Exceed Hourly Rates quoted are inclusive of Contractor staff and management overhead, travel and all other expenses.*
3. *The State may request additional Position Types, other than the Position Types listed above.*
4. *DTMB is not obligated to execute the contract for the full amount of hours estimated in the RFP. The State may choose to utilize some or all of the hours quoted. All hours shall to be billed monthly at actual hours utilizing the quoted firm fixed hourly rates or on completion and acceptance of specified deliverables.*
5. *It is the State's discretion to determine best value to the State, and to estimate the Contract value for the awarded Bidder.*

Appendix C - Migration and Integration Types

For bidding purposes, the Bidder will be expected to provide a flat fee per type in Appendix B Cost Table for the following existing Migrations and future Integrations based on the State defined Types.

MIGRATION

1. **IBM Tivoli Identity Manager/ Tivoli Access Manager** and **NetIQ Access Manger and Identity Manager**

   I. Type A – Automation of Shared Secret Validation Migration
      i. Main features typically require:
         - ID proofing during subscription
         - Usually requires custom screen development
         - May require web services calls
         - Validate the shared secret ; If valid, allow access
         - Usually requires some custom coding (Java in current system)

      ii. Typical work takes 140-180 hours
      iii. Frequency of occurrence: The State currently has fewer than ten of these

   II. Type B – COTS Application Migration
      i. Main features typically require:
         - Work with application vendor to determine configuration
         - Follow application vendor guidelines
         - Establish trust model
         - Integrate provisioning
         - Examples include Business Objects, FileNet, Siebel, etc.

      ii. Typical work takes 100-150 hours
      iii. Frequency of occurrence: The State has fewer than ten of these

   III. Type C – Standard Application Migration
      i. Main features typically require:
         - In-house (or contractor) developed Application
         - Mainly requires configuration work
         - Work with development team; training, assistance, etc., with integration

      ii. Typical work takes 50-100 hours;
      iii. Frequency of occurrence: This is the State’s primary model; the State has between 130 - 150 of these

   IV. Type D – Complex Application Migration
      i. Main features typically require:
         - Multiple application vendors or products involved
         - Possibly multiple applications involved
         - Application may have multiple methods for authentication
         - May involve EAI (External Authentication Interface)
         - Custom coding, development, or screens may be required

      ii. Typical work is difficult to estimate; likely 200-300 hours
      iii. Frequency of occurrence: This is a rare instance; the State currently has fewer than ten of these

   V. Type E – Highly-Customized Complex Application Migration
      i. Main features typically require:

- Custom interface development (login page, password change page, forgot password page, etc.)
- Web service calls for handling above UI pages
- API development
- LDAP integration
- Java or equivalent development
- Multiple Authentication methods
- Non-typical Authentication models

ii. Typical work is difficult to estimate; likely 400-600 hours

iii. Frequency of occurrence: The State currently has fewer than 15 of these

INTEGRATION

I. Type A – Automation of Shared Secret Validation Integration

i. Main features typically require:

- ID proofing during subscription
- Usually requires custom screen development
- May require web services calls
- Validate the shared secret ; If valid, allow access
- Usually requires some custom coding (Java in current system)

ii. Typical work takes 140-180 hours

II. Type B – COTS Application Integration

i. Main features typically require:

- Work with application vendor to determine configuration
- Follow application vendor guidelines
- Establish trust model
- Integrate provisioning
- Examples include Business Objects, FileNet, Siebel, etc.

ii. Typical work takes 100-150 hours

III. Type C – Standard Application Integration

i. Main features typically require:

- In-house (or contractor) developed Application
- Mainly requires configuration work
- Work with development team; training, assistance, etc., with integration

ii. Typical work takes 50-100 hours

IV. Type D – Complex Application Integration

i. Main features typically require:

- Multiple application vendors or products involved
- Possibly multiple applications involved
- Application may have multiple methods for authentication
- May involve EAI (External Authentication Interface)
- Custom coding, development, or screens may be required

ii. Typical work is difficult to estimate; likely 200-300 hours

V. Type E – Highly-Customized Complex Application Integration

i. Main features typically require:

- Custom interface development (login page, password change page, forgot password page, etc.)
- Web service calls for handling above UI pages
- API development

- LDAP integration
- Java or equivalent development
- Multiple Authentication methods
- Non-typical Authentication models

ii. Typical work is difficult to estimate; likely 400-600 hours

VI. Type F – Identity Federation Integration: Provider

i. Main features typically require:

- Standards-based federation as an Identity Provider

ii. Estimate: Typical work takes 50-100 hours

VII. Type G – Identity Federation Integration: Consumer

i. Main features typically require:

- Standards-based federation as an Identity Consumer
- Typically more difficult than an ID Provider integration

ii. Estimate: Typical work takes 200-300 hours

Appendix D: General and Technical System Requirements

− General and Technical System Requirements Will Identify the General Framework in Which the Product Must Work, Such As: System Architecture, Documentation, Audit and Backup and Recovery.

Bidder and bidder subcontractors are defined as Bidder. The Bidder's and all bidder subcontractors must comply with all State and Federal Policies and guidelines.

With Approval by the State of Michigan, all versions must meet or be above what is specified.

BIDDER RESPONSE INSTRUCTIONS:

The Bidder must respond whether or not their proposed product complies with each requirement as follows:

1. *Check the box that applies to each requirement in the columns labeled:* ***Yes****,* ***Yes with Modifications****, or* ***No.***

   a. ***Yes*** *– is defined as the Bidder's solution complies with all aspects of the requirement and is currently a standard feature.*

      o *In the* ***comment box*** *the bidder may provide comments and descriptions on compliance, but are not required to.*

   b. ***Yes with Modification*** *– is defined as the solution does not currently comply with the requirement but the Bidder can modify the solution through configuration, programming or source code changes which, in the Bidder's opinion, would result in their solution reaching full compliance with a requirement. If a modification is required to the solution, fill in the column with* ***A****,* ***B*** *or* ***C*** *as defined below:*

      A. *Configuration required to comply with the requirement*
      B. *Programming required to comply with the requirement*
      C. *Source code change required to comply with the requirement*

      o *In the* ***comment box*** *the Bidder must describe the modification that will be made and how it will comply with the requirement. All such modifications are considered to be part of the solution being proposed and included in the bid price. If the modification will not be complete by the "go live" date, the Bidder must specify an anticipated date when the modification would be added to the solution, at no additional cost to the State. The State reserves the right to reject the Bidder's proposed date and consider the solution not in compliance.*

   c. ***No*** *– is defined as the Bidder's proposed solution does not comply with all aspects of the requirement.*

      o *In the* ***comment box*** *the Bidder must describe the impact of not meeting the requirement.*

NOTE:
Emerge: In pilot or in deployment phase.
Standard: Enterprise-wide standard with full deployment and support.
Sunset: No implementation, development or support. Must justify use.
Follow db: Reporting tool must be same version as database version.

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
1000. Client/Workstation					
1000.1	If the Application is a Thin Client architecture it should use or explain the Thin Client implementation. The application shall function with: • Citrix version 5.0 • Windows Terminal • Server version 2008 and 2012	Yes			The proposed MICAM solution does not require thin client architecture.
1000.2	The Application must function with the following web browser(s) in an **INTRANET** environment: • Microsoft IE 8.0	Yes			The proposed solution will be designed to support the identified web browser standards.
1000.3	The Application must function with the following web browser(s) in an **INTERNET** environment: • Microsoft IE 6.0 or above • Firefox 3.0 and above • Chrome 3.0 and above • Safari 4.x and above	Yes			The proposed solution supports Microsoft IE 6.0 or above and Firefox 3.0 and above out-of-the-box (OOTB). While not officially supported by the COTS-based products in the MICAM solution, the versions of Chrome (version 28.0.1500.95) and Safari (version 6.0.5), based on our implementation experience, are known to function properly.
1000.4	The Application must function with the following desktop Operating System (OS): • Windows XP SP3 • Windows 7 Professional • Windows 8 versions	Yes			The proposed solution will be designed to support the identified desktop Operating System (OS) standards since the planned architecture uses Web-based technology. The proposed browser support in requirements 1000.2 and 1000.3 support the identified desktop operating systems. However please note that Windows XP SP3 will be no longer supported by Microsoft past April 2014, and subsequently the MICAM solution will no longer be able to maintain support for that OS past that time.
1000.5	The Application's desktop client install must function on the following standard SOM desktop hardware: Link to Desktop	Yes			The proposed architecture and solution does not require software to be installed on End User desktops to function.

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
	Standard: http://www.michigan.gov/dmb/0,1607,7-150-56355-108233--,00.html				
1000.6	The Application will support mobile devices and their Operating System (OS).	**Yes**			The proposed MICAM solution has prebuilt native applications for iPhone iOS and Google Android operating systems that provides select functionality. Contractor will work with the State to define, develop and support additional requirements that may need to be exposed to mobile interfaces.
1001. Documentation and Standards					
1001.1	Provide a logical network diagram that describes how the infrastructure components will meet the functional requirements.	**Yes**			Contractor will work with the State to develop functional requirements, define the infrastructure components and create the required documentation for requirements traceability in the planning and requirements phase of the project.
1001.2	Provide conceptual and logical data-flow diagrams.	**Yes**			Contractor will work with the State to develop requirements and to document the applicable conceptual and logical data flows in the planning and requirements phase of the project.
1001.3	Provide a complete installation and configuration documentation library.	**Yes**			Contractor will develop installation and configuration guides during the course of development and deployment.

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
1001.4	Provide a high-level architecture diagram, including logical and physical components.	Yes			Contractor will work with the State to refine the requirements and create high-level architecture diagrams in the planning and requirements phases of the project.
1001.5	System documentation will describe error logging and how to access the error logs. State of Michigan should have near real time access to all log files.	Yes			Contractor will develop maintenance and operation guides during the course of development and deployment.
1001.6	System documentation must describe Disaster Recovery capabilities (including Hot and Cold standby options, licensing implications, and critical vs. non-critical functionality and data).	Yes			Contractor will work with the State to develop a disaster recovery plan during the course of development and deployment.
1001.7	System documentation will describe any batch processing requirements for the application.	Yes			Contractor will develop maintenance and operation guides, which will include descriptions and troubleshooting information for batch processing tasks, during the course of development and deployment.
1001.8	System documentation will describe required application maintenance activities and time frames.	Yes			Contractor will develop maintenance and operation guides during the course of development and deployment.
1001.9	Application/System documentation will provide FAQ and/or Support Information for frequent issues staff/users may encounter.	Yes			Contractor will develop maintenance and operation guides during the course of development and deployment.
1003. Installation					
1003.1	Provide a detailed work plan (in hours) and duration (in days) of a typical installation of the base package, including all modules. Include both SOM and vendor effort.	Yes			In the planning phase of the project, Contractor will work with the State to draft a detailed plan including, but not limited to, the duration of a typical installation of the base packages for the in-scope modules and the effort required by the State and Contractor.
1003.2	Provide a high-level project plan outlining activity descriptions,	Yes			A high-level project plan is provided as part of our response. The project plan outlines the activities, work effort duration and

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
	work effort, duration and resources for a typical base-package installation.				resources required for a typical installation of the in-scope base packages.
1003.3	Provide a description of the skill sets of all resources required for a typical install of the base package.	Yes			
1003.4	Provide a list of **functional** issues encountered by other users during a typical implementation of your software.	Yes			Contractor will work with the State during the planning and analysis phases of the project to refine our understanding of the functional requirements. As part of the overall solution, with regard to the requirements, Contractor will identify, list and address relevant known functional issues based on our prior implementation experience.
1003.5	Provide a list of **technical** issues encountered by other users during a typical implementation of your software.	Yes			The MICAM solution is based on COTS IBM products. IBM continues to maintain a growing knowledgebase of technical issues encountered by our clients and other users of their software in the form of release notes, tech notes, PMR's and IBM RedBooks.
1003.6	The application will be remotely deployable and supportable using the following management tool(s): • Microsoft's SCCM (SMS) • Marimba • SSH (Secure Shell for UNIX OS)	Yes			SSH will be used for remotely managing/deploying the application.
1003.7	Provide a detailed list of any browser plug-ins (e.g., ActiveYes, Java, Flash) required by the application. All plug-ins, add-ons, or additional software must be approved in advance.	Yes			MICAM solution requires Java browser plugin for carrying out administrative tasks. Contractor will document a detailed list of the browser plug-ins required by the application as a part of the requirements phase.
1003.8	Provide a detailed list of client components (e.g. ODBC, JDBC, Java Beans, other) required by the application, including permission(s)	Yes			The MICAM solution leverages COTS products which currently exist at the State. These products have the detailed documentation on the client components (e.g., ODBC, JDBC) and the required permission level.

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
	levels.				Contractor will provide a detailed customized list of client components that will be used along with their respective permission levels, during the requirements and design phases of the project.
1003.9	All agents and bots used for monitoring or maintenance of servers and software must be listed including function, install location, permission level, resource usage and all patching and updating procedures.	**Yes**			The MICAM solution uses COTS based products that have documentation regarding sizing, access requirements, patching and updating procedures. Further refinement of capacity and other requirements will be elaborated in the Design and Installation guides of the project. We have provided a high-level estimate in the Capacity Planning section of our response.
1003.10	Provide a detailed list of any and all third-party tools, patching and updating procedures required by the application and how they will be supported over the System Development Life Cycle (SDLC).	**Yes**			The detailed list of the in-scope third-party tools is provided in *Appendix A – Breakdown of Software and Related Hardware*. We do not foresee the need of a third-party tool for patching and updating the components. The proposed solution uses COTS based products that have pre-defined patching and updating procedures. Further, Contractor will leverage State's existing change/Patch management process.

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
1004. Product Development done to support this SOW will follow the requirement listed below:					
1004.1	Provide a report of all known current application defects and the timeline for mitigation efforts.	Yes			The proposed MICAM solution uses COTS IBM security products. IBM routinely publishes product defects, fixes and/or workarounds for their customers.
1004.2	Provide a roadmap for all platform/application enhancements that are planned for the next three years.				The proposed MICAM solution uses COTS IBM security tools. IBM routinely publishes product roadmaps for their customers. IBM Security Solutions for Identity and Access Management help customers improve governance and reduce operational costs throughout the identity life cycle. IBM's Identity and Access Management solutions help manage user provisioning, account and password management and access control. IBM's roadmap for Access Management will focus on reducing the total cost of ownership and improving the time-to-value of IBM solutions through the software (virtual) and hardware appliances. The roadmap also intends to address emerging security use cases related to Mobile User Access Management and Bring Your Own Device (BYOD). The roadmap for Access Management will also focus on enhanced Web Application Protection with the Access Manager to address growing customer requirements for blocking in-bound vulnerabilities along with web access control using IBM threat protection capabilities. IBM will also focus on Improving Collaboration and Secure Data Sharing with Federation to simplify application security integration for SaaS adoption, cloud computing and enabling identity assurance. A recent step in this roadmap occurred when in November 2012, IBM announced IBM Security Access Manager (ISAM) V7.0 and IBM Security Web Gateway AMP 5100 Appliance V7.0, the next generation of IBM's web application security solutions. IBM Security Web Gateway AMP 5100 Appliance V7.0 hardware appliance combines IBM Security's industry leadership in both web access management (ISAM V7) and web application protection capabilities into a single integrated solution. With this appliance, IBM now offers Web single sign-

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
					on (SSO), Web access management, and an IBM X-Force-powered Web Application Firewall to protect Web applications from external threats such as cross-site scripting and SQL Injection.
1004.3	The application will follow the SUITE testing processes and documentation of testing and testing types/levels must be provided.	Yes			During Design phase, a detailed Test Plan will be created in accordance with the Testing Process Manual Version 1.0 of State's Systems Engineering Methodology (SEM). During Design and Build phase, test cases will be developed for the following types of tests: • Installation Confirmation Test • Unit Test • System Integration Test • Performance Test • User Acceptance Test • Security testing In addition, Regression testing will be performed for defect resolution and change implementation.
1004.4	Application development will be done in the following development framework: •.NET Framework 3.5 and above (standard) • JEE 5.x and above (standard)	Yes			The proposed MICAM solution consists of IBM security products that primarily provide Java and C SDKs/API's for product customizations. • IBM Security Identity Manager is a J2EE based COTS application, which provides a J2EE API for development. • IBM Security Access Manager is a C/C++ based COTS application, which provides a J2EE API/SDK, a.NET API/SDK and a C/C++ API/SDK for development. • IBM Security Identity Manager requires Java™ Runtime Environment (JRE), version 1.6, SR10 Fix Pack 1.
1004.5	Programming will be done in the current or newer versions of the following language(s): • ASP.Net 2008 (standard) • C# (standard) • Java (standard) • JavaScript (standard) • JDK 6.x (standard) • PHP 5.2 (standard) VB.NET 2008 (standard)	Yes			The proposed MICAM solution consists of IBM security products that provide Java and C SDKs/API's for product customizations. IBM Security Identity Manager is a J2EE based application. The solution does not provide.NET SDKs/APIs for ASP.Net, C#, VB.NET, or PHP based customization capabilities. Required custom development will be done using Java, JavaScript, JDK, C standards or the programming/scripting language supported by the product.

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
1004.6	Commercial Off-the-shelf (COTS) third-party libraries included within the application will be owned and supportable by the State. Inclusion of any third-party code library or tool must be approved by the State of Michigan Contract Manager or Project Manager.	Yes			IBM licensed program products include IBM Software Support for the first year and subsequent years while on software maintenance. The State and IBM currently have existing agreed-to ELA Terms and Conditions currently in place for IBM licensed program products and their sub-entitlements. Additionally, the following public Web site contains IBM's International Program License Agreement family of license agreements and individual program license information documents. http://www-03.ibm.com/software/sla/sladb.nsf Contractor will work with the State for the required approvals for using third-party libraries for the custom code development for the MICAM engagement. The custom developed code will be owned by the State.
1004.7	Custom-developed third-party libraries included within the application will be owned and supportable by the State. Inclusion of any 3rd party code library or tool must be approved by the State of Michigan Contract Manager or Project Manager.	Yes			IBM licensed program products include IBM Software Support for the first year and subsequent years while on software maintenance. The State and IBM currently have existing agreed-to ELA Terms and Conditions currently in place for IBM licensed program products and their sub-entitlements. Additionally, the following public Web site contains IBM's International Program License Agreement family of license agreements and individual program license information documents. http://www-03.ibm.com/software/sla/sladb.nsf Contractor will work with the State for the required approvals for using third-party libraries for the custom code development for the MICAM engagement. The custom developed code will be owned by the State.
1004.8	Bidder will provide a complete change/history log upon request of all software developed under contract.	Yes			The MICAM solution consists of COTS IBM security products and product changes between versions and fix packs are published by IBM. Contractor will work with the State to identify and use an existing source code version control repository to track changes and configuration management for custom development/configurations. The change log of such custom configurations and software development will be provided on

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
					request.
1004.9	Software development will use the following source code version control repositories: • Microsoft Team Foundation System (standard) • Serena Dimensions (PVCS/Ver Mgr) 2009 R1.x (standard) • Subversion 1.6 (standard)	Yes			Contractor will work with the State to identify and use a source code version control repository that is required by the State.
1004.10	Software development must adhere to the System Engineering Methodology (SEM) described in the State Administrative Guide (Section 1360): http://www.michigan.gov/documents/dmb/1360.00_281429_7.pdf	Yes			Contractor acknowledges this requirement.

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
1004.11	System documentation will clearly describe the type of caching, if any, the system employs.	Yes			The technical design document developed during the Design phase will describe the caching approaches for MICAM solution components, such as IBM Security Access Manager ACLs and policies caching, IBM Security Identity Manager configuration properties caching, and IBM WebSphere Application caching.
1005. Reporting					
1005.1	The reporting product technology will be compatible with n-Tier architecture (client-server & web).	Yes			The MICAM solution includes IBM's identity and access management technology. IBM's Tivoli Common Reporting (TCR) which is based on BIRT that follows the JSR 168 portal standard. JSR 168 defines a 2 tier architecture with a "portal tier" responsible for lay out, security and navigation and a "Portal/Widget Tier" for the hosting application.
1005.2	The reporting product technology will be compatible with the following Server Operating Systems: • (see requirement 1009.9)	Yes			As part of the MICAM solution IBM's Tivoli Common Reporting (TCR) tool will be used for IAM reporting. TCR supports Server Operating systems in requirement 1009.9
1005.3	The reporting tool/system will be certified for use with the VMWare x86 based virtualization platform.	Yes			IBM supports TCR's use with VMWare x86 based virtualization platform. We will work with IBM for product issues reported through IBM's Problem Management Request (PMR) process through which IBM supports its products. TCR is supported on RHEL OS which in-turn is certified on VMWare x86 based virtualization platform.
1005.4	The reporting product technology will be compatible with desktop virtualization.	Yes			TCR is a Web-based application which is deployed on an embedded version of IBM WebSphere Application server. Users/Auditors can log into the application through a web browser to create and access reports.

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
1005.5	The reporting product technology will not require any installed component on the user desktop. (Adobe Acrobat Reader is the State's standard)	Yes			TCR has OOTB capability to generate reports using the default report format in PDF format. The PDF reports can be viewed in Adobe Acrobat Reader as per the State's standard.
1005.6	The reporting product technology will not require any installed component in the user browser other than the following: • Plug-ins • Java run time	Yes			In the MICAM solution, TCR is capable of processing reports and display them using the appropriate browser plug-in. MICAM admins and auditors can view or save the formatted output using the browser or plug-in capabilities.
1005.7	The reporting product technology will be compatible with the following Job Scheduling tools: • BL/Sched 5.0 & 5.2 (standard) • GECS all versions (standard) • OpCon XPS 3.31.02 & 4.x, 5.x (standard) • Tidal Enterprise Scheduler 5.3.1 (standard) • Tidal Enterprise Scheduler 6.0 (standard) • Tidal Enterprise Scheduler 6.1 & 6.5 (emerge) • UC4 Global all versions (sunset) • UC4 Operations Mgr 6.0 & 8.0 (standard)		B		TCR provides functionality to schedule report snapshots with capability to configure scheduling parameters such as schedule start/end date and repeat schedule by using scripting. We will work with the State to integrate its existing scheduling tools with TCR using scripting.

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
1005.8	The reporting product technology will be compatible with one or more of the following Reporting tools: • Active Reports 4.0 (standard) • SAP Business Objects (BO) YesI R2 (standard) • SAP Business Objects (BO) YesI 3.x (standard) • SAP Business Objects (BO) YesI 4.x (emerge) • Crystal Reports 2008 (standard) • MSSQL 2008, R2 & 2012 Reporting Services (follow db) • Oracle Reports 11g (standard) • WebFOCUS		A		TCR has out of box capability to generate reports in a variety of formats, (e.g., CSV format) which are stored at a predefined location on a server. We will work with the State to enable consumption of TCR's reports into its existing reporting tools for enhanced reporting capabilities.
1005.9	The reporting product technology will be compatible with the State standard Extract Transform Load (ETL) tools.		A		In addition to the OOTB functionality in the proposed applications, IBM Tivoli Directory Integrator (ITDI) will be used in the solution to provide basic extract, transform and load (ETL) for exporting data to various systems as required.
1005.10	The reporting product technology will support ad hoc reporting via custom-built queries without requiring any custom programming or changes to the application. Query design must rely only on end-user configuration.		A		We will leverage IBM Cognos Query Studio included in TCR that will allow creation of ad hoc customized reports by using and combining a wide variety of simple queries.
1006. Application Security					
1006.1	The solution must have built-in security controls and meet or exceed current SOM security requirements as described in the State Administrative Guide http://www.michigan.gov/dmb/0,1607,7-150-9131_9347---,00.html#1300INFSTDSPLNNG	Yes			The MICAM solution leverages IBM's Identity Manager and Access Manager, which provides capabilities that can be configured to meet the controls set forth in Section 1300 (Information Standards and Planning) of the Administrative Guide to State Government. We will work with the State in order to further refine each individual requirement, control objective and control implementation in the requirements throughout the life the

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
					project.
1006.2	Application access must be loggable and have a viewable audit trail(s) near real time for the SOM to access	Yes			Our proposed solution leverages IBM Security Access Manager, which provides in-built audit capabilities, which log application access in near-real time.
1006.3	Changes to user permissions must be loggable and have a viewable audit trail(s) near real time for the SOM to access.	Yes			Our proposed solution leverages IBM Security Identity Manager, which provides audit capabilities that can be configured to log application access changes in near-real time.
1006.4	Access to audit trail logs must be able to be restricted to approved administrators near real time for the SOM to access.	Yes			Our proposed solution leverages IBM Security Identity Manager and Security Access Manager, which provides in-built audit capabilities that can be restricted to approved administrators or audit personnel.
1006.5	Application access and changes to application access must log near real time for the SOM to access, at least the following information: • Date/time • Nature of operation • Name of changed item • Name of who made the change • Before and after value of the changed item	Yes			Our proposed solution leverages IBM's Security Identity Manager and Security Access Manager, which provides in-built functionality to establish, document, and manage the allocation of user access rights with near real time audit capabilities, which can capture and report on the required information: • Date/time • Nature of operation • Name of changed item • Name of who made the change • Before and after value of the changed item
1006.6	The following application change event(s) must be logged near real time for the State of Michigan to access, at minimum: • Changes to individual permission level • Changes to role membership • Changes to role permissions • Changes to access to application functions	Yes			Our proposed solution leverages IBM's Identity Manager and Access Manager, which provides in-built functionality to establish, document, and manage MICAM application changes, which can capture and report on the required information. • Changes to individual permission level • Changes to role membership • Changes to role permissions • Changes to access to application functions
1006.7	The System Administrator must be able to control access to audit trail logs in near	Yes			Our proposed solution leverages IBM Security Identity Manager and Security Access Manager, which provides in-built audit capabilities, which log application access in near-real time. Access to the

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
	real time.				bare log data is controlled with file system controls and access to the reporting interface and correlated audit data can be managed independently.
1006.8	Access to program libraries (e.g. base code) must be restricted and controlled.	Yes			Access to program libraries, source code and compiled code will be restricted using the principle of least privilege. Separate controls and checks will be developed as part of the overall Secure Development Life Cycle and as part of the change management procedures.
1006.9	Passwords and User ID's must be able to: • Protect sensitive data • Restrict access to only those authorized • Meet State/Agency Security Standards • Be encryptable	Yes			Our proposed solution leverages IBM's Identity Manager and Access Manager, which provides capabilities for FIPS 140-2 and/or NIST SP800-131 compliance.
1006.10	User authentication methods, based on risk type and severity level, will include: • User ID and Passwords • Biometrics • Directories • Smart cards • Single sign-on solutions • Tokens • PKI and Certificates • Voice recognition • Shared secrets • Access control lists and files • Unique business process	Yes			Our proposed solution leverages IBM Security Access Manager, which provides interfaces for customized authentication and authorization schemes as well as capabilities for multi-factor authentication (MFA). Contractor will work with the State to define and refine MFA capabilities if required in the requirements phase.
1006.11	Session State will be stored and maintained in an encrypted manner.	Yes			Our proposed solution leverages IBM Security Access Manager, which provides in-built capabilities for secure session management.
1006.12	Session State will be stored and maintained in one or more of the following manners: • Cookie • URL String	Yes			Our proposed solution leverages IBM Security Access Manager, which provides in-built capabilities to store sessions in non-persistent cookies.

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
	• Database				
1006.13	A software solution will be accessible (and administrable) through State of Michigan approved Virtual Private Network (VPN).	Yes			The MICAM solution will be accessible using VPN technology. Contractor will work with the State to determine which project team members need access through VPN.

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
1006.14	A solution will comply with all applicable application and data processing standards, including but not limited to: • FERPA • HITECH • FIPS • NIST 800-53 • HIPAA • Sarbanes-Oxley • PCI-DSS • CJIS • IRS Pub.1075 Et.Seq. • Homeland Security	Yes			Contractor shall adhere to and take into consideration as needed State's Security Policies, State and Federal statutory and regulatory requirements, and rules; State's baseline business requirements e.g., Payment Card Industry (PCI) Data Security Standards, applicable National Institute of Standards and Technology (NIST) such as publications 800-53 only, Criminal Justice Information System (CJIS) and Internal Revenue Service (IRS),
1006.15	Application and database communication will use the following port(s) and protocol(s): • Internet Assigned Number Authority (IANA) registered ports • Oracle • Microsoft SQL Server • MySQL • Teradata • 80/443 • Others, as approved	Yes			The solution will follow the standard ports for database and applications inter process communications. Additionally, prior to the production deployment, Contractor will provide a list of required ports/privileges/prerequisites/services for setting up the application in the production environment to the DTMB Infrastructure Services and Michigan Cyber Security (MCS).
1006.16	Client application must support encryption of data both at rest and in motion, in accordance with the data classification.	Yes			The proposed MICAM solution supports protection of data in motion and at rest. Contractor will work with the State in the requirements phase to develop security requirements that will define the applicable level of data protection required.
1006.17	Applications and systems must adhere to SOM Policy 1350.10 regarding Access to Networks, Systems, Computers, Databases, and Applications: http://www.michigan.gov/documents/dmb/1350.10_184594_7.pdf	Yes			The proposed solution adheres to State's Policy 1350.10 regarding "Access to Networks, Systems, Computers, Databases, and Applications". The solution is designed to support/scale-up to support the technical methods listed in the policy document. Contractor will work with the State to select the profile associated with the in-scope resources and will accordingly define the required level of security.

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
					See also 1007.2 and 1008.5.
1006.18	Applications and systems must adhere to State of Michigan Policy 1350.20 regarding Access to Protected Data Resources: http://www.michigan.gov/documents/dmb/1350.20_184600_7.pdf	Yes			Our proposed solution leverages IBM's Identity Manager and Access Manager, which provides functionality to establish, document, and manage the allocation of user access rights for individuals accessing State information technology resources to prevent inadvertent and inappropriate access to resources not authorized for the individual user as identified in the State's policy 1350.20. See Also 1007.6 and 1008.6.
1006.19	End-user software applications, or components thereof, must **not** require privileged, super-user or administrator mode in order to function properly.	Yes			Once the installation and configurations of the application/components are complete, the privileged, super-mode or administrator mode is not required to function properly except for the rare occasions of application troubleshooting. See also 1008.2 and 1009.7
7. Network Security					
1007.1	Client applications must adhere to SOM Policy 1340.00 regarding "Information Security": http://www.michigan.gov/documents/dmb/1340_193162_7.pdf	Yes			The proposed solution adheres to the State's Policy 1340.00 regarding "Information Technology Information Security". The solution is designed with the security principals of Confidentiality, Integrity, and Availability (CIA) and provides protection against unauthorized access, use, disclosure, modification, destruction, or denial. Contractor will work with the State when gathering requirements to define the appropriate levels of protection.
1007.2	Applications and systems must adhere to SOM Policy 1350.10 regarding "Access to Networks, Systems, Computers, Databases, and Applications": http://www.michigan.gov/documents/dmb/1350.10_184594_7.pdf	Yes			The proposed solution adheres to the State's Policy 1350.10 regarding "Access to Networks, Systems, Computers, Databases, and Applications". The solution is designed to support/scale-up to support the technical methods listed in the policy document. Contractor will work with the State to select the profile associated with the in scope resources and will accordingly define the required level of security. See also 1006.17 and 1008.5.
1007.3	Web interface or browser technology will use TCP/IP protocol through Ports 80 or 443.	Yes			The solution will follow the standard ports for Web-based technology. Additionally, prior to the production deployment, Contractor will provide a list of required ports/privileges/prerequisites/ services for setting up the application in the production environment to the DTMB

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
					Infrastructure Services and Michigan Cyber Security (MCS).
1007.4	Applications and systems must conform with SOM Policy 1345.00 regarding "Network and Infrastructure": http://www.michigan.gov/documents/dmb/1345.00_282982_7.pdf	Yes			
1007.5	Application communication between users and system components over the network will be loggable and the log file accessible to the system administrator near real time for the SOM to access.	Yes			Our proposed solution leverages IBM Security Access Manager, which provides in-built audit capabilities, which log application access in near-real time.

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
1007.6	Applications and systems must adhere to SOM Policy 1350.20 regarding "Access to Protected Data Resources": http://www.michigan.gov/documents/dmb/1350.20_184600_7.pdf	Yes			Our proposed solution leverages IBM's Identity Manager and Access Manager, which provides functionality to establish, document, and manage the allocation of user access rights for individuals accessing State information technology resources to help prevent inadvertent and inappropriate access to resources not authorized for the individual user as identified in the State's policy 1350.20. See Also 1008.6.
8. Server Security					
1008.1	Application servers must be hardened prior to placing in production. The hardening process is handled by DTMB Infrastructure Services, in conjunction with Michigan Cyber Security (MCS).	Yes			Prior to the production deployment, Contractor will provide a list of required ports/privileges/prerequisites/services for setting up the application in the production environment to the DTMB Infrastructure Services and Michigan Cyber Security (MCS) for supporting the hardening process.
1008.2	End-user software applications, or components thereof, must **not** require privileged, super-user or administrator mode in order to function properly.	Yes			Once the installation and configurations of the application/components are complete, the privileged, super-mode or administrator mode is not required to function properly except for the rare occasions of application troubleshooting.
1008.3	Servers must have the most recent security patches applied to them and be configured in least privileged mode prior to placing in production in a non-trusted environment.	Yes			MICAM software updates will be planned and released to meet this requirement. Contractor will leverage the State's patch management process.
1008.4	All server-based agents, bots and monitoring components must be listed along with a description of their function, required permission level and resource usage.	Yes			The proposed solution uses COTS based products that have documentation regarding sizing, access requirements, patching and updating procedure. Further refinement of permission level, resource usage and other requirements will be elaborated in the Design and Installation guides of the project. A high level estimate of the resource usage is provided in the capacity planning section.
1008.5	Applications and systems must adhere to SOM Policy 1350.10 regarding "Access to	Yes			The proposed solution adheres to the State of Michigan Policy 1350.10 regarding "Access to Networks, Systems, Computers, Databases, and Applications".

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
	Networks, Systems, Computers, Databases, and Applications": http://www.michigan.gov/documents/dmb/1350.10_184594_7.pdf				The solution is designed to support/scale-up to support the technical methods listed in the policy document. Contractor will work with the State to select the required profile associated with the in scope resources and will accordingly define the required level of security.
1008.6	Applications and systems must adhere to SOM Policy 1350.20 regarding "Access to Protected Data Resources": http://www.michigan.gov/documents/dmb/1350.20_184600_7.pdf	Yes			Our proposed solution leverages IBM's Identity Manager and Access Manager, which provides functionality to establish, document, and manage the allocation of user access rights for individuals accessing State information technology resources to prevent inadvertent and inappropriate access to resources not authorized for the individual user as identified in the State of Michigan policy 1350.20.
1009.1	Application server software components will operate the same, without regard to the hosting platform or OS. They should expose the same functionality and API's regardless of OS.	Yes			Our solution is planned to be deployed on Red Hat Enterprise Linux operating system. However, it can run on other supported OS which will provide the same functionality. The APIs are OS agnostic and are cross-platform functional, compatible and interoperable.
1009.2	Application server software component updates will occur at the same time without regard to the hosting platform or OS, unless an exception is granted.	Yes			Software updates will be planned and released to meet this requirement. The patch management process would be included in the maintenance phase of the SDLC.
1009.3	The application tier will be certified for use with the VMWare x86 based virtualization platform.	Yes			IBM WebSphere Application Server is certified on RHEL OS which in-turn is certified on VMWare x86 based virtualization platform.
1009.4	Systems running on the application server will support **horizontal** scaling.	Yes			The proposed solution uses IBM WebSphere application server, which supports horizontal scaling.
1009.5	Systems running on the application server will support **vertical** scaling.	Yes			The proposed solution uses IBM WebSphere application server, which supports vertical scaling.
1009.6	Any job scheduling functions should be able to integrate with the following job scheduling agents: • Tidal 3.0, 5.x, 6.x		B		The project team may likely have to develop the scheduling scripts for integrating IBM WebSphere with the scheduling software directly. However, we do not foresee a need of scheduling a job related to Application Server functionality.

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
	(standard) • OpCon XPS 3.31.x, 4.x (standard) • BL/Sched 5.x (standard) • GECS 3.6, 4.0 (standard) • HAPS 1.7 (standard) • CA Auto Sys 4.5.x, r11 (standard) • Zeke 5.3.x, 6.0 (standard) • UC4 5.0, 6.0, 8.0 (standard)				
1009.7	End-user software applications, or components thereof, must **not** require privileged, super-user or administrator mode in order to function properly.	Yes			The End-user software application deployed on IBM WebSphere application server does not require privileged, super-user or administrator mode in order to function properly.
1009.8	The system must provide some form of remote connectivity which allows vendor acceptable bandwidth and access to facilitate remote diagnostics, monitoring and upgrading of the system. The form will be one that is acceptable to SOM and agreed to by SOM and the vendor.		B		MICAM components are deployed on UNIX based system and can be remotely diagnosed, monitored and upgraded using SSH. We can work with the State to define access restrictions and access level to the system.
1009.9	The application server must support the following Server Operating Systems (OS): • Linux Red Hat Enterprise Server 5.x (standard) • Linux Suse Enterprise 10.x (standard) • Microsoft Windows 2008 (standard) • UNIX HPUX 11i v3 (standard) • UNIX Sun Solaris 10.x (standard)	Yes			The proposed solution uses IBM WebSphere Application Server (WAS) version 7.0 and above. The list of supported Operating Systems (OS) is continuously updated. Currently following OS are supported: • Linux Red Hat Enterprise Server 5.x (standard) • Microsoft Windows 2008 (standard) • UNIX HPUX 11i v3 (standard) • UNIX Sun Solaris 10.x (standard) The WAS version 7.0 does not support the O/S versions Linux Suse Enterprise 10.x (standard) and VMWare vSphere 5

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
	• VMWare vSphere 5 (standard)				(standard). Linux Suse Enterprise 10.x (standard) is end of life but WAS 7.0 supports the newer version of Linux Suse Enterprise 11.x
10. Database Server- If the solution includes a database server the following requirements apply:					
1010.1	The database application software must support current multiple operating systems including Windows Server, Linux, and either Solaris or HP-UX per the State of Michigan EA Road map. Components of this architecture may run as appliance devices as required.	Yes			The MICAM solution is designed leveraging industry standard operating systems and virtualization technology. As such, the solution is designed with components that can be configured for high-availability and fail-over capabilities technologies. Contractor with work with the State to further develop the architecture per the State's EA Road map in the requirements phase of the project.
1010.2	The database tier will be certified for use with the VMWare x86 based virtualization platform.	Yes			IBM DB2 is certified on RHEL OS which in-turn is certified on VMWare x86 based virtualization platform
1010.3	The application must use the following database management systems (DBMS) and version: • MSSQL Server 2005 (standard) • MySQL 5.0 & 5.1 (standard) • Oracle 11g (standard) • TeraData A28V2R6.2 (standard)		A		The proposed MICAM solution used IBM DB2 database. We have proposed DB2 because DB2 integrates effectively and is packaged with other IBM products such as IBM Security Identity Manager. IBM Security Identity Manager also supports Oracle database. Hence if the State prefers to go ahead with Oracle databases, we can work with the State to use Oracle database for MICAM solution.
1010.4	The database server will support **horizontal** scaling by partitioning of tables and clustering of server instances.	Yes			DB2 supports horizontal scaling (also called scale out). DB2 manages (coordinates) the processing across database partitions and presents the database to the user or application as if it were a single database.
1010.5	The database server must support log shipping to a separate log server. State of Michigan should have near real time access to all log files.	Yes			DB2 Database server provides the support to place the log files and traces to a separate log server. DB2 provides the DB2 diagnostic tool "db2diag" for managing the log files. We will work with the State during the design phase of the project to decide the access permissions on the log files.
1010.6	The database server will support replication and mirroring across	Yes			MICAM solution uses IBM DB2 as the underlying database and DB2 OOTB supports replication and mirroring across

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
	multiple servers.				multiple servers.

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
1010.7	The database server shall support flashback capabilities for database, table, etc. for rapid recovery.	Yes			The MICAM solution uses DB2 technology OOTB which provides equivalent “Flashback” capability in the “DROPPED TABLE RECOVERY” of the “CREATE TABLE” clause.
1010.8	The database server must support **vertical** scaling by the addition of additional CPUs, CPU Cores, and RAM memory.	Yes			DB2 supports vertical scaling, also referred as scale up. It allows addition of the CPUs, CPU Cores, and RAM memory. It can make use of the additional computing resources to increase the processing capacity.
1010.9	The database server will support data compression.	Yes			The DB2 Storage Optimization feature gives the ability to transparently compress data on disk in order to decrease disk space and storage infrastructure requirements.
1010.10	The database server shall support table and index partitioning across multiple server instances.	Yes			DB2 database server supports table and index partitioning across multiple server instances and presents the database to the user or application as if it were a single database.
1010.11	The database server shall support parallel indexing operations.	Yes			DB2 database server supports when creating indexes and when maintaining indexes as the underlying data changes. The ability to create and maintain indexes in parallel applies to both the traditional binary radix and encoded vector index structures.
1010.12	The database server will support manual tuning and configuration.	Yes			DB2 database server provides tools and scripts to support manual tuning and configuration. DB2 gives the mechanism to do so using the GUI as well as command line interface.
1010.13	The database server will support automatic tuning and configuration.	Yes			DB2 server provides support for automatic tuning and configuration. It also provides scripts to perform the automatic tuning and configuration post installation.
1010.14	The database tier must support a shared connection with connection pooling.	Yes			DB2 uses connection pooling to maintain open connections to the database in a readily accessible pool.

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
1010.15	The database will support single-record recovery processes.	Yes			DB2 has utilities that can be used to recover an entire table space, index space, a partition or data set, pages within an error range, or a single page.
1010.16	The database must support transactions and support transaction rollback.	Yes			DB2 supports transactions and supports transaction rollback. DB2 uses "*savepoint*", named entity that represents the state of data at a particular point in time during a transaction. DB2 has ROLLBACK statement to back out changes only to a "*savepoint*" within the transaction without ending the transaction.
1010.17	The database must support encryption at the database table/column level.	Yes			DB2 has encryption functions that provide a simple way to encrypt the sensitive data. These functions can be used to implement column and row-column level encryption. DB2 can store encryption password hints to help with forgotten encryption passwords.
1010.18	The database must restrict access to data through the use of views, queries, roles and groups.	Yes			DB2 has the capability to restrict access to data through the use of views, queries, roles, and groups.
1010.19	The database will provide data archival functionality.	Yes			DB2 provides the tools called "Data Archive Expert" for archiving the data.
1010.20	The database will support assured record destruction by secure and permanent record deletion.	Yes			DB2 supports secured and permanent record destruction and once deleted the data is completely unavailable, so that a ROLLBACK statement cannot return the data.
1010.21	The database must be able to operate in an n-Tier server architecture.	Yes			The primary solution components support n-tier architectures.
1010.22	The database structure will be extensible, allowing the addition of new tables, new columns and new objects.	Yes			DB2 supports the extension of the databases. It allows the addition of new tables, new columns and new objects.

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
1010.23	The database must support pessimistic and optimistic record-locking strategies.	Yes			DB2 supports enhanced optimistic locking and pessimistic record locking strategies. With optimistic concurrency control, the database manager releases the row or page locks promptly after a read operation.
1010.24	The database will support table and row level locking during read/write operations.	Yes			DB2 supports both row-level locking and table-level locking during read/write operations.
1010.25	The database server shall support heterogeneous cross-DBMS and distributed transactions.	Yes			DB2 supports cross DBMS transactions and distributed transactions.
1010.26	The database transaction strategies must be configurable, allowing growth, shrinkage and backup-recovery.	Yes			DB2 supports configurable transaction strategies in the distributed database model using DB2 transaction manager or a XA compatible transaction manager.
1010.27	The database will not require components that are not part of the default database licensing model for supporting any functionality.	Yes			MICAM solution uses DB2. The solution does not require components that are not part of the default database licensing model for supporting the proposed functionality except for the spatial data support (requirement 1010.29). However, as part of the MICAM solution the support for spatial data would not be required.
1010.28	The database will allow full text indexing and search.	Yes			DB2 Text Search is an integrated component of DB2. It provides the following features: • Full text search in text, HTML, and XML documents, including Boolean and wildcard search • Fully integrated SQL, SQL/XML, and XQuery support, including XPath syntax subset to search XML documents • Linguistic processing with optional synonyms definition • Asynchronous index update with scheduling option
1010.29	The database will provide support for spatial data.	Yes			An additional component called "DB2 Spatial Extender" is required to support spatial data.

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
1010.30	The database will provide support for XML data.	**Yes**			DB2 has native XML data type, which provides the ability to store well-formed XML documents in the database alongside other relational data. XML data is stored in the database in the UTF-8 code set. XML documents can be inserted, updated and deleted using SQL data manipulation statements.
1010.31	The database server must support the following application development frameworks: (see section 1004.3- Product Development)	Yes			Contractor will work with the State to provide a detailed testing plan and perform solution testing in accordance with the State of Michigan SUITE/SEM methodology. Please refer to comments in section 1004.3 for more information.
1010.32	The database server must support auditing and logging for DML events (insert, update, delete). State of Michigan should have near real time access to all log files.	**Yes**			DB2 auditing facility generates and allows a DBA to maintain an audit trail for a series of predefined database events. We will work with the State during the design phase of the project to identify the required access restrictions on these auditing and log files.
1010.33	The database server must support auditing and logging for DCL events (grant, revoke, deny). State of Michigan should have near real time access to all log files.	**Yes**			DB2 auditing facility generates and allows a DBA to maintain an audit trail for a series of predefined database events. We will work with the State during the design phase of the project to identify the required access restrictions on these auditing and log files.
1010.34	The reporting product technology must be compatible with n-Tier architecture (client-server & web).	**Yes**			Our proposed solution includes IBM's identity and access management technology. IBM's Tivoli Common Reporting (TCR) which is based on Eclipse Business Intelligence and Reporting Tools (BIRT) that follows the JSR 168 portal standard. JSR 168 defines a 2 tier architecture with a "portal tier" responsible for lay out, security and navigation and a "Portal/Widget Tier" for the hosting application.

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
1010.35	The database must not require users to have elevated database privileges/accounts for normal operation.	Yes			DB2 has the capability to define different access levels. It can be configured not to require users to have elevated database privileges/accounts for normal operations.
1010.36	The database server will support licensing per CPU core.	Yes			DB2 can be licensed using the Processor Value Unit (PVU) processor model (also known as per capacity pricing). It is a pricing metric where the total PVU rating of the underlying server is derived and multiplied by the DB2 per-PVU price to determine the eventual license costs.
1010.37	The database server will support licensing per CPU socket.	Yes			DB2 can be licensed using the Processor Value Unit (PVU) processor model (also known as per capacity pricing). It is a pricing metric where the total PVU rating of the underlying server is derived and multiplied by the DB2 per-PVU price to determine the eventual license costs.
1010.38	The database server will support licensing per seat.	Yes			DB2 can be licensed using the authorized-user model. This licensing is derived by counting number of users that will be using DB2 and multiplying that number by a per-user price to determine your license costs.
1010.39	Audit record must contain: date and time of the event, subject identity, type of event, how data changed, where the event occurred, and the outcome of the event.	Yes			DB2 provides logging and auditing capabilities. The audit record will contain the information that is identified in this requirement when enabled.
1011. Web Server					
1011.1	The Web server will support the following Operating Systems (OS): • (see requirement 1009.9)	Yes			Our proposed solution uses IBM HTTP Server (IHS) web server. IHS supports Server Operating systems in requirement 1009.9.

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
1011.2	The Web Server components will operate the same without regard to the hosting platform or OS.	Yes			Our solution is planned to be deployed on Red Hat Enterprise Linux operating system. However, it can run on other supported O/S's which will provide the same functionality.
1011.3	The Web Server component updates will occur at the same time without regard to the hosting platform or OS.	Yes			Software updates will be planned and released to meet this requirement.
1011.4	The web server for this application will be: • MS IIS 2003, 2008 (standard) • Apache 2.2.x (standard) • IBM IHS 6.1, 7.0 (standard) • IBM WebSphere 6.1, 7.0 (standard) • Jboss 5.x (standard)	Yes			The proposed solution uses IHS and IBM WebSphere. The actual version of web server used for this solution will be decided at the time of planning and analysis of the project working with the State team.
1011.5	The application will be capable of sharing a web server with multiple applications.	Yes			The application will be capable of sharing a web server with multiple applications.
1011.6	The Web Server will support **horizontal** scaling.	Yes			Our proposed solution uses IBM IHS Web Server, which supports horizontal scaling.
1011.7	The Web Server will support **vertical** scaling.	Yes			Our proposed solution uses IBM IHS Web Server, which supports vertical scaling
1011.8	The application tier will be certified for use with the VMWare x86 based virtualization platform.	Yes			IBM IHS is certified on RHEL OS which in-turn is certified on VMWare x86 based virtualization platform.
1011.9	The application will support clustering and/or load balancing across several servers.	Yes			The application supports clustering and/or load balancing across several servers. Vertical as well as horizontal clustering is supported.
1011.10	The reporting product technology will be compatible with n-Tier architecture (client-server & web).	Yes			Our proposed solution includes IBM's identity and access management technology. IBM's Tivoli Common Reporting (TCR) which is based on BIRT that follows the JSR 168 portal standard. JSR 168 defines a 2 tier architecture with a "portal tier" responsible for lay out, security and navigation and a "Portal/Widget Tier" for the hosting application.
1011.11	The application will support rendering through the following	Yes			Contractor will work with the State to define the functionality that is required to be rendered in the designated portal

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
	portal implementations: • IBM Web Content Management 6.x (standard) • IBM WebSphere Portal 6.x (standard)				implementations and develop standards based integration points.
1012. Solution Architecture					
1012.1	The application's minimum technology requirements, including Operating System (OS) versions, vendor versions, and release level of each product, will be provided.	Yes			The proposed application landscape and infrastructure will leverage common off-the-shelf (COTS) products with minimally required customization. Common components include: • Windows Server 2008 • Red Hat Enterprise Linux (RHEL) • IBM Security Access Manager (ISAM) • IBM Security Identity Manager (ISIM) • IBM WebSphere IBM DataPower SOA Appliances • IBM Tivoli Federated Identity Manager (ITFIM) • IBM Tivoli Directory Integrator (ITDI) • IBM Tivoli Directory Server (ITDS) • IBM DB2 Database Enterprise Server Edition (ESE) • IBM Tivoli Common Reporting (ITCR) • VMWare vSphere Server • IBM AIX
1012.2	A detailed network/server diagram must be provided illustrating the relative architecture of the proposed system. It must include: • Network security zones and firewalls • Server types and network components (e.g., switches) • Ports and protocols used to cross security zones • How users will access the system • Clustering of servers	Yes			Detailed network and server diagrams will be developed as part of the requirements phase.
1012.3	The solution/application must use the features and capabilities of the SOM enterprise data storage services for the	Yes			The MICAM solution has been designed leveraging industry standard operating systems and virtualization technology, as such, the solution is compatible with SAN, NAS and CAS technologies. Contractor will

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
	following data storage needs: • Storage Area Network (SAN) • Network Attached Storage (NAS) • Content Addressable Storage (CAS)				work with the State to develop the storage architecture in the requirements phase of the project.
1012.4	The solution/application must support installation and operation in one or more disparate hosting centers. Fail-over from one hosting center to another must be possible without exceeding parameters specified in the Service Level Agreement (SLA).	Yes			The MICAM solution has been designed leveraging industry standard operating systems and virtualization technology, as such, the solution is designed with components that can be configured for high-availability and fail-over capabilities technologies. Contractor with work with the State to further develop the architecture per the SLA in the requirements phase of the project.
1012.5	A Service Level Agreement (SLA) must be in effect for the solution/system specifying, at a minimum, the following: • Criticality Level (Critical, High, Medium) • Recovery Point Objective (time in hours) • Recovery Time Objective (time in hours)	Yes			Contractor with work with the State to further develop the architecture and SLAs in the requirements phase of the project.
1012.6	The solution/application will support distributed deployment of application components and database tier components (n-Tier architecture).	Yes			The primary solution components support n-tier architectures.
1012.7	The solution/application must have an approved Enterprise Architecture (EA) Solution Assessment, prior to production.	Yes			
1012.8	Provide a technology roadmap for the proposed system showing a five (5) year plan for migrating to new software versions and when to de-implement dated versions as they reach	Yes			The proposed MICAM solution utilized IBM COTS based security products. IBM provides roadmaps, migration plans and published support lifecycles for their products. If required, Contractor will assist in developing an additional high-level technology roadmap in the Planning phase of the project.

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
	end of life.				

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
1012.9	Provide conceptual and logical application data-flow models.	Yes			Contractor will develop conceptual and logical application data-flow models in the Requirements phase of the project.
1012.10	Provide a logical network diagram that describes how the infrastructure components will meet the functional requirements.	Yes			Contractor will develop logical network diagram and a functional requirements mapping matrix in the requirements phase of the project. A high-level architecture diagram is provided in *Attachment 3 - Solution Narrative*.
1012.11	Provide a technology roadmap for the proposed system showing a five (5) year plan for new software version releases, support window, and sun setting.	Yes			The proposed MICAM solution utilized IBM COTS based security products. IBM provides roadmaps, migration plans and published support lifecycles for their products. If required, Contractor will assist in developing an additional high-level technology roadmap in the planning phase of the project.
1012.12	Provide a high-level architecture diagram, including logical and physical components.	Yes			
1012.13	Systems operating on an application server must interoperate with CA Unicenter monitoring agents.		B		Solution components that reside on application servers require functional levels of WebSphere 7.0 or 8.0. The current CA Unicenter Management for WebSphere (r3.6) does not support the proposed configuration. Scripts will be developed to integrate with the Unicenter NSM Script Agent to monitor status of the applications and application servers.
1012.14	Systems operating on an application server must interoperate with Veritas Backup and Recovery agents.	Yes			The MICAM solution leverages industry standard operating systems and virtualization technology, which are compatible with Veritas Backup and Recovery agents.
1012.15	The reporting product technology will be compatible with n-Tier architecture (client-server & web).	Yes			See response to 1005.1.
1013. Solution Integration					
1013.1	System integration will support the following method(s): • API • Web Services • SOAP • ODBC	Yes			The MICAM solution will be designed to support API's, Web Services, SOAP, ODBC, JDBC, REST and Plug-Ins. Typically IBM Tivoli Directory Integrator (ITDI) and will be used to create custom adapters since ITDI provides a rich set of connectors to connect to various data sources and targets. Contractor will work with the State to further refine and define

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
	• JDBC • REST • Plug-Ins				the integration methods and standards in the Requirements phase of the project.
1013.2	An Enterprise Application Integration (EAI) solution must be provided to the following services: • MQ Series (standard) • WebSphere (standard) • Message Broker (standard) • JMS	Yes			The MICAM solution will be designed to support and integrate with MQ Series, WebSphere ESB, WebSphere Message Broker and the JMS API Standard.
1013.3	An Application Programming Interface (API) will be supplied and supported for the following technologies: • Java (standard) •.NET (standard)	Yes			The proposed COTS identity and access management components provide an OOTB API to Java and Web Services. Components that do not natively provide a.NET API can use Web Services for interoperability.
1013.4	Bidder must provide pre-defined connector(s) to the following industry standard data source(s): • Oracle • PeopleSoft • Microsoft • SAP • Active Directory • Standard LDAP • IBM Tivoli security products	Yes			The proposed MICAM solution is designed around IBM Security Identity Manager which includes OOTB provisioning adapters and support for Oracle, PeopleTools, Microsoft Active Directory, SAP NetWeaver, LDAP, and other IBM Security Products.
1013.5	Provide a method to import data from proprietary sources.	Yes			IBM Tivoli Directory Integrator (ITDI) will be used in the solution to provide basic extract, transform and load (ETL) for importing data from across multiple proprietary, identity or generic data resources.
1013.5	System integration will support integration to DTMB services such as SQL server reporting services (SSRS) and SQL Server Integration Services (SSIS)	Yes			Microsoft SQL Server Reporting Services (SSRS) supports DB2 with Microsoft OLE DB Provider for DB2. SQL Server Integration Services (SSIS) supports DB2 integration using the Microsoft OLE DB Provider for DB2.
1013.6	Connectivity to the following relational	Yes			IBM Tivoli Directory Integrator (ITDI) will be used in the solution to provide basic

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
	database(s) must be provided and supported: • (see section 1011.5)				extract, transform and load (ETL) for importing data from a myriad of JDBC, JDBC-ODBC and JNDI compliant RDMBS data sources.
1013.7	The solution must be able to import and export data to and from the following external source(s): • Current Standard versions of Microsoft Office	Yes			IBM Tivoli Directory Integrator (ITDI) will be used in the solution to provide basic extract, transform and load (ETL) for importing data from Microsoft Office data sources including Access and Excel.
1013.8	The ability to export data in the following output formats must be available: • EDI • HTML • XML • Text file • CSV •Delimited, configurable	Yes			In addition to the OOTB functionality in the proposed applications, IBM Tivoli Directory Integrator (ITDI) will be used in the solution to provide basic extract, transform and load (ETL) for exporting data to various systems as required.
1013.9	The reporting product technology must be compatible with n-Tier architecture (client-server & web).	Yes			See response to 1005.1.
1014. System Administration and Licensing					
1014.1	Software licensing will be inclusive for all packages included in the solution, unless explicitly listed and detailed.	Yes			Contractor acknowledges this requirement. Please refer to *Appendix A - Breakdown of Hardware and Related Software* for details.
1014.2	Application/System documentation will provide access to FAQ and/or Support Information for frequent issues administrative staff may encounter.	Yes			The proposed MICAM solution uses IBM security products. IBM maintains information sites with extensive documentation for these products covering installation, configuration, administration, security, performance, troubleshooting and support. In addition, the installed products provide contextual help information. For post-production MICAM administration, operation and maintenance, Contractor will also develop an Operations Manual that will provide instructions for system monitoring, troubleshooting, and other administration tasks such as start/stop and backup procedures.

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
1014.3	Documentation will indicate recommended staffing requirements to administer and support the system.	Yes			During MICAM project Initiation and Requirements Definition phase, Contractor will work with the State to finalize project roles and responsibilities, for example: • Project Manager • Identity and Access Management (IAM) Analyst • IAM Specialist • IAM Administrator • Database/Directory Administrator • Server Administrator • Help Desk • Change Request Committee The Operations Manual will also contain the roles responsible for MICAM solution administration and maintenance.
1014.4	Documentation will provide backup/recovery information using the SOM Veritas solution, including information on hot/online backups.	Yes			Contractor will work with the State to document the backup/recovery procedures and other related details using the State's Veritas solution, during Construction and Implementation phases.
1014.5	A system maintenance window will be designed into the application which will allow the system to be taken off-line for updates, upgrades and maintenance.	Yes			The proposed MICAM solution will be designed to reduce the offline maintenance requirement. Contractor will work with the State to define a maintenance window for MICAM, considering various factors such as existing State maintenance schedule, period of low application usage, and availability of staff.
1014.6	Documentation describing how to take the system off-line for maintenance, updates and upgrades will be provided.	Yes			For post-production MICAM administration, operation and maintenance, Contractor will develop an Operations Manual that will provide instructions on monitoring, upgrades, start/stop, and backup procedures for MICAM solution components.
1014.7	Documentation will describe the level of effort and anticipated downtime for product upgrade installation.	Yes			The proposed MICAM solution consists of COTS IBM security products. The proposed product versions are listed in *Appendix A - Breakdown of Hardware and Related Software*. IBM sends out communication to registered users when a new fix pack is released for the security products. The Operations Manual will provide details on the upgrade process for fix packs application. During post-implementation,

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
					Contractor will periodically evaluate new applicable fix-packs and work with the State to prepare a plan with the dependencies, efforts, and schedule details.
1014.8	Documentation will provide the anticipated frequency and requirements of patches (releases, break-fix, 0-day), minor, and major releases.	Yes			The proposed MICAM solution consists of COTS IBM products. IBM regularly publishes and sends notifications for new fix-packs and versions available for download and use. The proposed Operations Manual will provide information on system monitoring tasks and frequency (daily, weekly, monthly, ad hoc as required, etc.) the Operations Manual will also include tasks for monitoring various resources for new releases, fix-packs/patches for the COTS IBM products.
1014.9	Documentation will provide information on certification/compatibility with OS patches, Service Pack, and upgrade paths.	Yes			Contractor will provide the applicable pre-requisites and compatibility details for an effective and supported MICAM solution prior to the Construction phase and during post-implementation.
1014.10	Documentation will address upgrade paths and procedures for each component/tier.	Yes			The Operations Manual will provide these details.
1014.11	Provide a complete configuration and set-up documentation library.	Yes			Contractor will provide detailed documentation on build, configuration, administration, and maintenance of the MICAM solution. These documents will be developed during the Construction and Implementation phases.
1014.12	System documentation will clearly describe any special requirements (such as middleware, Operating System (OS), hardware, etc.) that could affect the capabilities or performance of the system.	Yes			The build/installation document developed during the Construction phase will include details on the Hardware, OS, network, and middleware (e.g., Application Server, Database, Directory/LDAP) pre-requisites for an effective and supported MICAM solution installation.

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
1014.13	System documentation will clearly describe all critical factors in sizing or configuring the application (e.g., number of concurrent users, specific transaction volumes, number of products, number of layers in the product hierarchy, etc.).	Yes			Contractor will provide documentation on sizing considerations and performance tuning based on IBM's sizing guidelines.
15. System Performance					
1015.1	The application will provide performance-optimization capabilities.	Yes			The proposed MICAM solution uses IBM security products that will be sized appropriately and configured for performance optimizations.
1015.2	The application will have the capability to handle large-volume batch processing via multi-threading.	Yes			The proposed MICAM solution uses COTS IBM security products that will be designed to handle large-volume data processing.
1015.3	The application will maintain optimum performance over both Wide Area Network (WAN) and Local Area Network (LAN).	Yes			The MICAM solution will be designed and configured to function with required performance for server and network level communications. The MICAM performance requirements will be met for both internal and external users.
1015.4	The application will maintain optimum performance over Local Area Network (LAN).	Yes			The MICAM solution will be designed and configured to function with high-quality performance for server and network level communications. The MICAM performance requirements will be met for both internal and external users.
1015.5	System documentation will clearly describe all versions of the package that are deployed for different scaling situations.	Yes			The build document developed during the Construction phase will describe the versions and pre-requisites of the deployed MICAM solution components.
1015.6	System documentation will clearly describe any special requirements (such as middleware, Operating System (OS), hardware, etc.) that could affect the capabilities or performance of the system.	Yes			The proposed MICAM solution will be designed to meet the performance requirements through replication, clustering, least functionality, and other design considerations. In addition, the build/installation document developed during the Construction phase will include details on the Hardware, OS, network, and middleware (e.g., Application Server, Database, Directory/LDAP) pre-requisites and performance tuning configuration for MICAM solution.

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
1015.7	The application will integrate with the CA Unicenter for capacity and performance monitoring.	Yes			As we understand, the CA Unicenter does not integrate with IBM security products that are proposed for MICAM solution. Contractor will work with the State to develop the integration for capacity and performance monitoring in both MICAM and CA Unicenter solutions.
1015.8	System documentation will clearly describe what support will be provided to the State for performance optimization activities.	Yes			
1015.9	System documentation will clearly describe the type of caching, if any, the system employs.	Yes			The technical design document developed during the Design phase will describe the caching approaches for MICAM solution components, such as IBM Security Access Manager ACLs and policies caching, IBM Security Identity Manager configuration properties caching, and IBM WebSphere Application caching.
1015.11	System documentation will clearly describe all activities that affect optimum performance such as service recycling, rebooting, or batch jobs and their frequency.	Yes			The Build/Installation document and Operations Manual will provide details on performance tuning configurations and activities.
1015.12	The system must meet performance benchmark times for: • Page refresh in under three seconds • Database query execution in under two seconds	Yes			The proposed MICAM solution will be designed to meet the performance requirements. During the Construction and Testing phases, the MICAM solution will be configured and tested to meet the performance benchmarks.
1016. Application Configuration Management – (PCI-DSS)					
1016.1	All known security vulnerabilities must be addressed in accordance with industry-accepted system hardening standards. Industry-accepted standards include: • SysAdmin Audit Network Security (SANS) • National Institute of	Yes			Contractor acknowledges this requirement. The MICAM solution system will be appropriately hardened following the security principle of least functionality and adhering to SANS, NIST, PCI, CIS, and other applicable standards. In addition, the MICAM hosting services include regular vulnerability assessment, penetration testing, and anti-virus scanning with a structured and consistent process to manage the security issues. The steps followed as part security issue management process are Detect, Triage,

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
	Standards Technology (NIST) • Center for Internet Security (CIS)				Respond, Contain, Forensics & Recover, Document & Notify, and Risk Mitigation.
1016.2	Only one primary function can be implemented per server (i.e. web, database, domain, etc.).	Yes			The proposed MICAM solution will be designed to sufficiently segregate the solution functionality per server. For example, IBM Security Identity Manager 6.0 (ISIM) and IBM Security Access Manager for Web 7.0 (ISAM) components will have their own dedicated servers that will not be shared or used with other applications. •
1016.3	All unnecessary and unsecure services and protocols (those not directly needed to perform the device's specified function) are disabled.	Yes			The proposed MICAM solution will be designed and configured following the principle of least functionality. The MICAM servers and network will be appropriately hardened.
1016.4	System security parameters must be configured to prevent misuse (see 1017.1 for guidance).	Yes			
1016.5	All unnecessary functionality is removed, such as: • Scripts • Drivers • Features • Subsystems • File Systems • Unnecessary Web Servers	Yes			The proposed MICAM solution will be designed and configured following the principle of least functionality. The MICAM servers and network will be appropriately hardened.
1016.6	System changes are monitored and security impact analyses are performed to determine the effects of the changes.	Yes			Contractor will follow the approved change management process. Contractor will work with the State to review and update the process, as required.
1017. Application Development Management – (PCI-DSS)					
1017.1	Software applications must be developed in accordance with PCI DSS (for example, secure authentication and logging) and based on industry leading	Yes			It is our understanding that there is no specific requirement in RFP to store or process PCI data in the MICAM solution. However, we acknowledge that the PCI-DSS is one of the State's baseline business requirements and MICAM

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
	practices. Information security must be incorporated throughout the Systems Development Life Cycle (SDLC). State of Michigan will have near real time access to all log files.				solution will adhere to the PCI-DSS standard requirements. The MICAM hosting services will adhere to PCI and other security standards, using security design, processes and technologies such as segmented networks (security zones, VLANs), firewalls and routers, encryption of sensitive data-in-motion, authentication, logging of security events, anti-virus software, vulnerability assessments, and penetration testing. The proposed MICAM solution consists of COTS IBM Security products. The MICAM solution will be designed and configured to: Change the default system/application passwords Disable unnecessary services and ports Assign a unique user ID to each user of the MICAM solution Restrict access to MICAM systems based on the least privileges principle. Contractor will work with the State to define appropriate roles and identify authorized the State's staff to provide required access to the MICAM systems, log files and data.
1017.2	All security patches and system and software configuration changes must be tested before deployment, including but not limited to: •All input must be validated to prevent such things as cross-site scripting, injection flaws and malicious file execution. • Proper error handling must be incorporated into the software. • Data at rest must use secure cryptographic storage. • Data in motion must use secure communications. • Role-based access control (RBAC) must be used to control and audit user actions.	Yes			The proposed MICAM solution includes COTS IBM security products. The MICAM solution will be designed, developed and implemented to meet the applicable security requirements, such as: • Build an Identity credential and access management system for workers and citizens • Protect sensitive data (data-at-rest and data-in-motion), where applicable • Implement strong identity, authentication, and access control • System and communication protection In addition, proposed changes or security patches to the MICAM system will be analyzed and tested in development environment, before deployment in production environment.
1017.3	There must be separate development, test and production	Yes			The proposed MICAM solution will be deployed in following four environments:

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
	environments.				1. Production 2. QA/Staging 3. Development 4. Sandbox
1017.4	There must be separation of duties between development, test and production environments.	Yes			Contractor will work with the State to define access roles and separation of duties rules for MICAM system access in production and non-production environments.
1017.5	Production data are not used for testing or development purposes.	Yes			Contractor will work with the State to define the production grade test data for Integration Testing and User Acceptance Testing. The test data will be either custom generated or sufficiently altered and sanitized if leveraged from Production environment.
1017.6	All test data and accounts must be removed before production systems become active.	Yes			During Testing and Implementation phases, the test data loaded in the Production systems will be appropriately planned and tracked. During the pre-cutover activities, the Production systems will be cleansed to remove the test data created/loaded.
1017.7	All custom and developer accounts, user IDs, and passwords must be removed before applications become active or are released to agencies.	Yes			During Testing and Implementation phases, the test and developer user accounts created in the Production systems will be appropriately planned and tracked. During the pre-cutover activities, these user accounts will be completely removed from the Production systems.
1017.8	A code review must be performed of custom code prior to release to production or agencies, in order to identify any potential coding vulnerabilities.	Yes			The proposed MICAM solution consists of COTS IBM Security products. Contractor will use secure SDLC (Software Development Life cycle) to confirm that new vulnerabilities are not introduced in the system during development of custom IAM components. The secure coding practice, secure code review, and security testing are an integral part of the SDLC. Some of the secure coding guidelines include input validations before processing, error handling, and logging. As described in the section “Software Development – Salient Features” of the *Attachment 11 – Preliminary Software Development Plan*, Contractor will perform number of security related activities at

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
					different phases of MICAM implementation life cycle. During the construction phase, Secure Code Reviews will be performed for custom developed components.
1017.9	All web applications (internal, external, and web administrative access to applications) must be developed based on secure coding guidelines such as the *Open Web Application Security Project Guide.* http://www.owasp.org	Yes			The proposed MICAM solution includes leading security products from IBM. Contractor will use secure SDLC (Software Development Life cycle) to confirm that new vulnerabilities are not introduced in the system during development of custom IAM components. The secure coding practice, secure code review, and security testing are an integral part of the SDLC. Some of the secure coding guidelines include input validations, error handling, and logging. In addition, the MICAM solution will use security technologies such as firewalls, IPS/IDS, logging, encryption, anti-virus scan, vulnerability assessments, and implement security controls around authentication, authorization, session management, and encryption.

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
1017.10	Prevention of common coding vulnerabilities must be covered in software development processes, including: • Cross-side scripting (XSS). • Injection flaws, particularly SQL injection. Also consider LDAP and Yespath injection flaws. • Malicious file execution. • Unsecure direct object references. • Cross-site request forgery (CSRF). • Information leakage and improper error handling. • Broken authentication and session management. • Unsecure cryptographic storage. • Unsecure communications. • Failure to restrict URL access.	Yes			The proposed MICAM solution includes leading security products from IBM. Contractor will use secure SDLC (Software Development Life cycle) to confirm that new vulnerabilities are not introduced in the system during development of custom IAM components. The secure coding practice, secure code review, and security testing are an integral part of the SDLC. Some of the secure coding guidelines include input validations, error handling, and logging. In addition, the MICAM solution will use security technologies such as firewalls, IPS/IDS, logging, encryption, anti-virus scan, vulnerability assessments, and implement security controls around authentication, authorization, session management, and encryption.

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
1018. Application Password Management - (PCI-DSS)					
1018.1	Only DTMB approved personnel may add, delete, or modify user IDs, credentials, and other identifier objects on systems containing PCI data.	Yes			It is our understanding that there is no specific requirement in RFP to store or process PCI data in the MICAM solution. However, the proposed MICAM solution will be designed to adhere to the PCI-DSS requirement for strong access control measures, based on role based access control, principle of least privilege, individual User ID, strong password, and physical access restriction. During Functional Design and Construction phases, Contractor will work with the State to define access roles and identify authorized State personnel with access to the sensitive data.
1018.2	A user's identity must be verified before performing a password reset.	Yes			The proposed MICAM solution provides self-service password reset capabilities for users based on security questions and responses. Contractor will work with the State team to define the detailed requirements and processes for password reset functionality.
1018.3	First-time passwords must be set to a unique value for each user and each user change this initial password immediately upon first use.	Yes			The proposed MICAM solution provides capabilities to generate individual initial passwords based on configured password policy rules and can enforce password change on first login. Contractor will work with the State to define the detailed requirements and design.
1018.4	Access rights for any terminated user must be immediately revoked.	Yes			The proposed MICAM solution will be designed to support this requirement. Once a termination request is submitted in MICAM system either manually or through authoritative feed, the access rights of a terminated user will be revoked in near-real time on the applications managed by MICAM solution.
1018.5	Inactive user accounts must be removed or disabled at least every 90 days.	Yes			The proposed MICAM solution will be designed and configured to terminate user accounts that are inactive for 90 or pre-defined number of days. The terminated user accounts can be removed or disabled as per the requirement.

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
1018.6	All accounts used by vendors for remote maintenance must be enabled only during the time period needed and remain disabled otherwise.	Yes			The accounts used for remote maintenance will be enabled only for pre-defined approved tasks and will be managed by MICAM solution administrators.
1018.7	Password procedures and policies must be communicated to all users who have access to cardholder data.	Yes			Contractor will work with the State to define and communicate the password policies to users through either State security policies or display on the MICAM application screen or another medium.
1018.8	Group, shared, or generic accounts and passwords are prohibited.	Yes			The proposed MICAM solution will be designed for application accounts with single owner. In addition, the MICAM solution will be configured to disallow the concurrent user sessions.
1018.9	User passwords must follow State Enterprise Password Standards or specific system requirements, whichever are more restrictive.	Yes			The proposed MICAM solution will be designed to support the State's enterprise password standards. The MICAM solution will be configured to manage number of password parameters, such as length, complexity, pre-defined restrictions, history, and expiration. During the Requirements Specification phase, Contractor will work with the State to confirm the password requirements applicable for MICAM solution.
1018.10	All passwords lengths must follow Appendix F State Enterprise Password Standards or specific system requirements, whichever are more restrictive.	Yes			The proposed MICAM solution will be designed to support the State's enterprise password standards. During the Requirements Specification phase, Contractor will work with the State to confirm he password minimum and maximum length requirement applicable for MICAM solution.

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
1018.11	All passwords complexity must follow Appendix F State Enterprise Password Standards or specific system requirements, whichever are more restrictive.	Yes			The proposed MICAM solution will be designed to support the State's enterprise password standards. During the Requirements Specification phase, Contractor will work with the State to identify the password complexity requirement applicable for MICAM solution, such as number of upper and lower case characters, numbers, special characters, disallowed words or characters, etc.
1018.12	All password history must follow Appendix F State Enterprise Password Standards or specific system requirements, whichever are more restrictive.	Yes			The proposed MICAM solution will be designed to support the State's enterprise password standards. During the Requirements Specification phase, Contractor will work with the State to document the password history requirement applicable for MICAM solution.
1018.13	Password lock out rules must follow Appendix F State Enterprise Password Standards or specific system requirements, whichever are more restrictive.	Yes			The proposed MICAM solution will be designed to support the State's enterprise password standards. During the Requirements Specification phase, Contractor will work with the State to document the password lockout requirement applicable for MICAM solution.
1018.14	The user lockout duration must follow Appendix F State Enterprise Password Standards or specific system requirements, whichever are more restrictive.	Yes			The proposed MICAM solution will be designed to support the State's enterprise password standards. During the Requirements Specification phase, Contractor will work with the State to document the user lockout duration as applicable for MICAM solution. The solution supports both temporary and permanent lockout of user account after predefined number of failed login attempts.
1018.15	Idle/inactive Session locking must follow Appendix F State Enterprise Password Standards or specific system requirements, whichever are more restrictive.	Yes			The proposed MICAM solution will be designed to use one of the following information types to maintain session state with a client and follow the State's enterprise password standards: • SSL ID • Server-specific session cookie • Basic Authentication header data • HTTP header data • IP address The user specific session information maintained at the server side is used to manage the user state. This approach enables rapid response on the client browser, provides an additional layer of

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
					security by maintaining user state on the server side, and leaves business processing on the business layer.
1018.16	All access to any database containing cardholder data must be authenticated (this includes access by applications, administrators, and all other users.).	Yes			The proposed MICAM solution will be designed to adhere to the PCI-DSS requirement for strong access control measures, based on role based access control, principle of least privilege, individual User ID, strong password, and physical access restriction.
1018.17	A password cannot at any time be the same as a user ID.	Yes			The proposed MICAM solution will be designed to support the State's enterprise password standards. The solution will be configured to disallow use of user ID as the password.
1019. COTS Software					
1019.1	Commercial Off-the-shelf (COTS) third-party libraries included within the application must be owned and supportable by the State. Inclusion of any third-party code library or tool must be approved by the SOM Contract Manager or Project Manager.	Yes			The State will procure the required COTS software licenses listed in *Appendix A – Breakdown of Software and Related Hardware.*
1019.2	COTS software which handles credit card data or transactions must be certified to be Payment Card Industry - Data Security Standard (PCI-DSS) and PCI Payment Application - Data Security Standard (PA-DSS) compliant. Certification must be provided upon request.	Yes			It is our understanding that there is no specific requirement in RFP to store or process PCI data in the MICAM solution. However, we acknowledge that the PCI-DSS and PA-DSS are the State's baseline business requirements and MICAM solution will adhere to the PCI-DSS and PA-DSS standard requirements where applicable. The proposed MICAM solution consists of COTS IBM Security products. The MICAM solution will be designed and configured to: Change the default system/application passwords Disable unnecessary services and ports Assign a individual user ID to each user of the MICAM solution Restrict access to MICAM systems based on the least privileges principle. Contractor will work with the State to define appropriate roles and identify authorized State staff to provide required access to the MICAM systems, log files, and data.

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
1019.3	COTS software must have maintenance and support available from the developer, vendor or an approved 3rd party.	Yes			The proposed MICAM solution uses IBM security products that are supported by IBM.
1019.4	COTS software providers must make available for inspection the End User License Agreement (EULA) prior to purchase or contract signing.	Yes			The proposed MICAM solution uses IBM security products. EULA may be requested and inspected prior to purchase or contract signing.
1019.5	End User License Agreements (EULA) must be approved by DMB Purchasing or DTMB Enterprise Project Management Office prior to purchase or contract signing.	Yes			The State will review the EULA at the time of procurement of the required COTS software licenses listed in *Appendix A – Breakdown of Software and Related Hardware.*
1019.6	COTS software not already listed on the Enterprise Architecture Roadmaps must have an approved EA Solution Assessment completed prior to use or implementation.	Yes			The proposed COTS products listed in the section *Appendix A – Breakdown of Software and Related Hardware* is currently the existing technologies used by the State.
1020. Information Technology Network and Infrastructure					
1020.1	The information technology network and infrastructure must conform with SOM Policy 1345.00 regarding "Network and Infrastructure": SOM Technical Policies	Yes			The proposed solution adheres to State of Michigan Policy 1345.00 regarding “Information Technology Network and Infrastructure”.
1020.2	The solution must contain values for projected capacity and special needs requirements covering all aspects of data transport & security across the information technology network and infrastructure.	Yes			Contractor will provide documentation on sizing considerations and performance tuning.
1020.3	The solution must address projected capacity requirements for all aspects of the	Yes			Contractor will provide documentation on sizing considerations and performance tuning.

Req. No.	Technical Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
	information technology network and infrastructure.				

Appendix E: Functional Requirements

Functional requirements identify what the MICAM system must do to enable performance of work tasks and any Applicable Service Levels.

Bidder and bidder subcontractors are defined as Bidder. The Bidder's and all bidder subcontractors must comply with all State and Federal Policies and guidelines.

BIDDER RESPONSE INSTRUCTIONS:

The Bidder must respond whether or not their proposed solution complies with each requirement as follows:

1. *Check the box that applies to each requirement in the columns labeled:* ***Yes****,* ***Yes with Modifications****, or* ***No.***

   a. ***Yes*** *– is defined as the Bidder's solution complies with all aspects of the requirement and is currently a standard feature.*

      o *In the* ***comment box*** *the bidder may provide comments and descriptions on compliance, but are not required to.*

   b. ***Yes with Modification*** *– is defined as the solution does not currently comply with the requirement but the Bidder can modify the solution through configuration, programming or source code changes which, in the Bidder's opinion, would result in their solution reaching full compliance with a requirement. If a modification is required to the solution, fill in the column with* ***A****,* ***B*** *or* ***C*** *as defined below:*

      A. *Configuration required to comply with the requirement*
      B. *Programming required to comply with the requirement*
      C. *Source code change required to comply with the requirement*

      o *In the* ***comment box*** *the Bidder must describe the modification that will be made and how it will comply with the requirement. All such modifications are considered to be part of the solution being proposed and included in the bid price. If the modification will not be complete by the "go live" date, the Bidder must specify an anticipated date when the modification would be added to the solution, at no additional cost to the State. The State reserves the right to reject the Bidder's proposed date and consider the solution not in compliance.*

   c. ***No*** *– is defined as the Bidder's proposed solution does not comply with all aspects of the requirement.*

   o *In the* ***comment box*** *the Bidder must describe the impact of not meeting the requirement.*

Req. No.	Functional Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
1	**General Requirements**				
1.1	Solution will enable user identity authentication, establishment, management and federation and support access management of State of Michigan systems and services.	**Yes**			The proposed solution will implement the OOTB functionalities of IBM Security Identity Manager 6.0 (ISIM) and IBM Security Access Manager for Web 7.0 (ISAM) to enable user authentication, user identity creation, user identity life cycle management, and identity federation. Contractor will work with the State to determine the requirements and implement the Identity and access management functions for the State's systems and services.
1.2	Solution will provide an adoption solution that encourages adoption and use	**Yes**			The proposed solution will be designed to provide a viable, scalable, and extendible foundation aligned with industry frameworks and positioned for other agencies to adopt and use IAM services and components to manage access to their systems.
1.3	Solution will be an internal identity store that provides support for federation for use for both internal and external applications. The solution should support separate protected LDAP sources for internal only access and external public access. It is not the intent of the State to use an external identity store (LDAP) for internal SOM system user access when users are connecting from within the state network. The State's preferred solution is an internal identity store that provides support for federation for use for both internal and external applications.	**Yes**			The proposed solution will be designed based on leading practices and our experiences from other successful IAM deployments.
1.4	Solution must establish federation between SOM MICAM and MIHIN IDM.	**Yes**			The proposed solution supports Security Assertion Markup Language (SAML), WS-Federation, Information Card Profile, OpenID, and

Req. No.	Functional Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
					OAuth. Based on the information currently available, federation between the State, MICAM and MIHIN IDM would be implemented using SAML.
1.5	Solution must support federation with other IDM systems in and outside the SOM; National Strategy for Trusted Identities in Cyber Space	Yes			The proposed solution supports federation with other IDM systems, which are using open standards and specifications such as Liberty, SAML, WS-Federation, WS-Security, and WS-Trust.
1.6	The Bidder's and Bidder's subcontractors support staff must reside in the United States.	Yes			Contractor acknowledges this requirement and would staff the personnel residing in the United States.
1.7	Bidders and Users must not share accounts and/or tokens.	Yes			Contractor acknowledges this requirement of not sharing the accounts/tokens.
1.8	The application will support the following authentication requirement: • LDAP v3 • Tivoli Single Sign On • Active Directory 2003 • External radius server • Two factor authentication • Novell IDM v3.5 • User ID and Passwords • Biometrics • Directories • Smart cards • Tokens • PKI and Certificates • Voice recognition • Shared secrets • Access control lists and files • Unique business process		Yes (B)		The proposed solution leverages ISAM for user authentication. OOTB ISAM supports following authentication mechanisms: • LDAP v3 • Tivoli Single Sign On • Active Directory 2003 • Two factor authentication • User ID and Passwords • Directories • Public Key Infrastructure (PKI) and Certificates • Shared secrets • Access control lists and files Further ISAM supports integration with two-factor authentication services/solutions such as RSA SecurID using

Req. No.	Functional Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
					OOTB RSA authentication agent (plug-in) for passing authentication information to RSA Authentication Manager. To support the remainder of the authentication mechanisms provided in this requirement, ISAM provides the following interfaces that can be leveraged to extend the authentication capabilities: • C-Authentication API interface (former CDAS) • External Authentication Interface (EAI) The proposed solution supports configuring authentication mechanisms for business processes implemented as B2B/enterprise services.
1.9	Application authentication and authorization must be by individual user. User account information must be stored securely in a database. Users may belong to multiple groups and roles.	Yes			The proposed solution supports assignment of multiple groups and roles to a user. However, OOTB ISAM only supports a LDAP compliant directory as user registry for carrying user authentication and authorization. The user account information is stored securely in the directory.
1.10	The application will enforce the Michigan 1 (M1) standards or specific system requirements, whichever are more restrictive for individual passwords for allowable characters, length and expiration period.		Yes (B)		The proposed solution is capable of defining and implementing the password policy for allowable characters, length, and expiration period. An illustrative password policy is provided in *Appendix F – State Enterprise Password Standards*. Contractor will work with the State to

Req. No.	Functional Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
					analyze the specific password policy requirements and configure the system to comply with this requirement.
1.11	The application must follow the M1 standards or specific system requirements, whichever is more restrictive to lock out users after invalid login attempts.	Yes			The proposed system provides functionality to configure the number of invalid login attempts before locking out the user/system account.
1.12	The application must provide the system administrators with the capabilities to define different roles with different privileges.	Yes			This is standard functionality in IBM Security Role and Policy Modeler.
1.13	The application will provide the system administrators with the capabilities to create groups whose members can be either role-based or individual login account names.	Yes			This is standard functionality in IBM Security Role and Policy Modeler.
1.14	The application must be capable of integrating with the State of Michigan Standards "Identity and Access Management" tools.	Yes			ISIM and ISAM are the proposed IAM tools for the State of Michigan. ISIM and ISAM OOTB integrate with many well-known COTS applications and platforms. IBM regularly releases new adapter and agent/plugin for integration with different applications.
1.15	The solution shall support all currently approved FICAM Protocol Profiles for browser based SSO (OpenID 2.0 and SAML 2.0 required; IMI 1.0 support is optional).	Yes			Current FICAM supported profiles are: • OpenID 2.0 • SAML 2.0 • IMI 1.0 IBM Security Federated Identity Manager (ISFIM) Supports OpenID 2.0 and SAML 2.0
1.16	Vendor shall provide a detailed plan for supporting newly approved FICAM Protocol profiles within [90 days] of final approval by the ICAMSC. Final plan will be approved by both Vendor and the State.	Yes			As contributing authors of the FICAM Roadmap and Implementation Guidance and NSTIC, our subject matter specialists are knowledgeable of upcoming technologies, standards, and

Req. No.	Functional Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
					guidance. Contractor will leverage the specialists to work closely with the State to identify the technical and business benefits of newly defined profiles. If beneficial to the State, Contractor will draft a detailed implementation plan for integration into the State's solution within 90 days of approval.
1.17	The solution shall be capable of supporting all FICAM Adopted Trust Framework Provider Approved Credential Providers.	Yes			The new FICAM Adopted Trust Framework Credential Providers can be configured to be accepted in the same manner as existing providers.
1.18	The solution shall be capable of supporting PIV (for Government-to-Government use cases) and PIV-I Authentication. This support must include Trust Path Discovery and Trust Path Validation functionality.	Yes			ISIM and ISAM support PIV & PIV-I Authentication and certificate chain validation using Certificate Revocation Lists (CRL) or Online Certificate Status Protocol (OCSP).
1.19	If the solution implements a SAML 2.0 Attribute Query/Response mechanism, it shall support the FICAM SAML 2.0 Identifier and Protocol Profiles for BAE v2.0 and the associated FICAM SAML 2.0 Metadata Profile for BAE v2.0		Yes (B)		The proposed solution supports SAML 2.0 standards. Contractor will work with the State to determine FICAM requirements during the requirements gathering phase of the project.
1.20	The solution shall, at a minimum, support the following protocols and assertion formats for communication between itself and the relying party Agency application: • Protocols: HTTP(S), SAML 2.0 • Assertion Formats: SAML 2.0, XML, JSON	Yes			The proposed solution supports these protocols and assertion formats. Further, the solution aligns with following open standards and specifications: • Liberty • WS-Federation • WS-Security • WS-Trust profiles
1.22	Solution will allow the ability for local administrators with rights to add, disable, and modify user for their agency.	Yes			The proposed solution would allow administrators to add, disable, and modify user’s information for

Req. No.	Functional Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
					the in-scope users. The solution is also capable of supporting delegated administration.
1.23	Solution will allow users to centrally provisioned and de-provisioned; meaning accounts are enabled or disabled statewide from the Contractors identity vault	Yes			The proposed solution supports provisioning/de-provisioning/ termination/suspension of users based on the automated trigger from HR System or manual trigger by ISIM administrators. During the requirement and design workshops, Contractor will work with the State to determine life cycle rules for termination/suspending user access.
2	**Architecture Requirements**				
2.1	System must support full and policy or filtered interfaces with other directories, including at least Tivoli, Active Directory (AD), eDirectory and Lightweight Directory Access Protocol (LDAP) or equivalent functionality.	Yes			The proposed solution leverages Tivoli Directory server and integrates well with a wide range of other directories, including Active Directory, eDirectory, and LDAP.
2.2	User and account provisioning and de-provisioning within AD will continue unchanged	Yes			The proposed solution is designed to leverage current Active Directory provisioning processes. Contractor will work with the State during the Design phase to identify areas for improvement in the current provisioning and de-provisioning processes.
2.3	The solution must include support for a reverse proxy access control or equivalent functionality, authenticating the user for all applications for which the user has been granted access.	Yes			The proposed solution leverages ISAM for authentication and provides support for reverse proxy model.
2.4	The solution must integrate with the existing reverse proxy access control solution. The solution must provide a migration path for the existing Single Sign On (SSO) solution.	Yes			The proposed solution will leverage the ISAM component WebSEAL, a secure reverse proxy for access control and SSO.

Req. No.	Functional Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
2.5	The solution must support one identity per entity, with users possessing rights to multiple applications and resources. Users should have a single password with other factors such as PINS, tokens, biometrics, etc., as required. The same entity may have more than one identity depending on context, such as a State of Michigan employee who also logs in as a citizen.	Yes			The proposed solution is in line with the one identity per entity principle; however, it allows entities to have more than one identity depending on the context. Contractor will work with the State to develop requirements that address identity proliferation during requirement phase.
2.6	The proposed system must integrate with the State Of Michigan's network architecture and with published security policies posted on http://www.michigan.gov. Externally hosted components must comply where appropriate.	Yes			The proposed solution will integrate with the State's network architecture and will comply with published security policies.
2.7	System components must be deployable in tiers, such as putting the reverse proxy server, the portal server, and identity stores on separate physical servers, limiting the exposure of secure resources. The actual tiers should depend on best practices for the bidder's proposed solutions.	Yes			The proposed solution offers a tiered architectural design that allows deploying crucial components of the system on separate physical servers.
2.8	The solution must support current LDAP v.3 Application Program Interface (API) calls	Yes			The proposed solution leverages ISIM and ISAM which support LDAP V3 compatible servers.
2.9	The solution must provide user login application access web portal or enable integration with an existing portal environment through open standards.	Yes			The proposed solution provides a self-service and administration portal and can be accessed using a single-factor authentication, user ID, and password.
3	**Application Development Environment**				
3.1	The solution must provide a clear development path for integrating Web-based applications for reverse proxy portal integration or equivalent functionality.	Yes			The proposed solution deliverable(s) will cover these details.
3.2	The solution must provide a software development kit (SDK) for extensions surrounding workflow, custom provisioning, and triggers.	Yes			The proposed solution stack provides SDK for customization and extensions. ISIM has a rich set of published Java APIs, Web Service wrappers, JavaScript extensions for ISIM customizations

Req. No.	Functional Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
					(workflow, policies). ISIM also provides an Adapter Development Tool (ADT) to expedite custom provisioning adapter development using IBM Tivoli Directory Integrator. ISAM provides the following interfaces that can be leveraged to extend the authentication capabilities: • C-Authentication API interface (former CDAS) • External Authentication Interface (EAI)
3.3	The solution must support the use of open source or well supported leading industry development tools, subject to SOM approval.	Yes			ISIM is a J2EE application that can be customized using its Java APIs, Web Services, and JavaScript extensions. The open source or leading development tools such as Eclipse can be used for custom development.

Req. No.	Functional Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
3.4	The solution must provide support for integration with client server applications that are LDAP capable.	Yes			The proposed solution can provision users into LDAP based application user repository.
3.5	Any Java based development activities must support JEE and current JDK version	Yes			The custom development activities will support JEE and use the current JDK version as long as the proposed solution stack is also certified to work on the current JDK version.
3.6	Any Microsoft Windows specific development must be.NET based.	Yes			The proposed solution includes Adapter Development Tool (ADT) kit for integration with different applications/systems. OOTB ADT provides built-in connectors and supports WS-Trust for.NET (part of the Web Services Enhancements 3.0) for integration with Microsoft applications.
3.7	The system must support custom attributes of the bidder's LDAP.	Yes			The proposed solution uses LDAP as identity and authentication store. The identities in ISIM and ISAM are stored as user objects in LDAP and can be extended to support custom attributes.
3.8	The solution should provision and de-provision identities in non-LDAP targets.		Yes (B)		The proposed solution supports OOTB provisioning connectors for standard non-LDAP targets. For non-standard targets, Contractor will develop custom connectors, assuming that the user administration APIs for the target systems are available to develop the connector.
3.9	The solution shall not allow anonymous access to the production LDAP.	Yes			The proposed solution will implement access controls for the production LDAP to disable unauthorized and anonymous

Req. No.	Functional Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
					access.

Req. No.	Functional Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
4	**Workflow**				
4.1	The solution must provide the ability to support self-registration and user originated application requests with an approval queue for application administrators.	Yes			The proposed solution provides self-registration capabilities as well as custom approval workflow functionality.
4.2	The solution must support the ability to assign security attributes based on the user's context.	Yes			The proposed solution provides capabilities to assign security attributes based on user type or other user attribute.
4.3	The solution must support integrated workflows.	Yes			The proposed solution supports integrated workflows that will be configured to meet the State's specific requirements.
4.4	The solution must support automated provisioning and de-provisioning based on feeds from authoritative sources.	Yes			The solution includes ISIM, which supports automated provisioning based on feeds from authoritative sources.
4.5	Solution must support delegated administration for applications accessible through the bidder's portal.	Yes			The proposed solution supports a delegated administration model that will be configured to meet the State's specific requirements.
4.6	Solution must allow for self-requests for automated password reset where appropriate.	Yes			The proposed solution supports self-password reset from the self-service portal and from Windows desktop using Ctrl+Alt+Del when integrated with Active Directory domain.
4.7	Solution must support multiple workflow paths, depending on the type of user such as, but not limited to state employee, identified citizen, customized web experiences, etc.	Yes			The proposed solution allows defining separate workflow paths for different types of users. The workflow designer allows for a wide range of configurations.
4.8	Solution must support the development of customized workflows.	Yes			The proposed solution supports customized workflows that will be configured to meet the State's specific requirements.

Req. No.	Functional Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
4.9	Solution must support notification workflow capabilities.	Yes			The proposed solution supports notification workflow capabilities and will integrate with the State‘s mail system to distribute notification to appropriate workflow participants.
4.10	The system should support workflow approvals from secure authorized mobile devices.	Yes			The OOTB interface “works” on mobile, assuming the mobile device has a late generation browser.
5	**Encryption**				
5.1	The system must provide support for a minimum of 256 bit TLS encryption for transport.	Yes			The proposed solution provides support for a minimum of 256 bit TLS encryption for transport.
5.2	Components of the system must be configured to communicate using TLS/ SSL or other appropriate forms of encryption.	Yes			The proposed solution supports Transport Layer Security/ Secure Sockets Layer (TLS/SSL) encryption between the solution components. The communication channel between the End User and the system is encrypted using at the minimum, 256-bit key encryption, through HTTPS using TLS/SSL technology.
5.3	The system must provide encryption for all data at rest. Such as, but not limited to Advanced Encryption Standard (AES)- 256	Yes			IBM Tivoli Directory Server and DB2 OOTB capabilities would be leveraged to provide the encryption for sensitive data at rest.
5.4	System must support strong one- way encryption (hashed) of passwords.	Yes			The proposed solution uses Tivoli Directory Server (TDS) as the authentication store. OOTB TDS supports strong one-way encryption (hashing) and two-way encryption to encrypt user password. One-way encryption formats supported: • crypt • MD5 • SHA-1

Req. No.	Functional Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
					• Salted SHA-1 • SHA-2 (SHA 224, SHA 256, SHA 384, and SHA 512) • Salted SHA-2 (SSHA 224, SSHA 256, SSHA 384, and SSHA 512) Two-way encryption format supported: • AES (AES128, AES192, and AES256)
5.5	The system should support Public key Infrastructure (PKI) where appropriate.	Yes			The proposed solution will leverage OOTB capabilities to support PKI functions such as using the IBM Key Management Utility (IKEYMAN) to request a certificate, create key store database, exporting and importing keys, exporting certificates in Public -Key Cryptography Standards (PKCS) # 12 format and storing CA certificates.

Req. No.	Functional Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
6	**Administration**				
6.1	The system must provide central administration for manually manipulating identities, including password reset, user creation, granting roles/privileges, etc.	Yes			The proposed solution provides central administration of user creation, termination, role/access assignments, password management, etc., and different policy administrations.
6.2	The system must have a single web interface that allows for the management and administration of identity management systems.	Yes			By default, the solution stack supports web interfaces for performing different user administration tasks (creation, termination, role/access assignments, password management, etc.) and other configurations. The solution also supports tool administration through command line functions.
6.6	The system must have the ability to enforce password policies including: i.Expiration of passwords. Ii Challenge/response capabilities for forgotten passwords. Iii Password strength policies.	Yes			The proposed solution provides centrally managed and automated password management capabilities for administrators and End Users. The solution also has the ability to define password policies specific to an organization unit or a managed resource.

Req. No.	Functional Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
6.4	The system shall use preset values to reduce the time to create an account correctly.		Yes (B)		Automated provisioning is achieved by configuring provisioning policies for a target application. The proposed solution will leverage role based account provisioning with pre-defined values in the provisioning policy.
6.5	System must provide administration tools for manipulating certificates and encryption keys needed to support the system where appropriate.	Yes			The IBM Key Management Utility (IKEYMAN) included in the solution stack provides administration of digital certificate and encryption keys.
6.6	The solution must have limited and secure access to key stores, consistent with constraints of Federal and State law.	Yes			The IKEYMAN is a thick client application and can be accessed only by a system administrator. The key database is protected using a strong password and typically access is restricted only to authorized system administrators.
6.7	Administration privileges must be configurable by location, object classification, applications and other attributes.	Yes			The proposed solution has the ability to model access control OOTB based off organization structure or object type or attribute information or combination of two or more rules. Contractor will work with the State during the Design phase to model the access control by user type.

Req. No.	Functional Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
6.8	All administrators must have a uniform interface across the bidder's solution.	Yes			The self-service and administration user interfaces will be branded using the State's logo. The look and feel of the interfaces will be uniform for users in the proposed solution. The administration interface is accessed only by the authorized IAM administrators.
6.9	Remote Access for Administration: System must support the use of the State's VPN and two-factor authentication for Vendor remote Administrative access to the State's internal resources.	Yes			The proposed solution will be designed and deployed to support access from intranet and Internet for self-service functions. The administration functions of the solution will be available in intranet and remote access for administration shall be performed using the State's VPN and two-factor authentication.

Req. No.	Functional Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
7	**Auditing**				
7.1	System must provide full and configurable auditing capabilities, including the creation/deleting of users, password resets, role/privilege assignment, etc.	**Yes**			The proposed solution will log events such as user creation, deletion, modification, lock/unlock, password change, role assignments, policy enforcements, exceptions, failure and violation, etc., in ISIM. The solution also has the ability to increase or decrease the level of events to be logged through log level configuration settings.
7.2	System must provide full auditing of access to applications, access to resources, and access to individual users accounts.	**Yes**			The proposed solution will log events such as authentication authorization, session, group memberships or entitlements, policy enforcements, exceptions, failure and violation, etc., in ISAM. The solution also has the ability to increase or decrease the level of events to be logged through log level configuration settings.
7.3	All auditing logs must be reviewable by state security administrators and security policy staff.	**Yes**			The audit events are written to format log files and audit database for generating reports. The log files are readable by security administrator and other authorized users.

Req. No.	Functional Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
7.4	The system must support real-time replication of audit logs to the State's Security Information and Event Management (SIEM) solution for audit reporting.		Yes (A)		The proposed solution includes Common Auditing and Reporting Service (CARS) which is capable of collecting events from ISAM and processing the data so that reports can be viewed through Tivoli Common reporting package or other third-party reporting products. The solution shall leverage the State's SIEM solution's capability for audit reporting to collect events captured in these audit logs real-time.
7.5	The system must be configurable for auditing events.		Yes (A)		The proposed solution supports configuration of audit events. Contractor will work with the State to identify these events.
7.6	All system activity must be contributed to a single, unique system user, identifiable by individual persons.		Yes (A)		The proposed solution audits system activities with each activity being traceable to a system user.

Req. No.	Functional Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
8	**Authentication**				
8.1	System must support LDAP calls for username and password authentication, including passing an encrypted password string.	Yes			ISAM supports username and password based authentication and coarse-grained authorization for Web applications against numerous repositories including LDAP.
8.2	System must support integration with a two factor authentication services/solutions and/or adaptive authentication services/solutions as required, including at least RSA SecurID tokens.		Yes (B)		The proposed solution supports integration with two-factor authentication services/solutions such as RSA SecurID using OOTB RSA authentication agent (plug-in) for passing authentication information to RSA Authentication Manager. The additional following interfaces provided by ISAM can be leveraged to extend the authentication mechanisms: • C-Authentication API interface (former CDAS) • External Authentication Interface (aka EAI)
8.3	System must support elevated (step-up) authentication, meaning that as a user requests more secure access, authentication requirements increase.	Yes			The proposed solution supports elevated/step-up authentication for accessing more sensitive resources using a stronger authentication mechanism. The authentication levels required to access protected resources is defined and enforced using an authentication strength policy.
8.4	System must support location sensitive authentication, meaning authentication requirements increase as users attempt to access resources from less secure locations.		Yes (A)		The proposed solution leverages ISFIM along with ISAM to provide support for location sensitive authentication. ISFIM Risk-based access

Req. No.	Functional Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
					feature provides access decision and enforcement that is based on a dynamic risk assessment or confidence level of a transaction. Risk-based access uses behavioral and contextual data analytics to calculate risk. The solution can also integrate with the State-owned Risk-based authentication tool (if any) and may require customizations and/or configurations based on the actual requirements.
8.5	The solution must be able to integrate with the State's PKI for certificate based authentication (including support for revocation.)		Yes (A)		ISAM supports X.509 V3 client certificates for strong authentication to Web-based resources; support for many certificate providers, including VeriSign and Entrust.

Req. No.	Functional Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
8.6	System must provide mechanisms to prevent brute force attacks and other well-known attacks.	Yes			The proposed solution would lock out the user/system account in case of 'n' ('n' value would be decided by the State's password policy) consecutive wrong login attempts, thus preventing brute force attack.
9	**Authorization**				
9.1	The system must support role based access control (RBAC) for the granting of roles and privileges to users and to other groups.	Yes			The proposed solution leverages ISIM capability to support role based access control (RBAC) and Access Review certification.
9.2	System must provide a mechanism for assigning privileges for application and managed resource access.	Yes			The proposed solution provides both coarse-grained authorization models for Web-based applications to prevent unauthorized use of the system. ISAM provides coarse-grained authorization, while fined-grained access control is enforced at the application level providing the security enforcement required to limit application functionality where appropriate.

Req. No.	Functional Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
10	**System Availability**				
10.1	The system must support a clustered and failover configuration to ensure high availability. **System must not have a single point of failure.**	Yes			The proposed solution is designed to support high-availability by deploying load balanced redundant servers and horizontally clustered application servers.
10.2	The system must support full back up and restore capabilities so that the system can be restored from media with minimal additional intervention.	Yes			The daily incremental back-up and weekly full back-up of data will allow the system to be restored from the backup media in the event of a system failure.
10.3	System must support a minimum of 99.99 uptime for 24 x 7 x 365 operations.	Yes			The proposed solution will be hosted in primary and secondary data centers to provide required uptime.

Req. No.	Functional Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
11	**Desktop Environment**				
11.1	The administrative tools must be compatible with State's current Windows desktop standards. Must adhere to State Standard products: http://www.michigan.gov/dmb/0,4568,7-150-56355---,00.html	**Yes**			The proposed solution addresses the State's current Windows desktop standards.
11.2	Authentication support must operate as an HTML form in a browser without plugins or additional software. Must adhere to State standards and policies: http://www.michigan.gov/emichigan/0,4575,7-112-10666---,00.html	**Yes**			The proposed solution addresses the State's authentication support requirements.
11.3	Users must be able to access the application portal and login with any current and supported operating system, including but not limited to Windows, Mac OS, and Linux provided the user has a compatible web browser.	**Yes**			The proposed solution is supported on IE, Firefox, Chrome, and Safari browsers
11.4	User browsers must support HTTPS and session cookies.	**Yes**			The proposed solution will enforce SSL communication between user and the application.

Req. No.	Functional Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
12	**Reporting**				
12.1	System must provide authentication and access reports based on any arbitrary attributes the State requires.		Yes (A)		The proposed solution includes the Common Auditing and Reporting Services (CARS) and Tivoli Common Reporting (TCR) for IBM Security Access Manager. CARS will be configured to log security events such as authentication and authorization. Contractor will work with the State to identify the report requirements and configure OOTB reports and develop the required custom reports based on the identified attributes.
12.2	System must support report generation for administration tasks, including, but not limited to password resets, granting of privileges, account suspensions, and any other auditing event.		Yes (A)		The proposed solution includes TCR for reporting capabilities to generate various reports including, but not limited to password resets, granting of privileges, account suspensions, and other security events identified as part of the report requirements.
12.3	System must support report generation for security incidents such as, but not limited to, hacking attempts and attempts to access secure resources above an individual's access levels.		Yes (B)		The proposed solution leverages the State's currently owned SIEM reporting capabilities to generate various reports including but not limited to detailed security incident reports, trend analysis, and other reports on system activity based on security parameters.
12.4	System must support a number of standardized reports plus support the ability to provide ad hoc reports via a third party reporting tool to address special situations.		Yes (A)		The proposed solution supports a number of standardized reports and ad hoc reports OOTB. The solution allows integration with third-party reporting tool by running reports against the audit database. The audit data is captured and

Req. No.	Functional Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
					written to audit database and custom reports are run against the database using the OOTB reporting tool or third-party reporting tools.
12.5	The solution must support configuration of Ad hoc reports without requiring any customized programming.		Yes (A)		ISIM provides OOTB support for ad hoc reporting of user provisioning events. In addition, CARS and TCR provide capabilities to generate various reports on user access related events. Ad hoc Reports in ISIM, CARS, and TCR can be generated without any custom programming. For detailed security incident reports the proposed solution will leverage the State's SIEM solution.

Req. No.	Functional Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
13	**Monitoring and Alerting**				
13.1	System must include real time mechanisms for monitoring responsiveness, resource consumption, storage utilization, and overall system health.		**Yes (B)**		The proposed solution will integrate with the State's existing processes and systems mechanism used for monitoring responsiveness, resource consumption, storage utilization, and overall system health
13.2	System should include support for intrusion detection and other hacking attempts on identity stores.		**Yes (B)**		The proposed solution will leverage the State's existing SIEM tool to support intrusion detection and other hacking attempts on identity stores.
13.3	System must provide real-time notification to administrators and State monitoring staff for performance issues and any security event. Notification must be configurable for e-mail, mobile phone, text messaging, etc.		**Yes (B)**		The proposed solution will work with the State's existing SIEM tool to provide real-time monitoring of user activity, data access, application activity and incident management, and reporting capabilities to generate various detailed security incident reports. NetIQ Sentinel provides capabilities to send out alerts through e-mail.
13.4	Alerts need to be configurable by administration staff, not requiring code changes.		**Yes (B)**		The proposed solution will work with the State to configure its existing SIEM solution according to the State's requirements to configure alerts by administration staff.
14	**System Maintenance**				
14.1	Bidder must provide regular patching mechanism, consistent with SOM trust zone constraints (no Internet access allowable in certain zones).	**Yes**			The proposed solution will follow the State's change management processes to perform fix pack upgrades and patching.
14.2	State Of Michigan must be notified of any emergency maintenance activities that must be performed on internal or external components. A mutually approved procedure must be established by the Bidder.	**Yes**			The operations play book will identify the system maintenance activities/ procedures to be performed after production go live. The operations playbook

Req. No.	Functional Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
					will be reviewed and signed off by the State before the system goes into production.
14.3	The solution must enable patch(s) or upgrade(s) to individual components without shutting down access to the identity management system.	Yes			Applying patch(s) or upgrading an individual component will require downtime and some configuration changes. While one leg of the solution component is patched or upgraded the other leg will continue to allow user access to the system, thus not having to shut down the access. Our Operations play book will identify the frequency and timing of such activities and the procedures to be followed in conjunction with the State's change management procedures.
14.4	The solution must accommodate operating system and hardware maintenance on any individual server without shutting down access to the identity management system.	Yes			Operating system and hardware maintenance will require downtime and some configuration changes. While one leg of the solution component is patched or upgraded the other leg will continue to allow user access to the system, thus not having to shut down the access. Our Operations play book will identify the frequency and timing of such activities and the procedures to be followed in conjunction with State's change management procedures.
14.5	Bidder must comply with current State of Michigan Request for Change (RFC) and change control management procedures.	Yes			The proposed solution will comply with the State's change control management procedures.

Req. No.	Functional Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
15	**Regulatory Compliance**				
15.1	System must provide mechanism for compliance with all State and Federal laws and mandates that the State is subject to including, but not limited to HIPAA, CJIS, IRS Pub.1075 Et.Seq., Homeland Security, and PCI for access to and use of secure data and applications.	**Yes**			The proposed solution is designed to comply with the existing State policies, standards and processes to provide compliance with State and Federal laws and mandates that the State is subject to.
15.2	System must support federated identity management, using National Institute of Standards Technology (NIST) best practices and equivalent industry standards for interoperability and integration with external public and private institutions. Including, but not limited to the following sub sections of 15.2:	**Yes**			The proposed solution architecture supports NIST 800-53 standards, specifications, and guidelines.

Req. No.	Functional Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
15.21	System must follow NIST 800-53 control standards for secure access to data and systems. Per NIST SP800-53: "Remote access is any access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet)."	Yes			The proposed solution complies with NIST 800-53 security control for secure access to data and systems. The administration interface shall be made accessible only from intranet per requirement 6.9 in *Appendix E – General Functional Requirements*. The user must logon to the network through VPN and then allowed to access the administration interface. The self-service interface will be available externally but behind the secure reverse proxy (WebSEALs).
15.22	Must have an identity proofing service capable of implementing [remote and/or in-person] identity proofing processes at OMB-08-08 E-Authentication assurance levels (per NIST SP 80063-1)		Yes (B)		The proposed solution will integrate with Identity proofing service provider (Experian Credit Bureau) at the time of user account creation/setup.
15.23	Solution must integrate with the States existing advanced authentication system or provide NIST compliant advanced authentication per advanced authentication at level 3 or level 4 as defined in NIST SP800-63.		Yes (B)		The proposed solution, through custom development, will integrate with the NIST compliant advanced authentication mechanisms such as hardware tokens, one-time password and digital certificates.

Req. No.	Functional Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
16	**Response Times and Capacity**				
16.1	System must be capable of responding to a simple password authentication response within 10 Seconds 99% of the time, assuming an unencumbered network interface.	**Yes**			The proposed solution offers an industry leading IAM system. The response time for a simple password authentication depends on a large number of factors that are independent from the proposed solution (including but not limited to network, user's location, hardware, server health and web browser used and details of the actual portal being accessed.) The proposed solution hardware is sized to meet the authentication response requirements identified. Contractor will work with the State to define the non-functional requirements for the overall IAM system during requirements gathering phase of the project.

Req. No.	Functional Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
16.2	System must support:	Yes			The proposed solution hardware and software is sized to meet the total number of users and other entity requirements identified in the RFP. The proposed solution provides support for federation of identities (as identity provider) with the State agencies to authorize users to access agency owned applications. The ability to federate identities makes the enterprise IAM system as the system of record for user information across the State.
	55,000 State of Michigan employees				
	all State of Michigan citizens				
	500,000 other entities				
	All State of Michigan agencies				
	Hundreds of different user classifications and roles				
	State of Michigan applications across over all State agencies in a cost-effective manner.				
	Consistent, identity information across the agencies.				

Req. No.	Functional Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
16.3	Any portal or application list interface must be displayed to the user within 3 seconds 99.99 % of time, assuming an unencumbered network interface.	Yes			The proposed solution offers an industry leading IAM system. The response time depends on a number of factors that are independent from the proposed solution (including but not limited to network, user's location, hardware, server health and web browser used and details of the actual portal being accessed). The proposed solution hardware is sized to meet the response time requirements identified in the RFP.
16.4	System must support a peak load of 2x the expected maximum concurrency to ensure adequate spare capacity for growth and expansion without an unacceptable degradation of performance. The expected maximum concurrency is 20,000 users, but the Bidder is encouraged to adjust this number upward or downward with supporting data and estimation methods.	Yes			The proposed solution hardware and software is sized to meet the number of concurrent user requirements identified in the RFP. .

Req. No.	Functional Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
16.5	Additional maximum response times for the Identity Management user interface must include:	Yes			The proposed solution hardware is sized to meet the required response time identified in the RFP. Contractor will work with the State to define the non-functional requirements for the Identity and Access Management System during requirements gathering.
	Search screens – 5 seconds or less, unless approved and justified in advance by the State of Michigan and the Bidder.				
	Screen updates resulting in a modification of a single logical record must return results in 5 second or less.				
	Screen actions involving complex computations or rules engines evaluations must return results within 3 seconds unless approved and justified in advance by the State of Michigan and the bidder.				
16.6	The batch and backup operations must not degrade the response times of the system in off hours, assuming a lower request load to be estimated and justified by the bidder.	Yes			The backup operations will be performed only during off hours and the load during off hours is considered to be less than or equal to 10% of the load during peak hours.

Req. No.	Functional Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
17	**Project and Configuration Management**				
17.1	All project deliverables and software artifacts must be manageable and deployable from a configuration management system.	Yes			Contractor acknowledges this requirement.
17.2	All project tracking activities and work plans must not require any special tools beyond MS Project.	Yes			Contractor acknowledges this requirement.
17.3	All written project deliverables and documentation must be converted to MS Word and MS Visio using PDF documents for diagrams and other file formats that will not readily convert to MS Word.	Yes			Contractor acknowledges this requirement.
18	**Disaster Recovery (DR)**				
18.1	Bidder's hosted DR site must be in the United States.	Yes			The DR site for the proposed solution is located within the United States.
18.2	Bidder's hosted DR site must be a minimum of 50 miles from the primary hosting facility and away from prevailing winds.	Yes			The data centers are strategically located for resilient connection to power utilities and a diverse Tier 1 carrier network for the high levels of reliability, redundancy and performance. The DR site is located ~100 miles away from the primary hosting facility.
18.3	Bidder must comply with the State's RPO and RTO to support Red Card (Business Critical) Applications.	Yes			
18.4	Bidder must execute annual DR testing and provide the State with documented results.	Yes			
19	**Portal Interface Design**				
19.1	On user login, the solution will support the ability to present a custom web portal to the user that shows application links that the user has rights to.		Yes (B)		The proposed solution will carry out customization/branding of self-care interface for End Users. In addition a custom web portal will be developed with application/SSO links that the user has rights to. The custom portal is available on successful user login. With one click of the

Req. No.	Functional Requirement	Yes	Yes, with Modification (A, B or C)	No	Comments
					application link, the user experiences SSO.
19.2	Portal must have the ability to allow/disallow users to modify the user's portal home page.		**Yes (A)**		The proposed solution will allow/disallow IAM administrators to define different views for the self-service and administration portal. Typically the views are defined based on user type and role assignments.
19.3	Portal should have user's self-care capabilities, such as, but not limited to, user's changing passwords, challenge response and personal information.		**Yes (A)**		The proposed solution provides a self-care interface that can be customized for this requirement.
19.4	Portal should provide the ability for System Administrators to post communications/notifications.		**Yes (B)**		The proposed solution can be customized to provide this capability.
19.5	System Portal should allow dynamic additions and deletions of applications to the portal without impacting other applications.		**Yes (B)**		The application link will be automatically added or deleted from the custom web portal based on the user entitlements.