Mississippi, Rhode Island, Maine Unemployment Insurance Consortium

Infrastructure as a Service Request For Proposal

Circulation Date
April 20, 2015

Bidders Webinar/Teleconference
June 29, 2015 – 3:00 PM EDT
http://naswa.webex.com
Keyword Search: "RFP"
Click "Register"

Proposal Submission Date
August 21, 2015; 5:00 PM EDT
rfp_responses@itsc.org

National Association of State Workforce Agencies

Center for Employment Security Education and Research

Information Technology Support Center

Dated: 4/20/2015 Version 7.0

TABLE OF CONTENTS

I. BACKGROUND AND PURPOSE

The US Department of Labor offered an opportunity to develop a joint, multi-tenant UI (Unemployment Insurance) technology system in consortium through UIPL-18-12. The state agencies responsible for administration of the unemployment insurance (UI) programs of Mississippi, Rhode Island, and Maine (MRM), their governors, and their executive directors have committed to create this development, contingent upon adequate funding provided by the US Department of Labor. The Mississippi Department of Employment Security (MDES) has completed the modernization to their UI System, which will be the basis for Maine and Rhode Island's modernization. The multi-tenant solution will be based upon the MDES existing UI System and will be created in a cloud environment, operated by the MRM and funded through subscriptions paid to the MRM by each state.

In 2012, MDES received grant funds to partner with additional states and develop a multi-state UI Benefits and Tax system. Refer to Appendix A, Technical Architecture, for a detailed technical description of MDES UI System and MRM. Refer to Appendix E for a high-level MRM consortium deployment schedule that depicts planned deployment dates and environment availability dates.

The National Association of State Workforce Agencies (NASWA) together with its subsidiary, Center for Employment Security Education and Research / Information Technology Support Center (ITSC) is releasing this RFP for an Infrastructure as a Service (IaaS) cloud solution on behalf of MRM. For purposes of this RFP, NASWA, CESER, and ITSC will be referred to collectively as ITSC. The purpose of the RFP is to procure a vendor for cloud infrastructure and managed services to host and manage MRM unemployment insurance infrastructure.

ORGANIZATIONAL BACKGROUND

NASWA - The National Association of State Workforce Agencies (NASWA) is an organization of state administrators of unemployment insurance laws, employment services, training programs, employment statistics, labor market information and other programs and services provided through the publicly funded state workforce system. The mission of NASWA is to serve as an advocate for state workforce agencies, as a liaison to workforce system partners, and as a forum for the exchange of information. NASWA was founded in 1937. Since 1973, it has been a private, non-profit corporation, financed by annual dues from its member agencies and other revenue. To learn more about NASWA, you may visit the NASWA website at: http://www.naswa.org.

CESER - NASWA's Center for Employment Security Education and Research (CESER). Created in 1994 is a leading education, research and information technology center focused on workforce development and unemployment insurance issues.

ITSC - The Information Technology Support Center (ITSC) was created in 1994 by USDOL in partnership with the state of Maryland, to promote the development of information

technology enhancements and information technology sharing among the state UI agencies. On September 1, 2009, NASWA/CESER became the home of the ITSC. ITSC is funded by grants from USDOL's Employment and Training Administration's (ETA) Office of Unemployment Insurance (OUI). The ITSC directly supports state UI agencies with UI IT initiatives. ITSC is governed by a Steering Committee composed of state UI Directors, state IT Directors, state workforce agency administrators along with staff from the USDOL Office of Unemployment Insurance. To learn more about ITSC, you may visit the ITSC website at: http://www.itsc.org.

II. DEFINITIONS

MS UI System: Mississippi Department of Employment Security modernized UI Benefits and Tax application

MRM: Mississippi, Rhode Island, and Maine Consortium

III. SOLUTION OBJECTIVES

The primary objectives of MRM in procuring the IaaS vendor are:

- Leverage a common infrastructure for the 3 states, when possible.
- Allow for independence in operations between the states via separate instances and/or multiple environments with a minimum of 3 environments.
- Adhere to state and federal security standards and guidelines.
- Maintain environments to conform to all state-required audit levels.
- Allow for economies of scale with shared infrastructure and application support costs.
- Cloud vendor, rather than states, to manage infrastructure, including networks, servers, load balancers, firewalls and up to and including the OS.
- Common environment(s) should allow for rapid and cost effective modernization of UI application for MRM.
- Interface with state and federal systems on behalf of MRM.
- Benefit from an elastic supply of infrastructure capacity; avoid paying for maximum capacity on continuous basis
- Clear responsibility and cooperation between the IaaS Vendor and other vendor(s), who will maintain and support layers above the OS including the application and 3rd party products

IV. PROPOSAL FORMAT AND TIMELINE

A. FORMAT

Proposals shall be received on or before the proposal deadline of August 21, at 5:00 PM Eastern. The bidder will then receive a confirmation receipt within 24 hours of their submission. Responses will be sent to the email address of the sender along with any additional email addresses included in the submittal.

Please ensure that the submittal is in PDF format. All proposals must be submitted electronically to the following email address: rfp_responses@itsc.org. **Late proposals will not be accepted**. It is the responsibility of Bidder to ensure that its proposal is received by NASWA/ITSC, on or before this deadline.

The Bidder should submit a reasonably concise response that fully illustrates its proposed Solution. Therefore, Bidder shall make every effort to limit its full RFP response to 200 pages or less.

Bidders shall respond to every item listed within Section 4 – Bidder Response Format and label its proposal with the corresponding number for each question or request for information.

B. TIMELINE

The following RFP Schedule of Events represents ITSC's best estimate for this RFP.

EVENT	TIME (EST)	DATE (all dates are business days)
1. RFP Issued		April 20, 2015
2. Pre-proposal Webinar	3:00 p.m.	June 29, 2015
3. Written "Questions & Comments" Deadline	5:00 p.m.	July 17, 2015
4. Response to Written "Questions & Comments"		July 24, 2015
5. Proposal Deadline	5:00 p.m.	August 21, 2015
6. Completion of Technical Proposal and Oral Presentation Evaluations		TBD
7. Opening & Scoring of Cost Proposals		TBD
8. Best and Final Round		TBD
9. Evaluation Notice Released		TBD

10. Contract Negotiations Deadline		TBD
11. Contractor Contract Signature Deadline		TBD

NASWA/ITSC reserves the right, at its sole discretion, to adjust the RFP Schedule of Events as it deems necessary. Any adjustment of the Schedule of Events shall constitute an RFP amendment, and ITSC will communicate such to potential Bidders from whom ITSC has received a Notice of Intent to Propose.

C. GUIDELINES FOR QUESTIONS AND COMMENTS

All questions pertaining to this RFP must be submitted via e-mail to rfp_responses@itsc.org, by 5:00 PM EST on July 10, 2015. Questions submitted after this date and time will not be considered. The consolidated questions and answers will be posted under the MRM IaaS RFP link on the landing page of www.itsc.org. Only answers transmitted in this manner will be considered official and valid.
.

V. PROPOSAL REQUIREMENTS

This section outlines specific information required in your response and will be used by ITSC and the MRM Consortium as a basis for Contractor selection, and form part of the contractual requirements with the IaaS contractor. Please provide proof where applicable.

A. ELIGIBILITY REQUIREMENTS

1. Must be FedRAMP CSP and provide proof of certification with their proposal.
2. Minimum of 5 years as an IaaS vendor.
3. Must have 24 x 7 x 365 customer support.
4. Datacenters must have at least two levels of physical authorization.
5. There must be at least two physical barriers of entry to the servers.
6. There must be two levels of authentication to access the servers.
7. Primary datacenter and secondary data center must be at least 1,000 miles apart and must be in the continental United States.
8. Provide the Proposer's most recent independent audited financial statements. The financial statements must:

a. reflect an audit period for a fiscal year ended within the last 36 months
b. be prepared with all monetary amounts detailed in United States currency
c. be prepared under United States generally accepted auditing standards
d. include: the auditor's opinion letter; financial statements; and the notes to the financial statements
e. be deemed, in the sole discretion of the C.P.A. employed by the Bidder's State and charged with the financial document review, to reflect sufficient financial stability to undertake the subject agreement with the State

In lieu of the aforementioned independent audited financial statements, provide a financial institution's letter of commitment for a general Line of Credit in the amount of three million dollars ($3,000,000.00), U.S. currency, available to the Proposer. The letter must specify the Proposer's name, be signed and dated within the past three (3) months by an authorized agent of the financial institution, and indicate that the line of credit shall be available for at least 18 months.

Note:

Reviewed or Compiled Financial Statements will not be deemed responsive to this requirement and will not be accepted.

All persons, agencies, firms, or other entities that provide opinions regarding the Proposer's financial status must be properly licensed to render such opinions. ITSC may require the Proposer to submit proof of such licensure detailing the state of licensure and licensure number for each person or entity that renders the opinions.

B. VENDOR INFORMATION

Proposals must have a cover page that includes:

Name of Prospective Vendor
Project Title
Contact Person
Address
Telephone, Fax Number, and E-Mail Address

C. REFERENCES

Provide at least three (3) to five (5) references that match the scope of work outlined in this solicitation for projects that were completed successfully. In addition, provide at least three (3) to five (5) references for relevant projects/experience for any Commercial off-the-self Software (COTS) products which are proposed as a part of the Solution. Provide the principal contact, telephone number and email address, as well as a brief description of work performed. At least three (3) references must be available and responsive. Points will be deducted from the score for this criteria if the evaluation committee is unable to reach three (3) of the references provided. ITSC reserves the right to include other

governmental entities as additional references. ITSC also reserves the right to call references only on the selected Bidder's as a method of determining responsibility.

D. FINANCIALS

Provide a copy of the last certified, audited financial statements for your company. ITSC reserves the right to review financials only on the selected Bidders as a method of determining fiscal responsibility.

E. PROPOSAL PLAN.

The IaaS Vendor will work with ITSC and MRM to design, develop, and implement a System infrastructure, delivered as a service "Infrastructure as a Service," or "IaaS", satisfying the requirements set forth in this RFP.

The IaaS Vendor's integration of IaaS services into the System delivery will allow MRM to benefit from the pricing of such services, and promote functionality of the System. Some high-level features of this single, integrated operating model that the Bidder shall meet are presented below. For each of the enumerated contractual requirements below, the Bidder must indicate their compliance and provide a detailed explanation of how they will fulfill each requirement. Each requirement and response constitutes a contractual obligation on the part of the Bidder, and will be evaluated as part of the award process.

1. High-Level Features of the integrated infrastructure:

   a. Continuity. The IaaS Vendor will support the System for three (3) years. There will be three additional subsequent one (1) year option for support.

   b. Expertise. The IaaS Vendor shall meet all requirements set forth in this Contract and Proposal section of the RFP, and all appendices.

   c. Quality. The IaaS Vendor shall deliver services in accord with, or exceeding, the Service Level Agreement ("SLA") standards set forth in Operational Service Agreement (OSA) (see Appendix B). **Bidder shall list any exceptions or confirm that it has no exceptions to any of the terms, conditions or requirements within this Appendix B, which may impact the Bidders scoring. Exceptions shall be accompanied by alternative or substitute language, which would be acceptable to Bidder. Conflicts with stated requirements shall be noted in the corresponding paragraphs within Bidder's response format. Additional terms, conditions, or requirements proposed by Bidder for consideration shall be provided with a reference to the corresponding paragraph in the Appendix Document.**

   d. Assignability. ITSC at any time may terminate the contract, in compliance with Appendix C Terms and Conditions. The IaaS Vendor shall be

responsible for all transition costs to another IaaS Vendor. The transition period must not exceed 90 days, with final acceptance determined solely by ITSC and the MRM Consortium. **The Bidder must describe how they will achieve and implement this requirement.**

e. Security. IaaS Vendor shall ensure the System meets state and federal security requirements for the UI program and shall remain compliant with those requirements. The IaaS contractor shall also host the MRM TOP technical implementation, which has to comply with federal regulations, including but not limited to IRS Publication 1075. Finally, the IaaS contractor shall, as a condition precedent to the Consortium states entering into the Contract, execute and deliver Data Security Agreements with the Consortium states, to ensure data protection standards consistent with existing state laws. See Appendix D for Data and Network Security.

f. Warranty and Maintenance. Once implemented, the System will require continuous performance, functionality, and technical currency. The IaaS Vendor shall, therefore, deliver a maintenance program that commences with the nine month period, and continues, seamlessly at the Consortium's discretion, election of one or more of the three year option periods, which is after the initial nine months. The maintenance solution shall include everything necessary to maintain levels of performance, functionality, currency and/or compatibility, and be compliant with the OSA. Security

2. Security

a. Have FedRAMP CSP certification and must provide proof of certification with the proposal.

b. Additional certifications in ISO/IES 27001:2005 or Skyhigh CloudTrust are preferred.

c. Maintain operational security procedures which:

i. Restrict access to confidential information by authorized personnel only, with an established and documented process to request and grant access.

ii. Establish and provide secure media handling and destruction procedures for all data.

iii. Provide protection for the entire stack, from network through the entire infrastructure stack.

iv. Provide constant network monitoring for latencies and intrusion prevention.

v. Conduct an annual independent audit review of the hosting compliance for security and operating procedure (e.g. SAS 70 etc.).

vi. Legal Privacy and Confidentiality. Because MRM will use the System to collect data and personal information about residents of certain U.S. states, the Contractor represents and warrants that:

1. The System is as, or more, technologically secure as the higher comparable vendor security standards.

2. Upon request from any Consortium State, the Contractor shall provide a report comparing the security standards contained in the System and hardware to the then-current highest comparable security standards offered by other vendors.

d. Disallow external (untrusted) systems from accessing trusted zone systems. These systems will interact with application front end servers in the transition zone that will provide authentication and act as intermediaries to trusted services and data using standard mechanisms, such as VPN.

e. Utilize a centrally installed and managed Antivirus solution.

f. Secure network communications ensuring authenticity, confidentiality and integrity of data.

g. Deep packet inspection or content filtering for files that will be coming to the system will be handled by the firewall system.

h. Include an incident alerting system for both application intrusion as well as intrusion into the physical facility location.

i. Monitor and detect system intrusion and report such activity to a central security monitoring station.

j. Maintain current patch levels on the operating systems, servers, and services.

k. All operating systems are kept current with the most recent security patches.

l. Root level access shall be provided based only on need and the approval of MRM Consortium.

3. Capacity, Elasticity, Performance, Environments

a. Provide an IaaS that is capable of scaling in size and performance to accommodate claims doubling every three months for one year (see workloads below).

b. Provide an assessment to determine the bandwidth requirements needed for the MRM consortium.

c. Provide an elastic supply of infrastructure capacity; avoid paying for maximum capacity on continuous basis.

d. IaaS vendor will adhere to the requirements set forth in the OSA.

e. Be accessible 24 x 7 x 365 with availability defined in the OSA.

f. Schedule all maintenance to be done after business hours with minimal impact to the user community and no impact to scheduled processes. Typical business hours specified in the OSA.

g. Make minor repairs, perform routine maintenance, perform system checks, archiving and backups, etc. without taking the application out of service.

h. System must be scalable to meet fluctuating levels of activity. Bidder will describe how this will be met, including virtualization if used.

i. MRM shall finalize response time requirements and how they will be measured prior to going live. MRM will coordinate with application vendor and the IaaS Vendor on this effort.

j. Environments: At a minimum, there will be three (3) con-current production environments, 1 for each state. There is also an option to have one staging environment, which can be shared by all 3 MRM states. Refer to the Appendix E for a high-level MRM Consortium Deployment schedule for when the environments may be needed.

4. Environment Configurations and Sizing

Based on MDES UI System, MRM has conducted an initial sizing estimate. The Bidder is required to provide their sizing estimates and their optimum deployment of environments given licensing, use of instances and virtualization along with other underlying rationale including use of capacity analysis models. The Bidder must also address how the MRM consortium will achieve elasticity. The state's workload is presented below.

a. State's Workload: Please note the values below represent approximate numbers and intended to provide an average volume of the transactions.

Mississippi Workload			
S. No	Item	Peak Count	1st Feb 2015
1	Number of Active Employers	55,000	55,000
2	New claims per week	5,000	3,000
3	Weekly certifications filed per week	80,000	20,000

Rhode Island Workload			
S. No	Item	Peak Count	1st Feb 2015
1	Number of Active Employers	33,400	33,400
2	New claims per week	2,800	1,000
3	Weekly certifications filed per week	33,000	13,500

Maine Workload			
S. No	Item	Peak Count	1st Feb 2015
1	Number of Active Employers	41,400	40,000
2	New claims per week	3,800	1,500
3	Weekly certifications filed per week	33,000	16,600

b. Current VMWare Infrastructure Software below:

No.	Software	Version
1	ESXi	5.5.0
2	vCenter Server	5.5.0b
3	vCenter Orchestrator Appliance	5.5.0
4	vCenter Hyperic Server	5.8.0
5	vCenter Infrastructure Navigator	5.8.0
6	vCenter Operations Manager Enterprise	5.8.0
7	vCenter Site Recovery Manager	5.5
8	vCenter Configuration Manager	5.7.1
9	vCloud Application Director	5.5
10	vCloud Connector	2.5 Advanced
11	vCenter Chargeback Manager	2.6.0

c. Refer to Appendix F for infrastructure sizing specifications.

5. Hardware and Software

a. Provide the server hardware, applicable infrastructure software, and maintenance contracts to operate and maintain the System.

b. Provide rack space, power and network infrastructure to house the following appliances:

   i. Vormetric Data Security Manager (DSM) – 1 Appliance along with a failover option, Per State
   ii. IBM Guardium – 1 Virtual Appliance, Per State
   iii. IBM DataPower – MRM Consortium is evaluating IBM DataPower. 1 Appliance along with a failover option, Per State

c. Perform all environment establishment and configuration, in collaboration with the application vendor and per jointly developed specifications with application vendor, including but not limited to all network components, computer hardware platforms, servers, third party software, data storage, backup, operating system, reporting tools, databases, firewall (with VPN and DMZ), security and monitoring software, and needed bandwidth to support the System.

d. Utilize more than one network service provider carrier to achieve internet diversity. Each network service provider shall enter data centers at separate points to ensure uninterrupted service due to complete service failures caused by a network cut by one of the providers.

e. The IaaS Vendor must provision sufficient bandwidth from the network service providers to meet the response requirements of MRM.

f. Restrict access to hosting infrastructure based on port, request type, originating IP address, etc.

g. Utilize a purpose-built facility for maintaining a proper environment for hosting infrastructure, telecom connections and physical resources (cooling, power, humidity, etc.).

h. Utilize fire suppression systems in each of its facilities to stop fires from spreading in the unlikely event one should occur.

i. Maintain most current, compatible versions of all software and hardware components.

j. Production and staging environments shall be priced separately in the payment schedule. Refer to Appendix F for Infrastructure sizing.

6. Disaster Recovery and Business Continuity

a. Develop an IT Disaster Recovery Plan (DRP) that is designed to reduce the impact of a major disruption of key business functions and processes in the proposed system during the development and operational phases of the proposed solution. The Disaster Recovery Plan developed by the Bidder must address the alternative processing facility for the solution with at least 1,000 miles geographic separation; resulting recovery capabilities of major IT services, systems, and data; instructions on how stakeholders will be notified of changes to the plan and how it will be distributed to the stakeholders; how the plan will be tested on a regular basis; location of offsite backup storage facilities being used for the solution; how "post-resumption reviews" will be held following the successful resumption of services following a system outage; step-by-step instructions that the Bidder's staff will follow for recovery and resumption of services; maintenance of the plan during development and system maintenance phases of the project; training to its personnel on their assigned roles and responsibilities per the plan.

b. Use multi-location (geographic failover) maximum up time in event of a disaster in the primary hosting environment. The conditions that would perpetuate a disaster recovery failover shall be defined in the disaster recovery plan. The Bidder is required to submit a high-level disaster recovery plan with the information available from this RFP. A detailed disaster recovery plan will be developed prior to production go-live by the Bidder.

c. Configure backup equipment and software to meet agreed upon requirements.

d. Continuous database and directory server replication are required as part of the recovery plan.

e. This plan should be priced separately in the payment schedule.

7. Troubleshooting and Monitoring

a. Provide virtualization capacity planning to help, allocate and consolidate computing resources to optimize application performance.

b. Provide SSL VPN/Router management.

c. Provide support to contracted third party vendor performing penetration testing for MRM.

d. Provide troubleshooting and monitoring of all IaaS hardware and software.

8. Roles and Responsibilities

The IaaS Vendor will be responsible for the below items in the production and staging environments:

a. Servers/SAN/Network/Load Balancer Hardware and Software
b. Virtualization/Hypervisor
c. Redhat Enterprise Linux OS (If IaaS provider can provide the license which is cost effective compared to the MRM Consortium providing the license, then MRM will prefer that)
d. Server Security
e. Server Backup
f. Network Security (firewalls, reverse proxy, etc.)
g. Internet Diversity
h. Power and Cooling
i. Physical Security
j. Business Continuity

9. Other Requirements

a. The MRM system will contain Federal Tax Information (FTI). The MRM solution will use the following products in combination to safeguard this data as part of compliance with IRS 1075; the Appendix A Technical Architecture describes this is more detail. The IaaS Contractor must host this system as well.

- Appliance – Guardium S-Tap and S-Gate
- Appliance – Vormetric Data Security Manager (DSM)
- Appliance – IBM DataPower
- IBM Database Encryption Expert agent software
- Guardium File Encryption agent software

The MRM consortium has already procured the above appliances / software components. The Bidder shall allow the use of these appliances in the proposed cloud infrastructure.

b. The primary and secondary (DR) Data centers must be located in the continental United States.
c. FTI data cannot be accessed remotely by agency employees, agents, representatives, or contractors located offshore—outside of the United States territories, embassies, or military installations. Further, FTI data may not be received, processed, stored, transmitted, or disposed of by IT systems located offshore.
d. Identify all safeguards and methods that the provider will implement and maintain to protect a customer's confidential business data, such as FTI data, personal identification information (PII) data, social security administration (SSA) data, etc., from being accessed by the provider's employees or other contractors. Specifically address how FTI, PII, and SSA data encryption in transit, at rest, root access control, etc. is handled.

10. Detailed Architecture Assessment

    a. The purpose of the detailed architecture assessment is manifold. In the Bidder's proposal and during the oral presentation, the Bidder will respond to the scenario statements below using the following instructions:

        i. Demonstrate the Bidder understands the scenarios below.

        ii. Describe how the proposed conceptual or existing architecture will accommodate and satisfy each of the scenarios.

        iii. Describe architectural approaches that are used, trade-offs, any associated concerns and risks, and address items identified as "Issues" with the scenario. Include tradeoffs identified between architecture solutions and business functionality.

        iv. Provide architecture views such as the one below but not limited to:

            Hardware View – Topics: CPUs, storage, external devices and sensors, along with the networks and communication devices that connect them.

    b. Scenarios Statements

        i. System Monitoring and Response – The system begins to experience performance issues. The system provides monitoring of system problems and is able to immediately identify where the problem is occurring and notifies support staff.

        ii. Stopping the System – The system in one consortium state needs to be stopped. The system is stopped while the other states' system availability and operations are not affected.

        iii. Public Facing System Availability – The system is in the process of running daily batch processing. Public-facing self-service functionality continues and is not impacted during batch transaction processing. The public-facing self-service functionality meets the availability and response time requirements specified in the state and federal regulations, including but not limited to Publication 1075.

        iv. A New State Joins the Consortium – A new state is implemented and the system scales to maintain the same response rates and quality of service as before implementation. The system is configured to accommodate the new state(s) without modifying the common system.

v. End-user Response Time – A user invokes an online transaction with no external dependencies. The system processes the online transaction per requirements already specified in this RFP.

F. PRICING

Bidders shall segregate and submit via e-mail separately the portion of the proposal that contains the cost and proposed payment schedule. The payment schedule shall include three (3) years cost along with costs for production environments, disaster recovery plan, and capacity plan deliverables. Additionally, the proposed payment schedule shall include yearly costs for the three additional subsequent one (1) year option for support. This information will be evaluated by the Evaluation Committee.

G. CONFLICTS WITH TERMS, CONDITIONS, OR REQUIREMENTS

1. Bidder shall list any exceptions or confirm that it has no exceptions to any of the terms, conditions or requirements of this RFP and/or documents contained in the Appendices.

2. Exceptions shall be accompanied by alternative or substitute language, which would be acceptable to Bidder. Conflicts with stated requirements shall be noted in the corresponding paragraphs within Bidder's response format.

3. Additional terms or conditions proposed by Bidder for consideration shall be provided with a reference to the corresponding paragraph in the RFP or Appendix Document.

VI. PROPOSAL SCORING AND SELECTION

A. PROPOSAL RATING CRITERIA & EVALUATION

Proposals will be evaluated as described in this section. Proposals that do not meet the minimum eligibility criteria will be automatically disqualified and will not be scored. The criteria and the level of importance associated with each is listed below:

Scoring Criteria	% of points
Technical Expertise	
Solution	10%
Security and Compliance	15%
Vendor Experience	
Financial Stability	5%
Past Experience and References	5%
Organization/ Product/Service Maturity	5%

Operation Service Agreement	15%
Scalability/Elasticity/ Portability	10%
Terms and Condition	10%
Cost	25%

Bidders may be given an opportunity to provide an oral presentation or demonstration at the discretion of the MRM Consortium. ITSC reserves the right to limit the selection of the number of Bidders. ITSC reserves the right to select the site where the oral presentation will be demonstrated. During the presentation, Bidder shall provide specific responses to the questions posed to it and may also make a summary presentation of its proposal. The presentation shall include a description of how Bidder's revisions, if any, may have affected the over-all nature of its offer as compared to the initial proposal. If the Evaluation Committee members believe it to be necessary, a question/answer period may follow. The entire oral presentation, by the award winning Bidder, will become part of the contractual artifacts and will be legally binding on the Bidder unless and otherwise overridden by subsequent contract negotiations in writing.

B. AWARD AND NOTIFICATION

1. Award Recommendation

   Upon completion of the evaluation process, the Evaluation Committee will formulate a recommendation as to which proposal(s) is/are determined to be most advantageous to the MRM Consortium within available resources. A formal recommendation of the Evaluation Committee will be forwarded to the MRM Consortium Executive Committee for review and joint approval pursuant to the terms of the MRM Memorandum of Understanding.

2. Notice Of Intent To Award

   Upon approval of the recommendation, a Notice of Intent to Award will be published by NASWA/ITSC. The awarded Bidder(s) will be contacted by ITSC to complete post-award requirements.

VII. RFP EVALUATION PROCESS

A. PROPOSAL EVALUATION

An Evaluation Committee will judge the merit of proposals timely received in accordance with established evaluation criteria set and process (see below for the high-level factors).

B. EVALUATION PROCESS

The Consortium will undertake an intensive, thorough, complete and fair evaluation process. All Bidders shall be afforded fair and equal treatment throughout the evaluation process.

C. EVALUATION COMMITTEE

Each Evaluation Committee member will independently evaluate the merits of proposals received in accordance with the evaluation factors stated within this RFP, followed by discussion of the entire Evaluation Committee. The sole objective of the Evaluation Committee will be to recommend for award the proposal determined most advantageous to the MRM Consortium.

D. BASIS FOR AWARD

The purpose of this RFP is to solicit proposals for the goods/services specified herein. The requirements stated within this RFP represent the minimum performance requirements necessary for response as well as desired elements of performance.

E. CLARIFICATIONS/DISCUSSIONS

The Consortium may conduct discussions with selected Bidders for the purpose of promoting understanding of the Consortium's requirements and Bidder's proposal, clarifying requirements, and making adjustments in services to be performed and in prices and or rates. Bidders engaged in such discussions may be sent a list of questions and will be given a specified number of days in which to formulate and submit written responses to the questions and provide any related revisions to their initial proposals. The nature of the questions will be, generally, clarifying in nature and will permit related revisions to proposals. Such revisions will be at the option of Bidder, but will be limited to the guidelines set forth in the Consortium's requested clarifications. No major changes will be permitted, nor will the Consortium accept any additional written materials not relevant to the questions/clarifications requested.

F. BEST AND FINAL OFFERS ("BAFO")

Adjustments may also be allowed in conjunction with clarifications, discussions, presentations and or demonstrations, but only to the extent such revisions are consistent with the proposal requirements.

These revisions will be considered as best and final offers. Such adjustments shall be submitted in writing.

G. FINAL EVALUATIONS

After completion of clarifications, presentations, and BAFOs, as may be required, the Evaluation Committee will re-consider the initial proposal ratings and may make any adjustments they believe to be warranted as a result of the additional information obtained.

H. NOTICE OF INTENT TO AWARD

Upon approval of the recommendation, a Notice of Intent to Award will be published by ITSC and the Awarded Bidder will be contacted by ITSC to complete post-award requirements.

I. ADEQUACY AND COMPLETENESS OF RESPONSE

In general, all aspects of a proposal will be evaluated based on its adequacy and completeness with regard to the information requested in the RFP and its appendices; i.e., compliance with terms, conditions and other provisions contained in the RFP, as well as Bidder's ability to read and follow instructions. Failure of Bidder to provide the information required in this RFP may result in disqualification of the proposal.

This responsibility belongs to Bidders.

J. CONTRACT REVIEW

Bidders shall review the attached sample Terms and Conditions, Operational Service Agreement, and Data Security Agreement and list any exceptions or confirm that no exceptions are taken to the each contract. Any exceptions to the aforementioned shall be accompanied by alternative or substitute language which would be acceptable to Bidder. ITSC will review the proposal to ensure Bidder has not taken any exceptions which may be deemed unacceptable or exceptions to stated requirements which may be deemed unacceptable in meeting the RFP requirements of the Consortium or any MRM State. Any exceptions taken could result in elimination of Bidder's proposal from further consideration, or result in delay or failure to execute a contract, whereby ITSC could terminate the award and commence negotiations with another Bidder.

APPENDIX A

MRM CONSORTIUM

TECHNICAL ARCHITECTURE

Version 2.1

April 20, 2015

Document Revision List

Rev#	Date	Description	New Page #	Prev Page #	Revised By
1	09/23/2013	Document updated as per the review comments given by ITSC.			TCS
2	09/23/2013	Document updated as per the review comments given by State of Maine.			TCS
3	10/02/2013	Document updated as per the review comments given by State of Rhode Island.			TCS
4	10/21/2013	Document updated as per the review comments given by State of Maine on Version 1.1.			TCS
5	10/25/2013	Document updated as per the review comments given by ITSC on Version 1.1.			TCS
6	10/29/2013	Document updated as per the review comments given by State of Rhode Island on Version 1.1.			TCS
7	01/27/2014	Document updated with changes given by MDES. ACCESS MS Server details have been added along with updated logical diagram on Version 2.0.			TCS
8	02/24/2014	Document updated with changes given by MDES. ACCESS MS logical diagram has been updated along with few Software components on Version 2.1.			TCS
9	04/25/2014	Document updated with changes given by MDES. ACCESS MS logical diagram has been updated along with sentence modification for Access environment under chapter 3.			TCS

Table of Contents

Table of Figures

1. Introduction

This document contains the technical architecture for the Automated Comprehensive Claims and Employment Service System (ACCESS) of MRM Consortium being developed as part of the Phase III of Unemployment Insurance Modernization (UIM) project for the Mississippi Department of Employment Security (MDES).

This document will form the technical basis for the subsequent phases of the project such as technical detailed design, construction and enhancement.

1.1 Target Audience

The target audience for this document is the MDES development team, the MDES business user and the Tata Consultancy Services (TCS) development team.

1.2 References

The technical architecture is created based on the following artifacts:

- Technical Architecture document for ACCESS MS Tax and Benefits System
- Scope of Work document for the MRM Consortium

2. Acronyms and Abbreviations

S No	Acronyms	Description
1.	ACCESS	Automated Comprehensive Claims and Employment Service System
2.	ALJ	Administrative Law Judge
3.	API	Application Programming Interface
4.	AS	Application Server
5.	BI	Business Intelligence
6.	BIRT	Business Intelligence and Reporting Tools
7.	BOR	Board of Review
8.	CSR	Customer Service Representative
9.	CSS	Cascading Style Sheets
10.	DAO	Data Access Object
11.	DBMS	Database Management Systems
12.	DHS	Department of Human Services
13.	DMS	Document Management System
14.	DMZ	Demilitarized Zone
15.	DNS	Domain Name Server
16.	EAP	Enterprise Application Platform
17.	EJB	Enterprise Java Beans
18.	ES	Employment Services
19.	ETL	Extract, Transform and Load
20.	FEIN	Federal Identification Number
21.	FTP	File Transfer Protocol
22.	HTML5	Hyper Text Mark-up Language 5
23.	HTTP	Hypertext Transfer Protocol
24.	HTTPS	HTTP over SSL

S No	Acronyms	Description
25.	Iaas	Infrastructure as Service
26.	IBM	International Business Machines
27.	ICON	Interstate Connectivity
28.	IDE	Interactive Development Environment
29.	IIOP	Internet Inter-ORB Protocol
30.	IP	Internet Protocol
31.	IRS	Internal Revenue Services
32.	IT	Information Technology
33.	ITS	Information Technology Services
34.	IR	Interactive Response
35.	JEE	Java Platform Enterprise Edition
36.	JAAS	Java Authentication and Authorization Service
37.	JAF	Java Activation Framework
38.	JAXP	Java API for XML Parsing
39.	JDBC	Java Database Connectivity
40.	JDO	Java Data Objects
41.	JMS	Java Message Service
42.	JMX	Java Management Extensions
43.	JNDI	Java Naming and Directory Interface
44.	JPA	Java Persistence Architecture
45.	JSP	Java Server Pages
46.	JSTL	Java Standard Tag Library
47.	JTA	Java Transaction API
48.	KPI	Key Performance Indicator
49.	LDAP	Lightweight Directory Access Protocol
50.	MDES	Mississippi Department of Employment Security

S No	Acronyms	Description
51.	ME	Maine
52.	MQ	Message Queue
53.	MRM	Mississippi, Rhode Island and Maine
54.	MS	Mississippi
55.	MVC	Model View Controller
56.	OCR	Optical Character Recognition
57.	ODBC	Open Database Connectivity
58.	ODBO	Object Linking and Embedding, Database for Online Analytical Processing
59.	OLAP	Online Analytical Processing
60.	OMG	Object Modelling Group
61.	ORB	Object Request Broker
62.	ORM	Object Relational Mapping
63.	RI	Rhode Island
64.	RMI	Remote Method Invocation
65.	RTC	Rational Team Concerts
66.	SAN	Storage Area Network
67.	SDK	Software Development Kit
68.	SIEM	Security Information and Event Management
69.	SOA	Service Oriented Architecture
70.	SSH	Secure Shell
71.	SSL	Secure Sockets Layer
72.	SSO	Single Sign On
73.	TCS	Tata Consultancy Services
74.	UAT	User Acceptance Test
75.	UDB	Universal Database

S No	Acronyms	Description
76.	UI	User Interface
77.	UIM	Unemployment Insurance Modernization
78.	VSAM	Virtual Storage Access Method
79.	WAN	Wide Area Network
80.	XML	eXtensible Mark-up Language

3. Technical Architecture Validation

This section describes the technical architecture validation decisions made for the ACCESS System based on the Access MS Benefits and Tax Systems. ACCESS-MS current system is having two environments namely UAT and Production.

Application Hosting

The UI application for all the MRM Consortium states will be hosted out of a third party data center. The infrastructure for ME, MS & RI will be hosted separately on a cloud (IaaS) infrastructure that will be also managed by a third party such as IBM, Savvis, AT&T, BULL or others. The entire platform will be virtualized so that any requirement for scaling up / down can be easily achieved. This will also enable any future consortium member state to deploy the new UI application within a very short turnaround time. The modular architecture will enable any future state to be part of the MRM consortium within a very short time span.

The new MRM application will be based on the IaaS cloud platform and will have three logically separate infrastructures for each of the member states. Each state will have the below mentioned servers for their state specific application with a common code base and business rule sets.

MDES had discussions with IBM & Sun Guard regarding the application hosting on cloud infrastructure (IaaS). They will also explore the options with a few more vendors and keep all the MRM consortium member states informed as more information is available.

The following table presents the various architectural software and hardware components and any applicable upgrade paths.

S. No	Software Component	Current Version (Mississippi)	Upgrade To	Remarks
3.1	**Programming Language**			
1.	Java Programming Language	Java 6	Java 7	
2.	Java Enums	Java 5 Based Enums	Java 7 Based Enums	
3.	Objective C	None	2.0	iOS programming language
3.2	**Commercial Software**			
4.	DB2 UDB Database	9.7	10.5	Upgrade the fix packs as and when need arises.

S. No	Software Component	Current Version (Mississippi)	Upgrade To	Remarks
5.	WebSphere Application Server	7.0+ (Supports JEE 5 specifications and Java 6)	8.5 (Supports JEE 6 specifications and Java 7)	Options are being explored if JBoss Enterprise Application Platform v 6.1 can replace WebSphere 8.5.
6.	Drools Workflow	5.1	Same	
7.	LDAP Server	Sun Directory Server 5+	RedHat JBoss Directory Server 8.2	
8.	Spectrum Address Validation	Spectrum Software	Same	Current licensing is at 3 million records hit per year.
9.	Mail Stream Plus	Mail Stream Plus	Same	Current licensing is at 3 million records hit per year
10.	Reporting Servicer	JReport 9.0+ / BIRT	BIRT 4.2	JReports will have to be migrated to BIRT server.
11.	Microsoft MS Access – Adhoc Reporting	Microsoft MS Access 2003	IBM Infosphere	
12.	IR	Avaya	Same	IR Software is out of scope. State will continue to use their existing software which the Application will Interface with Weekly Certification filing functionality.
13.	Spell Check Software	Rapid Spell - http://www.keyoti.com/products/rapidspell/javaWeb/#	Same	
14.	Drop Down Menu Software	UDM 4.5	Same	
15.	IBM Cognos BI	None	IBM Cognos BI 10.1	Refer 8. Business Intelligence for Cognos features and comparison with other BI products.
16.	IBM App Scan	None	IBM Security App Scan 8.7	Refer 6.2.3. Security for more details

S. No	Software Component	Current Version (Mississippi)	Upgrade To	Remarks
17.	IBM Infosphere Guardium Data Activity Monitor	None	9.0	Refer 9.1 IBM Infosphere Guardium Data Activity Monitor for more details.
18.	IBM Infosphere Guardium Data Encryption	None	9.0	Refer 9.3 IBM Infosphere Guardium Data Encryption for more details.
19.	EMC AVAMAR	6.1	Same	Refer 10.1.14 Backup Process for more details.
20.	Connect Direct	4.6	Same	Software Tools used for TOP requirement. Refer 10.1.12 TOP (Treasury Offset Program) for more details.
21.	JSCAPE MFT Server	JSCAPE MFT Server Professional Edition 7.2	JSCAPE MFT Server Professional Edition 8.8	JSCAPE MFT Server is a platform independent managed file transfer solution that centralizes all file transfer processes. JSCAPE MFT Server supports all major file transfer protocols including FTP/S, SFTP, SCP and HTTP/S.
22.	Vormetric Data Security Manager	None	Latest available version	Centrally manages policies and keys for all Vormetric products.
23.	Vormetric Transparent Encryption	None	Latest available version	Secures any database, file or volume across servers.
3.3	**Open Source Software**			
24.	DMS - Apache Jackrabbit	1.5	2.6	Upgrade as and when need arises and a stable version is available. Refer 10.1.7 Document Management System for more details

S. No	Software Component	Current Version (Mississippi)	Upgrade To	Remarks
25.	Batch Scheduler Software - Quartz	1.7.3	Same	Upgrade as and when need arises and a stable version is available
3.4	**Application Framework Software (Open Source)**			
26.	User Interface Layer - Apache Struts	1.3.5	Same	Decision taken to remain with Struts 1 and not upgrade to Struts 2 as it will require major change and there won't be much benefits.
27.	Data Access Layer - Hibernate	3.3.2 with Annotations.	4.2	
28.	Logging – Log4j	1.2.2	Same	
29.	Display Tag Library (Search Result Screens)	1.2	Same	
30.	Bitronix Transaction Manager (BTM)	1.3+	Same	It's used as standalone transaction manager for BizServer
31.	Business Rules Engine	None	JBoss Drools Expert 5+	Rules Engine to be integrated for implementing State Specific Rules.
32.	Cocoa Touch	None	2	Framework Collection for iOS app development
3.5	**Development Software/Tools**			
33.	Requirements Management – Rational Requirements Composer	None	Jazz Platform 4.0	For requirements, use case management and impact analysis.
34.	Rational Team Concerts	None	Jazz Platform 4.0	Configuration management tool with version control and work item management

S. No	Software Component	Current Version (Mississippi)	Upgrade To	Remarks
35.	Rational Software Architect	None	IBM Modelling Tool	Modelling during analysis and design phase.
36.	Rational Quality Manager	None	IBM Testing Tool	Managing test plan, test design, test implementation, execution and evaluation
37.	Rational Performance Tester	7.1	8.1	
38.	Robo Help			Help file generation
39.	Prototype	Axure	Axure	http://www.axure.com/
40.	Eclipse IDE	3.4.2 , 3.5+	RTC Client	
41.	Ant	1.7+	1.8+	Apache Ant is a Java-based build tool.
42.	JBoss – Development Application Server	5.0+	7.0+	For development environment
43.	SQL Client - Squirrel	3.5	Same	Update as and when need arises and a stable version is available.
44.	XDoclet (1.2.3)	1.2.3	Same	Struts Configuration Generator, Struts Validation Generator
45.	Eclipse with ADT	None	3.5+	Eclipse with Android Development Tools plugin
46.	Google CodePro AnalytiX	7.0	Same	CodePro tools used for code quality
47.	Android SDK	None	4.3	Android mobile app development kit
48.	Xcode	None	4.6.3	IDE for iOS app development
49.	iOS SDK	None	6	Software Development Kit for iOS

S. No	Software Component	Current Version (Mississippi)	Upgrade To	Remarks
3.6	**Software Systems (Production)**			
50.	Consortium DB2 Database	Benefits & Tax Database for MS	DB2 Schema is common for all three consortium states.	
51.	Web Application	Separate Benefits and Tax Web application	Each state will have its own Benefits and Tax application instance	Pros and Cons discussed later on in this section.
52.	Drools Database	Drools Tables resides in the ACCESS database.	Same	
53.	BizServer	MS Biz Server	Deploy as a separate application for each state.	
54.	Batch Server	MS Batch Server	Deploy as a separate application for each state.	
55.	Report Server	MS Report Server	Separate Reporting server for each state.	
56.	Mail Stream Plus Server	Mail Stream Plus server	Same server	
57.	DMS Repository	DMS repository	2 DMS Repositories with Current and Old documents for each state	

3.7 Separate vs. Bundled Application

The main purpose of separating the Tax and Benefits applications is to reduce the dependency of the Tax application to the Benefits application and vice versa. To further separate the existing applications, the common features that are used by both the Tax and Benefit applications will be restructured and maintained in the core framework. As a result, the Tax and Benefits applications will use all these common objects and methods from the framework layer. By maintaining this architecture, we can avoid code repetition in each state specific application, increasing maintainability and developers' productivity.

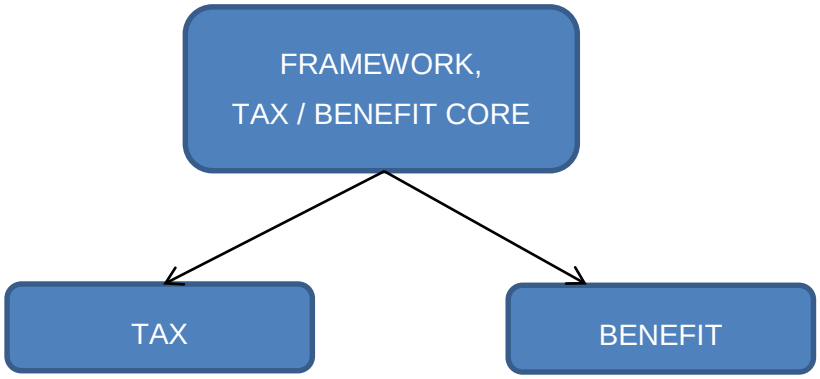

Figure 1: Build process for separate application

The following table lists the pros & cons of providing the Tax system as a separate application vs. bundling the Tax application with the Benefits application.

Comparison between Tax and Benefits as a separate application and bundled application

S. No	Separate Application	Bundled with Benefits Application
1.	Problems of each application are isolated. Problems occurring in one application will not affect the others.	Problems of one application can affect the working of other application.
2.	Each application can be brought down on their own times, independent of each other. Tax application will be up and running even when Benefits is down and vice versa.	If there is an issue in either Benefits or Tax, the whole application has to be brought down for the fix/new build to be deployed.
3.	Availability of the system increases.	Availability of the system decreases
4.	Maintainability of the system increases. Software system or component can be modified to correct faults, improve performance or other attributes, or adapt to a changed environment without having any adverse effect on the other system.	Maintainability of the system decreases.
5.	Deployment benefit increases, as the codebase gets smaller the build and deployment time will decrease.	Build and deployment time will increase as codebase will get bigger.
6.	Any issue related with multiple application login can be easily resolved with Single Sign On between these two applications.	None
7.	Developer's productivity increases as the development build time decreases due to small codebase	Developer's productivity decreases as the development build time increases due to larger codebase
8.	Performance of the system increases as the software size decreases along with the distribution of the number of concurrent users accessing the system.	Performance of the system can easily decrease due to larger number of concurrent users even when they are accessing quite different modules of the system.

Recommendation: Deploy Tax as separate application

4. General Description

This section describes a high-level architecture overview of the ACCESS System, which will be on a distributed computing environment.

4.1 Architecture Overview

The ACCESS System will be built on Java Platform Enterprise Edition (JEE 6) based multi-tier architecture. ACCESS will have three main tiers:

- Client Tier
- Middle Tier
- Enterprise Information System (EIS) Tier

These tiers contain multiple layers, which interact with each other to perform business functions. The main reasons for dividing the application into tiers/layers are:

- Each layer has a specific system abstraction and specific responsibilities.
- When an application is divided into layers, each layer can be monitored, tuned, and upgraded independently.
- The partitioning of the application enables rapid design and development of the system.
- Separating the functions into distinct layers enables ease of monitoring and better optimization of the performance of each layer.
- Load balancing and addition of capacity can be performed independently in each layer.
- Multi-tier architecture makes it simpler to scale the system across multiple processors on different machines.
- The separation of operations provides the ability to add features easily without having to redesign the entire system.

Figure 2 depicts the logical view of the ACCESS layered architecture. The design of ACCESS will predominantly be based on this architecture.

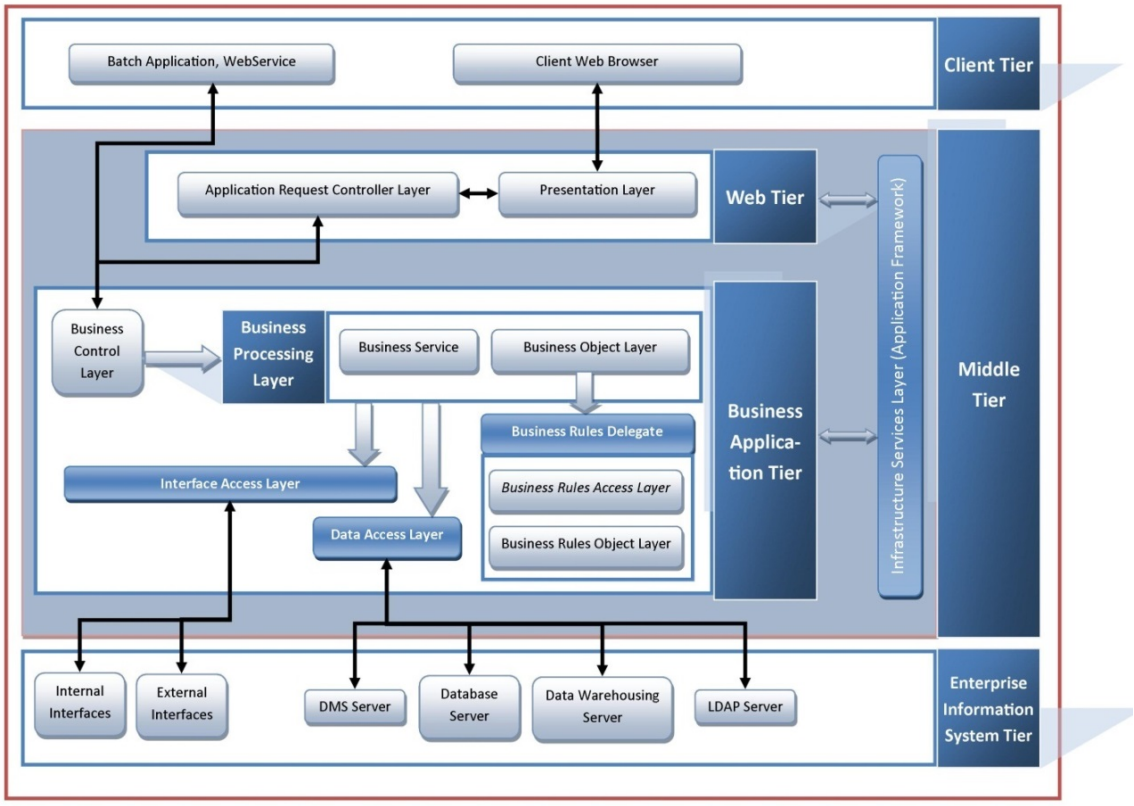

Figure 2: Logical View of ACCESS Layered Architecture

4.1.1 Client Tier

For the ACCESS system, the client tier will be the combination of browser, batch application and IR web service.

4.1.1.1 Browser

A browser is the means by which the users will connect to the system. Browsers are the thinnest of clients; they display data to the users and rely on servers for application functionality.

4.1.1.2 Batch Application

A batch application will also act as a client for the main application business processing. To take the load off the main server, another server application (BizServer) will be deployed to process requests coming from the batch application.

4.1.1.3 Web Service

4.1.1.3.1 IR Application

An IR application will also act as a client for the main application business processes. This IR application will send the request to the main business processes via the wrapper web services. The request will be processed and response will be sent back via the synchronous two way request-response mechanism.

4.1.1.3.2 Mobile Application

A Mobile application will also act as a client for the main business processes. This mobile application will interact with the ACCESS system via web services to provide access to business services to the end user. This request will be processed and response will be sent back to mobile devices synchronously. Details of mobile application for ACCESS system has been described in detail in the Mobile Application section of this document.

4.1.2 Middle Tier

The middle tier receives and processes requests from the client tier. This eliminates the need for client programs to deal with the complexity of databases and other complex back end systems. The middle tier is made up of the following:

- Web Tier
- Business Application Tier
- Infrastructure Services Layer (Application Framework)

4.1.2.1 Web Tier

Web Tier will have two main layers and they are:

- Application Request Controller Layer
- Presentation Layer

Application Request Controller Layer

The Application Request Controller Layer receives the request from the client tier and forwards to the appropriate User Interface (UI) model of the Presentation Layer and also to the Business Control Layer for processing. It also acts as a mediator between the Presentation Layer and the Business Layer.

Presentation Layer

Most of the end user interactions (except batch processing and internal messaging invocation for workflow components) with the system will be through the Presentation Layer. The Presentation Layer will be used to display information and for receiving inputs from the end user. This layer has been sub-divided into four parts:

- User Interface (UI) View
- User Interface (UI) Model

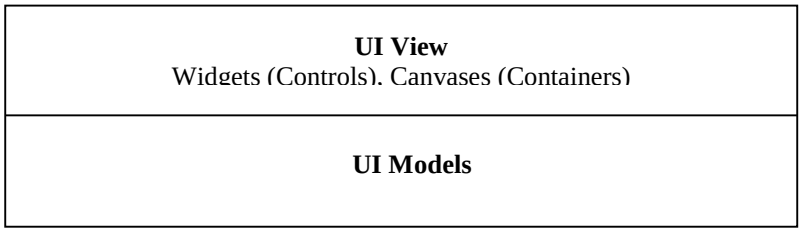

Figure 3: Presentation Layer

The UI view layer is responsible for managing the user interaction and visual aspects of the system. Examples of user interaction management are:

- Navigation scheme (Both screen and field navigation)
- Graphical widgets used for capturing data and to issue a command

Examples of visual aspects are:

- The static text displayed in a screen
- The language used to display static text
- Graphical Widgets used to display dynamic/static system information
- The order in which the information is presented

The main focus of the presentation layer is to provide the ability to change the visual aspects of the system without affecting other parts of the system. This is achieved by separating the UI model from the UI view layer. UI model is the layer beneath the UI view layer. UI Model is a non-graphical representation of the UI view layer. The advantages of dividing the presentation layer are:

- UI view (see Figure 3) is not required to drive other layers. This facilitates automated testing of components belonging to other layers and independent development of other layers without requiring any UI to drive them.
- Provides flexibility to choose from a variety of widgets and canvases and have different views of the same model.

UI view will be an extremely thin layer, which will capture the user inputs and will have the ability to perform very basic functions and then pass the information to the UI model. The UI model retains all the information that is displayed in presentation and will interact with the application layer to accomplish the end user's request. One UI model can be linked to a number of UI views.

4.1.2.2 Business Application Tier

Business Application Tier will have four main layers and they are:

- Business Control Layer
- Business Processing Layer
- Business Rules Delegate
- Interface Access Layer
- Data Access Layer

Business Control Layer

The Business Control Layer passes the request from the application request controlling layer to the business processing layer. This is the only way for the UI model of the presentation layer to get data from the business processes.

Business Processing Layer

The Business Processing Layer contains the "business rules" or the main processing logic of the application. Business processing layer will have two sub layers:

- Business Service Layer (also known as the Business Function Layer)
- Business Object Layer

The Business Object Layer houses all the real world entities (physical as well as logical) that are stakeholders of the system. Each entity has attributes and operations that can be performed by the entity / on the entity. Business objects are connected to the database through the Data Access Layer. The Business Service Layer assembles the information from business object layer to serve a distinct business purpose. Each assembly represents a method in Business Service Layer. This layer receives inputs from UI Layer, invokes business objects and subsequently modifies the state of the system.

Business Rules Delegate

The Business Rules Delegate implements the delegate pattern for Business Rules Implementation. The implementation contains of following two sub layers:

- Business Rules Access Layer
- Business Rules Object Layer

The Business Rules Access Layer represents the framework classes that abstract the logic of accessing the Business Rules Knowledgebase from the calling Business objects. The Business Rules Object Layer consists of the Fact model required for Business Rules implementation. The Business Rules Delegate is explained in detail in the Business Rules Framework and Guidelines document checked in at: *"<consortium_main_view>\ACCESS_CONSORTIUM_VOB\20-Standards And Guidelines\Business Rules\ Business Rules Framework and Guidelines Doc.docx"*

Interface Access Layer

The Interface Access Layer will manage the abstractions for any external and internal systems. Business Processing Layer will be the only layer that interacts with this layer, which helps in isolating the dependencies of other system.

Data Access Layer

The Data Access Layer helps the components of business layer to access data and hides the implementation details of the underlying Enterprise Information System Tier.

4.1.2.3 Infrastructure Service Layer

The Infrastructure Service Layer is also called the Application Framework and has been described in detail in the Application Framework section of this document.

4.1.3 Enterprise Information System Tier

EIS tier provides the information infrastructure that is vital to the business processes of an enterprise. The EIS tier handles software and includes enterprise infrastructure systems such as database servers, directory servers, and internal/external systems.

4.1.4 Business Rules Engine

The Business Rules Engine is used to write all the business validation rules in a specific rule file. It will provide a separate layer from the development code (Business logic). Whenever any changes will be required to those validations it will only be necessary to change the rule files. So, there will be no need to change the code. Implementation for the Business Rules Engine has been described in detail in the Business Rules Implementation section of this document. The Business Rules framework component will be rolled out into Production well before the MS Benefits 1 rollout to serve as the POC for the implementation. This framework component rollout will be planned along with the MS support builds planned.

Key Features and Advantages of the Business Rules Engine:

- Declarative Programming
- Logic and Data Separation
- Speed and Scalability
- Centralization of Knowledge

5. Core and State Specific Component Implementation

For the MRM Consortium project, a single code base for all the three states and individual state specific deployment architecture is proposed. The single code base will be comprised of core and state specific components. This will support centralized application support for all the states thus reducing overall maintenance cost. The individual state specific deployment of the application will provide flexibility in terms of life cycle management to each state application thus allowing scheduling of application builds and upgrades for each state to be independent of the others.

5.1 Codebase Setup

For code configuration management it is suggested to upgrade to Rational Team Concert which is an upgrade of the current software Rational Clearcase-Clearquest UCM implementation. The Figure 4 depicts the various components that will be configured for the MRM consortium.

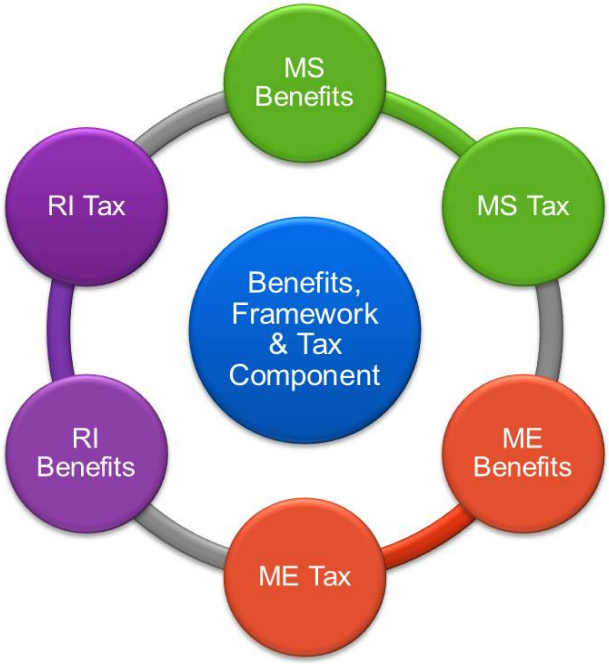

Figure 4: Components of MRM Consortium

This suggests a single code base repository for all the consortium member states. The single code base will facilitate centralized maintenance of the system. For Application deployment, each state will have its own instance of the application which will contain the common core component and the state specific component constituing the application. This is the same concept that is currently implemented in MS for Benefits and Tax with each application containing the common framework component. The application with the common and state specific component will be prepared by using the ant scripts. Following example explains the movement of a code(Activity) for multiple states in different builds.

Scenario: Activity 1 contains code changes corresponding to the common core component. This needs to be moved to all 3 states.

Following are the steps for moving this CQ for all 3 consortium states; these steps will further be finalized and elaborated once we have the RTC setup in place:

1. Developer works on the activity in local and delivers the code to the UAT stream after performing Testing and approval.
2. Developer resolves the activity marking that this is a core component change and requires build for all 3 states.
3. From UAT stream UAT build is done for the CQ where it is properly tested for moving to Production.
4. Once the CQ is verified, the code is moved to the Integration stream. From here the code will be moved to the staging stream for each state.
5. Based on each states scheduled build time, the code will be moved to the PRODUCTION stream for that state. And with the build, the code will be running in PRODUCTION for the state.

For cases where the build is only required for 1 state, i.e. the code change is only in the state specific component, the steps will remain the same as above. Only difference would be that the builds (UAT/Production) will be done only for that 1 state.

5.2 Framework services and capabilities for Core and State Specific Implementation

The application framework will be enhanced to accommodate the state specific differences at various points in the application with ease. The following points describe each of the identified areas for advancement.

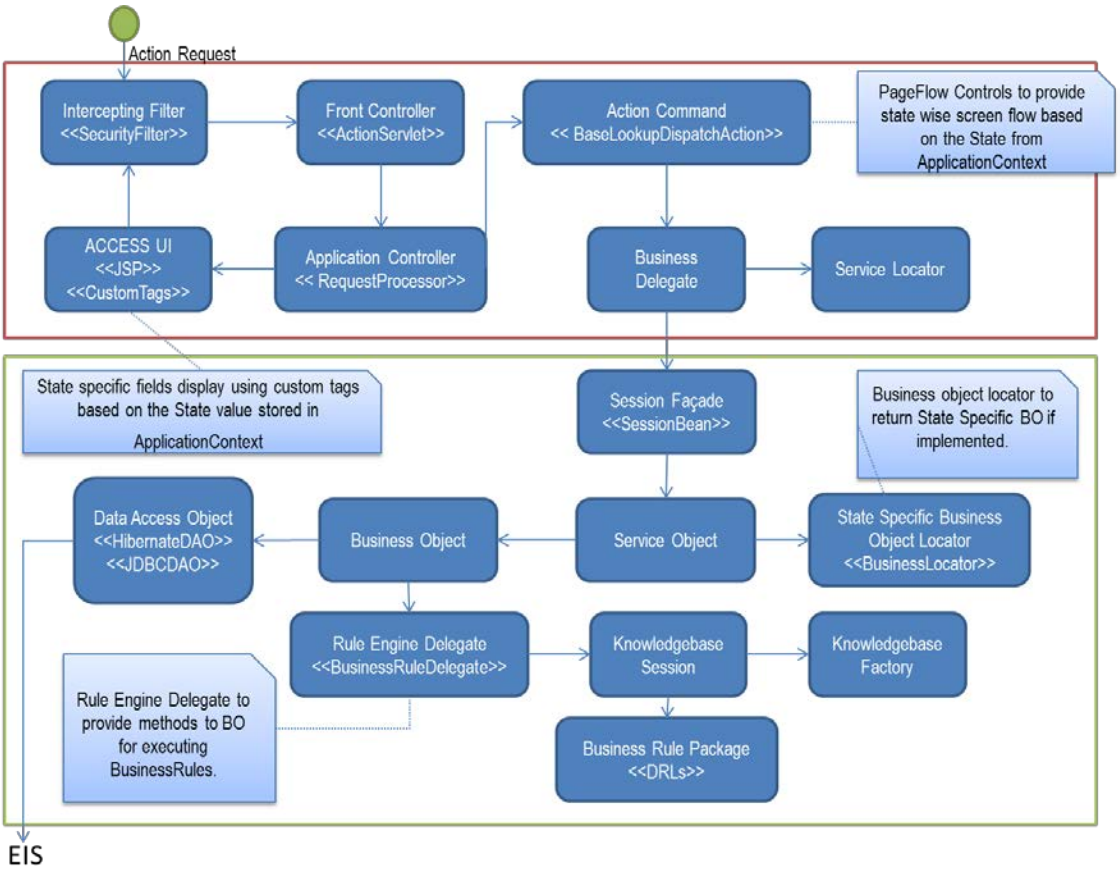

Figure 5: Component Diagram for Framework Services corresponding to Core and State Specific Implementation

5.2.1 State Specific GUI components to be displayed

The current ACCESS framework consists of a rich collection of framework tag libraries as well as a custom built tag library created specifically for the project. These tags enable consistent browser/platform GUI representation and enforce standardized coding practice.

The tag libraries will be enhanced to include tags for state specific GUI component display.

5.2.2 State Specific Screen flow

The ACCESS framework keeps track of pages visited by the users. It gives the framework methods to traverse automatically back to previous pages visited. The page flow framework will be upgraded to have option of dynamically provide the screen based on state specific business rules that needs to be displayed beyond for a state specific application.

5.2.3 Business Rules Implementation for State Specific Business rules

JBOSS Drools Rules Engine will use DRL or Decision Table (XLS) files to write all the business validation rules.

Two approaches can be possible to write the state specific business rules.

1. To write all the state specific business rules in single state specific DRL file.

Implementation:

In this approach we can write all rules in a single DRL file and make one such DRL file for each different state implementation.

For execution of rules the Knowledgebase instance is required which uses the DRL files as an input. Using the Knowledgebase factory container will create one instance by passing all the state specific DRL files which contain all the state specific business rules.

Once the business objects need to execute some rules for any state it requires this Knowledgebase instance. After getting this instance it will create a Knowledgebase session from it, insert the required rules object into the session and then execute the rules.

Pros and Cons for using single Rule file

S. No	Pros	Cons
1.	In this approach only a single state specific DRL file will be created which contains all the business validation rules of specific states.	Creating a single file for all the business rules is difficult to manage.
2.	Deployment will be easy, since after modification only one file would be deployed.	If we need to change only one rule we need to modify this file and if any error exists it will not execute any rules.
		For every change in the single file complete testing of all rules would be required.

2. Creating state specific Rule package which contain several DRL files.

   Implementation:

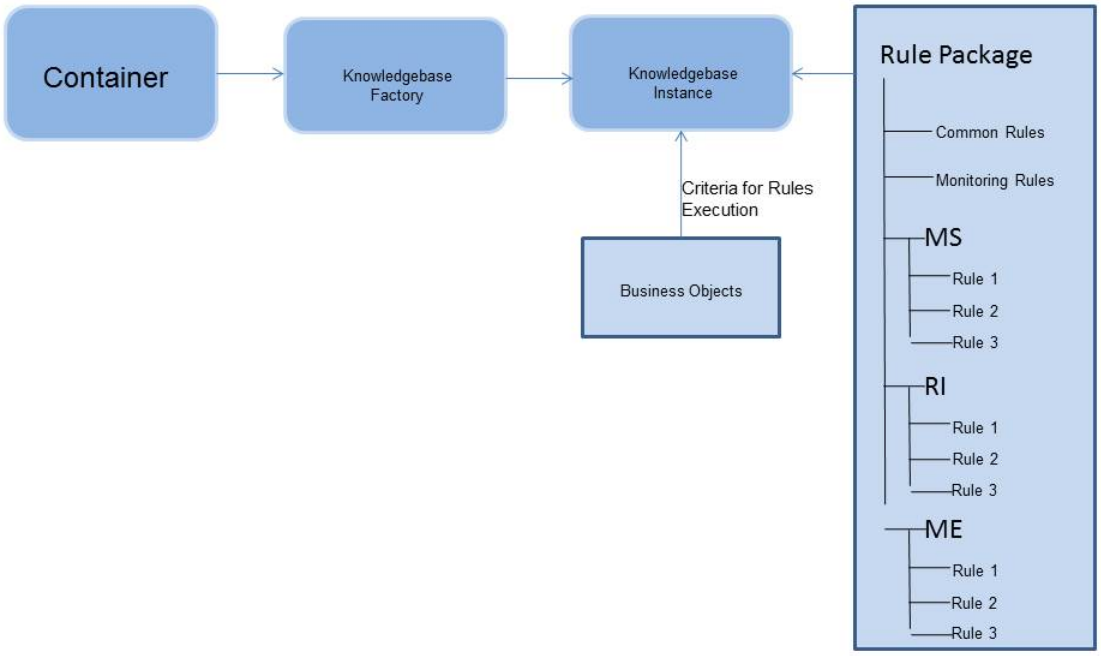

Figure 6: Business Rules Implementation

In this approach we can create one Rule package which contains all the common DRL files which can be used across the state. Along with this we need to create state specific packages inside that Rule package which should contain only state specific business rules. After that we need to create one XML or Property file to provide the mapping of the actual DRL file path to some logical name.

For execution of rules Knowledgebase instance is required which uses the DRL files as input. Using Knowledgebase factory container will create one instance of Knowledgebase by passing this XML or Property file.

Once the business objects needs to execute some rules it will use the Knowledgebase instance and provide the criteria for which rules needs to be fired. After getting this instance it will create a Knowledgebase session from it, insert the required rules object into the session and then execute the rules.

Pros and Cons for using Rule Package with multiple Rule file

S. No	Pros	Cons
1.	For specific combination of rules, different DRL files are provided to easily manage.	Many files will be created for single state specific business validation rules.
2.	For any little change we need to test those specific rules only. No need to test entire state business rules.	Deployment activity should be done in proper manner to handle the changes of various rules.

5.2.4 Extend Core business layer for State specific implementation

The core business logic for the ACCESS MRM application will reside in the Core component of the application. For requirement of business logic that cannot be part of the core component and is required to be implemented as state specific peace, State specific peace can extend the core business component and override the business method for the state specific functionality.

The framework will be enhanced to provide framework methods to dynamically provide the state specific instance of the business object if available to the Service layer. This will require change in the application code instantiating the business object to use the framework method of getting the business instance.

5.2.5 Mobile Application

This section outlines the requirements and strategy of mobile application development for ACCESS system.

Some components of ACCESS would be developed for mobile platforms. The target platforms are - Android and iOS.

Since we are targeting two different mobile platforms, a comparison of different possible approaches for developing apps for multiple platforms follows. Basically, there are two ways to developing applications for multiple mobile platforms.

1. Using Native SDKs
2. Using Non-Native SDK

Using Native SDK – This is the straight-forward approach, using the native programming languages (Java for Android and Objective-C for iOS) to code.

Pros and Cons for Native SDK

S. No	Pros	Cons
1.	No 3rd party dependency.	For each platform, a separate development.
2.	No extra licensing and cost.	Requires knowledge of each multiple platforms' development tools and native programming languages.
3.	Development tools and programming languages are used and recommended by the platform developers.	
4.	All the features that the platform has to offer are readily available for the application to utilize via software frameworks and libraries provided by the platform developers.	
5.	Application performance is always better than the non-native.	
6.	Less chances of platform upgrade on the device breaking the application.	
7.	Smoother distribution process.	

Using Non-Native SDK –

In this approach, a non-native SDK can be used to develop an application that could be built for multiple (supported) platforms.

An example of such framework is the Corona-SDK (most popular in the market), which uses the Lua programming language for coding. It claims to support the platforms like iOS, Android, Kindle, and Nook.

Pros and Cons for Non-Native SDK

S. No	Pros	Cons
1.	Develop one application but build and distribute for both the platforms.	Introduces dependency on a 3rd party.
2.	Knowledge of only one development framework, tools and programming language needed.	Requires extra licensing and cost.
3.		Upon new releases by the native platforms, have to wait till the new features are implemented by the 3rd party.
4.		Platform features limited to what the non-native SDK supports.
		Can introduce application inconsistency. Platform A might not have a feature which is available on platform B and the non-native framework.

Recommendation:

Based on the research, suggested approach for mobile app development is by using native SDKs.

Mobile Application Integration

Mobile application will be integrated with ACCESS system via WebService calls.

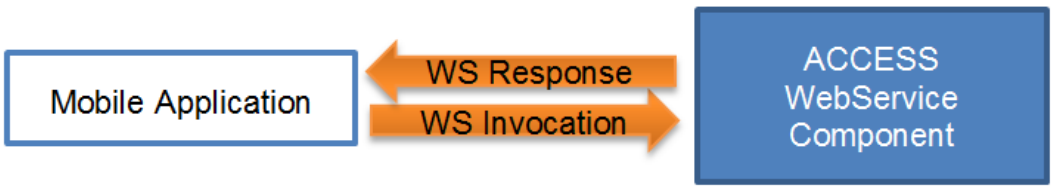

Figure 7: Mobile App Integration

5.2.5.1 Android

This section covers the mobile application development for ACCESS in Android OS (Operating System).

5.2.5.1.1 Targeted SDK and OS

According to the data collected by Google Inc., less than 5% of all android devices user uses Android OS version prior to 2.3 (Gingerbread). So the mobile application for ACCESS system would be targeted for all android OS running Android 2.3 to 4.3.

I.e. The minimum required SDK for the android devices to run ACCESS mobile application would be Android 2.3 (Gingerbread) with API 9 and targeted SDK would be the latest SDK available in the market, which is Android 4.3 with API 18.

Figure 8: SDK selection for Android App Development

5.2.5.1.2 Targeted Devices

The devices that use Android OS are divided into four different size based on their screen dimension viz. small, normal, large and xlarge.

Figure 9: Hardware Classification by screen size

Application developed for one specific type of screen will automatically fit on the other size of screens however it may cause difference in display. Hence, the application will be targeted and tested primarily for normal screen. Dimension for the GUI objects will be provided in DP (density independent pixels) wherever possible; in order to minimize the variation in display caused by devices with different pixel densities per inch.

5.2.5.1.3 Development

During the Android mobile application development, Eclipse would be the primary integrated development environment (IDE). Targeted Android operating system will be 4.3 but the application will be compatible to as earlier as Android 2.3. Testing in the local environment will be performed in AVD (Android Virtual Device Manager) on virtual device Nexus 4 by Google.

5.2.5.1.4 Required Devices for Testing

During the development, the application can be tested on a local machine using AVD (Android Virtual Device Manager). But before sending it to the Google Play Store or in the market, it has to be thoroughly tested on real devices.

The application should be tested on at least one smartphone device. The preferred device for testing is the Nexus 4 by Google which has 4.7" screen (normal).

5.2.5.1.5 Installation Guidelines

There are two possible ways to install an android application on android devices.

The first and most widely adopted path is to publish the installable package in Google Play from where users can download and install it on their devices. To publish the application in Google Play, an organization has to be registered with the Google Play store which costs $25. Google will test and verify the application before it actually publishes it in the market, and provides a certain level of security guarantee to the user.

The second option is to upload the Android installable package to our own server and provide the link to users. Users can click the link and start the installation process. Depending upon the device, a user may need to change the default settings (Users have to allow the unverified application to be installed) since Google does not verify the android applications that are not on Google Play. In this case, users are expected to have intermediate knowledge of their devices.

5.2.5.2 iOS

This section covers the mobile app development of ACCESS for iOS smartphones using native SDK.

5.2.5.2.1 Requirement for Development

A system with Mac OSX will be required to develop iOS app. Following table lists recommended specifications for hardware components that will be used for development

S. No	Hardware	Specifications
1.	Processor	3.x GHz Quad core
2.	RAM	16 GB
3.	Hard disk Drive	500 GB

Following table lists tools and software components that will be used for development

S. No	Software Component	Description
1.	**Mac OSX**	Operating System
2.	**Objective-C**	Programming Language
3.	**Cocoa Touch**	Software Framework collection
4.	**XCode**	Integrated Development Environment

5.2.5.2.2 Targeted SDK and OS

According to Apple Insider, as of June 06, 2013, below are the iOS version distributions on iOS smartphones –

1. iOS 6 – 92.7%
2. iOS 5 – 5.5%
3. iOS 4 – 1.7%
4. iOS 3 – 0.1%

Based on the above iOS version distribution information, the target iOS smartphones should be running iOS version 6, but the app will also support version 5.

5.2.5.2.3 Development

All the development will be done using XCode (free official IDE for iOS app development) on a Mac OSX system. Objective-C will be the programming language for coding. Cocoa Touch - the collection of application frameworks, the will used by to develop application components. The SDK for the target iOS version will be used for development, keeping compatibility for the least supported version. During development the application will also be tested on an iOS device simulator.

5.2.5.2.4 Testing

During the development, the application can be tested on the iOS device simulator within the development system. But before sending it to the App Store for distribution, it should be thoroughly tested on real devices running the target iOS versions.

5.2.5.2.5 Installation Guidelines

The application would be available on App Store from where users can download and install it on their mobile devices.

6. Application Framework

A framework is a set of common and prefabricated software building blocks that programmers can use, extend or customize for specific computing solutions. With frameworks, developers do not have to start from scratch each time when they are building different parts of the application. Frameworks are built from a collection of objects so both the design and code of the framework may be reused.

6.1 Framework Services

ACCESS application framework will have two sets of services and they are:

- **Business Services:** A group of services that directly drive ACCESS business requirements.
- **Essential and Support Services:** A group of services that collaborate with each other to constitute the core application framework and provide an infrastructure to facilitate business services.

Figure 10 depicts various services that fall into the above two categories. These services are spread across the different layers of the middle tier.

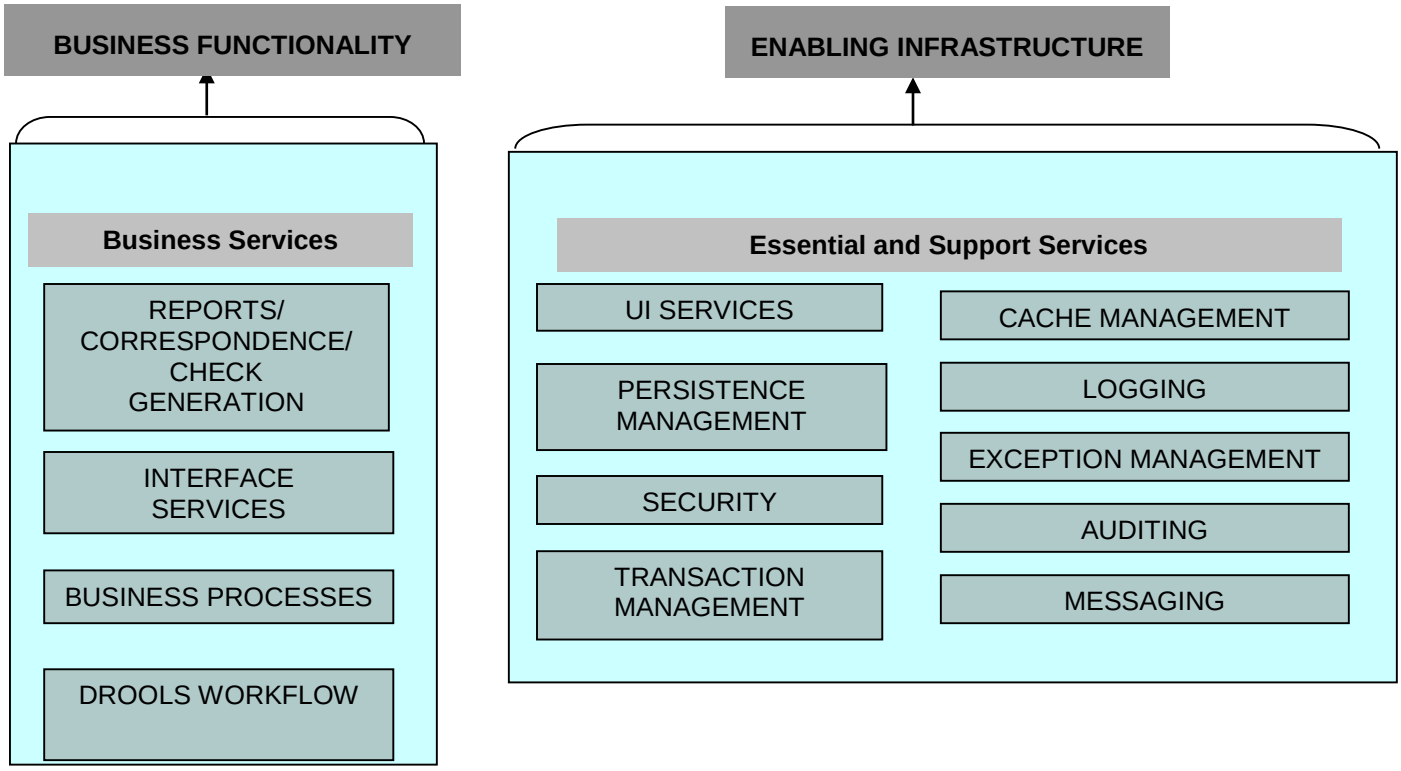

Figure 10: Application Framework

6.2 Essential and Support Services

6.2.1 UI Services

UI services will implement both the UI view and UI model of the presentation layer. This facility will not build any user interface but will help in building the user interface and transferring the user request into a form that is suitable for business functions (data transfer objects) to use. This service will maintain meta-information about the user interface components such as display labels of controls and data constraints on various fields among others. Meta data repository will supply the information required to build the UI. In addition to this, the UI services will use field level security information, provided by the security services, to provide/deny access to the fields on the UI. UI Services will use Struts, Tiles, Custom Tag Libraries and Java Standard Tag Libraries (JSTL).

Several configuration files will be used to supply necessary meta-data to UI services to carry out its responsibilities. Some of these configurations files are:

Struts Action Configuration: This xml file will provide all the configuration data for the presentation layer. It will maintain information about a web page e.g. list of commands that can be issued using a page, page navigation rules among others.

Struts Tiles Configuration: This xml file will be used to map a physical file to the logical name of the web page that will be used in the struts action configuration.

Meta data repository serves the configuration data (Website and UI Model), and the security layer provides necessary information to the UI services for managing the security of the UI component.

The following JEE components will form the UI services and they are:

- Servlet: For page navigation
- Java Server Pages (JSP)/HTML/Cascading Style Sheets (CSS)/ Custom Tags: For web page generation
- eXtensible Markup Language (XML): For UI services configuration

6.2.2 Persistence and Data Access Management

Transferring the state of any business object to any underlying persistent store is referred to as persistence. Access to data varies depending on the source of the data for example relational database, Lightweight Directory Access Protocol (LDAP) server, flat files, legacy systems and so forth. Often the performance of the data source and the strategies that are used to access it, will dictate the performance and scalability of a JEE application. One of the key tasks is to achieve a clean and efficient interface between business objects and data source.

Data Access Goals

These are some of the important data access goals that should be handled by the data access facility and they are:

- It should be efficient.

- It should ensure data integrity.
- It should ensure correct behavior on concurrent attempts to access and manipulate the same data.
- It should be possible to change an application's persistence strategy without rewriting its business logic.
- Data access code should be maintainable.

Business and Persistence Logic

Business logic is concerned with the application's core workflow and is independent of the persistent data storage. In contrast to business logic, persistence logic concerns the application's access to and manipulation of persistent data. Persistence logic normally has the following characteristics:

- It does not require the application of business rules.
- It is unlikely to change on updates to business rules.
- It does not need to handle security issues.
- It involves preserving data integrity.
- It requires knowledge of the target persistence store to implement operations.

Persistence and Data Access Strategies

There are several ways of achieving persistence and data access in the JEE environment and they are as follows:

- Java Persistence Architecture (JPA)
- Java Database Connectivity (JDBC)
- Java Data Objects (JDO)
- Object Relational Mapping (ORM) Software

For any complex web based application, just one method of persistence will not adequately meet the requirements and hence a combination of methods will often be used. O/R mapping solutions are a good choice in On-Line Transaction Processing (OLTP) systems, in which users typically perform operations on a small dataset. For ACCESS, a combination of the following persistence strategies will be used:

- Hibernate (ORM) – will be used for simple OLTP queries
- JDBC – will be used for complex and batch queries
- Stored Procedures – will be used for handling a complex business process that requires access to a large number of records

6.2.3 Security

The security architecture identifies the criteria and techniques associated with protecting and providing access to ACCESS information resources. It facilitates identification, authentication, authorization, and administration services.

Authentication

This is a mechanism to ensure that a user (person or another application component) trying to use the system has legitimate access to do so. It is used to confirm his identity, establish a certain amount of trust on the system for the user. There are two types of authentications.

One-Way Authentication: This authentication is done by the system using the question "Who are you?" This helps the system in establishing the identity of a user and allowing or disallowing access to the system depending upon the credentials supplied by the user.

Bi-directional Authentication: This authentication by the system examines the user's credentials and at the same time provides its own credentials to the user (Who are you? I'm Access System), this helps in improving the confidence level of the user to provide sensitive information with trust e.g. credit card details. LDAP authentication provider will be responsible for proving identity.

There are three primary mechanisms by which a user can be authenticated:

- Basic Authentication: This is an authentication mechanism in which a Web server authenticates an entity with a user name and password, obtained using the Web client's built-in authentication mechanism.
- Form Based Authentication: This is an authentication mechanism in which a web container provides an application specific form for logging.
- Mutual Authentication: This is an authentication mechanism employed by two parties for the purpose of proving each other's identity to one another.

Authentication Solution for ACCESS

ACCESS will be using form-based authentication over Secure Sockets Layer (SSL). The rationale for selecting form-based authentication is to keep the look and feel of the login form in agreement with the look and feel of the ACCESS application. Hypertext Transfer Protocol (HTTP) over SSL communication has been chosen for securing the communication, as it is not advisable to transfer sensitive information about the user's security (Userid and password) as plain text to the web server.

Single Sign On

Single Sign-on is a capability of systems where user logs in one system and gets access to multiple systems without providing login details again. Single Sign on (SSO) capability will be provided to have a seamless integration between Tax and Benefits applications for all state. This SSO feature for ACCESS would be custom built rather than any third party software.

However, SSO capability of ACCESS to other ES (Employment Services) application for RI and ME is beyond the scope of this document.

Mississippi has decided to implement OPEN AM for SSO between ES application.

Authorization

Authorization is the process whereby the interactions between users and application resources are controlled, based on user identity or other information. In other words, authorization answers the question “What a user can do?” Authorization is used to limit the interactions between users and application resources to ensure integrity, confidentiality and availability.

Authorization is based on the concept of security roles. A security role is a logical grouping of users. Each security role is mapped to the users. A security role can be used with declarative security or programmatic security.

Authorization Solution for ACCESS

Authorization information will be maintained at two levels.

- Authorization at the business function level
- Authorization at the field level

Authorization at business function level is about the capability of a user i.e. what a user can do. Authorization at field level shows the permissions granted to a user. This approach helps in implementing security policies, for instance, multiple users can have different level of access (read, modify) on different data of the same entity. Maintaining field groups and defining access rights on these field groups will implement field level security. The system will be designed in such a way that it only maintains the fields in the Meta-Data repository that do require security profiles.

Security Information

Application security related information will be stored in an LDAP enabled directory server. Currently options being explored for Red Hat JBoss Directory server deployment which will be utilized for the security of the ACCESS System. The security service will encapsulate all the security functionality, including communication with the LDAP Server using the Java Naming and Directory Interface (JNDI) Application Programming Interface (API).

Infrastructure Security

The infrastructure required for hosting the ACCESS System is:

- Domain Name Server
- Web Server
- Application Server
- Database Server
- Sub systems like Email Server, Reports Server, Drools Workflow Server, Data Warehouse Server and DMS Server.

The application server, database server and sub system servers should be protected by an inner firewall. The Internet edge servers and the Internet web servers should be placed in the De-militarized zone (DMZ), which is a layer between the outer firewall and the inner firewall.

Encryption

All system access data transfer and web page access will use 256 bit encryption. Any insecure protocols that are currently being used by the application will be updated with secure protocols unless any third party software / server are not capable of handling 256 bit encryption or secure protocols.

http://www.irs.gov/uac/Encryption-Requirements-of-IRS-Publication-1075

Information Encryption

For information encryption across the web, SSL protocol with 256 bit keys will be used. To operate a Web Server in a secure SSL mode, a signed certificate from the certification authority (CA) needs to be obtained for the consortium member states and installed on the web server. SSL accelerators will be used for the encryption and decryption of the transactions between the users and the system. The process of encryption and decryption can severely overload the server and these SSL cards can take over this responsibility and help reduce the load.

Business Data Encryption

The sensitive data that is required to be encrypted, as per the business requirements will be making use of the Java Cryptography encryption/decryption method to store these values in the database.

Tool for Application Security

IBM Security App Scan 8.7 will be used for application security testing. It automates application security testing by scanning applications. It will do vulnerability assessments including SQL-injection, cross-site scripting, buffer overflow, and Web 2.0 exposure scans. It also generates reports with intelligent fix recommendations to ease remediation.

6.2.4 Auditing

Audit trails will be maintained in the system using the logging framework of the ACCESS System. The Log Information will contain the User ID, Timestamp, Internet Protocol (IP) Address (this only will be stored once when the user logs into the system, Edge server should be able to send the sender IP) of users computer and the business process name. This facility enables the administrator to track user actions. For all the transaction records in the database the following information will be maintained irrespective of any other auditing facility:

Created By	Created Date	Updated By	Updated Date	Update Process

The application log and the database information will assist in managing user actions. System logs will also be maintained in the Web Server, Application Server and the drools workflow.

6.2.5 Cache Management

Caching is a tried and tested method for dramatically speeding up applications. High performance applications should cache the data that is fairly static and is used often throughout an application. Various data that qualifies for being cached in the application server are:

- Application Configuration Meta data
- Lookup Database Tables
- Application Static Data

Caching Solution

One of the most prominent open source caching solution is OSCache from OpenSymphony. It is a widely used, high performance JEE caching framework. OSCache can be used as a generic caching solution for any Java application. A few of its generic features include:

- Caching of Arbitrary Objects – It is not only restricted to caching portions of JSP pages or HTTP requests. Any Java object can be cached.
- Comprehensive API - The OSCache API gives full programmatic control over all of OSCache's features.
- Persistent Caching - The cache can optionally be disk-based, thereby allowing expensive-to-create data to remain cached even across application restarts.
- Clustering - Support for clustering of cached data can be enabled with a single configuration parameter. No code changes are required.
- Expiry of Cache Entries – It provides the developer with great control over how cached objects expire, including pluggable cache refresh rules if the default functionality does not meet the system requirements.

Caching Solution for ACCESS System

ACCESS System will use OSCache.

6.2.6 Messaging

This component will serve all the messaging needs of ACCESS. A repository of functions that need to send messages will be maintained by this service. There will be an event monitor that will keep observing all the business functions being executed by controller and as soon as a business function registered with messaging service is executed, a message queue (message provider) is updated storing details of business function and context in which the message was executed. There will be message consumers that subscribe to the messages from the message provider on certain topics. These consumers will be updated as soon as the message provider is updated. Finally these consumers will execute the necessary messaging commands.

Messaging Solution for ACCESS System

Messaging will be implemented with the Java Message Service (JMS) provided by the JEE container of the application server.

6.2.7 Transaction Management

Transaction management is a mechanism for simplifying the data integrity and the development of distributed multi-user enterprise applications. JEE platform provides this as a standard service. Transaction management frees an application programmer from dealing with the complex issues of data access, including synchronized updates, failure recovery, and multi-user programming. A transaction is a logical unit of work that either modifies some state, performs a set of operations, or both.

JEE platform and the Java Transaction API (JTA) define the overall transactional behavior. There are two different ways to start the transaction, either explicitly in code or the EJB server starts it.

Transaction Management Solution for ACCESS System

In ACCESS solution all calls to the Business Delegate are initiated within a transaction.

Transaction management services are provided by following mechanisms:

- Container Managed transactions provided by the EJB container from the Application Server. All the transactions initiated within the Application server are initiated and managed by the JEE Application Server.
- Transaction Manager managed transactions provided by Bitronix Transaction Manager. For the BizServer functionality ACCESS implements transaction management using the Bitronix Transaction manager. The Bitronix Transaction Manager (BTM) is a complete implementation of the JTA 1.0.1B API. It provides all services required by the JTA API for while trying to keep the code as simple as possible.

6.2.8 Logging

Logging is an important component of any software system. Logging offers several advantages. First and foremost, it provides precise context about a run of the application. Once inserted into the code, the generation of logging output requires no human intervention. Secondly a log output can be saved in a persistent medium to be studied at a later stage. Logging is merely a process of creating logs, documenting and storing certain system or user activities for various reasons such as debugging and security. From a security point of view, logging can provides proof of malicious activity or acts as an indicator for potential malicious activity.

Logging Solution for ACCESS System

ACCESS System will use Log4j.

6.2.9 Exception Management

The design of the system must ensure that the exceptions do not cause problems to the end users of the system. One of the key requirements in maintaining the system is the ability to detect errors when they occur and to obtain sufficient information to enable the diagnosis and repair of the underlying root causes of the problems.

Principles of Exception Handling

The errors that occur in an application can be classified as 'Domain errors' and 'Technical errors'. Domain errors are those that can be caused by the errors in the business logic or business processing. Technical errors are those that are caused by problems in the underlying technology platform (e.g. could not connect to database, LDAP server and others).

ACCESS is designed to handle these kinds of errors and a proper message is being displayed to the user, hiding any details that might confuse him. Full stack trace of the errors gets logged so that the developers can take a look at it for the resolution of the problem. In a production system, when an exception is thrown it is likely that the system is unable to process the user's request. When such an exception occurs, the end user normally expects the following:

- A message indicating that an error has occurred
- An unique error identifier that the user can use while reporting it to a support person
- Quick resolution of the problem

The following are some of the generally accepted principles of exception handling:

- If you cannot handle an exception, do not catch it
- Catch an exception as close as possible to its source
- If you catch an exception, handle it, do not swallow it
- Log an exception where it is caught, unless the plan is to re-throw (send the exception back to the caller) it

- Preserve the stack trace when you re-throw the exception
- While logging the exception, generate an unique identifier to the exception so that it can be analyzed easily when the user reports the error
- There should be a way to inform the system administrators in real time when any severe error occurs in the system.

Logging of Exception

For any system, without proper logging of the errors and exceptions, it would be difficult to have a quick resolution of the problems. ACCESS System will be making use of Log4j an open source java library for logging the exceptions and errors.

6.3 Business Services

6.3.1 Business Processes

These set of components form the integral part of the system. This is where the business processes will be implemented. Business Process components will be created as plain old java objects (POJO). Requests from the user to initiate any business processes will be first handled by the framework controller.

The presentation layer interacts only with the Controller. The Controller helps in coordinating business services provided by various sub-systems to serve the user request and produce the required output. This component functions as follows.

- It receives a service request from the user and performs a look up to resolve the request by referring the business function configuration repository.
- After the request is resolved, the controller makes use of the various system resources that are necessary to fulfill the request for any business process.
- Controller notifies the event monitor about the business function being invoked and the context in which the business function is invoked.
- After the request is validated, the appropriate business function(s) is executed and subsequently, the presentation will be performed by the UI services.

6.3.2 Drools Flow

This system/component helps in maintaining the repository of business processes and lists of persons, systems, and business functions involved in those business processes. The drools workflow system will keep track of all the workflows that are initiated. Drools platform provides a unified and integrated way of combining rules and processes into a single software product. Drools 5.0+ is split into 4 sub projects and they are:

1. Drools Expert → This provides the rule engine functionality.
2. Drools Flow → This provides the process & workflow functionality.
3. Drools Fusion → This provides the Complex Event Processing (CEP) functionality.
4. Drools Guvnor → This provides the Business Rules Management System (BRMS) functionality.

ACCESS system will be making use of the Drools Flow product to provide the workflow functionality in the system. For the Business Rules Implementation ACCESS will use the Drools Expert product.

6.3.3 Interface Services

The interface services will be responsible for hiding the intricacies/details of any internal or external system. Hence, any changes in the interface systems will not have any ripple effect changes across the system. All the external and internal systems will register with this service before they can be used by any business component of the system.

6.4 Architecture Collaboration

Figure 11 depicts the ACCESS architecture collaboration showing the various services and systems interacting with each other and also provides the holistic view of the ACCESS System architecture.

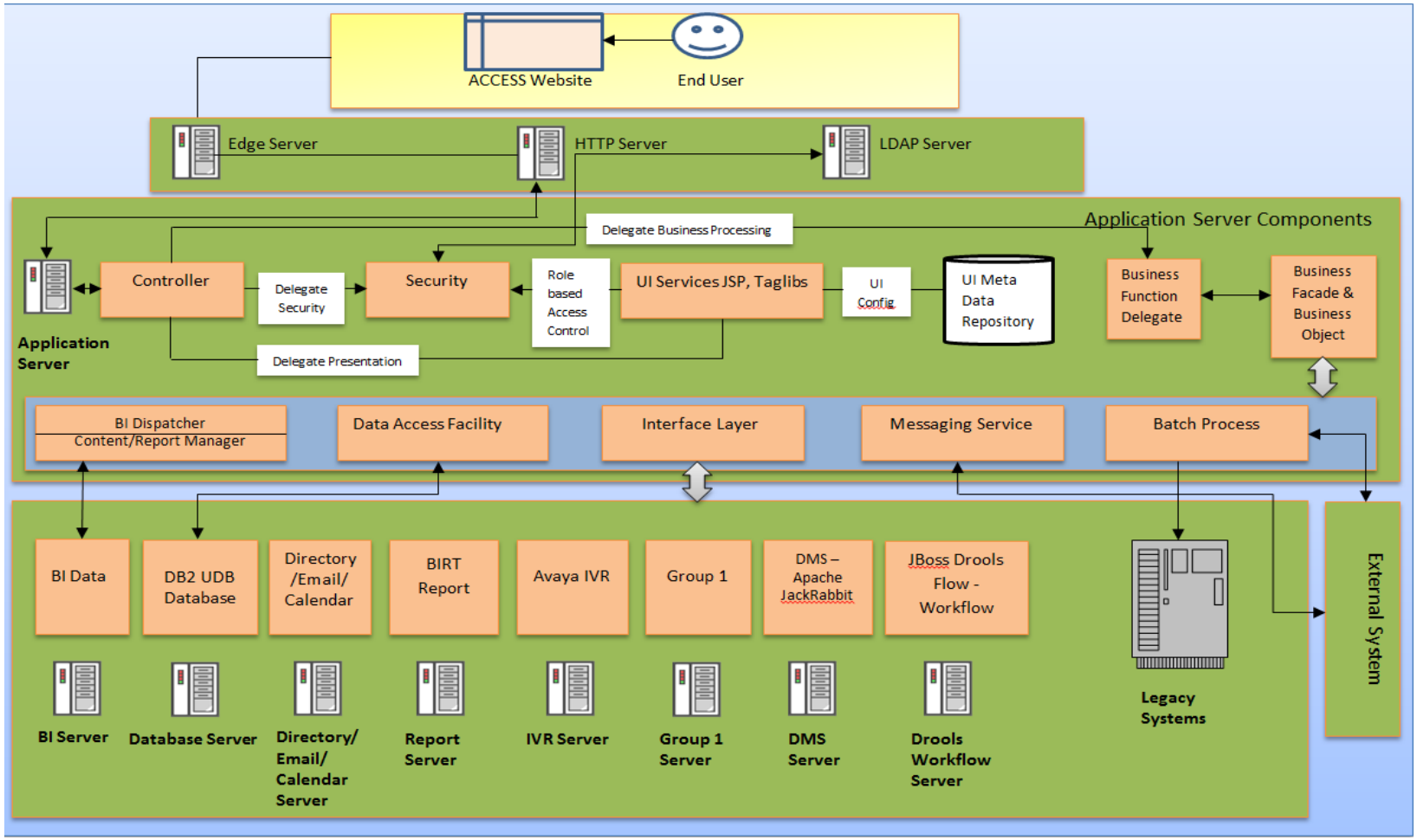

Figure 11: ACCESS - Architecture Colloboration Diagram

6.5 **Component Diagram**

Figure 12 depicts the framework component interaction diagram. It shows the high level model of the framework for the ACCESS System.

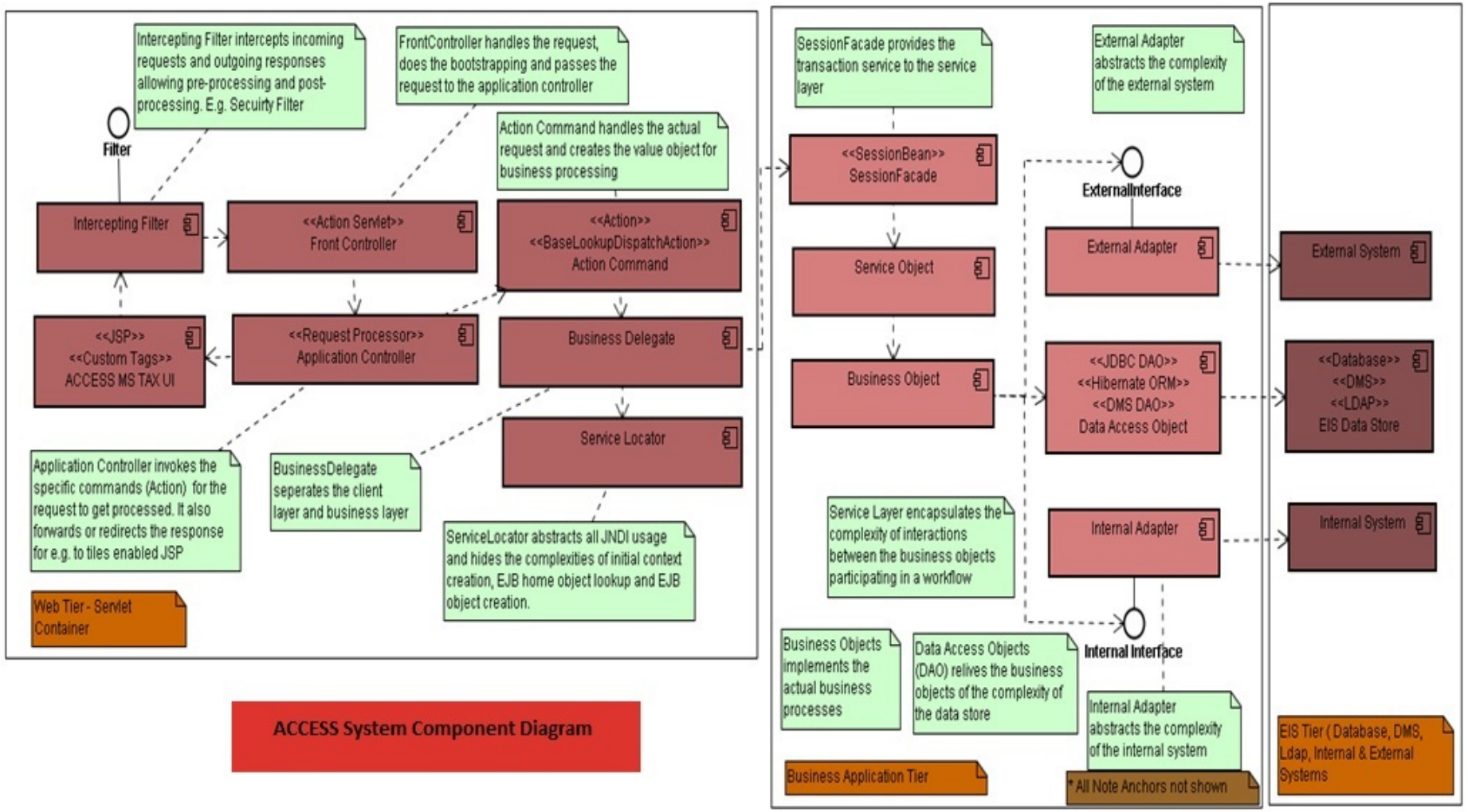

Figure 12: Framework Component Diagram

6.6 Sequence Diagram of Generic Business Function

Figure 13 and Figure 14 depict the sequence diagram of the execution of a generic business function at a very high abstraction level.

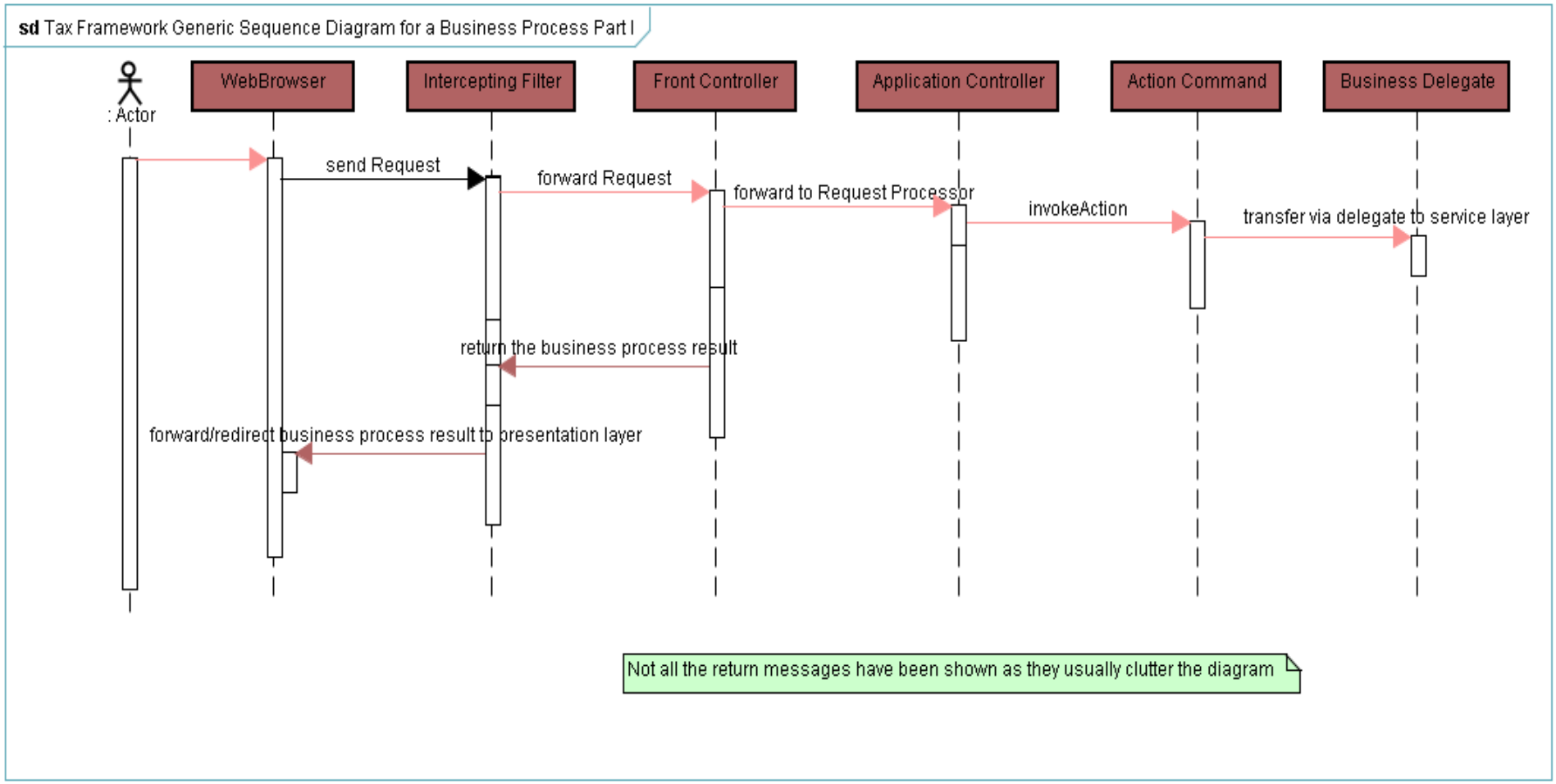

Figure 13: Sequence Diagram – Part I - Generic Execution of Business Function

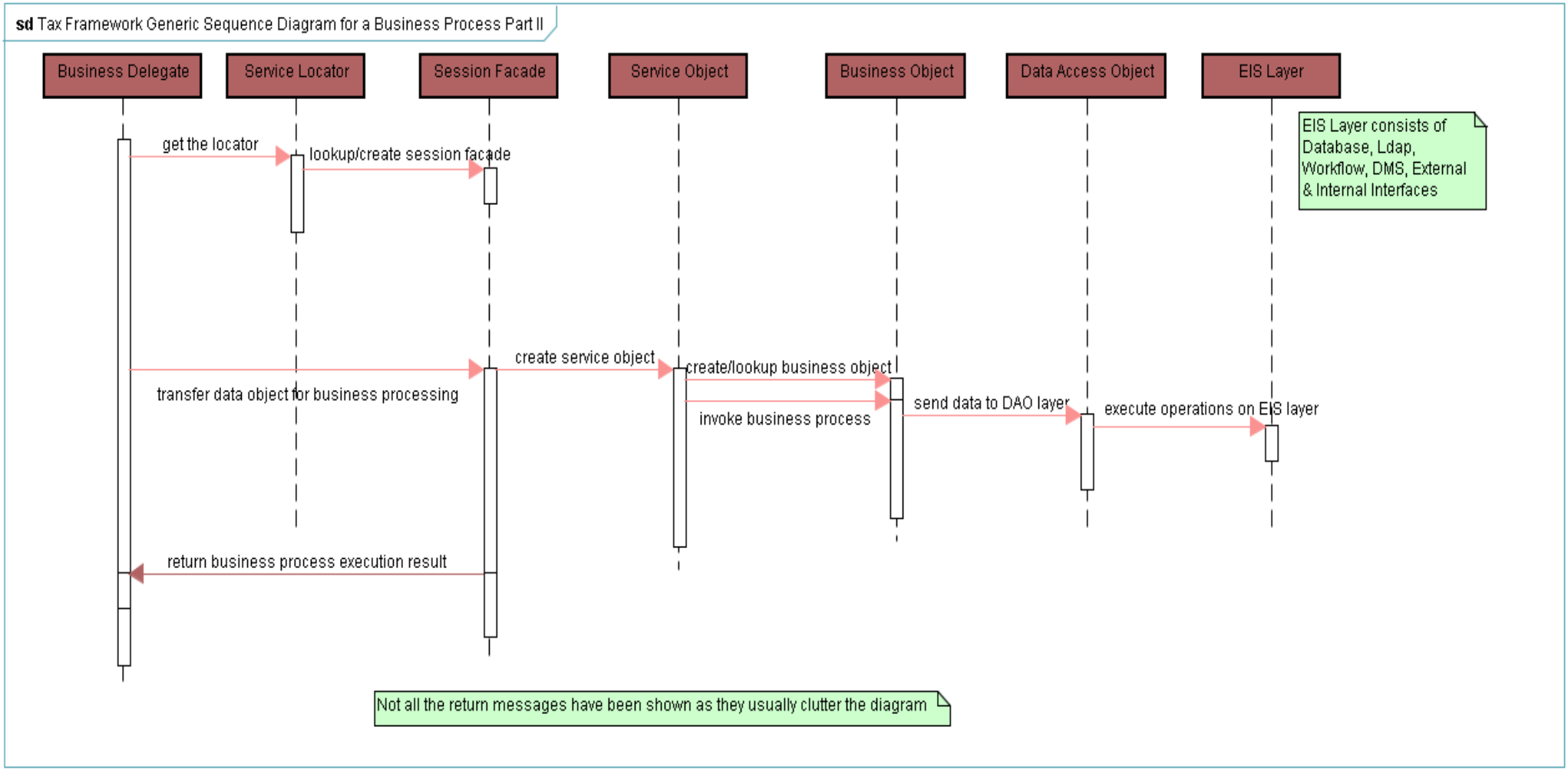

Figure 14: Sequence Diagram – Part II - Generic Execution of Business Function

7. Interfaces

Interfaces for the ACCESS system are classified as Internal or External.

The ACCESS system can communicate with the external/internal systems either in a synchronous or an asynchronous mode. In the case of a synchronous communication, the interaction will always be real time and can be triggered by a user action or any other application component. In the case of an asynchronous communication, the interaction can be real time or in a batch.

7.1 Internal Interfaces

The ACCESS system will have application level integration with the internal systems. The table below lists the various internal interfaces that impact the technical architecture and design of the system.

S. No.	Interface Name	Communication (Synchronous /Asynchronous)	Real-Time/Batch	Integration Software
1.	JBoss Drools Flow	Both	Both	JBoss Drools Client API
2.	Report	Both	Both	Report Server Java API
3.	Document Management System	Synchronous	Both	Java API
4.	Directory Server (LDAP)	Synchronous	Real-Time	JNDI
5.	Interactive Response (IR)	Synchronous	Real-Time	Web Services
6.	Email	Asynchronous	Both	Java Email API's
7.	Address Validation	Synchronous	Both	Spectrum Address Validation Java API
8.	Address PreSort	Synchronous	Batch	Mail Stream Plus API
9.	Employment Services (ES)	Asynchronous	Batch	Secure FTP

7.1.1 Mainframe Connectivity

The ACCESS system and the legacy system need to exchange data on a regular basis for the member states legacy systems. Data files (pre-defined format) will be transferred at regular intervals with File Transfer Protocol (FTP). If on the mainframe operating system, secure FTP can be installed, configured and used for maintaining the security of the data transmission.

7.2 External Interfaces

The ACCESS system will have application level integration with the external systems. External interfaces[1] are referred to those components that will interact with the application hosted by an external agency. The table below lists the various external interfaces that impact the technical architecture and design of the system.

S. No.	Interface Name	Communication (Synchronous /Asynchronous)	Real-Time/Batch	Communication Protocol	Integration Software
1.	MDES to Payroll Service Companies (vice versa)	Synchronous	Batch	FTP	Flat File
2.	Internal Revenue Service (IRS)	Synchronous	Batch	SSH	Flat File
3.	Bureau of Labor Statistics (BLS)	Synchronous	Batch	FTP	Flat File
4.	Bank (Regions and others)	Synchronous	Batch	SSH	Flat File
5.	ETA Sun System	Synchronous	Batch	FTP	Flat File

[1] Detailed requirements will document the complete list of external interfaces

8. Business Intelligence

Business Intelligence is a set of theories, methodologies, processes, architectures and technologies that transform raw data into meaningful and useful information for effective decision making and predictive analysis.

8.1 Business Intelligence Topology

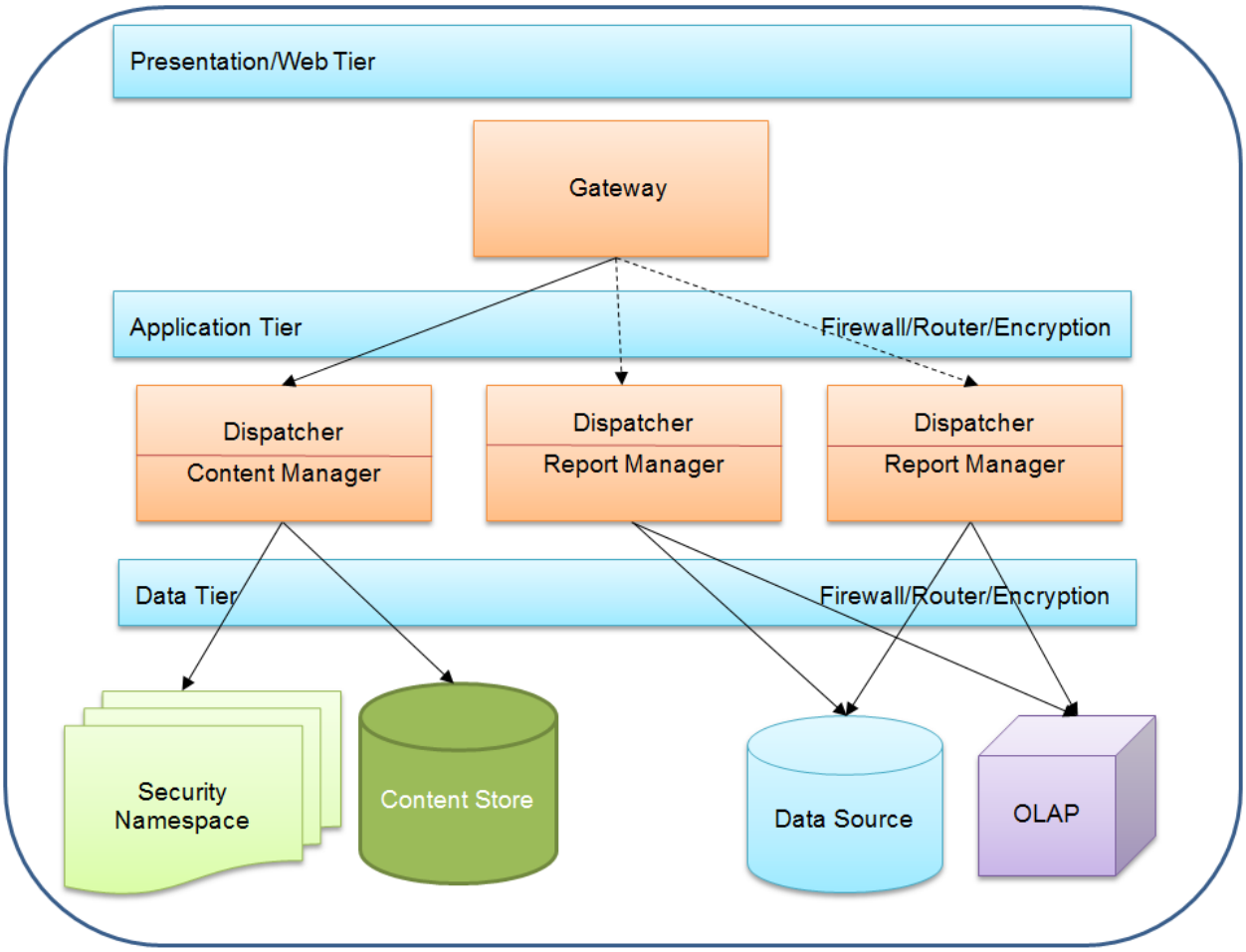

Figure 15: Typical Distributed Topology of Business Intelligence

8.2 Technical Aspects

Below are the technical aspects of using Business Intelligence.

- Graphical interpretation of data in different dimensions.
- Interactive data interpretation (Ad hoc reporting).
- Data interpretation integrated with maps, charts and widgets.
- Separate administrator and user privileges.
- Real-time monitoring.
- Auto scheduling of graphical reports.
- Ease of integration with existing products.
- Integration with LDAP server.
- Web based analytics.
- Enhancements to Mobile BI possible in future.
- Open access to all data sources.
- Common integrated security model.
- Enterprise class SOA platform architecture.
- Can be integrated into existing application.

8.3 Benefits

The key benefits of using BI are,

- Eliminates guesswork.
- Instant answers to department questions.
- Instant department metrics and reports as and when needed.
- Effective streamlining of operations.
- Improve efficiency.
- Greater insights into each component.
- Easy usability and self-generation of analytics reports by users requiring less IT intervention.
- Future Prediction with higher probability.
- Where is, was, will be the trend of MDES.

8.4 Data Movement (Extract, Transform and Load)

The Data movement services run and schedule builds and job streams on remote computers Connection. Extract, transform, and load (ETL) is a process in data warehousing that involves extracting data from outside sources, transforming it to fit business needs, and ultimately loading it into the data warehouse.

The ETL features are used to extract data from various sources, transform that data through encoded business rules, and load the transformed data into a data mart. During this process, operational data is retrieved from the product source, normalized, and mapped to fact and dimension tables.

8.4.1 Extraction

The ETL framework accepts extracts data through direct database access and through ODBC drivers, including the Rational Insight XML ODBC driver. An organization stores data in traditional relational databases or in other source formats (such as XML). Since Data Manager supports data in tabular format, incoming XML must be converted to relational form prior to the core ETL extraction process.

8.4.2 Transformation

This step is to transform the data using business rules. This is done in a two-step process.

- Normalize the data and modify using business rules. These business rules, when executed, perform business logic such as calculating or deriving a column based on other columns.
- Store it into physical tables. These physical tables implement the star schema convention, and add dimensions and facts – the characteristics elements of a data warehouse.

8.4.3 Loading

The last step is to load this transformed data into the data mart, a separate area of the warehouse.

8.4.4 Implementation

In Data Manager, each piece of ETL process is a fact or dimension build. The builds can be organized into job streams for different sets of data or tables. The job streams can be executed in the Data Manager directly, or published as a data move task, and then scheduled for execution in the Insight report server. The primary ETL builds are normalized form builds, non-entity builds, look-up builds, dimension builds, and fact builds.

8.5 BI Tool Evaluation

8.5.1 IBM Cognos BI

The key capabilities of Cognos Enterprise edition are,

- Reports – View business information.
- Analysis – Explore BI data from different angles & perspectives
- Scorecards – Monitor & track performance.
- Dashboards - Offer an at-a-glance view of what’s most important to department.
- Mobile BI - Enables to view information on the road or offline.
- Self-service BI - Adds the flexibility to visualize and analyze information and more without its help.
- Collaborative BI - Makes it easier to share insights with colleagues and stakeholders.
- Modeling - Presents alternative scenarios for more informed decision-making.
- Real-time monitoring - Shows current operational KPIs for up-to-the-minute decisions.

8.5.2 Jaspersoft BI suite

The key capabilities of Jaspersoft BI suite are,

- Reports – View business information.
- Analysis – Explore BI data from different angles & perspectives
- Mobile BI - Enables to view information on the road or offline.
- Data Integration – ETL capabilities
- Interactive Report Viewing – Browser based report viewer.
- OLAP server – Analyze large relational data sets with powerful analytic queries.
- Server Repository – Centralized repository to store data.

8.5.2.1 Comparison b/w Jaspersoft BI Enterprise Edition and Community Edition

S. No	Jaspersoft – Enterprise Edition	Jaspersoft - Community Edition
1.	Ad Hoc report Designer is available.	Ad Hoc report Designer is not available.
2.	Dashboard is available.	Dashboard is not available.
3.	Metadata layer is available.	Metadata layer is not available.
4.	Data Virtualization is available.	Data Virtualization is not available.
5.	Data Integration is available.	Data Integration is not available.
6.	Interactive visualization is available (HTML5).	Interactive visualization is not available.
7.	Multi-tenancy is available.	Multi-tenancy is not available.
8.	Audit logging available.	Audit logging is not available.
9.	Vendor support is available.	Support is available only through Forums & wiki.
10.	Commercial license.	GPL License.
11.	Supported Application Servers • Apache/Jakarta Tomcat • JBoss AS • JBoss EAP • IBM WebSphere (WAS) • GlassFish • Oracle WebLogic Server	Supported Application Servers • Apache/Jakarta Tomcat • JBoss AS • JBoss EAP

S. No	Jaspersoft – Enterprise Edition	Jaspersoft - Community Edition
	• SpringSource tc Server	
12.	Supported Portal Servers • Liferay Portal • JBoss Portal	Supported Portal Servers • Liferay Portal • JBoss Portal
13.	Supported Databases • Oracle RDBMS • PostgreSQL • IBM DB2(9.7,10.1) • MySQL • Microsoft SQL server • Infobright • Vertica • JBoss Metamatrix Enterprise Data Services Platform • JBoss Teiid • Greenplum Database • Sybase ASE	Supported Databases • PostgreSQL
14.	Supported Operating Systems • Microsoft • Red Hat Enterprise Linux • Apple Mac OS X • Apple iPad iOS • Android – Mobile SDK • Solaris SPARC • Fedora • HP-UX • FreeBSD • IBM AIX • Ubuntu • Novell SUSE Linux Enterprise Server (SLES)	Supported Operating Systems • Microsoft • Red Hat Enterprise Linux • Apple Mac OS X • Apple iPad iOS • Android – Mobile SDK • Solaris SPARC (not fully tested) • Fedora • HP-UX • FreeBSD • IBM AIX • Ubuntu • Novell SUSE Linux Enterprise Server (SLES)
15.	Java Virtual Machines (JVM) • Oracle/Sun Java JDK / JRE • IBM Java JDK / JRE (for WebSphere) • OpenJDK RunTime Environment	Java Virtual Machines (JVM) • Oracle/Sun Java JDK / JRE

S. No	Jaspersoft – Enterprise Edition	Jaspersoft - Community Edition
16.	Jaspersoft ODBO Connect is available • Microsoft Excel • Microsoft Windows • Microsoft .NET Framework	Jaspersoft ODBO Connect is not available
17.	Supports ETL capabilities.	Doesn't support ETL capabilities.

8.5.3 Pentaho BI suite

The key capabilities of Pentaho BI suite are,

- Operational and interactive reporting.
- Data discovery and interactive analysis.
- Integrated reporting, data visualization and analysis and predictive analytics.
- Data access and integration (ETL).
- Predictive analytics.
- Data warehousing.
- Big Data integration and job orchestration for Hadoop, NoSQL databases and Analytic Databases.
- Application consolidation.
- Data synchronization.

8.5.3.1 Comparison b/w Pentaho BI Enterprise Edition and Community Edition

S. No	Pentaho - Enterprise Edition	Pentaho - Community Edition
1.	Interactive Analysis & Visualization is available.	Basic reporting is available.
2.	Dashboard Reporting is available.	Dashboard Reporting is not available.
3.	Data Integration is available.	Basic Data Integration is available without auto scheduler.
4.	Expanded & Big Data source connectivity is available.	Basic connectivity is available.
5.	Secure Data Integration is available.	Secure Data Integration is not available.
6.	Mobile BI is available.	Mobile BI not available.
7.	Vendor support available.	Support through forums.
8.	Commercial License (Annual subscription).	Open source License.

S. No	Pentaho - Enterprise Edition	Pentaho - Community Edition
9.	Audit reporting is available.	Audit reporting is not available.
10.	Supported Application Servers. • JBoss 5.1.X • Tomcat 6.0.X	Supported Application Servers • Liferay • Websphere (not tested)
11.	Supported Operating Systems • Apple Macintosh OS 10.7 & 10.8 • Microsoft Windows 7 • Microsoft Windows 2008 Server R1 & R2 • Red Hat Enterprise Linux 5 & 6 • Solaris 10 • CentOS Linux 5 & 6 • Ubuntu Server 10.X and 12.X	Supported Operating systems • Windows XP SP 2 • SUSE Linux • Enterprise Desktop and Server 10 • Red Hat Enterprise Linux 5 • Solaris 10 • Mac OS X 10.4
12.	Supported Data sources • Apache Derby • AS/400 • InfiniDB • Exasol 4 • Firebird SQL • Greenplum • H2 • Hypersonic • IBM DB2 • Infobright • Informix • Ingres • Ingres VectorWise • LucidDB • MaxDB (SAP DB) • MonetDB • MySQL • MS SQL Server • Neoview • Netezza • Oracle • Oracle RDB • PostgreSQL • SQLite • Teradata • UniVerse database • Vertica • Other SQL-92 compliant	Supported Data sources • AS/400 • Apache Derby • Borland Interbase • Calpont InfiniDB • ExtenDB • Firebird SQL • Greenplum • Gupta SQL Base • H2 • Hypersonic • IBM DB2 • Infobright • Informix • Ingres • Ingres VectorWise • Intersystems Cache • KingbaseES • LucidDB • MS Access • MS SQLServer • MS SQL Server (Native) • MaxDB (SAP DB) • MonetDB • MySQL • Neoview • Netezza • Oracle • Oracle RDB • PostgreSQL

S. No	Pentaho - Enterprise Edition	Pentaho - Community Edition
		• Remedy Action Request System • SAP ERP System • SQLite • SybaseIQ • Teradata • UniVerse database • Vertica • dbase III/IV/5
13.	Authentication systems • CAS • Integrated Microsoft Windows Authentication • LDAP • RDBMS	Authentication systems • Acegi Security • Spring Security • LDAP

8.5.4 Recommendation

Following are the key differentiators between the three BI Tools:

S. No	Cognos BI	Pentaho BI	Jaspersoft BI
1.	Supports High performance load.	Supports Medium performance load.	Supports medium performance load.
2.	Ad Hoc report Designer is available.	Ad Hoc report Designer in not available in community Edition.	Ad Hoc report Designer in not available in community Edition.
		Ad Hoc report Designer is available in Enterprise edition.	Ad Hoc report Designer is available in Enterprise edition.
3.	Vendor support is available.	Vendor support is not available in community edition.	Vendor support is not available in community edition.
		Vendor support is available in Enterprise edition.	Vendor support is available in Enterprise edition.
4.	Compatible with all data sources.	Compatible with limited data sources.	Compatible with limited data sources.
5.	High reliability vendor.	Medium reliability vendor.	Medium reliability vendor.

		Low reliability vendor -for the community edition.	Low reliability vendor – for the community edition.

Considering all the technical capabilities, we recommend to go for IBM Cognos BI Enterprise Edition.

9. Data Security

This section outlines various software products to be used to secure data in ACCESS System.

9.1 IBM Infosphere Guardium Data Activity Monitor

This software prevents unauthorized data access, alerts on changes or leaks to help ensure data integrity, automates compliance controls and protects against internal and external threats. Continuous monitoring and real time security policies protect data across the enterprise without changes to databases or applications or performance impact.

The key capabilities of IBM Infosphere Guardium Data Activity Monitor are given below:

9.1.1 Monitor and audit all data activity

- Understand and develop complete visibility into all transactions for all platforms and protocols by users including database administrators, developers, outsourced personnel and applications.
- Identify application users who make unauthorized changes from common service accounts.
- Provide user and application access monitoring independent of native database logging and audit functions.
- Improve data security by detecting unusual database read and update activity from the application layer.
- Automate sensitive data discovery and classification.

9.1.2 Enforce security policies in real time

- Monitor and enforce security policies for sensitive data access, privileged user actions, change control, application user activities and security exceptions.
- Use access policies to identify anomalous behavior by comparing data activity to a normal behavior baseline.
- Support exception policies based on definable thresholds such as SQL errors.
- Use extrusion policies to examine data leaving the database for specific value patterns such as credit card numbers.
- Support policy-based actions such as near real time security alerts, software blocking and user quarantines.

9.1.3 Create a centralized repository of audit data

- Aggregate data throughout your enterprise for compliance auditing and reporting, correlation and forensics without enabling native database audit functions.
- Provide a tamper-proof audit trail that supports the separation of duties required by auditors.
- Deliver customizable compliance workflow automation to generate compliance reports and distribute them to oversight teams for electronic sign-offs and escalation.

9.1.4 Support heterogeneous environments

- Monitor and audit Hadoop-based systems such as IBM Infosphere Big Insights and Cloudera.
- Support enterprise databases and operating systems including IBM DB2, Teradata, IBM Pure Systems, Sybase, Microsoft SQL Server, UNIX and Linux.

- Support key enterprise resource planning and customer relationship management applications as well as custom and packaged applications.
- Provide capabilities to track file-sharing activities on major platforms including Microsoft SharePoint.
- Discover and classify sensitive enterprise data for all platforms and protocols.

9.2 IBM Guardium S-GATE

This software safeguards critical enterprise information by continuously monitoring access and changes to high-value databases. Guardium's real-time database security and monitoring solution monitors access to sensitive data, across all major DBMS platforms and applications, without impacting performance or requiring changes to databases or applications.

- Blocks privileged users from viewing or changing sensitive data, creating new user accounts or elevating privileges.
- Implemented as a lightweight, host-based software agent with fine-grained security policies.

Guardium S-GATE provides automated, real-time controls that prevent privileged users from performing unauthorized actions such as,

- Executing queries on sensitive tables.
- Changing sensitive data values.
- Adding or deleting critical tables (schema changes) outside change windows.
- Creating new user accounts and modifying privileges.

9.3 IBM Infosphere Guardium Data Encryption

This software provides encryption capabilities to help safeguard structured and unstructured data and comply with industry and regulatory requirements. This software performs encryption and decryption operations with minimal performance impact and requires no changes to databases, applications or networks.

The key capabilities of IBM Infosphere Guardium Data Encryption are given below:

9.3.1 Transparent, rapid implementation

- Performs encryption and decryption above the file system or logical volume layer so it is transparent to users, applications, databases and storage subsystems.
- Requires no coding or modification to applications or databases.
- Protects both structured and unstructured data.
- Provides scalability for large and complex environments including thousands of systems and files. Infosphere Guardium Data Encryption also scales to help protect data in new computing models like cloud and big-data environments.
- Provides extensible protection to log files, configuration files and other database output.

9.3.2 Centralized key and policy management

- Provides a secure, centralized method of administering encryption keys and policies.

- Enables consistent and common best practices for managing the protection of structured and unstructured data.
- Supports established data classification and acceptable use policies.

9.3.3 Compliance-ready capabilities

- Enforces separation of duties by supporting separate database management system (DBMS) and security administration.
- Provides granular and configurable auditing and reporting of access requests to protected data, as well as changes to policies and keys.
- Provides audit management to reduce audit scope.
- Integrates with existing security information and event management (SIEM) solutions.

10. Products

This section outlines various software and hardware products to be used for the ACCESS System.

10.1 Software Products

This section outlines the various software products to be used for the ACCESS System.

10.1.1 Browsers

All the users (Customer Service Representative - CSRs, employers and third party agents) will mainly use Internet Explorer 6.0 (or above) and Netscape 7.0 (or above) to access the ACCESS System. User Interfaces will be designed to work equally on both types of browsers. Mozilla (1.7 above) and Mozilla Firebox (1.0 above) support will also be provided.

10.1.2 Web Server

International Business Machines (IBM) HTTP Server 7.0 and above will be used as the web server.

10.1.3 Application Server

IBM WebSphere Application Server (WAS - Network Deployment Edition) 8.0 and above will be used as the application server. The Network Deployment edition of WAS will be used to provide clustering capabilities. This product requires WebSphere Application Server Base Edition to be installed. Options are being explored if JBoss Enterprise Application Platform v 6.1 can be deployed instead of WebSphere 8.0 for substantial cost benefits.

10.1.4 Database

Legacy data related to ACCESS is present in Virtual Storage Access Method (VSAM) and flat files. This data will be migrated to DB2 Universal Database (UDB) as part of the ACCESS Project. ACCESS System will be using the DB2 UDB 9.7 or above.

10.1.5 Workflow Management

A successful implementation of a workflow system can be achieved only through an effective integration of the users and the infrastructure. JBoss Drools Flow will be used as the workflow management solution for the ACCESS System.

10.1.6 Reports Generation

For implementing the correspondence and report generation requirements, the Eclipse BIRT will be utilized. Eclipse BIRT Designer will be used for creating the report templates.

10.1.7 Document Management System

Apache Jackrabbit Document management system will be used for storing and retrieval of correspondences and reports. The product supports the following requirements of the document management system:

1. Electronically stores, organizes and manages documents, files and other business critical information.
2. Support for virtually any type of content

DMS is the centralized documents repository for the Tax and Benefits Applications. ACCESS system generates correspondences and reports in PDF format. These documents are stored in DMS in a structured format.

Figure 16 depicts the proposed node structure configuration for Active and Archive DMS system for each state. The ACCESS node is the root node which contain one YEAR node and it will contains 6 different nodes as Claimant, Employer, Appeal, Reports, FEIN and EEER. These nodes are further divided into child nodes like Claimant node will use the SSN number for further division and document related to all claimants will be stored using predefined SSN structure. Employer node will use the Employer account number (EAN), Appeal will use the Docket number and Reports will use the report name for further division. Year node will describe the storage of document year wise and this is use full for archival of data year wise.

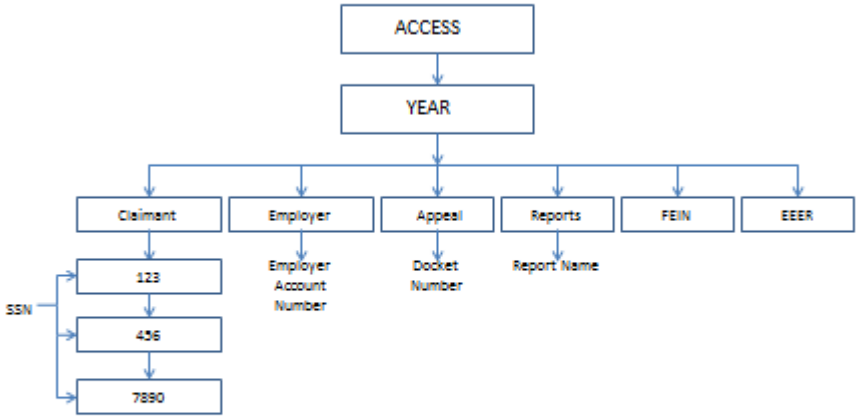

Figure 16: DMS Node structure

10.1.8 Imaging Solution

Existing Imaging systems for the state will continue to exist. ACCESS System can interface with the Imaging system by providing capability to upload the imaged documents to the Document Management System via:

1. Multiple file upload by batch processes.
2. On demand single file upload by the authorized users.

10.1.9 Interactive Response

Avaya will be used for the IR application for MS for ME & RI it is out of scope as of now. State will continue to use their existing software which the Application will Interface with Weekly Certification filing functionality.

10.1.10 Address Validation

Universal Coder will be used for the validation of the address. ACCESS System will use this software to validate employers or claimants physical and/or mailing address. The software provides Java API's for performing the address validation.

10.1.11 Batch Scheduler

The ACCESS System will have batch jobs in cases where an online transaction processing is not possible or in cases where the business functionality warrants batch processing. Open source software Quartz scheduler will be used to schedule the batches.

10.1.12 TOP (Treasury Offset Program)

TOP is administered by Federal government known as Financial Management Service or Internal Revenue Service (IRS). Under this program, two flat files are received and one is sent back to IRS weekly. Under TOP, there are limited numbers of software that can be used for these file transfers which includes Connect Direct, Cyber Fusion etc. For this purpose, MS uses Connect Direct 4.6.

As depicts by Figure 17 Connect direct need human interaction to complete additional processes which required movement of these two files to the physical batch box manually and execute on demand batch that follows execution of two child batches which applies all the repayments and also checks for the reversal. All the IRS data is encrypted before storing into database. Similarly, a single flat file is created once a week using the information from database and sent back to the IRS.

Guardium is implemented for audit of all the tables those are somehow related to the consumption and creation of flat files associated with IRS.

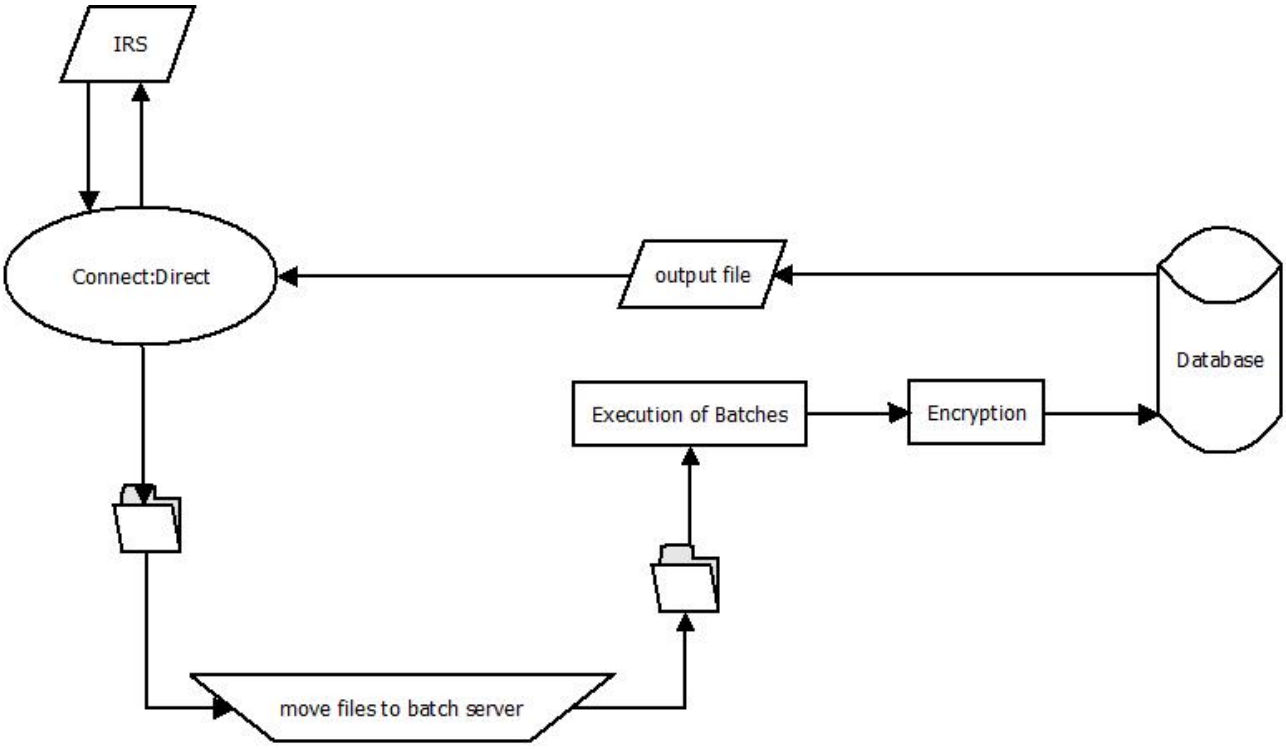

Figure 17: TOP Data flow diagram

10.1.13 Printing and Mailing

ACCESS Framework generates Correspondence in multiple runs depending on the business requirement. It has the capability to group correspondences in different runs and further group them based on the type of correspondence. These generated correspondences are then grouped in the form of a single PDF file for each group which can be sending to the print department. Currently for Mississippi these PDFs are uploaded to a file server and the links along with the print instructions are emailed to the printing department. In a cloud environment, the mode of sharing these generated PDFs with each state can be defined once the hosting is finalized.

The key features of the correspondence generation framework are:

- Configuration for Stuffers and Self Mailer correspondences.
- Address presorting on Bulk mailing.
- Correspondence grouping and merging for ease in printing.
- Upload to DMS for the configured correspondences.

10.1.14 Backup Process

EMC AVAMAR is used as software tools for all servers backup.

- Database server backup taken by DB2 software client itself within the server.
- Daily full backup of required files / folders are taken and put into disc or tape.
- These discs and tapes are encrypted.
- This disc or tape will be stored in disaster recovery site through manual process.
- At time of recovery this disc or tape will be used to restore the rest of the server.

11. Deployment Architecture

11.1 ACCESS MS Production Environment

The existing production environment for MDES is architected with the objectives of handling a large number of transactions, where important factors like scalability, availability, and expandability among others are addressed.

Attached Spreadsheet contains the as-is Server details along with sizing information for ACCESS MS System.

AccessMS server infrastructure info wit

Each of these servers will be migrated VMware/Linux infrastructure. Currently options are being explored for cloud based hosting for all three states. The sizing information for the upgrade will remain same as the as-is servers and the Server/Processor models will be finalized along with the Cloud Infrastructure RFP.

11.2 Existing System Overview

Requests from the Internet users are resolved to an Internet address by a Domain Name Server (DNS) server hosted at ITS. Once the connection comes through ITS's PIX the Internet IP address is translated to a local IP address on the internal Local Area Network (LAN). The request then hits the edge server that establishes a static connection with the Internet user and forwards the request back to one of the two http servers, load balanced by the edge server. The edge server has a cryptographic coprocessor installed to facilitate encryption processes. SSL sessions are kept static between the edge server and the end users browser. A Sun Access Manger client will reside on either the http servers or on the application servers and will communicate with a Sun Directory Server where user profiles and roles will be stored and read for authentication and authorization information. Application server will use the following software for the execution of business processing logic:

- IBM DB2 UDB Database
- JBoss Drools Flow
- Report Server
- Apache Jackrabbit
- Directory Server

All servers in the architecture (application server, http server, database server, drools workflow server, drools workflow database server, access manager, access & directory server, reporting server) will be implemented in a mirrored fashion for load balancing and failover recovery. These servers use Storage Area Network (SAN) as their external storage mechanism. The servers are connected to the SAN Storage hardware through Gigabit switches to enhance the system and network performance. Fiber channel connections are being used to connect the servers to the SAN. The Falcon Store software running on the blade servers manages the SAN. A tape backup system will be used to backup all servers to tape. Remote IP replication will be employed across the Wide Area Network (WAN) to the Disaster Recovery site utilizing a 45MB MB DS3 Link to Information Technology Services (ITS). The Servers are connected with Gigabit Switches. The routers and switches have Gigabit speed connectivity to enhance the network performance.

Figure 18 depicts various hardware and software and their interaction in production environment for MS.

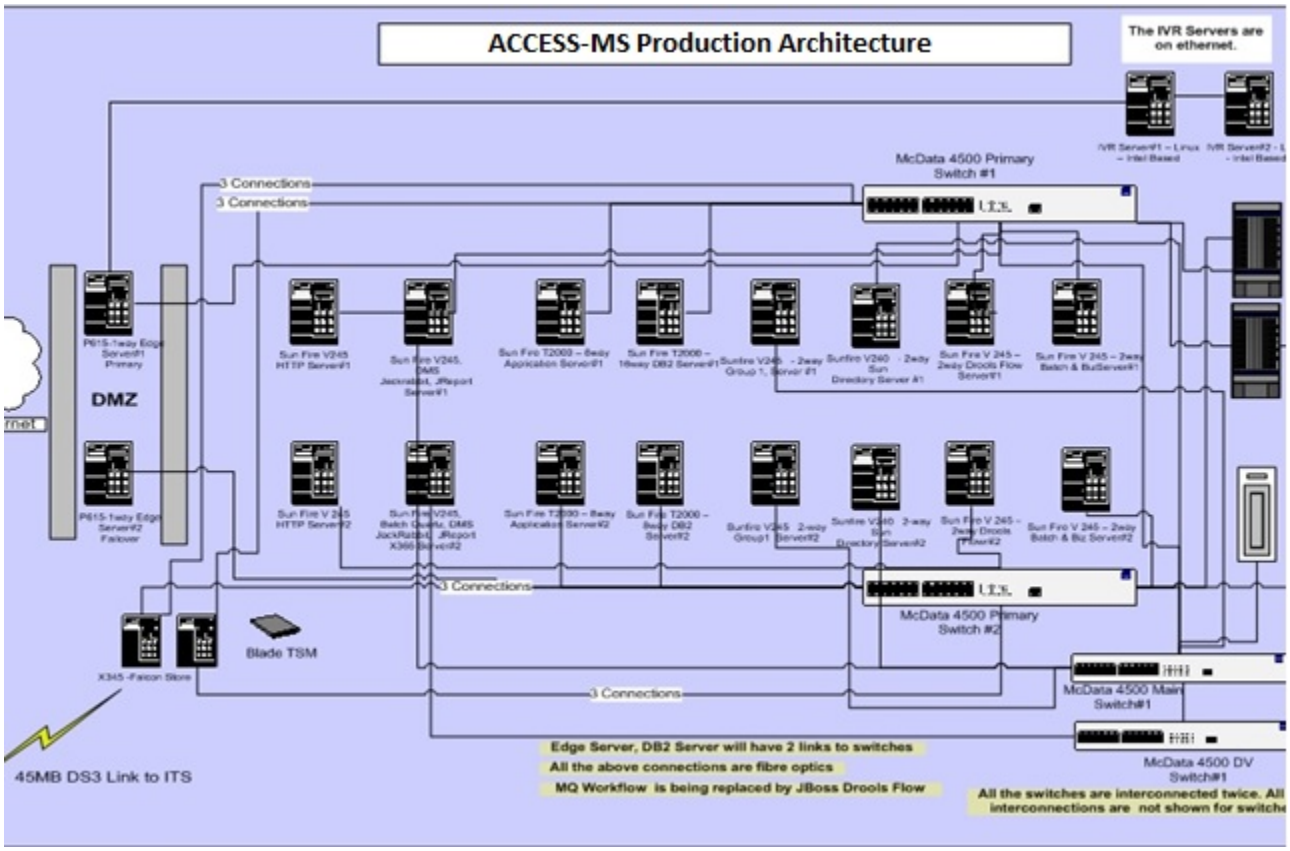

Figure 18: ACCESS-MS Production Architecture

Figure 19 depicts Logical architecture diagram for ACCESS MS System.

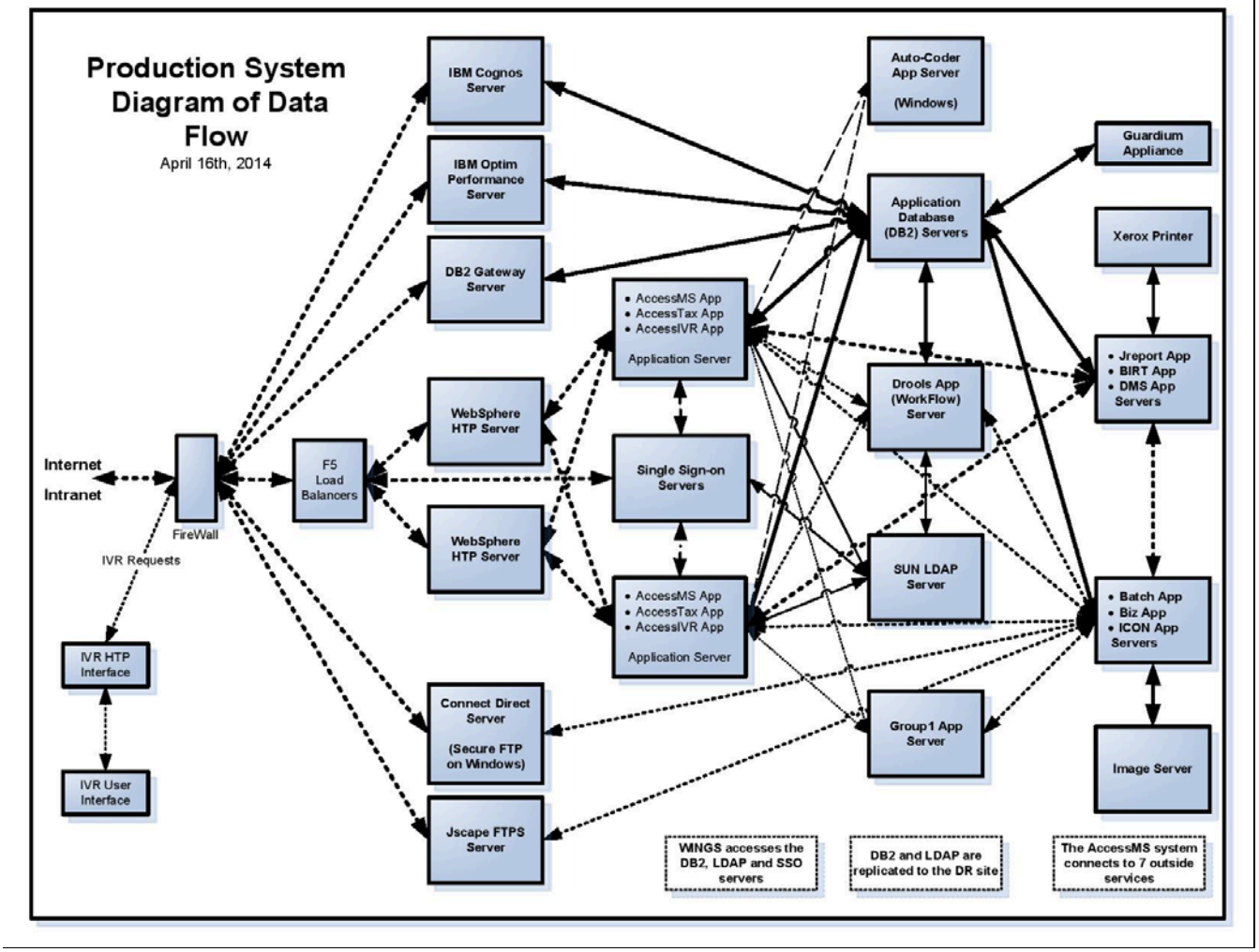

Figure 19: ACCESS-MS Production Logical Architecture

11.3 **Proposed cloud based architecture advantages**

Agility: It will improve with users' ability to re-provision technological infrastructure resources.

Application Programming Interface: (API) accessibility to software that enables machines to interact with cloud software in the same way that a traditional user interface (e.g., a computer desktop) facilitates interaction between humans and computers. Cloud computing systems typically use Representational State Transfer (REST)-based APIs.

Cost: Cloud providers claim that computing costs reduce. A public-cloud delivery model converts capital expenditure to operational expenditure. This purportedly lowers barriers to entry, as infrastructure is typically provided by a third-party and does not need to be purchased for one-time or infrequent intensive computing tasks. Pricing on a utility computing basis is fine-grained, with usage-based options and fewer IT skills are required for implementation (in-house).

Device and location independence: It will enable users to access systems using a web browser regardless of their location or what device they use (e.g., PC, mobile phone). As infrastructure is off-site (typically provided by a third-party) and accessed via the Internet, users can connect from anywhere.

Virtualization technology allows sharing of servers and storage devices and increased utilization. Applications can be easily migrated from one physical server to another.

Multi-tenancy will enable sharing of resources and costs across a large pool of users thus allowing for:

- Centralization of infrastructure in locations will lower costs (such as real estate, electricity, etc.)
- Peak-load capacity will increase (users need not engineer for highest possible load levels)
- Utilization and efficiency - improvements for systems that are often only 10–20% utilized.
- Reliability improves with the use of multiple redundant sites, which makes well designed cloud computing suitable for business continuity and disaster recovery.

Scalability and elasticity via dynamic ("on-demand") provisioning of resources on a fine-grained, self-service basis near real-time without users having to engineer for peak loads.

Performance is monitored and consistent and loosely coupled architectures are constructed using web services as the system interface.

Security can improve due to centralization of data, increased security focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels. Security is often as good as or better than other traditional systems, in part because providers are able to devote resources to solving security issues that many customers cannot afford to tackle. However, the complexity of security is greatly increased when data is distributed over a wider area or over a greater number of devices, as well as in multi-tenant systems shared by unrelated users. In addition, user access to security audit logs may be difficult or impossible. Private cloud installations are in part motivated by users' desire to retain control over the infrastructure and avoid losing control of information security.

Maintenance: Maintenance of cloud computing applications is easier, because they do not need to be installed on each user's computer and can be accessed from different places.

The Private Cloud Infrastructure should offer the following:

1. Hardware (Server, Storage & Networking)
2. Virtualization & OS software
3. Monitoring of Application and Infrastructure
4. Management - Usage & Billing
5. Backup
6. Business Continuity & Disaster Recovery
7. Security & Access Control
8. Compliance with IRS 1075 guidelines
9. Audit
10. Upgrades & patching (software & firmware)

12. Audit, Security, Compliance and Risk Management

12.1 Audit

All system logs, access logs, database transaction logs, application logs will be preserved for specified time period as agreed upon with the states. Since these logs will be residing on the Linux file systems in the event it is required for forensics purposes, the file systems can be exported to different target systems where it can be analyzed with the help of the forensic tools. The auditing can be done through the application tools & reports or it can be done through forensic tools which will analyze the available logs and present in a report format for easy detection of any irregularity that might exist.

12.2 Log Management

All logs need to be securely stored for future audit and forensics purposes. Logs from all the production systems for OS, databases and applications need to be collected and periodically analyzed for any discrepancy. There are various vendor and open source software available for these purposes. The forensics software can be integrated with the log management tool to provide a comprehensive forensics and audit of the entire platform if needed. The architecture of the log management system can be added once it is decided which software will be implemented. The following software is available:

1. SolarWinds
2. vCenter Log Insight
3. Splunk
4. OSSEC
5. Logalyze

Figure 20 depicts Log Management and Forensics details.

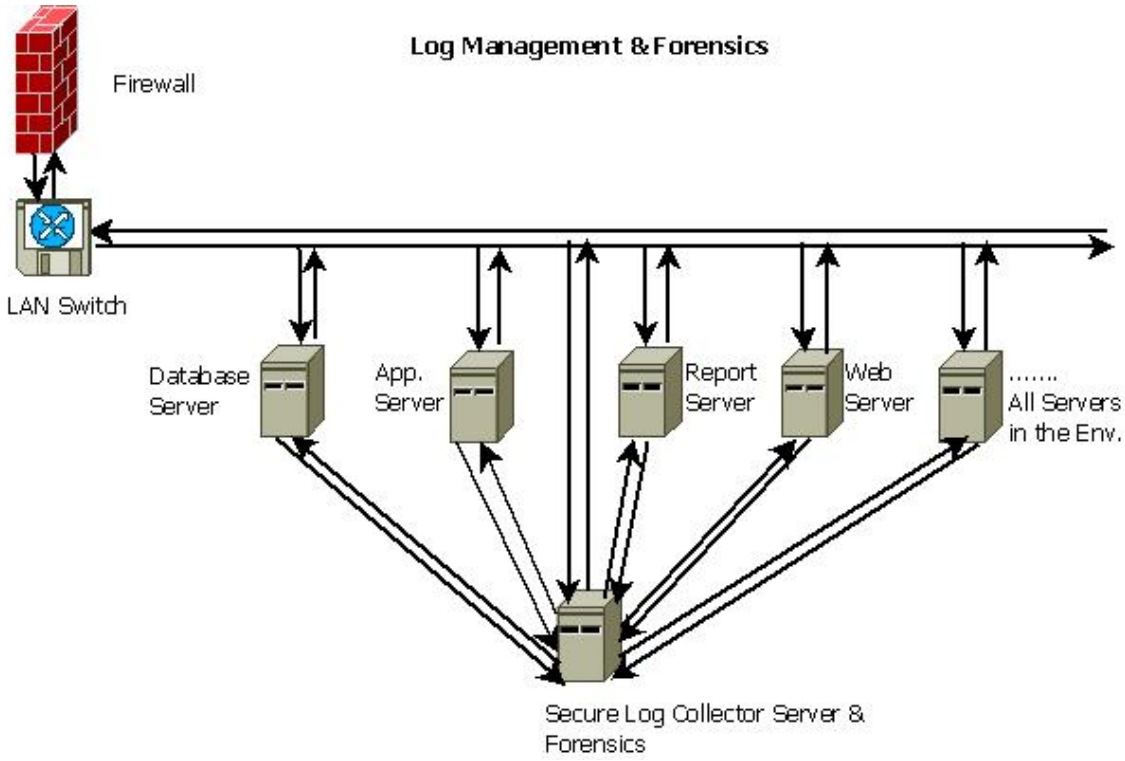

Figure 20: Log Management & Forensics

12.3 **Security**

All access to the UI system will through the application or the servers that house the UI application. Access will only be allowed upon following through the established access management process. The application will use AD/LDAP authentication and single sign on where needed for access purposes. A two-step access control process to be adopted by use of secure tokens. All access logs will be preserved for future reviews. All application web pages to use secure connections through the use of SSL certificates to reduce the risk of unauthorized access. There should be no developer access to production systems. All privileged access like that of system administrator, database administrator should be only allowed only after thorough review and approval. All records of access requests need to be preserved for future reviews.

12.4 **Web Services Security**

TCS is currently exploring various options for securing the web services and will add the details in the next release of the document. The framework will be JAVA based since the current platform runs on JAVA. In the meantime, all existing vulnerabilities for the current platform will be checked and appropriate actions will be taken for mitigating the risk.

12.5 **Compliance**

Any server that contains tax payer information needs to be configured as per the Federal Tax Information Security Guidelines for Federal, State and local agencies, as stated in the IRS Publication 1075. Since the servers will be installed and managed by the third party, it is important to ensure that all relevant guidelines are being met. All changes to the systems housing the UI application should be done through the established change management process. In the event of problem management, an incident management process should be established and for every incident there should be a root cause analysis and a corresponding fix should be applied in order to avert such incidents in the future. All servers and applications should be monitored for proactive problem resolution and future capacity need purposes. Also, there should be segregation of duties i.e. the requester cannot be the approver. A configuration management process should be in place in order to validate all required server/software configurations are as per guidelines.

The MRM Consortium application will be following the IRS 1075 FTI guidelines. The link and the related documentation are attached below:

http://www.irs.gov/uac/Safeguards-Program

Appendix A. JEE and Design Patterns

ACCESS System will adopt open technologies for building the system. It will be very similar to the Object Modeling Group's (OMG's) model driven architecture approach where the architecture will provide platform independent design and wherever there is a need for the platform specific functionality, abstractions will be provided to hide the underlying technology, hence reducing the cost involved in porting to different platforms. The ACCESS System will have a framework that will be built upon the JEE model/environment with the JAVA programming language.

JEE

JEE is a platform that enables solutions for developing, deploying and managing multi-tier server-centric/Web based enterprise applications. JEE builds on Java to extend a complete, stable, secure, fast Java platform to the enterprise level. It delivers value to the enterprise by enabling a platform that significantly reduces the cost and complexity of developing multi-tier solutions, resulting in services that can be rapidly deployed and easily enhanced. The JEE platform consists of a set of services, API's, and protocols that provide the functionality for developing multi-tiered, Web-based applications. This model is intended to both standardize and simplify the kind of distributed applications required for today's networked information economy.

Major JEE Standard Services

The JEE standard services include the following:

- HTTP
- HTTP over SSL (HTTPS)
- JTA
- Remote Method Invocation – Internet Inter Object Request Broker (ORB) Protocol (RMI-IIOP)
- Java Interface Definition Language (Java IDL)
- JDBC
- Java Persistence Architecture (JPA)
- JMS
- JNDI
- Java Mail
- JavaBeans Activation Framework (JAF)
- Java API for XML Parsing (JAXP)
- JEE Connector Architecture
- Java Authentication and Authorization Service (JAAS)

Some of the above standard services are actually provided by Java Platform Standard Edition (JSE), the base services for Java platform. Figure 21 depicts the Sun JEE architecture.

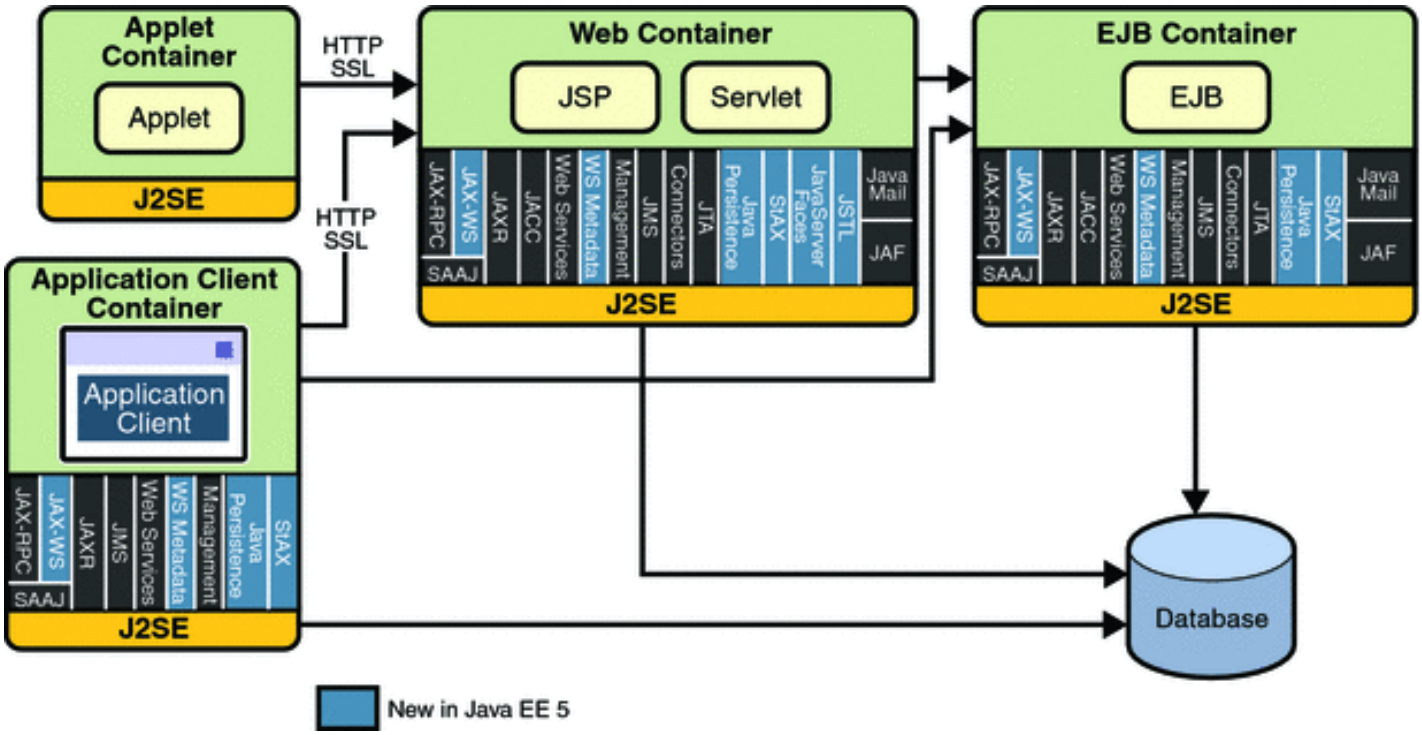

Figure 21: JEE Architecture – Courtesy Sun Microsystems

Design Patterns

The ACCESS technical framework will be built upon industry standard JEE design patterns.

Why Design Pattern?

A design pattern is a **solution** to a general software **problem** within a particular **context**.

- **Context:** A recurring set of situations where the pattern applies.
- **Problem**: A system of forces (goals and constraints) that occur repeatedly in this context.
- **Solution**: A description of communicating objects and classes (collaboration) that can be applied to resolve those forces.

Design patterns capture solutions that have evolved over time as developers strive for greater flexibility in their software. Patterns are generic, reusable design descriptions that are customized to solve a specific problem. The study of design patterns provides a common vocabulary for communication and documentation, and it provides a framework for evolution and improvement of existing patterns.

The section below outlines the Model-View-Controller (MVC) design pattern that will be used in ACCESS System.

Model-View-Controller Design Pattern

MVC is a classic design pattern often used by applications that need the ability to maintain multiple views of the same data. The MVC pattern hinges on a clean separation of objects into one of three categories:

- **Models** for maintaining data
- **Views** for displaying all or a portion of the data
- **Controllers** for handling events that affect the model or view(s)

Because of this separation, multiple views and controllers can interface with the same model. Even new types of views and controllers that never existed before can interface with a model without forcing a change in the model design.

The goal of the MVC design pattern is to separate the application object (model) from the way it is represented to the user (view) from the way in which the user controls it (controller).

How MVC Works

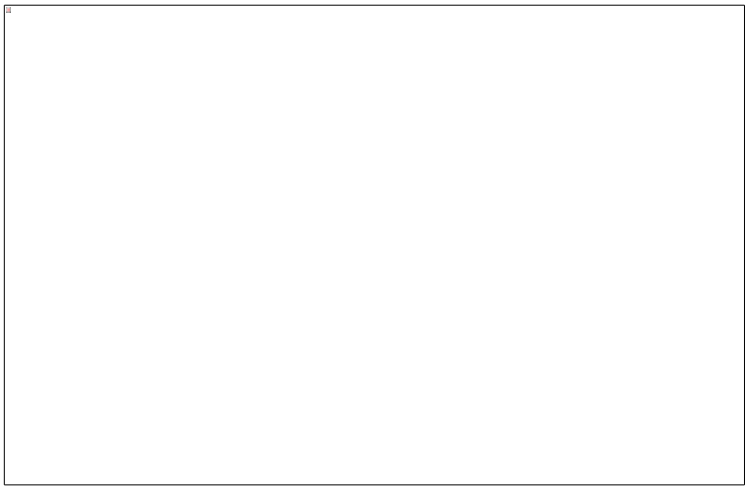

Figure 22: The MVC Abstraction

Events typically cause a controller to change a model, or view, or both. Whenever a controller changes a model's data or properties, all dependent views are updated. Similarly, whenever a controller changes a view, for example, by revealing areas that were previously hidden, the view gets data from the underlying model to refresh itself.

Dependency Injection

Ideally a Java class should be as independent as possible from other java classes. This forms the foundation of a loosely coupled and flexible framework. A Java class has a dependency on another class if it uses an instance of this class. Thus the java class cannot be tested independently.

Dependency Injection pattern describes how one object resolves or finds other objects on which it needs to invoke methods. Dependency Injection can be done manually using Factory Helper or automatically using annotation. ACCESS framework will employ Dependency Injection to reduce code dependency between various components of the framework.

JEE Design Pattern

MVC Design pattern will be making use of several others JEE design patterns to achieve the overall goal and they are:

- Application Controller – Manage the lifecycle of the individual commands and mapping the requests to specific commands.
- Command - An operation to process an individual request. In some cases multiple similar requests might be handled by the same command.
- Composite View - Provides a means of composing a single view from a set of individual views. The composition will be defined by the metadata present in an XML file.
- Data Access Object (DAO) - A generalized way of accessing a specific type of data. It helps to allow the change of the data access mechanisms independently of the business logic that uses the data.
- Dispatcher View - The dispatcher view is responsible for dispatching a request to a specified view based on the results of the Command processing.
- Session Facade – It encapsulate the complexity of interactions between the business objects participating in a business process. The Session Facade manages the business objects, and provides a uniform coarse-grained service access layer to clients.
- Fast Lane Reader – It provides a more efficient way to access tabular, read only data, as reading a list of read–only data using EJBs through individual bean instances can be costly and slow and incurs a high performance overhead.
- Front Controller - Point of entry for requests to update UI model. The controller is responsible for processing requests.
- Intercepting Filter - All requests are subject to Intercepting Filters, which allows an application to preprocess a request before it is handled by the controller. An intercepting filter can pre-process or redirect application requests, and can post-process or replace the content of application responses.
- Service Locator - Locate a service or resource needed within an application such as a JNDI resource, JDBC connection, or an EJB component.
- Transfer Object – These will be used to encapsulate the business data. A single business method call is used to send and retrieve the Transfer Object. When the client requests the enterprise bean for the business data, the enterprise bean can construct the Transfer Object, populate it with its attribute values, and pass it by value to the client.

- Value List Handler - This can be used to control query execution functionality and results caching. It will access a DAO that can execute the required query. It can also store the results obtained from the DAO as a collection of Transfer Objects. The client requests the 'ValueListHandler' to provide the query results as needed.
- View Helper – This can be used by the UI view components to access the UI model data. View helpers include JavaBean components, which may have been placed in the request. Tag libraries may also be used as view helpers.
- Figure 23 depicts the interactions between the different JEE patterns on which the ACCESS System will be based upon.

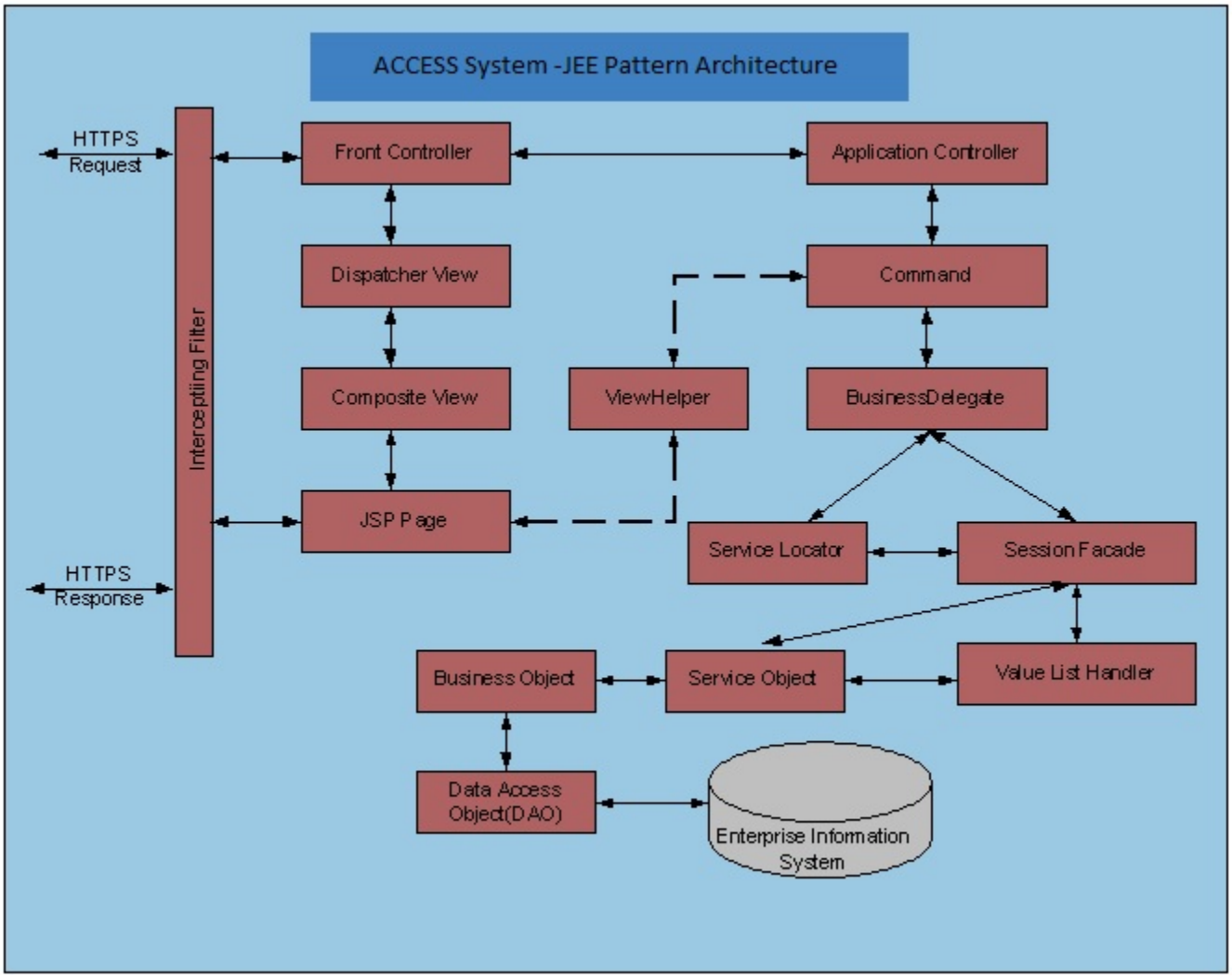

Figure 23: JEE Pattern Architecture

Appendix B. Review Comments

ITSC Review Comments

Questions & Comments from ITSC on the Architecture document:

Comment - Overall a good draft however need the following clarifications.

1. What is overall approach to multi-tenancy? 5.2.3 Covers BRMS aspect but what about runtime execution of state specific code? Or will everything that is state specific be implemented in DROOLS and only common functions in code? How will ACCESS be migrated and tested? **Answer**: Application code base will be categorized into CORE (Benefits, Framework & Tax) which includes Business Rules Implementation and State Specific Components (Benefits & Tax). Each state will have its own instance of Benefits and Tax application which will include CORE and the particular State Specific piece. Section 5.2 refers various Framework services to implement the State Specific functionality. Section 5.2.4 has some details on this item.

2. Was an ESB considered, particularly to accommodate changing I/Fs and adding states? **Answer**: Based on the Site visit and requirement sessions so far, the current architecture capabilities for Interfacing and messaging meet the MRM requirements.

3. For Web Services, is REST being considered vs. SOAP?

Answer: We currently have SOAP based WebService Implementation, REST based WebService if required will be implemented.

4. Need prototype/proof of concepts in the Phase I of benefits. This is generally going to happen but just to make sure.

Answer: Architecture changes will be implemented and rolled out in parts before the first phase of Benefits I is rolled out. Also, before rolling out any component, the changes will be going thru the development & testing cycles.

5. How will TCS manage interoperability of products into the future?

Answer: Current software list along with the versions and the planned upgrade version is maintained in the document. TCS will ensure these software versions are compatible.

6. Is there an overall approach to third party product substitution if needed?

Answer: Any third party software will be evaluated and then will go thru the development (for any changes that may or may not be required), & testing (integration & functional) cycles. If required, POCs will be carried out.

7. Great stuff on patterns. Will IOC/DI and/or AOP be used?

Answer: Dependency Injection is used in the current Architecture. It's depicted in the Sequence Diagrams for the architecture in section 6.6. We will add a description of the design pattern in the Appendix as well along with other design patterns.

8. Need to have architecture decision matrix for facets still under consideration e.g. WebSphere vs. JBoss. ITSC will provide a sample template.

9. As suggested, a data flow diagram added (Refer Figure 5: Component Diagram for Framework Services corresponding to Core and State Specific Implementation).

10. As suggested, the first paragraph for "Application Hosting has been updated to reflect IaaS and the items related to procurement removed.

11. How far did the POC go for Drools? Where all layers of the arch traversed? What about full scale performance and when more states are added?

Answer: We have installed JBoss Drools software and verified the second option (Refer Section 5.2.3 second option: state specific Rule package which contain several DRL files) which we chosen for implementation. "DROOLS framework changes will be moved to production before Benefits 1 release". Performance testing will be conducted during that time.

12. How far did the POC for mobile application development.

Answer: The attached PPT is describe the mobile application development POC.


Mobile_App_POC.pptx

Review comments given for Version 1.1

13. There are only 4 external interfaces listed. Further, there is no discussion regarding pros and cons of using an ESB which could promote onboarding downstream in a few areas including interfaces.

Answer: The four external interfaces were noted as examples for the types of interfaces that impact the architecture document. TCS will be evaluating the risks and requirements for moving to ESB based architecture for the MRM Consortium as a future plan.

14. Is the plan to comply with WS-Security? I think there should be a reference to the standards to which the solution will comply.

Answer: Yes, there is a plan to comply with Web Services security framework and the reference will be added to the technical architecture / standards documentation.

15. Where relevant, I believe there should be mention of proofs of concept, like the multi-tenant aspect.

Answer: TCS will update the coding standards doc. with the details of practices on common code and customization of state specific components.

16. There is no mention of each state being able to access their relevant data regarding log files (see page 75).

Answer: The current infrastructure plan is to house the three states in three logically separate platforms which will have a common underlying VIrtualized IaaS base. Hence all the member states will have logs (application, database etc...) separately available for forensics purposes. These details will be updated in the application hosting part of the technical architecture document as discussed.

17. Page 82, the e-FISCAL reference needs further elaboration.

Answer: Appropriate changes will be made to this section of the document as pointed out.

18. Page 43, use of stored procedures has benefits for bulk complex processing but there should be mention of impacts on DB substitution.

Answer: Since there are only a few stored procedures in use and the member states are also going to use DB2, TCS will evaluate the conversion of the stored procedures to Java based queries in the future. This will be also useful for any DB substitution in the future. Since the use of stored procedures are limited, TCS doesn't perceive any problem in the conversion for a more efficient process for handling the related queries, at this time.

19. How will code quality be ensured? Any tools used in combination with build processes?

Answer: TCS mentioned Google Code Pro Analytics is being used for code quality and the technical architecture doc. will be updated with the details.

20. Page 16, what is the basis for the configurations? Were capacity analysis and tools used? Where the 3 state's workloads considered? The IaaS should be included in this.

Answer: TCS evaluated the capacity related data received from MS and MO along with the experience with the platform and came up with a standard configuration. It was also mentioned that since the infrastructure is based on IaaS, any changes / tuning that will be required can be easily achieved with very little turnaround time.

State of MAINE Review Comments

Questions & Comments from Maine on the Architecture document:

1. Mobile App. development for Java.

Answer: The Mobile App. components have been listed and Android SDK has been mentioned in the list of Development Software.

2. Struts 1 beginning end of life this year. Why is TCS continuing with Struts 1 which is not supported.

Answer: Struts 1.3.5 EOL announcement was released April this year. But moving from Struts to other framework is a major architectural change and needs re-development of application code. Also, the current application will not benefit from the additional features that the new framework will bring. However, at this time since Struts 1.3.5 has reached EOL we will evaluate the changes that will be required for migrating to Struts 2.0http://struts.apache.org/struts1eol-announcement.html

3. Separate tax & benefits on separate servers, middle tier is duplicated on tax and benefits system?

Answer: The two applications will be running on one server as it does in the current MDES configuration. Both applications have the runtime code completely independent of each other with a common middle tier that includes the base code.

4. Deployed as separate independent Apps. - duplicated on tax & benefits.

Answer: The two applications - tax and benefits are to be deployed separately so that maintenance and deployments can be independently carried out. Currently, the two applications have similar configuration for MDES. A modular approach has been taken so that any future application can be easily ported on this platform.

5. One rule set vs smaller rule sets.

Answer: BRMS there was a question on the possible number of rules in the application for the approach, and we had mentioned that there would be many rulesets and hence our recommendation is the second approach which is more modular and easily manageable in terms of performance. During the development the rulesets a thorough testing will be done to avoid any failures in the later stages.

6. Native vs responsive web apps. for mobile devices; documentation for this comparison. **Answer**: The attached document and the links will provide you with the data comparison that we did for deciding which is a better option for us - native or the Web Application.

http://venturebeat.com/2013/07/29/native-v-web-chart/

http://www.businessinsider.in/HTML5-vs-Native-Mobile-Apps--HTML5-Is-Down-But-Not-Out/articleshow/21829859.cms

Mobile Development Approach.docx

7. Lack of awareness of how fast native environments are evolving. HTML 5 CSS 3 is agnostic, Corona, Sibco, Antenna etc.. Write in an intermediate language source to source comparison. **Answer**: Same as in item 6.

8. Audit handled at DB level or business layer?

Answer: The audit is handled in both levels. The business layer produces the business level reports and the OS level audit logs can be used for DB level audit trails.

9. How is access to logs provided? Access is on server available to developer. Add information in document related to IBM Infosphere Guardium.

Answer: Application generates Debug and Error logs in the file system which are currently used by the developers. These logs can be mounted and made available on remote file servers. For the Forensics, and auditing tool like IBM Infosphere Guardium product can be integrated in the solution.

10. Why is Pentaho and Jaspersoft not suitable here? Can we assume nightly refresh?

Answer: This has been answered in the document, only pending item is BI part for which we have requested you to get in touch with Mohammed as IBM had some presentations and Use cases already presented to MDES and can be shared.

11. Update the paragraph on Application Hosting.

Answer: This paragraph is updated in the the Technical Architecture Doc.

12. We have added ection for Audit, Compliance, Security, and Risk management.

Review comments given for Version 1.1

1. Mobile Development

- Request a detailed discussion on Responsive Web v. Native v. MEAP-Middleware.
- As of now, there is only a comparison between Native v. Corona-Lua-MEAP-Middleware; Please expand this…
- What if we adopted one unified Responsive Web UI w/ Mobile-first? If bandwidth could be released from native mobile development, perhaps we could choose a modern Web framework.
- Our concern is that different stakeholder groups' requirements be considered in arriving at this decision.

TCS response:

The details of the mobile application are given in the updated technical Architecture document - Section 5.2.5.

Maine response:

- Nothing new or relevant to our questions & concerns is presented in Section 5.2.5.
- TCS has simply refused to consider Responsive Web UI w/ Mobile First.

Meeting(10/21/2013) discussion:

Explained that the comparison and features of Native and Web development approach is included in the Appendix B Review Comments section and the recommendation of native development is due to the best GUI and performance which is the roadmap for mobile app development that is set for the Consortium.

2. Likewise, choosing a more modern Web Framework would also help us deal with the Struts 1 end-of-life dilemma.

TCS response:

This was discussed in the meeting that the most logical step would be to migrate to Struts 2 however, nothing would be gained from the application perspective since whatever extra features Struts 2 offers, the application is not dependant on it. Also, moving to Struts 2 would add time to the development cycle which may delay in the porting of the application on the new platform. In the past, there were no support needed for the Struts 1.3.5 and until we decide to move/upgrade or not to different framework, it is expected to remain the same.

Maine response:

- Nothing new or relevant to our questions & concerns is presented in Section 5.2.5.
- TCS has simply refused to consider Responsive Web UI w/ Mobile First.

Meeting(10/21/2013) discussion:

Explained that the current architecture that is struts 1 based is been customized and upgraded for MS solution and suffice the solution requirements. Also, looking at the past record of Benefits and Tax development for MS, we have never faced any issue or need for support or bug fixes from struts community. So considering the effort required to move to struts 2 and the consortium timeline, we don't see any gains in moving to struts 2 yet.

3. Forensics & Log Management

- Request (1) more granular tracking of who-what-when-how, as well as (2) Exportability to external (third-party) SIEM toolsets.
- Restated, we believe that a manual forensics strategy is not the correct approach.

TCS response:

We have added more details on this topic in chapters 6.2.7, 6.2.9, 9 and 12 of the updated Technical Architecture Doc.

Maine response:

- Some improvement, yet there does not appear to be an awareness of the basic problem of log aggregation and correlation. Sections 6.2.7 and 6.2.9 referenced in this context have nothing to do with forensics. The suggestion to bring IBM Guardian product in is not addressing the SIEM problem. Also, adds another expensive piece of software without solid articulation of how that selection was made.
- Section 12 is not helpful in describing anything related to the 'architecture' of the system dealing with risk, compliance, or security.
- We need an architecture diagram from TCS that illustrates how one of these products would be integrated.

Meeting(10/21/2013) discussion:

TCS will provide a diagram showing the product and its integration with the system.

4. Request more details on the Distribution Model of Jars & Rules. What about wiring performance management into the various components & layers from the ground up? Also request more detailed Architectural Diagrams (both physical and logical) diagrams. Please see the attached examples.

TCS response:

We have added more details as requested, in chapters 4.1.4 & 5.2.3. The deployment architecture have been attached in section 3.6, 3.7 and 11.

Maine response:

- Non-answer, the requested details have not been added.
- Our request to receive clean physical, logical, and deployment views of the architecture was not satisfied.
- Given that TCS is using the Rational toolset for development, we do not understand why the Rational Unified Process was not adhered to in the creation of the Architecture Document.

Meeting(10/21/2013) discussion:

Explained scenario of code movement to Production. This will be added to the architecture document. ME also requested an diagram of the physical architecture to be added.

5. BI Solution

We would like to review the Use Case examples (i.e., the customer –facing details in support of the solution proposal).
This information will help us support our business clients in assessing the delta between their current data warehouse solution and the proposed project offering.

TCS response:

The details of all BI related items can be found in chapter 8 of the updated Technical Architecture doc. As previously discussed, we would request Mohammed to forward you the details including the use cases received from IBM on the BI software.

Maine response:

- Non-answer; TCS has relegated their responsibility of working with our business clients to build the necessary Use Cases to MDES.
- Use Cases should NEVER originate from the vendor; conversely, the vendor's role is that of the facilitator, the analyst, the recorder of the Business Case obtained during interview sessions with the business clients.
- We strongly advise, that if the Use Cases have not been recorded, do not waste money on the BI tool this early in the project. A BI solution can always be bolted on when needed. Restated, there is no opportunity cost to not acquiring a BI solution until the Use Cases can be demonstrated. As a matter of fact, cost is typically minimized once the Use Cases are finalized and formally accepted by the Business Client.

Meeting(10/21/2013) discussion:

Explained that the decision to get a BI is already in place and currently MS is going ahead with procuring the BI solution outside the consortium and later it can be added for Consortium

6. Deployment & Change Management Strategy

How will changes to hardware/software be managed across the three tenants post-Go Live? Is there an SLA template you can share with us so that we can understand the metrics that will be used?

TCS response:

We suggest that one change management system be used for the new MRM or we can use the system that each state has, to start with and the processes will remain same for managing any hardware/software change in the platform.
Regarding the SLA part, we would request Mohammed to send you any template that the MDES team uses.

Maine response:

- Non-answer; the responsibility for this critical aspect of on-going support clearly belongs to TCS, not MDES. We would not expect that the current process in place for MS would be adequate for the consortium – it is an entirely different problem space to deal with three separate tenants/clients, each residing in different physical locations.

Meeting(10/21/2013) discussion:

This is covered under the examples of code deployment which was described in details during the meeting.

7. Disaster Recovery
While not mentioned explicitly on the 9/24 call, the comment regarding the high cost of securing the remote hosting vendor/data center for the project, brought this to mind for us. Is a full DR site still part of the overall plan?

TCS response:

We do not have the detailed information on the data center strategy yet. As we receive information from consortium member states, we update the document to reflect the details. Currently, Mohammed and team are working on the hosting with various vendors and we hope the details will be available soon.

Maine response:

- Non-answer; the DR strategy is a major consideration for Maine, as is the Data Center selection process, the former clearly dependent on the latter. Given the priority of both, we question the choice made by the project to focus on other much less critical areas such as selection of the Business Intelligence tool suite.

Meeting(10/21/2013) discussion:

For MRM cloud option is currently been explored, and its expected that the DR will be finalized along with that. ME expressed the need for them to test the DR site.

State of RHODE ISLAND Review Comments

1. Application hosting has been updated in Chapter 3 Architecture Validation.
2. Cloud base architecure has been proposed for Consortium states and related advantages has been given in section 11.1.2.
3. Detiled analysis for Mobile application development approach has been given in question no. 6 within Maine review comments.
4. Following required section added / updated.

   Transaction Management: Section 6.2.7

   Security : Section 6.2.3

   Imaging Solution : Section 10.1.8

   Printing & Mailing : Section 10.1.12

   Backup Process : Section 10.1.13

   TOP : Section 10.1.14

5. Chapter 9 has been added for data movement tools.
6. Chapter 12 has been added for Audit, security and Compliance specific which covers the required security standards like IRS.
7. All lillte changes like “Pros and Cons for budled vs separate application”, “Workflow software version”, “Address validation software update”, “details for Guardium”, “Single sign on”, “External systtem interface” are updated in document at respective sections.

Review comments given for Version 1.1

1) “The infrastructure for ME, MS & RI will be hosted separately”
   a) This was originally supposed to be hosted together with a core system shared by all and a business rules engine specific for each state.

   Answer: The system will be hosted on a multi-tenant cloud computing environment. It is logically a single system with business rules engine but hosted independently for each state.

   b) Will this new structure increase costs for licensing, maintenance, administration?
   Answer:No. With multi tenancy and virtualization we will see a cost sharing of licensing fee. Maintenance and support costs for the software will see significant reductions.

   c) Is MS in the cloud or are they locally hosted?
   Answer: All 3 states will be hosted identically on the cloud.

2) Why are we doing a mobile app now? Shouldn’t we concentrate on getting the core work done now and add enhancements later?
   Answer: MS wrote a SBR grant to do a mobile app for weekly cert and work search. MS is obligated to complete this. This will be available to RI and ME as part of the core.

3) Hardware out of scope, where is it being located and who is paying for this? Is this an additional expense to be assessed to ME, RI, & MI?

Answer: Production hardware will be on the cloud. Test and Development will be in MS Data center. Majority of the cost will be paid from Mississippi's $10 million. The rest if any would come from remaining $60 million and/or state specific $10 million.

4) SSO out of scope for ME & RI.
    a) Will this mean that ME & RI users will be required to present logon credentials at different places as they pass through the different parts of the application?
    Answer: The single signon only applies to the integration of Mississippi's ES and UI systems. ACCESS MS is a single integrated application where you need to login only once.

    b) Will there be a central accounts database for all three states
    Answer: We will use 3 different LDAP repositories, one for each state.

    c) Active Directory/ LDAP authentication- will this be state by state or one AD?
    Answer: Different LDAPs for each state. We do not use AD.

5) Overwhelming reliance on IBM proprietary software versus the original open source vendors
    a) Analysis of recommended software has pro & cons but lacks reason why one vendor was recommended over another. Need clarification on vendor selection
    Answer: This is already discussed during the meeting.

6) Need clarification on SAN connectivity. " The servers are connected to the SAN Storage through Gigabit switches …." "Fiber optic cables are used to connect the servers to the SAN"
    a) the first statement seems to imply iSCSI SAN connection
    b) the second statement seems to imply Fiber Channel SAN connection
    Answer: This is already discussed during the meeting. Fiber channel related information will be provided in Architecture document

7) Costs: does MS/TCS have any idea of the yearly cost to operate and maintain the system.
    Answer: We do not an exact estimate of costs yet.

8) Employment Services -- Job Orders: MS currently matches customers to job orders during claim intake. I believe they indicated they can match to out-of-state jobs. Can RI take advantage of their job match process? Does it include all out-of-state job orders?
    Answer: This is ES functionality and is considered out of scope for this project.

9) State-specific Imaging Systems: how will RI continue to use workflow in their existing OnBase application?
    Answer: State imaging systems will operate independently of the ACCESS MS system. RI will not be able to continue the use of workflow present in their existing systems. Business Process Redesign has to be take place to adhere to ACCESS MS process.

10) IVRs: will RI be required to develop their own system or can they use the Avaya solution used by MS? Would it be more cost effective for all states to use the same solution?
    Answer: RI can use the MS system if they wish. The requirements need to match with MS. MS is trying to reduce its reliance on IVR systems and move to an internet based model. Less than 15% of claimants use IVR in MS.

11) Printing: there have been discussions in this area but nothing new to date. Where will RI's printing occur? What type of data will be sent -- pdf files or will RI continue to use Elixir/Xerox laser?
Answer: ACCESS MS produces PDF files and bundles the correspondence in various groups. RI can choose to use the Xerox printers to print them. Elixir will not be needed. Maine is planning to outsource.

12) The document states that hardware configuration is not part of the scope under the categories: Suggested Staging and Production Hardware List for each state, Suggested UAT and System Test Hardware List for each state.
Answer: This is already discussed during the meeting.

13) Will each state be responsible to purchase all hardware and software/licenses listed?
Answer: MS is taking the lead in all hardware and software procurement.

14) Reporting Tools: IBM's Cognos is listed. What staff will be generating ad-hoc queries -- contractors or state staff? If state staff, will each state be required to administer their own?
Answer: RI can decide who will have access to Cognos. Cognos will be administered centrally on the cloud jointly by the support team.

Appendix
B

Operational Service Agreement

I. OPERATIONAL SERVICE AGREEMENT INTRODUCTION

A. Purpose and Objectives

This Appendix B, Operational Services Agreement (OSA), sets forth and describes the ongoing services to be performed by the IaaS Vendor, commencing with the deployment and acceptance of the environments in the development phase and during production, up to and including the fifth (5th) year of production operations. There will be subsequent one year options for up to an additional five (5) years.

B. Definitions, Acronyms, and Abbreviations

The capitalized terms in this OSA shall have the same meaning as set forth herein. In addition, the following terms when used in this OSA shall have the meaning set forth below:

1. "Available" has the definition given in the section **V.A.** entitled **Service Level of System Availability** below.

2. "Business Hours" means 6:00 a.m. to 9:00 p.m. (local time for the applicable MRM State), Monday through Friday, excluding Saturday and Holidays.

3. "Contact List" has the definition given in section **III.I.** entitled **Contact List** below.

4. "Credit" has the definition given in section **V.A.3.** entitled **Credits for System Availability Service Level Failures** below**.**

5. "Critical Support Hours" means business hours and Sundays from 12:00 a.m. to 11:59 p.m. local time for the applicable MRM State.

6. "Disaster Recovery Plan" (DRP) means actions to be taken before, during, and after a disaster.

7. "Enhancement" means any change to the System requested by one or more MRM State(s), but expressly excludes any:
   a. Updates
   b. Upgrades
   c. Update, upgrade, improvement, fix, correction, version, release, enhancement, replacement, or other change associated with maintenance services or error handling

notifications.

8. “Environments” means the test, staging, Cognos, and production environments.

9. “Error” means any failure, outage, or other condition that results in the system or any of the ongoing services failing to meet any of the documentation, specifications, or other requirements set forth in the OSA or the Agreement.

10. “Failure” has the definition given in section **V.D.** entitled **Service Failures** below.

11. “Force Majeure Event” means any event that is caused by a factor beyond the reasonable foreseeability and control of a party, including, without limitation, a natural disaster, tornado, civil disturbance, war, fire, flood, or earthquake, provided that the factor could not have been prevented by reasonable and customary precautions, including, in the case of the IaaS Vendor, implementation of and compliance with the DRP.

12. “Help Desk Hours” means 6:00 a.m. to 9:00 p.m. local time for the applicable MRM State, seven (7) days a week.

13. “Holidays” means those days other than Saturday or Sunday when an MRM state business office is closed and funding institutions are closed, as set forth in section **XI** entitled **MRM STATE HOLIDAYS** below.

14. “Incident” has the definition given in section entitled **Tickets** below.

15. “Maintenance Services” has the definition given in section **III.** entitled **MAINTENANCE AND SUPPORT SERVICE LEVELS** below.

16. “Measurement Interval” means the applicable interval of time over which a service level is measured.

17. “Month” means the period commencing 12:00:00 a.m., local time for the applicable MRM State, on the first day of each calendar month and ending 11:59:59 p.m., local time for the applicable MRM State, on the last day of such calendar month.

18. “Ongoing Services Phase” means the phase commencing upon final system acceptance under the Agreement and continuing through the Agreement Term and any applicable Transition Phase.
19. “Primary Point of Contact” (PPOC) means the primary point of contact(s) for the OSA and its MRM scope of activity.

20. “Priority Level” has the definition given in section **III.G.** entitled **Priority Level** below.

21. “Regulatory Update” means any update to the system necessary to

enable one or more MRM state(s) to comply with applicable federal and/or state law(s).

22. "Request" has the definition given in section **III.D.** entitled **Requests for Support** below.

23. "Scheduled Maintenance" means maintenance services scheduled to occur outside of Critical Support Hours and following at least thirty (30) days' notice to the MRM States, or as mutually agreed upon by MRM, ITSC, and the IaaS Vendor.

24. "Service Level" has the definition given in section **V.** entitled **SYSTEM SERVICE LEVELS** below.

25. "Service Level Credit" has the definition given in section **VI.** entitled **SERVICE LEVEL CREDITS** below.

26. "Service Level Termination Event" has the definition given in section **VI.D.** entitled **Service Level Termination Event**.

27. "System Availability" has the definition given in section **V.A.I.** entitled **System Availability Calculation** below.

28. "Ticket" has the definition given in section **III.F.** entitled **Tickets** below.

29. "Tracking System" has the definition given in section **III.E.** entitled **Tracking System** below.

30. "Update" means a change in the character in the version to the right of the decimal point (e.g., 5.X). It is usually denoted by a minor change to the software, such as bug fixes or small changes to functionality.

31. "Upgrade" means a change in the character in the version to the left of the decimal point (e.g., X.0). It is usually denoted by a significant change to the software, normally a major change.

II. OVERVIEW

A. Services

During the Ongoing Services Phase, the IaaS Vendor shall host, provide, maintain, and make available the System and Environments Infrastructure as a Service (IaaS) to MRM and their respective End Users as applicable, and provide all hosting, maintenance, support, and other Services in connection with the operation of the System and Environments, in accordance with the terms and conditions of this OSA.

B. Roles and Responsibilities

The IaaS vendor will be responsible for the below items in the production and staging environments:

1. Physical Servers/SAN/Network Hardware and Software
2. Virtualization/Hypervisor
3. Redhat Enterprises Linux OS
4. Server Security
5. Server Backup
6. Network Security (firewalls, reverse proxy, etc.)
7. Internet Diversity
8. Power and Cooling
9. Physical Security
10. Business Continuity

III. MAINTENANCE AND SUPPORT

During the Ongoing Services Phase, the IaaS vendor shall, at the IaaS vendor's sole cost and expense, provide maintenance and support services. The Maintenance and Support Services shall include all such services as are required to maintain and support the System in both Production and Staging environments. The Maintenance and Support Services shall include, but are not limited to:

- Perform upgrades to all infrastructure software and server operating systems.
- Scale solution infrastructure to accommodate claims doubling every three months for one year and provide an elastic supply of infrastructure capacity to avoid paying for capacity that is not required on continuous basis.
- Perform recovery operations as needed.

In addition to Maintenance and Support Services, vendor will be responsible for addressing the following, but not limited to, in both the Production and Staging environments:

A. Errors

In addition to any Maintenance and Support Services and any applicable procedures set forth in this OSA, The IaaS Vendor shall promptly investigate and correct all Errors (including, without limitation, any Failures) in accordance with this OSA, at no charge to MRM or any MRM State.

B. Security

The IaaS Vendor must adhere to security policies of each MRM State as set forth in the RFP and the data security agreements. The IaaS Vendor shall also maintain an Annual Cyber Security Plan ("ACSP") that include coverage of all MRM environments, and shall update the ACSP annually, at a minimum. The IaaS Vendor shall provide the updated ACSP to MRM for review by security officers of each MRM State by May 31st of each year. The IaaS Vendor, ITSC and each MRM entity shall sign the ACSP each year during the term of the Agreement, verifying that the information was accurate as of the date it was presented to MRM States. The IaaS Vendor and security officers of each MRM State shall keep a copy of the ACSP, and The IaaS Vendor and the MRM States shall treat the ACSP as a highly confidential document. The IaaS Vendor shall permit state and Federal auditors with access to the ACSP during any audit or inspection in accordance with the approved ACSP. Access shall be granted solely by written permission from the IaaS Vendor and MRM States. The IaaS Vendor is required to handle, document, timely resolve and track all security incidents, including any attempts to access the ACSP without express written permission from the IaaS Vendor's, ITSC and MRM States' security officers. The IaaS Vendor shall ensure the ACSP includes:

1. IP tracking and reporting.
2. A checklist of potential threats.
3. Identified vulnerabilities.
4. Pending action items to mitigate identified vulnerabilities.
5. A standard operating procedure for all security breaches
6. All security Incidents including:
    a. Date of the Incident
    b. Severity of the Incident based on the potential impact to the c. system
    c. Actions taken to resolve the Incident
    d. Actions taken to prevent similar Incidents from recurring

C. Cloud Update/Upgrade Services

The IaaS Vendor, at its sole cost and expense, shall apply hardware upgrades, operating system patches and upgrades as necessary to maintain the underlying infrastructure operating at or exceeding all System Service Levels (see Section V). The IaaS Vendor shall provide at least thirty (30) days advance written notice to ITSC, and MRM of potential implementation of any such upgrades and/or patches. If an immediate need arises for an upgrade and/or patch, MRM, ITSC and the Iaas Vendor can mutually agree to expedite the process. The IaaS Vendor shall ensure that infrastructure upgrades are completed while maintaining all service levels and other requirements of the OSA.

D. Requests for Support

The MRM States and their respective End Users, through the application vendor shall place requests for IaaS Maintenance and Support Services (each, a “Request”) through an automated system or by contacting the designated representative in the Contact List. At a minimum, the following information shall be submitted in connection with each Request:

1. Name of End User or other person making the Request.
2. Any corresponding tracking number in use by the MRM State(s) or application vendor.
3. Name of person to be contacted with respect to the Request.
4. Telephone number/extension of contact person.
5. Functionality of the System affected by the Error.
6. Brief description of the applicable Error.
7. Initial Priority Level for the Error.

The IaaS Vendor is expected to have 24 x 7 x 365 on call support to address any issues. Additionally, an acknowledgement receipt will be sent via email to the requesting End User stating their request was received.

E. Tracking System

The IaaS Vendor shall provide a tracking system available to the MRM States and the application vendor for the purpose of tracking each Request and the resolution of each Error (the “Tracking System”). The Tracking System shall include:

1. Incident details as outlined in Section 4.5 (Tickets).
2. Ability to associate related Incident Tickets.
3. Ticket workflow.
4. Ticket tracking queue.
5. Ticket release plan repository.
6. Release plan details.
7. Release plan approval workflow.

F. Tickets

Upon becoming aware of an Error from MRM through the application vendor, whether through receipt of a Request or through any other means (in either case, an “Incident”), the IaaS Vendor’s Support Services group shall assign the Incident a unique tracking number in the Tracking System (a “Ticket”). The Ticket shall include pertinent information collected throughout the life of
the Incident, including all information referenced under Section 4.2 Requests for Support, as well as the following:

1. Current Priority Level.
2. Status of Ticket.
3. Requester State.
4. Group assigned to Ticket.

5. Open date.
6. Close date.
7. Last modified date.
8. Resolution date.
9. Total time spent on Incident by the IaaS Vendor staff.
10. Root cause information

G. Priority Level

Each Incident subject to a Ticket shall be assigned a priority level (the "Priority Level" of the Incident) based on the severity of the Incident and the effect of the Incident on the System, Ongoing Services, and affected End User(s). The initial Priority Level for each Incident shall be as specified by the MRM States or the application vendor when making the applicable Request with the IaaS Vendor. If no Priority Level is provided by the MRM State(s) or the application vendor when making a Request, the IaaS Vendor shall assign a Priority Level to the applicable Incident resulting from the Request based on the following criteria:

Priority Level	Incident Description
Level 1	When one or more of the following: ☐ Financial risk to MRM States or End Users ☐ Severely impact delivery of services ☐ Faulty data transmissions ☐ Data corruption. Or, when the System or a core business function is unusable or unavailable.
Level 2	When major disruption to limited business functions or minimal impact to all or many business functions. A System work around may be available.
Level 3	When business functions are useable, but there is some degradation of a normally-provided business function, or when a user's ability to perform a portion of their business function is partially impacted.

If any MRM State reasonably disagrees with any Priority Level assigned to any Incident by the IaaS Vendor, or if any MRM State reasonably requires a change in any Priority Level at any time before Resolution of an Incident, such MRM State(s) may change the Priority Level at any time upon, effective upon notice to the IaaS Vendor through communication channels as noted above. Response time and

escalation procedures are addressed below. Level 1 and 2 items will generate an email to the MRM and the application vendor contacts.

H. Help Desk

The IaaS Vendor's Help Desk ("Help Desk") shall be used as a central contact point for Incident progression, escalation, and resolution. The Help Desk shall be responsible for the following activities:

1. Providing first line of support for any issues encountered in the System
2. Creating, maintaining, and making use of rich set of FAQs and knowledge base for responding to user queries and providing solutions to known problems.
3. Logging all Incidents into Tracking System to create Tickets
4. Escalating and monitoring Tickets based on Priority Levels and SLAs.

I. Contact List

At least thirty (30) days prior to the start of the Ongoing Services Phase, the Parties (MRM states, ITSC, application vendor, and IaaS Vendor) shall jointly complete a Contact List to identify and document the designated representatives who shall be contacted regarding Support matters under this OSA. In addition, the Contact List shall identify the specific points of contact for Incident progression, escalation, and resolution. The Contact List shall be maintained and updated, at least annually, by the Parties as necessary during the term of this OSA. There shall be a MRM Primary Point of Contact (PPOC) named upon contract signing by ITSC.

J. Contact Procedures

Upon becoming aware of each Incident, the IaaS Vendor shall contact the appropriate application vendor personnel as set forth in the Contact List to establish the exact nature of the applicable Error and begin the Incident resolution process. All Incidents shall be Resolved by the IaaS Vendor as set forth in this OSA and otherwise in accordance with the IaaS Vendor's then- current Support policies.

K. Request Resolution and Closure Procedure

When the IaaS Vendor believes that any Incident has been Resolved, the IaaS Vendor shall notify the applicable application vendor personnel in the Contact List. The application vendor will coordinate with the MRM Personnel to verify that the underlying Error has been corrected to their

reasonable satisfaction (a “Resolution”). Upon such independent verification, such application vendor personnel shall notify the IaaS Vendor that the applicable Ticket may be closed in the Tracking System. The IaaS Vendor may thereafter close the applicable Ticket in the Tracking System.

L. Support Records

The Tracking System shall maintain a record of each reported Incident for a period of three (3) years after closure of the Incident. Such record shall include, at minimum, all information regarding such Incident as outlined in Section 4.

IV. MAINTENANCE AND SUPPORT SERVICE LEVELS

The IaaS Vendor shall provide the Ongoing Services at or above the applicable Service Levels.

A. Service Level for First Contact Resolution Rate and Call Waiting Time

1. First Contact Resolution Rate and Call Waiting Time Calculation
   For purposes of this OSA and the Agreement:
   a. “First Contact Resolution Rate” is equal to the percentage of Incidents resolved during the first contact between the IaaS Vendor and the person placing the Request upon which the Incident is based or, if the IaaS Vendor otherwise becomes aware of the Incident, the first contact between the IaaS Vendor and the End User initially contacted by the IaaS Vendor to resolve the Incident
   b. “Call Waiting Time” is equal to the period of time starting when a call by the application vendor to make a Request is placed (or via secure electronic transmission by a MRM State(s) to make a Request is sent) and when that call or email is answered by a live IaaS Vendor Support Services desk staff member.
2. First Contact Resolution Rate Service Level
   The IaaS Vendor shall achieve a First Contact Resolution Rate of not less than Seventy-Five Percent (75%) for all Incidents during each Month.
3. Call Waiting Time Service Level
   The IaaS Vendor shall achieve a Call Waiting Time of not more than two (2) minutes on Ninety-Five Percent (95%) of all calls during Help Desk Hours in each Month.

B. Service Level for Response and Resolution Times

1. Response and Resolution Time Calculations
   For purposes of this OSA and the Agreement:

a. “Response Time” is the period of time starting when a call by the application vendor to make a Request is placed (or via secure electronic transmission by the MRM State(s) to make a Request is sent) and when a the IaaS Vendor Support Services staff member begins taking material action toward implementing a Resolution for the Incident
b. “Resolution Time” is the period of time starting when a call by the application vendor to make a Request is placed (or via secure electronic transmission by a MRM State(s) to make a Request is sent) and when the Incident subject to that Request actually reaches Resolution and the applicable Ticket closed in accordance with the terms of this OSA.

2. Response Time and Resolution Time Service Levels
The IaaS Vendor shall:
a. Respond to each Request for Support Services within the applicable Response Time set forth below
b. Arrive at a Resolution for and close the applicable Ticket for each Request for Support Services within the applicable Resolution Time set forth below. In each case the Response Time and Resolution Time shall be based on the Priority Level of the Incident subject to the Request and the time period in which the Request is made, as set forth below:

Priority Levels	Required Response Time		Resolution Time
	During Critical Support Hours	Outside Critical Support Hours	
Level 1	15 minutes	1 hour	Defect/Fault Identified: 30 Minutes Solution Agreed: 1 Hour Solution Implemented: 3 Hours Ticket Closed: Upon mutual agreement
Level 2	1 hours	3 hours	Defect/Fault Identified: 2 hours Solution Agreed: 4 Hours Solution Implemented: 6 Hours Ticket Closed: Upon mutual agreement
Level 3	2 hours	8 Hours	Defect/Fault Identified: 1 Business Day Solution Agreed: 1.5 Business days Solution Implemented: 3 Business Days Ticket Closed: Upon mutual agreement

3. Service Level for Resolution Rate
The IaaS Vendor shall achieve a Resolution of all Service Levels in each Priority Level at or above the following percentages:

Priority Level	Service Level Requirement	Measurement Interval
Level 1	A Resolution of Ninety-Eight Percent (98%) of Priority Level 1 Tickets shall be reached within Twelve (12) hours of Incident creation or receipt	Monthly
Level 2	A Resolution of Ninety-Eight Percent (98%)of Priority Level 2 Tickets shall be reached within Two (2) Business Days of incident creation or receipt	Monthly
Level 3	A Resolution of Eighty-Five Percent (85%)of Priority Level 3 Tickets shall be reached within Five (5) Business Days of incident creation or receipt	Monthly
All Levels	A Resolution of Ninety Percent (90%) of all Tickets (all Priorities) shall be reached within the applicable resolution time set forth in this chart	Monthly

C. Maintenance and Support Applicable Credits.

Maintenance and Support service level compliance is critical for MRM and ITSC. If any of the Service Levels specified in this section are not met by the IaaS Vendor during any Month, the IaaS Vendor shall issue to ITSC a Credit of Two Thousand Dollars ($2,000) for each instance in which an applicable Service Level is not met. (Also, see section VI for a consolidated enumeration of all credits related to maintenance and support and system service level non-compliance.)

D. Escalation Process and Procedures

To meet the Service Level Requirements, the IaaS Vendor shall implement an automated process to identify any Incident that has not reached Resolution within Seventy-Five Percent (75%) of the applicable Resolution Time. Such process shall include a notification update to the designated IaaS Vendor and application vendor personnel via electronic means. These notifications shall continue no less than every two (2) hours for Level 1 and Level 2 Incidents until the Incident has reached Resolution.

If a Ticket remains outstanding beyond the applicable Resolution Time set forth in this section, the IaaS Vendor shall escalate the Incident to the designated the IaaS Vendor senior management set forth in the Contact List, who shall contact the application vendor PPOC to agree to a course of action to be taken. The IaaS Vendor shall notify the application vendor PPOC if it is apparent that resolution of an Incident may result in a

protracted timeframe. The application vendor PPOC may escalate any Incident at any time should they deem it to be appropriate. As an Incident is escalated, regular contact shall be maintained between the IaaS Vendor and a designated member of the MRM State(s) or the application vendor as set forth in the Contact List.

E. Emergency Response Process

If the IaaS Vendor becomes aware of any Level 1 Incident, the IaaS Vendor response shall include, at minimum, the following emergency escalation process:

- The appropriate the IaaS Vendor support personnel shall be contacted by the IaaS Vendor's Support Services group immediately via the IaaS Vendor's Tracking System and by phone if necessary.
- The manager over the team responsible for resolving the Ticket shall also be contacted.
- If deemed appropriate by the manager, the Delivery Service Director shall also be informed.
- The IaaS Vendor shall update the Tracking System detailing the issue, and notify the appropriate IT contact at the affected agencies via e-mail and/or phone.

V. SYSTEM SERVICE LEVELS

A. Service Level of System Availability

1. System Availability Calculation
   For purposes of this OSA and the Agreement:
   a. The System shall be deemed "Available" when the System is available for access by End Users from the public Internet;
   b. "System Availability" is calculated as follows:

$$\text{System Availability} = \frac{\text{(Minutes per Measurement Interval in which the System is Available)}}{\text{(Total minutes in the Measurement Interval – minutes of Scheduled Maintenance during such Month)}} * 100$$

2. System Availability Service Level
The System and all Ongoing Services shall be provided by the IaaS Vendor at or above the following levels of System Availability in both production and non-production environments:

System Environment	Required System Availability Service Level	Measurement Interval
All Non Production Environments (excluding Development Environment)	99.950% of Business Hours	Month
Production	99.950%	Month

3. Credits for System Availability Service Level Failures
System Availability service level compliance is critical for MRM and ITSC. If any of the required System Availability Service Levels set forth in sub- section2 above are not met with respect to MRM or any MRM State during the Measurement Interval set forth in sub-section 2 above, the applicable Credit to ITSC for such Month shall be calculated as follows:

Minutes per Month Beyond the Allowed Non-Available Minutes that the System or any Ongoing Services are not Available to each affected MRM State	Credit Payable per MRM State Affected
1 – 21.4 minutes	$2,000
21.5 – 42.9 minutes	$2,000
43–64.4minutes	$4,000
Each 21.4 minutes thereafter (assessed at beginning)	$6,000

See section VI for a consolidated listing of all credits related to maintenance and support and system service level non-compliance.

4. Additional Credits for Repeated System Availability Service Level Failures.
In addition to the Credits set forth elsewhere in this OSA, if the System or any Ongoing Services are not Available to any MRM State during Critical Support Hours more than three (3) times and in excess of one-hour each time during any Month, the IaaS Vendor shall pay a Credit to ITSC a minimum of $5,000 per Incident in which the System or any Ongoing Services were not Available during Critical Support Hours (including the three (3) initial Incidents). See section VI for a consolidated listing of all credits

related to maintenance and support and system service level non-compliance.

B. Service Levels for Enhancement Request Responses

The following table sets forth the committed service levels, measurable event, and target levels for the IaaS Vendor responses to Enhancement Requests:

Measurable Event	Service Level Requirement	Measurement Interval
The applicable MRM State's receipt of the IaaS Vendor's written concurrence or disagreement with the MRM designation of an Enhancement Request as major or minor.	Five (5) Business Days of the IaaS Vendor's receipt of the applicable Enhancement Request	N/A
The applicable MRM State's receipt of the IaaS Vendor's proposal for Ninety- Five Percent (95%) of all Enhancement Requests designated as major.	Ten (10) Business Days of the IaaS Vendor's receipt of the Enhancement Request.	Fiscal Quarter

Measurable Event	Service Level Requirement	Measurement Interval
The applicable MRM State's receipt of the IaaS Vendor's proposal for Ninety- Five Percent (95%) of all Enhancement Requests designated as minor.	Five (5) Business Days of the IaaS Vendor's receipt of the Enhancement Request.	Fiscal Quarter
The applicable MRM State's receipt of the IaaS Vendor's proposal for all Enhancement Requests designated as urgent.	One (1) Business Day of the IaaS Vendor's receipt of the Enhancement Request.	N/A
Completion of all mutually agreed upon Enhancement Requests in accordance with the applicable schedule	Eighty-Five Percent (85%) of all mutually agreed upon Enhancement Requests	Fiscal Quarter

C. Additional Service Requirements

If any portion of the Ongoing Services does not have an applicable Service Level set in the RFP and this Appendix B, that portion of the Ongoing Services shall be provided in a timely manner using best efforts in accordance with all Documentation, Specifications and other requirements in the Agreement and in all events consistent with high industry standards.

D. Service Failures

Upon any failure of the System or any of the Ongoing Services to meet any applicable Service Level (a "Failure") the IaaS Vendor shall follow all applicable procedures set forth in this OSA that are applicable to such Failure.

VI. SERVICE LEVEL CREDITS

A. System Service Level Credits

IaaS service level compliance is vital for MRM and ITSC. ITSC shall have the right to receive, from the IaaS Vendor, all applicable credits for

any Failure as specified in this OSA (each, a “Service Level Credit” or “Credit”); provided that no Credit shall be owed to the extent that the Failure giving rise to such Credit resulted from a Force Majeure Event.. All SLAs and applicable Credits shall remain in effect during and notwithstanding any efforts by the IaaS Vendor to correct any Failure. Unless agreed to in writing by MRM, the IaaS Vendor shall deduct any Credit from the next succeeding invoice under the Agreement following the applicable Failure. Any unused Credits owed by the IaaS Vendor pursuant to the Agreement shall be paid to MRM within fifteen (15) days after the earlier of the expiration or termination of the Agreement Term. The payment (or deduction from payment) of any Credit shall not constitute a waiver or release of any other remedy that MRM or any MRM State may have under the Agreement, including without limitation any termination right.

The aggregated list of maintenance and support and system service levels is presented below:

1. Credit of Two Thousand Dollars ($2,000) to the ITSC for each instance in which a Maintenance and Support Service Level is not met
2. Credits to the ITSC for System Level Availability non-compliance:

Minutes per Month Beyond the Allowed Non-Available Minutes that the System or any Ongoing Services are not Available to each affected MRM State	Credit Payable per MRM State Affected
1 – 21.4 minutes	$2,000
21.5 – 42.9 minutes	$2,000
43–64.4minutes	$4,000
Each 21.4 minutes thereafter (assessed at beginning)	$6,000

3. Credits to the ITSC for Repeated System Availability Service Level Failures:
   If the System or any Ongoing Services are not Available to any MRM State during Critical Support Hours more than three (3) times and in excess of one-hour each time during any Month, the IaaS Vendor shall pay a Credit to the applicable MRM State(s) a minimum of $5,000 per Incident in which the System or any Ongoing Services were not Available during Critical Support Hours (including the three (3) initial Incidents).

4. Credits for Transaction Response Time Service Level Failures:

Transaction Response Time Percent in excess of Minimum Transaction Response Time Service Level Percent	Credit Payable
95.0% to 98.9% of transactions	$1,000
90.0% to 94.9%% of transactions	$2,000
88.0% to 89.9% of transactions	$4,000
Less than 87.9% of transactions	The IaaS Vendor agrees to negotiate in good faith a Credit that reflects the diminished value of the System to the applicable MRM State

B. Calculation of Service Level Credits

In the event of a Failure with respect to any Service Level specified in this OSA, the IaaS Vendor shall provide Credits as set forth herein for each such Failure.

C. Multiple Service Level Credits

If more than one Failure occurs in a single month, the sum of the corresponding Credits shall be credited to MRM.

D. Service Level Termination Event

In addition to MRM's right to receive Credits and without limiting MRM’s ability to pursue any other rights or remedies it may have under the Agreement or at Law or in equity, MRM shall be entitled to terminate for material breach the Agreement, or at its election the affected portions of the Agreement, without the IaaS Vendor having a right to cure, upon the occurrence of any one of the following events (each, a "Service Level Termination Event") the IaaS Vendor’s failure to meet a given Service Level for: (i) three (3) consecutive months; or (ii) four (4) months out of any eight (8) month period.

E. Exclusions and Exceptions

The SLAs, and ITSC's entitlement to Credits, shall not apply if a Failure was due solely to one of the following circumstances: (i) the performance of the portions of the public Internet controlled by

companies other than the IaaS Vendor; (ii) any equipment supplied by MRM or a MRM State (including but not limited to browsers, modems, telecommunications lines, or other communication software or equipment) which are not the IaaS Vendor- managed and are used to access the System or the Ongoing Services; or (iii) when the Failure occurs and is resolved during the Scheduled Maintenance period in which the Failure was reported.

VII. REPORTING

A. Measurement and Monitoring

During the Ongoing Services Phase, the IaaS Vendor shall implement such systems, tools and procedures as are specified in this OSA or the Agreement and as are otherwise necessary to: (i) measure, monitor, and verify the IaaS Vendor's performance of the Ongoing Services against the applicable SLAs and other requirements of this OSA and the Agreement; and (ii) permit reporting to the ITSC and MRM States at a level of detail sufficient to verify compliance with the SLAs and other requirements of this OSA and the Agreement.
Upon the reasonable request of any MRM State(s) and ITSC, the IaaS Vendor shall provide the MRM States with information and access to such measurement and monitoring systems, tools and procedures for inspection and verification purposes. The IaaS Vendor shall revise and augment any such systems, tools, or procedures at the reasonable request of MRM if such systems, tools, or procedures fail to meet the requirements of this OSA or the Agreement, but shall not implement any change to such systems, tools and procedures without approval of the MRM.

B. Monitoring Tools

The IaaS Vendor shall implement both intrusion detection and real time logging and monitoring for the System, and integrate such solution with the Log Manager Security services. The System shall integrate user and application transaction monitoring with system management infrastructure. It shall also include:

1. Availability and performance visualization of databases, network, sockets, etc. with user simulation and synthetic transaction processing.
2. Failure identification and recovery leveraging advanced discovery capabilities of application monitoring tools.

C. Performance Dashboard

As a part of the tracking tool, the IaaS Vendor shall provide a highly-configurable performance dashboard with service hierarchy views and include service level management views that consolidate System infrastructure and application data in view of observed service level agreements. This dashboard shall also include business service management views including application availability, response time, resource utilization, usage trend and transactional data points determining points of failures. The IaaS Vendor shall utilize these instruments as the foundation for incident reporting process and also to facilitate impact assessment procedures through operational metrics collection for the System in production.

D. Required Reports

The IaaS Vendor shall provide the ITSC and each of the MRM States with the following Reports regarding the Ongoing Services in a mutually-agreed format and level of detail:

1. System Outage Report
   For each system outage exceeding 15 minutes, the IaaS Vendor shall submit an incident report within five (5) business days detailing the root cause of the outage and steps that the Vendor shall take to prevent reoccurrence of the root cause.
2. Monthly Status Report
   This report is intended to allow the MRM States to monitor and track performance of all Ongoing Services, and the IaaS Vendor shall provide this within five (5) business days after the end of each Month.
3. Quarterly Service Level Report
   This report shall be made available to all involved parties/support groups participating in the regularly scheduled quarterly Service Level Agreement performance review.
4. Annual Service Level Report
   This report shall be made available to all involved parties / support groups participating in the annual Service Level Agreement performance review.

E. Report Details

Each Report identified in Section 8.4 above shall include all detail and back- up information reasonably required for the MRM States to verify the cause, impact, extent, and resolution of any such Failure. In addition to any details specified above, such Reports shall summarize at minimum:

1. Each Error occurring during the applicable period to which the Report applies
2. Any Failure with respect to any Service Level during the applicable period to which the Report applies (including the applicable Service Level, root cause of the problem resulting in such Failure, immediate solution to such Failure, and proposed permanent correction of such Failure)
3. All Credits, if any, imposed for any such Failures; and
4. The raw calculation data for all such Service Levels and Credits.
5. The IaaS Vendor shall be responsible for the cost of all software, hardware, and other equipment necessary to perform the required measurements necessary to generate all such reports and for all labor and other personnel costs associated with measuring and reporting performance of the System and the Ongoing Services against all Service Levels and in accordance with all Documentation, Specifications and other requirements in this OSA and the Agreement. The IaaS Vendor shall provide detailed supporting information for each report to the MRM States electronically (in a form agreed to by the MRM States) as well as in hard copy format.

VIII. SYSTEM CONTINUITY/DISASTER RECOVERY SERVICES

At least ninety (90) days prior to start of the Ongoing Services Phase, the IaaS Vendor shall develop and provide to the MRM States an updated Disaster Recovery Plan ("DRP"). The DRP shall be approved as part of the Final System Acceptance and in any case prior to the commencement of the Ongoing Services Phase. During the Ongoing Services Phase, the IaaS Vendor shall fully implement and comply with the provisions of the DRP at all times. The IaaS Vendor or any MRM State may propose changes to the DRP from time to time during the Ongoing Services Phase. All such changes shall be subject to mutual approval in advance of such changes becoming effective or any implementation
of such changes by the IaaS Vendor. For the avoidance of doubt, if any MRM State does not approve any such changes, the IaaS Vendor shall continue to perform in accordance with the then-current DRP. The DRP shall provide for the following requirements, at a minimum, the IaaS Contractor shall provide:

- A disaster recovery service that is at least one-thousand (1,000) miles from the primary site
- In coordination with the application vendor:
  1. A Restoration of System functionality and all Ongoing Services within four (4) hours of any service interruption, including, without limitation, any Failure or Error;
  2. Daily incremental backup of all application data;

3. Full weekly backup of all application data;

- Data to be stored locally at the IaaS Vendor premises and also stored remotely via disk based replication;
- Ability for MRM States' local sites disk-based restoration on-demand
- Weekly back up of operating systems and any IaaS 3rd party tool.

IX. GOVERNANCE

During the Ongoing Services Phase, the IaaS Vendor shall meet, in person or via conference call, with the ITSC, MRM States (collectively) and application vendor no less than once per calendar quarter to: (i) review the Ongoing Service delivery process; (ii) discuss improvements in the Ongoing Service delivery process; (iii) review the status of outstanding Failures, Errors, and complaints; (iv) review commendable performance; and (v) discuss, as needed, possible improvements or other revisions to the Service Levels. In addition to such scheduled meetings, MRM, ITSC or application vendor may require a review of the Ongoing Services as needed to ensure compliance with any Service Levels.

X. DOCUMENTATION AND SPECIFICATIONS

Prior to the Ongoing Services Phase and again prior to the implementation of any Updates, Upgrades, or Enhancements to the System or Ongoing Services, The IaaS Vendor shall provide each MRM State free of charge with all Documentation and Specifications for the System and such Updates and Upgrade.

FORCE MAJEURE EVENT

A. The IaaS Vendor

The IaaS Vendor shall not be liable for any Service Level Credit resulting from nonperformance or delay in performance of any obligation due to a Force Majeure Event, provided that the IaaS Vendor: (i) provides each MRM State with reasonable written notice under the circumstances prior to (if possible) such nonperformance or delay; and (ii) uses best efforts to resume performance as soon as possible despite such Force Majeure Event. In all cases, if such nonperformance or delay in performance persists for 30 days, MRM may terminate the Agreement upon notice to the IaaS Vendor. For the avoidance of doubt, (a) upon any such termination of this Agreement by MRM, MRM may request and the IaaS Vendor shall provide to the MRM State(s), Transition Assistance as set forth in Agreement, and (b) the existence of a Force Majeure Event shall

not excuse the IaaS Vendor from the obligation to implement and comply with the IaaS Vendor's DRP.

B. MRM and MRM States

MRM and each MRM State shall not be liable for nonperformance or delay in performance caused by any Force Majeure Event, provided that MRM: (i) provides the IaaS Vendor with reasonable notice under the circumstances prior to (if possible) such nonperformance or delay; and (ii) uses best efforts to resume performance as soon as possible despite such Force Majeure Event.

XI. MRM STATE HOLIDAYS

1. State of Mississippi Holidays
   http://www.sos.ms.gov/education_and_publications_holidays.aspx

2. State of Rhode Island Holidays http://sos.ri.gov/library/stateholidays/

3. State of Maine Holidays
   http://www.maine.gov/bhr/employee_center/holiday.htm

APPENDIX C
TERMS AND CONDITIONS

FOR THE:

INFRASTRUCTURE AS A SERVICE (IAAS) HOSTING SERVICES AGREEMENT

BETWEEN:

THE INFORMATION TECHNOLOGY SUPPORT CENTER
AND
[NAME OF THE VENDOR]

IN SUPPORT OF THE MISSISSIPPI/RHODE ISLAND/MAINE CONSORTIUM

This INFRASTRUCTURE AS A SERVICE (IAAS) HOSTING SERVICES AGREEMENT ("**Agreement**") is entered into by and between the Information Technology Support Center, a subsidiary of the National Association of State Workforce Agencies ("**NASWA**" and collectively, "**ITSC**") and ***[NAME OF THE VENDOR]*** ("**Vendor**") as of _____, 2015 (the "**Effective Date**").

WHEREAS, contingent upon adequate funding provided by the US Department of Labor ("**US DOL**"), Mississippi and the States of Rhode Island and Maine (together, "**MRM**," the "**MRM Consortium**," the "**MRM States**," or the "**States**," as further defined herein) have committed to create a joint, multi-tenant, state unemployment insurance benefits and tax technology system based on the MDES System for use by the MRM States (the "**MRM System**"); and

WHEREAS, pursuant to its agreement with MDES, ITSC has procured Vendor to provide the IaaS Services and the other services and obligations set forth in this Agreement (as further defined herein, "**Services**") to ITSC for the benefit of the MRM States as set forth herein; and

WHEREAS, the MRM States presently expect and are planning for onboarding of the States of Rhode Island and Maine onto the MRM System, and the transfer of the completed development of the MRM System to the MRM Consortium in the future with expectations that each state will have the ability to utilize and / or contract the procured IaaS Services for their own development and production environments of the MRM System, as set forth herein;

NOW THEREFORE, ITSC and Vendor agree as follows:

1. DEFINITIONS AND CONSTRUCTION.

1.1 Definitions. All capitalized terms used in this Agreement and defined in the context in which they are used herein will have the meanings given to them herein. All other terms used in this Agreement will have their plain English meaning as commonly interpreted in the United States.

1.2 Construction. This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof, and supersedes all previous agreements among the parties, written and oral, in respect of the subject matter hereof. English (as commonly interpreted in the United States) shall be the language used in all written communications between the parties pursuant to this Agreement, including all notices, reports, consents, authorizations and approvals under this Agreement. This Agreement has been prepared jointly and will not be strictly construed against either party. Ambiguities, if any, in this Agreement will not be construed against any party, irrespective of which party may be deemed to have authored the ambiguous provision. The words "include," "includes" and "including" means "include," "includes," or "including," in each case, "without limitation." References to this "Agreement" shall include all Appendices and Addendums to this Agreement, unless otherwise expressly noted.

2. EFFECTIVENESS AND AUTHORIZATION.

2.1 Effective Date. ITSC is not bound by this Agreement, and this Agreement is not valid and effective (and the Effective Date will not be deemed to have occurred), unless and until this Agreement is: (a) signed and dated below by the authorized representatives of both ITSC and Vendor; (b) as required by the applicable Laws of any MRM State, approved in writing by the authorized and applicable representative(s) of each such MRM State; and (c) approved by appropriate officials of the US DOL authorized to sign for the parties and in accordance with the Laws governing US DOL grants.

2.2 Authorization for Performance. Vendor is not authorized to perform or provide Services or Deliverables or undertake any other obligations under this Agreement until such time as the requirements of Section 2.1 have been met. If Vendor begins performance of any Services or any other obligations of Vendor under this Agreement prior thereto, ITSC is not obligated (and no MRM State is obligated) to pay Vendor for such performance or for any Services or Deliverables provided hereunder.

3. AGREEMENT STRUCTURE.

3.1 Attached Appendices. This Agreement includes the following Appendices referenced herein and attached hereto, each of which are hereby incorporated into and made a part of this Agreement:

Schedule [●]	***IaaS Services and Deliverables***
Schedule [●]	***Service Levels and Additional Specifications***
Schedule [●]	***Operational Service Agreement***
Schedule [●]	***Compensation***
Schedule [●]	***Transition Services***
Schedule [●]	***Reports***
Schedule [●]	***Data Security and Data Privacy***

Unless an applicable Schedule expressly states that such Schedule controls in the event of a conflict between the Agreement and that Schedule, the terms of the body of this Agreement will control in the event of any such conflict.

3.2 Additional Addendums.

(a) Existing MRM States. Vendor acknowledges that each state in the MRM Consortium may have certain state-specific requirements with respect to the IaaS Services to be provided to that state. Simultaneously with or following the Effective Date of this Agreement, as directed by ITSC, Vendor will enter into a separate participating addendum to this Agreement with ITSC and, as applicable, each such MRM state (each, a "**MRM State Addendum**"). Each MRM State Addendum will set forth and describe certain specific terms, conditions, and specifications required by ITSC and such MRM State to meet the unique requirements of such MRM State. This Agreement will include each such MRM State Addendum.

(b) Additional of Future MRM States. Vendor acknowledges that the MRM Consortium may, in its sole discretion, elect to additional states to the MRM Consortium at any time. Should the MRM Consortium decide, in its sole discretion, to add any additional state(s) to the MRM Consortium, Vendor will at the direction of ITSC enter into a separate MRM State Addendum with ITSC and, as applicable, each such state. Each such MRM State Addendum will set forth and describe the specific terms, conditions, and specifications required by ITSC and such MRM State for the IaaS Services and other Services and obligations to be provided to such newly added MRM State to meet the unique requirements of such MRM State. This Agreement will include each such MRM State Addendum.

(c) Removal of MRM States. Vendor acknowledges that the MRM Consortium may, in its sole discretion, remove states from the MRM Consortium at any time, including any states in the MRM Consortium as of the Effective Date, and that there is no guarantee that any states will remain in the MRM Consortium. Should the MRM Consortium

decide, in its sole discretion, to remove any MRM State from the MRM Consortium, or should any MRM State otherwise leave the MRM Consortium, Vendor will enter into a separate addendum to this Agreement with ITSC and, as applicable, such MRM State (each, a "**MRM Removal Addendum**"). Each MRM Removal Addendum will set forth and describe the terms, conditions, and specifications required by ITSC and such MRM State for the removal of such MRM State from the MRM Consortium. Terms and Conditions for removal must be consistent with section 14 Transition services of this agreement only otherwise agreed in writing. This Agreement will include each such addendum.

(d) Construction. In the event of a conflict between the terms of any MRM State Addendum or MRM Removal Addendum (collectively, an "**Addendum**") and the other terms of this Agreement, the terms of the applicable Addendum shall take precedence over this Agreement, but solely with respect to such Addendum and the IaaS Services and other Services and obligations provided to the applicable MRM State to which such Addendum relates. The terms and conditions of any Addendum shall have no force or effect with respect to this Agreement or any other Addendum (or any other IaaS Services and other Services and obligations of Vendor). The scope and term, including any renewal term, of an Addendum shall not exceed the scope and term (including any renewals) of this Agreement. The termination of this Agreement, for any reason, shall result in the termination of each Addendum.

3.3 RFP. In addition to the terms and conditions stated in this Agreement, Vendor's obligations under this Agreement include those obligations, duties, responsibilities, and associated performance requirements set forth and described in that certain "Mississippi, Rhode Island, Maine Unemployment Insurance Consortium Infrastructure as a Service Request For Proposal," issued by MDES, dated ***[●]***, 2015 (the "**RFP**"), including all appendices and exhibits thereto.

4. CHANGE CONTROL AND MODIFICATION.

4.1 Change Control. If either party desires to modify any Service or Deliverable set forth herein, such party may notify the other party and describe the modifications in a proposed revision or amendment to this Agreement, such notice in the form of the Change Order attached hereto as ***Schedule [●] (Change Order Form)*** and including all adjustments to the fees or other amounts due under this Agreement due to such revision or amendment (provided that the total compensation to Vendor under this Agreement shall not increase by more than 10% of the amounts set forth in ***Schedule [●] (Fees)*** due to Change Orders agreed upon under this Agreement). The other party will respond in writing with any proposed modifications to such proposed revision or amendment. Upon mutual agreement by the parties to any such proposed revision or amendment, the parties may execute a change order setting forth the applicable revisions and amendments to this Agreement (a "**Change Order**"). Upon signature by an authorized representative of each party, such Change Order will become a part of this Agreement and modify the applicable Service or Deliverable under this Agreement. No Change Order will be deemed valid and entered into under this Agreement until accepted through signature by an authorized representative of each party. All Change Orders will be governed by the terms of this Agreement. Unless an applicable Change Order expressly states that such Change Order controls in the event of a conflict between the Agreement and this Change Order, the terms of such Change Order will control in the event of any such conflict.

4.2 Modification and Amendment. Except as set forth in a Change Order, this Agreement can be amended or modified only by a written amendment signed by all parties and approved in writing by all officials authorized to sign such amendments. In the event of such an anticipated Change Order or other amendment to this Agreement, Vendor shall inform ITSC of the potential change at least 60 days in advance, therefore allowing ITSC and each applicable MRM State to discuss any/all of the potential changes and impact to the MRM System.

5. SCOPE AND PERFORMANCE.

5.1 General Scope. ITSC has procured Vendor to Mississippi to enable the MRM System to be provided through an as-a-service model to Mississippi and, as applicable, to enable the MRM System to be provided through an as-a-service model to the other MRM States. ITSC and Vendor acknowledge and agree that it is a primary objective of this Agreement to allow Mississippi and the other MRM States to benefit from the performance and pricing of such services, including high availability and disaster recovery, based on multi-tenancy.

5.2 Initial Scope. Vendor acknowledges and agrees that the initial scope of this Agreement will be limited to the MDES System. However, the scope of this Agreement may subsequently be expanded to incorporate the MRM System for the additional MRM States in accordance with the terms of this Agreement. This Agreement is non-exclusive in all respects and provides Vendor with no expectation or entitlement to provide Services or other obligations other than the Services as expressly set forth herein, whether with respect to Mississippi and the MDES System or the MRM System for any other MRM State.

5.3 Services and Deliverables.

(a) Services. Vendor shall perform and provide all IaaS Services as set forth in ***Schedule [●] (IaaS Services and Deliverables)***, including all applicable implementation, training, support, maintenance, consulting, and other services specified, described, and detailed in this Agreement (the IaaS Services and such other services and obligations of Vendor under this Agreement, collectively, the "**Services**") as set forth in this Agreement.

(b) Deliverables. Vendor shall provide all deliverables specified in ***Schedule [●] (IaaS Services and Deliverables)*** and all other deliverables that Vendor is required to develop or deliver as part of the Services or that otherwise result from or accompany the Services ("**Deliverables**") , as set forth in this Agreement.

(c) Specifications. All Services and Deliverables shall meet all service levels set forth in ***Schedule [●] (Service Levels and Additional Specifications)*** and all other requirements, specifications, standards, and timelines as set forth and required by this Agreement and each other applicable Schedule (collectively, "**Specifications**"). Vendor will propose updates to the Specifications to ITSC from time to time as necessary to ensure the Specifications meet the requirements for the MDES System and MRM System. Upon the approval of ITSC, such changes proposed by Vendor shall become part of the "Specifications" for purposes of this Agreement.

Resources and Responsibilities. Vendor acknowledges and agrees that any equipment, tools, utilities, facilities, hardware, software, systems, materials, personnel, goods, services, functions, obligations, or other resources or responsibilities ("**Resources**") not specifically described in this Agreement that are an inherent part of performing or providing any Services or Deliverables or are required to meet any Specifications or for the proper operation of any Services or Deliverables, will be deemed included within the "Services" for the purposes of this Agreement. Vendor shall procure and perform all such Resources necessary to perform and provide all Services and Deliverables under this Agreement at its own expense. Vendor shall accomplish such procurement and performance within the compensation stated in this Agreement and shall not increase the Maximum Compensation Amount (as defined below). Except as set forth in each applicable Addendum, Vendor shall not require access to or use of Resources of ITSC or any MRM State, and ITSC and each MRM State will be under no obligation to supply Vendor with any such Resources or any other assistance or services, in performing or providing the Services and Deliverables and any other obligations of Vendor under this Agreement.

5.4 Project Phases. The Services and Deliverables under this Agreement form a project (the "**MRM Project**" or the "**Project**"). The Project will be designed, developed, and implemented in accordance with the following phases (each, a "**Phase**") in the sequence listed:

[Phases to be included in definitive Agreement]

Vendor shall perform its obligations under each Phase of this Agreement in accordance with the Specifications applicable to such Phase.

5.5 Operational Service Agreement. The parties acknowledge that following Acceptance of the MDES System or any MRM System for a given MRM State, all Services and Deliverables relating to the ongoing operation, maintenance, and support of the MDES System or such MRM System, as applicable, shall be provided herein and under the Operational Service Agreement ("**Operational Service Agreement**" or "**OSA**") attached as ***Schedule [●] (Operational Service Agreement)***, including all requirements and Specifications set forth therein. The OSA will form a part of this Agreement and the services and deliverables set forth therein will form part of the Services and Deliverables hereunder. As requested or required by ITSC, Vendor will further enter into an ongoing services agreement specific to any MRM State, such agreement setting forth and describing certain specific terms, conditions, and specifications required by ITSC

and such MRM State to meet the unique requirements of such MRM State with respect to the ongoing operation of the MRM System for such MRM State.

5.6 Relationship to MRM System and Application Vendor.

(a) Vendor acknowledges and agrees that the IaaS Services and other Services under this Agreement are provided for purposes of procuring the services necessary to host and manage the MRM System as a service for Mississippi and, as applicable, the other MRM States and that the MRM System itself is provided by the Application Vendor, Tata Consultancy Services (TCS), under the Application Vendor Agreement. Vendor agrees to collaborate with Application Vendor in all respects to perform and provide all Services and Deliverables under this Agreement and to enable the Application Vendor to perform and provide all Application Vendor Agreement Services under the Application Vendor Agreement.

(b) Parties acknowledge and agree that the requirements of this Section are not intended to and shall not be construed as conferring on Vendor any right to enforce any claim or rights against the Application Vendor or any MRM State directly. With respect to this Agreement and all Services and Deliverables hereunder, Vendor shall be entitled to seek remedy solely against ITSC and not against the Application Vendor or any MRM State.

(c) Parties acknowledge and agree to adhere to the following policies for the state of Maine as applicable to IaaS hosting.

- **http://www.maine.gov/oit/policies/Application-Deployment-Certification.htm**
- **http://www.maine.gov/oit/policies/OIT_App_Deployment_Certification_Guidelines.htm**
- **http://www.maine.gov/oit/policies/RemoteHostingPolicy.htm**
- **http://www.maine.gov/oit/policies/SecurityPolicy.htm**

(d) The following link is a sample contract between Maine and ITSC. Parties acknowledge and agree to incorporate applicable terms and conditions from this sample contract as part of the terms and conditions of the contract between ITSC and the IaaS Vendor.

- **http://www.maine.gov/purchases/info/forms/BP54_IT.docx**

5.7 Continuity of Services. In the event of any dispute, including any dispute regarding payments due under this Agreement, Vendor shall not terminate, suspend or delay the completion of any Service or Deliverable, restrict or adversely affect access to or use of the MRM System or any Data, or exercise any right of set-off or other self-help measure.

6. TESTING AND ACCEPTANCE.

6.1 Testing. Vendor will develop procedures to test all applicable Services (and any accompanying Deliverables) prior to the making those Services (and Deliverables) available, or otherwise delivering those Services (and Deliverables), to any MRM State. The Vendor testing procedures will be sufficient to reasonably determine whether the Services and any Deliverables, as applicable, taken together with any other related Services or Deliverables, meet the Specifications and other requirements applicable to such Services or Deliverables. Vendor will not make available or deliver any Service (or Deliverable) until such Services and Deliverables have passed all applicable testing procedures. Upon the request of ITSC or any MRM State, Vendor will provide copies of all such testing procedures to ITSC or such MRM State.

6.2 Submission and Review. Vendor shall complete all Services and Deliverables in accordance with the terms of this Agreement, including all applicable Specifications and any other requirements mutually agreed upon by the parties. Vendor shall notify ITSC, or any applicable designee identified herein, when any Services (and any accompanying Deliverables) are to be made available or otherwise delivered to any ITSC or its identified designee by the delivery of a completion notice in form and manner acceptable to ITSC (or such applicable designee). Vendor shall make available or otherwise make available each Service (and any Deliverable) to ITSC or its identified designee in accordance with all applicable instructions provided by or on behalf of ITSC.

6.3 Acceptance. Unless otherwise set forth herein, or mutually agreed upon in writing by the parties, ITSC or its designee shall provide notice to Vendor of its acceptance (an "**Acceptance**") or rejection (a "**Rejection**") of each applicable Service (and any Deliverable) following such Service (or Deliverable) having been made available or otherwise delivered to ITSC by Vendor. ITSC or its designee will provide such Acceptance or Rejection within a reasonable time period specified by ITSC, such time period not exceeding any relevant period established in ***Schedule [●] (IaaS Services and Deliverables)***. If ITSC or its designee rejects any Service (or Deliverable), the Rejection for such Service or Deliverable shall set forth with reasonable specificity the Service (or Deliverable) requiring re-performance, refactoring, and/or correction and the deficiencies in or other basis for such rejection of such Service (or Deliverable).

6.4 Correction and Resubmission. Unless otherwise agreed in writing by the parties, Vendor shall correct all deficiencies in any Service (or Deliverable) identified in any Rejection within such time period for correction as is specified in the applicable Rejection. Upon completion of all required corrections and re-performance, Vendor shall again make available or otherwise deliver the corrected Service (or Deliverable) to ITSC or its designee. Unless otherwise provided herein or mutually agreed in writing by the Parties, ITSC or its designee shall Accept or Reject the corrected Service (or Deliverable) within a reasonable time period specified by ITSC, such time period not exceeding any relevant period established in ***Schedule [●] (IaaS Services and Deliverables)***. If the corrected Service or Deliverable are rejected by ITSC or its designees, ITSC shall provide a Rejection to Vendor. The parties shall thereafter repeat the foregoing submission, review, and approval or rejection process until all deficiencies have been corrected and the applicable Service (or Deliverable) have been accepted by ITSC or its designee. Acceptance of any Service (or Deliverable) will not waive any available claims by ITSC , including any claims for breach of warranty or indemnification. Any Service (or Deliverable) receiving 2 or more Rejections from ITSC or its designee without an Acceptance will be deemed a material breach of this Agreement by Vendor.

6.5 Submissions Under Addenda. A MRM State shall accept or reject any Service (or accompanying Deliverables) provided under any MRM State Addendum to which it is a party in accordance with any applicable acceptance and rejection process and criteria set forth in such MRM State Addendum. If no such applicable acceptance and rejection process is set forth in such MRM State Addendum, then such MRM State shall accept or reject such Service (or accompanying Deliverable) provided under such MRM State Addendum in accordance with the acceptance and rejection process established by this Section.

7. REPRESENTATIONS AND WARRANTIES.

Vendor makes the following representations, warranties, and covenants set forth in this Section, each of which has been relied on by ITSC in entering into this Agreement. All such representations, warranties, and covenants are made by Vendor to ITSC and to each applicable MRM State. Except as expressly stated to the contrary, the representations, warranties, and covenants in this Section are continuing and shall continue to apply to and be true and correct throughout the term of Agreement and for a period of 1 year following any expiration or termination of this Agreement. The warranties set forth in this Section shall supersede any warranties, whether express or implied, provided by the Uniform Computer Information Transactions Act (UCITA).

7.1 Authority. Vendor is organized, validly existing, and in good standing under the Laws of the state of its incorporation. Vendor has all required legal and corporate power and authority to enter into the Agreement and carry out its duties and obligations hereunder. Vendor has sufficient rights and authority to carry out its duties and obligations hereunder and to grant all rights and licenses set forth in this Agreement. The person executing this Agreement on behalf of Vendor has sufficient authority, by operation of law or corporate act, to bind Vendor by his or her signature to all obligations herein.

7.2 Compliance. Vendor is responsible for compliance with and will comply with all laws, statutes, rules and regulations promulgated by federal, national, state, provincial, city, local, municipal, or other government authority, including any governmental division, subdivision, department, agency, bureau, branch, office, commission, council, court or other tribunal ("**Laws**") applicable to Vendor or Vendor's performance hereunder. The performance of the Services

and any other Vendor obligations by or on behalf of Vendor hereunder does not and will not violate any applicable Laws, the rights of any third party, or any agreement by which Vendor is bound, nor will the performance of the Services or any other Vendor obligations by or on behalf of Vendor hereunder cause ITSC or any MDES State to violate any Law applicable to ITSC or such MDES State. The MDES System and MRM System will be designed and operated by Vendor in all respects in full compliance with all applicable Laws and the use and operation thereof will not cause ITSC or any MRM States to violate any applicable Law.

7.3 Required Authorizations. At all times during the term hereof Vendor shall have and maintain, at its sole expense, all licenses, certifications, approvals, insurance, permits, and other authorizations required by Law ("**Required Authorizations**") to perform and provide all Services, Deliverables, and any other obligations hereunder. Vendor shall obtain and maintain all Required Authorizations, without reimbursement by ITSC or any MRM State or other adjustment in any compensation due Vendor under this Agreement. All employees, agents, and contractors of Vendor performing any portion of any Services or other obligations under this Agreement shall hold all licenses, certifications and other Required Authorizations, if any, to perform their responsibilities. Vendor, if a foreign corporation or other foreign entity transacting business in any MRM State, currently has obtained and shall maintain any applicable certificate of authority to transact business in such MRM State and shall designate a registered agent in such MRM State to accept service of process. Vendor will provide immediate notice to ITSC of any revocation, withdrawal or non-renewal of any applicable Required Authorization.

7.4 Standard of Performance. Vendor will perform and provide all Services, Deliverables and any other obligations hereunder in conformance with the highest standards of care, skill, and diligence in Vendor's industry, trade, or profession, including, as applicable, in conformance with the service levels specified in this agreement, ITIL v3:2011 standards, Vendor's ISO20000 certification and comparable industry practices and standards. Vendor will perform and provide all Services, Deliverables and any other obligations hereunder in the sequence and manner set forth herein, with the care and diligence normally practiced by firms performing services of a similar nature, and in all cases in conformance with all applicable Specifications and the other requirements of this Agreement. Vendor's performance of all Services and any other obligations hereunder will be adequate in all respects to serve its intended purposes and achieve its intended results as specified herein. Notwithstanding the foregoing, where this Agreement specifies a particular standard or criteria for performance, this warranty is not intended to and does not diminish that standard or criteria for performance. Vendor agrees to provide all Services, Deliverables and any other obligations hereunder to meet or exceed the minimum requirements as set forth in this agreement.

7.5 Infrastructure.

(a) General. The Infrastructure and all Resources, including the hypervisor virtualization software, physical servers, physical storage, and physical networking equipment, used or required to perform or provide any Services (or accompanying Deliverables), including pursuant to a Change Order ("**Infrastructure**") shall be compliant in all respects with all Specifications and the other requirements of this Agreement. The Infrastructure and all Services (and any accompanying Deliverables) will be free from errors, defects, deficiencies or deviations. The Infrastructure and all Services (and accompanying Deliverables) will perform (and be performed) in such a manner as required by the Specifications and other requirements of this Agreement, and in all cases so that the intended function of the MRM System, Infrastructure and all Services (and accompanying Deliverables) is accomplished in all respects as intended and in a manner otherwise consistent with all applicable industry standards.

(b) Additional. Without limiting the foregoing:

(i) Compatibility. All portions of the Infrastructure and all other Services (and any accompanying Deliverables) are fully compatible and interoperable with the MRM System and with each other and all third-party software, hardware, equipment, and systems with which the Specifications, Vendor's response to the RFP, or Vendor's applicable marketing materials or documentation claim compatibility.

(ii) Scalability. All portions of the Infrastructure and all other Services (and accompanying Deliverables) will meet or exceed the scalability requirements required by the Specifications or by this Agreement.

(iii) Capacity. All Infrastructure that the Vendor uses, provides, or recommends is of sufficient capacity and capabilities to consistently and reliably meet all Specifications and other requirements of the Agreement.

(iv) No Data Loss. The use of and access to the Infrastructure and all other Services (and accompanying Deliverables) as contemplated hereunder will not result in the loss, destruction, or deletion of any Data of any MRM State that is not easily retrievable or the alteration of any of ITSC's or any MRM State's Data that is not easily reversed.

7.6 Viruses and Traps. The Infrastructure and all Services (and accompanying Deliverables) do not and will not contain any virus, worm, trap door, back door, timer, clock, counter or other limiting routine, instruction or design that could damage, disable, or erase any Data or any portion of the MRM System, Infrastructure, any Services (or accompanying Deliverables), or any other software or system, or cause the MRM System, Infrastructure, any other Services (or accompanying Deliverables), any Data, or any other software or system to become encumbered, inoperable, or incapable of being used in the full manner for which it was designed, or which would permit unauthorized access to any of the foregoing (collectively, "**Viruses and Traps**"). Vendor shall use such efforts as are necessary to detect and screen out any Viruses and Traps through the use of one or more current detection programs. If despite these efforts Vendor fails to detect a Virus or Trap, or if Vendor incorporates any Viruses and Traps into the MRM System, Infrastructure, or any other Services (or accompanying Deliverables), then Vendor shall be liable for all damages of ITSC and all MRM States resulting from any failure to comply with any Specifications or other requirements of this Agreement caused by such Virus or Trap, whether direct, indirect, consequential, incidental or special, including, but not limited, to, damages for lost income or lost revenue resulting from any failure caused by such Virus or Trap.

7.7 Third Party Code. Except disclosed to and approved in advance in writing by ITSC, Infrastructure and Services (and any accompanying Deliverables) will not contain, are not based upon, and do not refer to or rely upon for their use or operation, any third party software, methodologies, or other technology or derivatives thereof not owned by Vendor, including any "open source" software, public source software, freeware, or other software licensed or distributed under a similar or analogous licensing model that purports to require the distribution of or access to source code or purports to restrict one's ability to charge for distribution of or to use software for commercial purposes, or any modification or derivative thereof.

7.8 Documentation. All documentation for the Infrastructure and Services (and accompanying Deliverables) ("**Documentation**") contains an accurate and complete description of the material functions of the Infrastructure and Services (and accompanying Deliverables) and the use and operation thereof. The Infrastructure and Services (and accompanying Deliverables) will be fully documented. Vendor has or will take all actions necessary to document the Infrastructure and Services (and accompanying Deliverables) owned by Vendor or any affiliate and its operation, such that the Infrastructure and Services (and accompanying Deliverables) have been written in a clear and professional manner so that they may be understood, modified and maintained in an efficient manner by reasonably competent resources.

7.9 Non-Infringement. The Infrastructure and Services (and accompanying Deliverables) and operation thereof by or on behalf of Vendor, and all use thereof and access thereto by ITSC or any MRM State in accordance with the terms of this Agreement, does not and shall not infringe upon, misappropriate, or otherwise violate any IPR or other right of any third-party.

7.10 No Litigation. There is no outstanding litigation or dispute to which Vendor (or any Vendor contractor) is a party that, if decided unfavorably to Vendor (or such contractor), would reasonably be expected to have a material adverse effect on Vendor's ability to fulfill its obligations under this Agreement. Vendor has not received any government inquiries, complaints, lawsuits or investigations concerning the adequacy or sufficiency of its data or information security or privacy programs.

7.11 Vendor Statements. Nothing contained in this Agreement or any statement, document, or certificate provided or delivered to ITSC or any MRM State, including Vendor's responses to the RFP, contain any untrue statement of a material fact nor, to Vendor's knowledge, omit to state a material fact necessary in order to make the statements contained herein or therein not misleading. The Infrastructure and Services (and accompanying Deliverables) fully comply with all Vendor statements at any oral presentation to ITSC or any MRM State during the proposal process, and with all product demonstrations, representations, or other sales-related exhibitions provided by Vendor.

7.12 Time Frames for Warranty Services. Following breach of any representation, warranty, or covenant contained in this Agreement, Vendor shall promptly, within the applicable time-frame specified by ITSC, remedy such breach and

correct any applicable errors, defects, deficiencies or deviations in the Infrastructure or Services (or accompanying Deliverables). Vendor shall apply all resources necessary within the resources, staff allocation and scope of this Agreement to complete remedy of such breach or correction of such errors, defects, deficiencies or deviations. Such efforts shall be made without additional cost or expense to ITSC or any MRM State. Any such remedy or correction of any applicable errors, defects, deficiencies or deviations will be deemed resolved only following notice from ITSC of such remedy or correction. If Vendor fails to remedy and breach or correct any error, defect, deficiency or deviation covered by any representation, warranty, or covenant, ITSC may, in its sole discretion, act to correct or repair the error, defect, deficiency or deviation, in which case the Vendor shall be required to reimburse ITSC for all costs and expenses incurred to conduct such remedy or correction. The remedy of any such breach or the correction of any such errors, defects, deficiencies or deviations shall not detract from or interfere with the operation of the Infrastructure or the performance of any Services or other obligations of Vendor under this Agreement.

8. TERM.

8.1 Initial Term. The initial term of this Agreement shall commence on the Effective Date and shall terminate at the end of the third (3rd) year of the Effective Date ("**Initial Term**"), unless extended or sooner terminated as specified herein.

8.2 Option to Extend. ITSC may (acting in conjunction with any of the MRM states), at its sole option, extend the term of the Agreement for up to three (3) additional 1 year terms (each, a "**Renewal Term**," and collectively with the Initial Term, the "**Term**" of the Agreement). Any Renewal Term shall be under the same prices, terms, and conditions as the Initial Term of this Agreement. If ITSC exercises this option, it shall provide written notice to Vendor at least 30 days prior to the end of the current Term. If exercised, the provisions of such notice shall become a part of and be incorporated into this Agreement. Vendor acknowledges and affirms that ITSC shall have no obligation for Services rendered by the Vendor that were not performed within the applicable Term.

8.3 Early Termination in the Public Interest. ITSC is entering into this Agreement for the purpose of carrying out the public policy of the MRM States. If maintaining ITSC as a party to this Agreement ceases to further the public policy of Mississippi or the other MRM States, then the MRM States acting together and in full agreement, may assign this Agreement to any one of the MRM States or another entity not yet named. If under this circumstance, no other MRM State accepts assignment of this Agreement and another entity that the MRM states have agreed upon cannot accept assignment of this Agreement, the MRM states can terminate this Agreement in whole or in part. This Section shall not apply to termination of this Agreement for cause or breach by Vendor, which shall be governed by the terms hereof as otherwise specifically provided for herein.

8.4 Extension of Addenda Terms. ITSC may elect, in its sole discretion, to renew the term of any MRM State Addendum relating to any MRM State for a renewal term that is co-extensive with any Renewal Term under this Agreement, on the terms and conditions set forth in such MRM State Addendum, provided that no MRM State Addendum shall be renewed beyond the expiration of the Term of this Agreement.

8.5 Notice of Transfer. ITSC may elect to transfer the contract (assignment of rights) to any or all MRM states or manage services company representing the MRM consortium states with the same terms and conditions.

9. COMPENSATION AND PAYMENT.

9.1 Compensation. ITSC shall pay Vendor in accordance with the provisions of this Section, in the amounts and using the methods set forth in this Section. Payment by ITSC in accordance with the provisions of this Section shall constitute payment in full for all Services (and any accompanying Deliverables) and any other obligations of Vendor performed under this Agreement and Vendor shall not receive any additional compensation hereunder.

9.2 Maximum Compensation Amount. Independent of the use or operation of the Infrastructure, in no event shall the maximum compensation amount due or payable Vendor under this Agreement exceed the maximum compensation amount stated in ***Schedule [●] (Compensation)*** (the "**Maximum Compensation Amount**"). The Maximum Compensation Amount represents the maximum available amounts payable to Vendor hereunder and does not serve as any guarantee payment of any such funds under this Agreement. The payment rates in ***Schedule [●] (Compensation)***

shall constitute the entire Maximum Compensation Amount due Vendor for all Services and any other Vendor obligations regardless of costs incurred by Vendor. The payment rates include, but are not limited to, all applicable taxes, fees, overheads, and all other direct and indirect costs incurred or to be incurred by the Vendor.

9.3 Compensation Firm. The payment rates and amounts (including the Maximum Compensation Amount) are firm for the duration of the Agreement and are not subject to escalation, unless agreed upon in writing by the parties, provided that:

(a) The amounts payable under this Agreement may be changed through a Change Order under this Agreement.

(b) The amounts payable under this Agreement may be renegotiated, in the sole discretion of ITSC, if a new MRM State joins the Consortium and enters into a new MRM State Addendum under this Agreement, as applicable.

(c) At the request of ITSC, the parties shall meet to evaluate and compare the quality and cost of all or any portion of the Services against the quality and cost of other service providers performing similar services to ensure that the MRM States are receiving from Vendor pricing and levels of service that are competitive with market prices and service levels and other specifications, given the nature of the Services. If ITSC determines in good faith that the amounts paid by ITSC (or any MRM State under any MRM State Addendum) for any Services (or any accompanying Deliverables) or any portion thereof are materially greater than the prices charged by other service providers for services of a similar nature, the applicable parties shall meet and negotiate in good faith as to reductions in the amounts paid by ITSC (or such MRM State) under this Agreement (or the applicable MRM State Addendum) to eliminate any such unfavorable variance. In addition to the foregoing, if Vendor at any time provides any third party with more favorable pricing terms in connection with any of the Services provided under this Agreement or any MRM State Addendum (or any services that are similar in function to the Services provided under this Agreement or such MRM State Addendum), Vendor will promptly offer such more favorable terms to the MRM States in connection with the Services (and accompanying Deliverables) under this Agreement or any MRM State Addendum and, following acceptance from the applicable MRM State, adjust the applicable pricing terms under this Agreement or MRM State Addendum on a prospective basis to match such more favorable pricing terms.

9.4 Pricing. Vendor shall perform and provide all Services and Deliverables under this Agreement for the amounts set forth in ***Schedule [●]*** (Compensation), in accordance with the payment schedules set forth in ***Schedule [●] (Compensation)***. Vendor is not entitled to be paid only in accordance with the payment rates detailed in ***Schedule [●] (Compensation)***.

9.5 Expense Compensation. Vendor shall not be compensated or reimbursed for any costs or expenses incurred under this Agreement, including, travel, meals, or lodging, except as expressly set forth in ***Schedule [●] (Compensation)***.

9.6 Non-Appropriation. It is expressly understood and agreed that the obligation of ITSC or any MRM State to proceed under this Agreement is conditioned upon the appropriation of funds by the MRM State's legislature and receipt of state and/or federal funds for the performances required under this Agreement. If the funds anticipated for the continuing fulfillment of the Agreement are, at anytime, not forthcoming or are insufficient, either through the failure of the federal government to provide funds or the MRM State's Legislature to appropriate funds or the discontinuance or material alteration of the program under which funds were provided, ITSC shall give Vendor thirty (30) days prior written notice of same and shall have the right to terminate this Agreement without damage, penalty, cost, or expense to ITSC or any MRM States of any kind whatsoever. ITSC or the MRM States shall have the sole right to determine whether funds are available for the payments or performances due under this Agreement. In the event ITSC terminates this Agreement, Vendor and ITSC shall mutually agree on just and equitable compensation for services deemed satisfactory to ITSC and completed by Vendor prior to such termination.

9.7 Payment. Unless otherwise specified in an applicable MRM State Addendum, Vendor shall initiate a payment request under this Agreement by submitting an invoice to ITSC, in the form and manner specified herein or otherwise approved by ITSC. Vendor will not initiate any payment request with respect to any Services (or accompanying Deliverables) hereunder except following the Acceptance of such applicable Services (or Deliverables) as provided herein. All invoices shall be accompanied by documentation verifying ITSC's Acceptance of such Services (or Deliverables). All invoices for any advance payments allowed under this Agreement shall comply with all applicable Laws

or each MRM State. ITSC will pay each properly issued invoice within ***[●]*** days of receipt thereof. ITSC will be under no obligation to pay any invoices not properly issued in accordance with the terms of this Agreement.

9.8 Invoice Prerequisite Documentation. Vendor shall not invoice ITSC under this Agreement until ITSC has received the following documentation:

(a) Properly completed and signed, "Authorization Agreement for Automatic Deposit Form" ("**ACH Credits Form**") provided by ITSC. Vendor acknowledges and agrees that, once the ACH Credits form is received by ITSC, all payments to the Vendor, under this or any other Agreement shall be made by electronic transfer through the Automated Clearing House ("**ACH**").

(b) Properly completed and signed "Substitute W-9 Form" provided by ITSC to Vendor. The taxpayer identification number provided by the Vendor on said form must be the same as the Vendor's Federal Employer Identification Number.

9.9 Invoice Requirements. Vendor shall invoice ITSC only as permitted herein. Vendor shall present invoices to ITSC not more often than once monthly in Development and quarterly during Operations. All invoices shall be submitted (with all necessary supporting documentation) to:

[APPLICABLE ITSC ADDRESS INSERTED HERE]

Each invoice shall clearly and accurately detail all of the following required information (calculations must be extended and totaled correctly).

(a) Invoice Number (assigned by Vendor)

(b) Invoice Date

(c) Contract Number (assigned by ITSC)

(d) Customer Account Name: ITSC

(e) Customer Account Number (assigned by the Vendor to the above-referenced Customer)

(f) Vendor Name

(g) Vendor Contact for Invoice Questions (name, phone, and/or fax)

(h) Vendor Remittance Address

(i) Description of Delivered Service

(j) Complete Itemization of Charges, which shall detail the following:

- **(i)** Service or Milestone Description (including name & title as applicable) of each service invoiced
- **(ii)** Number of Completed Units, Increments, Hours, or Days as applicable, of each service invoiced
- **(iii)** Applicable Payment Rate as stipulated in Exhibit F of each service invoiced
- **(iv)** Amount Due by Service
- **(v)** Total Amount Due for the invoice period

Vendor understands and agrees that an invoice under this Agreement shall: (1) include only charges for Services (and accompanying Deliverables) described in this Agreement and in accordance with payment terms and conditions set forth in this Agreement; (2) only be submitted for completed Services (or Deliverables) and shall not include any charge for future work; and (3) not include sales tax or shipping charges.

9.10 Erroneous Payments. At the discretion of ITSC, payments made to Vendor in error for any reason, including, but not limited to, overpayments or improper payments, and unexpended or excess funds received by Vendor, may be recovered from Vendor by deduction from subsequent payments under this Agreement or by other appropriate methods and collected as a debt due to ITSC. Such funds shall not be paid to any person or entity other than ITSC. At the discretion of a MRM State, payments made to Vendor in error under any Addendum applicable to such MRM State may be recovered as provided under such Addendum.

9.11 Payment of Invoice. A payment by ITSC shall not prejudice the rights of ITSC or any MRM State to object to or question any payment, invoice, or matter in relation to this Agreement. A payment by ITSC shall not be construed as acceptance of any part of the work or service provided or as approval of any amount invoiced.

9.12 Invoice Reductions. Vendor's invoice shall be subject to reduction for amounts in any invoice, or any payment previously made, that are determined by ITSC not to constitute proper remuneration for compensable Services.

9.13 Deductions. ITSC reserves the right to deduct from any payment due and owing Vendor liquidated damages assessed under this Agreement, damages incurred by ITSC or the State for Vendor's failure to comply with the terms of this Agreement, or any other amount due and owing ITSC or any MRM State.

10. OWNERSHIP.

10.1 Applicable Definitions.

(a) "**Vendor-Owned Software**" means software and supporting documentation, in both source code and object code form, that is: (i) created prior to the execution of this Agreement; (ii) owned by the Vendor; (iii) included in, or necessary or helpful to, the operation, maintenance, support or modification of any Infrastructure or Services; and (iv) not licensed to ITSC or any MRM State prior to entering into this Agreement. Vendor-Owned Software shall further include all Updates to any Vendor-Owned Software that meets (i)-(iv) above.

(b) "**IPR**" means all intellectual property and proprietary rights throughout the world, including all: (i) patents and patent applications, domestic or foreign, all licenses relating to any of the foregoing, all rights to sue for past, present or future infringement thereof, all rights arising therefrom and pertaining thereto and all reissues, divisions, continuations, certificates of invention, renewals, reexaminations, extensions and continuations-in-part thereof; (ii) trademarks, service marks, logos, mask works and trade names, and applications for registration thereof, whether domestic or foreign; (iii) copyrights and rights in computer software (in both source code and object code form) and documentation; (iv) trade secrets and information, whether or not patentable or copyrightable and whether or not reduced to practice, know-how, manufacturing and production processes and techniques; (v) rights in data or databases; and (vi) other proprietary rights and processes, inventions, discoveries, ideas, concepts, methods or works of authorship fixed in a medium of expression.

(c) "**Third-Party Software**" means software and supporting documentation that is: (i) not owned by ITSC, any MRM State, or Vendor; and (ii) included in, or necessary or helpful to the operation, maintenance, support or modification of the Infrastructure.

(d) "**Updates**" means all updates, upgrades, patches, enhancements, translations, modifications, derivatives, or improvements.

10.2 MRM System. As between ITSC and Vendor, the MRM System is and shall remain the sole and exclusive property of the MRM states. This Agreement does not transfer or convey to Vendor, expressly or by implication, estoppel or otherwise, any rights in or to the MRM System or any IPR therein or related thereto.

10.3 Vendor-Owned Software. All right, title, and interest in and to Vendor-Owned Software shall at all times remain with Vendor, subject to the rights and licenses granted herein to and reserved herein by ITSC, the MRM States, and the US DOL. Vendor grants to ITSC (for the benefit of the MRM States) a nonexclusive, irrevocable, unlimited and unrestricted, royalty-free, fully paid, cost-free, perpetual, fully transferrable and sublicensable, non-cancelable, non-terminable, sub-licensable right and license to use, copy, make, sell, offer for sale, display, perform, transmit, disclose, prepare derivative works based on, distribute and otherwise exploit ("**Use**") all Vendor-Owned Software. Vendor covenants and agrees that Vendor has and will have throughout this Agreement all rights and authority necessary to grant the rights and licenses related to Vendor-Owned Software granted by Vendor to ITSC under this Agreement. The Infrastructure and all Services (and accompanying Deliverables) will only incorporate or rely upon any Vendor-Owned Software identified in written notice to ITSC and agreed to in writing in advance by ITSC.

10.4 Third-Party Software. All right, title, and interest in and to the Third-Party Software shall at all times remain with the third-party vendor of such Third-Party Software, subject to any license granted thereby and the licenses

granted herein. Vendor covenants and agrees that Vendor will obtain from each such third party vendor for ITSC (for the benefit of the MRM States) a nonexclusive, irrevocable, unlimited and unrestricted, royalty-free, fully paid, cost-free, perpetual, fully transferrable and sublicensable, non-cancelable, non-terminable, sub-licensable right and license to Use all Third-Party Software. Vendor covenants and agrees that Vendor has and will have throughout this Agreement all rights and authority necessary to grant the rights and licenses related to Third-Party Software granted by Vendor to ITSC under this Agreement. The Infrastructure and all Services (and accompanying Deliverables) will only incorporate or rely upon any Third-Party Software identified in written notice to ITSC and agreed to in writing in advance by ITSC.

10.5 Reservation of Rights. As provided in 29 CFR § 97.34, the United States Department of Labor reserves a royalty-free, nonexclusive, and irrevocable license to reproduce, publish or otherwise use, and to authorize others to use for Federal Government purposes, the copyright in any work developed under this Agreement.

(a) Nothing in this Agreement shall prohibit Vendor's use for its own purposes of the general knowledge, skills, experience, ideas, concepts, know-how, and techniques obtained and used during the course of providing the services requested under this Agreement.

(b) Subject to the MRM States' IPR and to Vendor's confidentiality obligations hereunder, nothing in the Agreement shall prohibit Vendor from developing for itself, or for others, materials that are similar to and/or competitive with those that are produced under this Agreement.

10.6 Bankruptcy. The IPR in and to any this Agreement are subject to 11 U.S.C. § 365(n) of the U.S. Bankruptcy Code. Prior to filing any petition in bankruptcy, the Vendor shall provide the MRM States with written notice of its intent to file such a petition. In addition, in the event that a petition in bankruptcy is filed against the Vendor, the Vendor shall promptly provide the MRM States of notice that such a petition has been filed.

11. BREACH.

11.1 Breach. A party shall be deemed to have breached the Agreement if any of the following occurs:

(a) failure to perform in accordance with any Specifications or terms or provisions of this Agreement;

(b) partial performance of any term or provision of this Agreement;

(c) any act prohibited or restricted by this Agreement or applicable Law; or

(d) violation of any representation, warranty or covenant.

For purposes of this Agreement, each of the foregoing items shall be referred to herein as a "**Breach**."

11.2 Notification of Breach.

(a) By Vendor. In the event of a Breach of Agreement by ITSC, Vendor shall notify ITSC in writing within 30 days of such Breach. Such notice shall contain a description of the Breach. Failure by Vendor to provide such written notice within such time period shall operate as an absolute waiver by the Vendor of such Breach by ITSC. In no event shall any Breach on the part of ITSC excuse Vendor from full performance under this Agreement. ITSC shall have 60 days from receipt of any such timely issued notice to cure any Breach identified therein.

(b) By ITSC. ITSC may notify Vendor in writing of any Breach. Any such notice shall contain a description of the applicable Breach. Upon receipt of such notice, Vendor shall present ITSC with a written plan detailing the efforts and time it will take to cure the Breach identified in such notice and the time period for such resolution. Vendor acknowledges that, upon timely receipt of any written plan to cure, ITSC has the sole authority to determine the scope of any cure and the time within which any cure may be performed ("**Cure Period**"). Vendor further acknowledges that ITSC has the sole authority to determine the timeliness and effectiveness of any attempt to cure by Vendor. Vendor shall have the applicable Cure Period specified in such notice from ITSC to cure any Breach identified therein. Such Cure Period shall be at least 10 days from the date of such notice, unless:

(i) Vendor has intentionally withheld Services or otherwise refused to perform;

(ii) Vendor has Breached Sections [To be provided];

(iii) Vendor has committed repeated similar breaches, evidencing an inability or unwillingness to cure said breaches;

(iv) ITSC determines, in its sole discretion, that a cure period would cause a delay that would impair the effectiveness of ITSC operations or jeopardize public safety or cause public crisis.

Notwithstanding the foregoing, in event of a Breach by Vendor, ITSC shall have available any and all remedies set forth herein and any other remedy available at law or equity and Vendor shall not be relieved of liability to ITSC for damages sustained by ITSC due to any Breach.

12. TERMINATION.

12.1 Termination for Convenience. ITSC may terminate this Agreement or any Addendum hereunder without cause for any reason or no reason. Such termination shall not be deemed a breach of this Agreement by ITSC. ITSC shall give Vendor at least 30 days written notice before the effective termination date (a "**Termination Notice**"). Vendor shall be entitled to compensation for satisfactory, authorized and accepted Services completed as of the termination date, but in no event shall ITSC be liable to Vendor for compensation for any Service or other obligation that has not been completed and accepted, or for any unauthorized Service performed in any manner, or for any Service performed in a manner unsatisfactory to ITSC. Upon such termination, the Vendor shall have no right to any actual general, special, incidental, consequential, or any other damages whatsoever of any description or amount. Upon any expiration of this Agreement or termination of this Agreement for any reason, Vendor shall provide transition assistance services to ITSC and each MRM State as set forth in *Schedule [●] (Transition Services)* ("Transition Services") and defined in section 14 Transition services.

12.2 Termination for Cause. ITSC may, in its sole discretion, terminate all or any part of this Agreement and withhold all future payments due and owing to Vendor upon any Breach by Vendor that remains uncured following the applicable Cure Period specified by ITSC. ITSC will provide Vendor with a Termination Notice specifying: (a) in reasonable detail the nature of the Breach; and (b) the effective date of termination.

12.3 Effect of Termination or Expiration.

(a) Obligations and Rights. Upon any expiration of this Agreement or termination of this Agreement for any reason, except as specified by ITSC in the applicable Termination Notice and as needed to accommodate any Transition Services:

(i) Cessation of Services. Vendor shall complete all Services (and deliver to ITSC any accompanying Deliverables) as directed in the applicable Termination Notice and by ITSC. Vendor shall otherwise cease providing all or any portion of the Services.

(ii) Vendor Confidential Information. Subject to public record requirements, ITSC shall return all Vendor Confidential Information in its possession to Vendor.

(iii) Data and ITSC and MRM Confidential Information. Vendor shall either return all Data and all ITSC or MRM Confidential Information in its possession to ITSC, for the benefit of ITSC and all MRM States, transfer Data and ITSC Confidential Information in its possession to another Hosting Vendor, or destroy in a manner consistent with standard operating procedure and / or a process directed by ITSC. This shall be done at no cost to ITSC or MRM States. Upon expiration or termination of part, but not all, of the Services being provided under this Agreement, Vendor shall either return all Data and all ITSC or MRM Confidential Information relating solely to such terminated Services to ITSC, for the benefit of ITSC and all MRM States, transfer Data and ITSC Confidential Information in its possession to another Hosting Vendor, or destroy in a manner consistent with standard operating procedure and / or a process directed by ITSC. This shall be done at no cost to ITSC or MRM States. Following such return of any portion(s) of such Data and ITSC or MRM Confidential Information, Vendor shall permanently destroy such Data and Confidential Information in a manner and using a process directed by ITSC, as directed by ITSC

(iv) Return of Additional Materials. (1) all materials owned by ITSC or any MRM State in the possession or control of Vendor shall be immediately to ITSC or the applicable MRM State; (2) Vendor shall notify ITSC of the then current status of all Deliverables and shall, at the direction of ITSC, deliver all Deliverables to ITSC or its

designee (all of which shall become the property of ITSC); and (3) any other records, documentation, reports, data, hard copy and electronic files, recommendations, etc. of any kind or nature which were required to be developed or provided under the terms of the Agreement shall be delivered to ITSC or its designee. Vendor shall take timely, reasonable and necessary action to protect and preserve all of the foregoing in the possession or control of Vendor.

(v) Service Contracts. At the sole discretion of ITSC, Vendor shall assign to ITSC or its designee all of Vendor's right, title, and interest under any orders or subcontracts under which Vendor obtains any portion of the Services under this Agreement.

(vi) Payments. ITSC may, in its sole discretion, require Vendor to return to ITSC, within 30 days of the date of the applicable Termination Notice, all payments made to Vendor hereunder prior to the date of the Termination Notice.

12.4 Survival of terms. The following Sections will survive any expiration or termination of this Agreement for any reason: [To be provided]. In addition all other terms and conditions of this Agreement that by their nature are intended to survive termination or expiration of this Agreement will do so.

13. ADDITIONAL REMEDIES.

ITSC shall have all of the remedies listed in this Agreement or otherwise available at law or in equity. ITSC may exercise any or all such remedies available to it, in its sole discretion concurrently or consecutively. Notwithstanding any expiration or termination of this Agreement, ITSC may, in its sole discretion, exercise any one or more of the following remedies in addition to other remedies available to it hereunder or under applicable Law.

13.1 Corrective Action Plan. Upon any Breach or other failure by Vendor to meet any of the requirements set forth in this Agreement, ITSC may, in its sole discretion, request a corrective action plan, such plan may include applicable corrective action(s) to be taken by Vendor, a date by which Vendor shall take all such corrective correct, and such other details established by ITSC in its reasonable discretion (a "**Corrective Action Plan**"). Until such time as Vendor has successfully completed the corrective action specified in any Corrective Action Plan in a manner satisfactory to ITSC, ITSC may, in its sole discretion: (a) suspend Vendor's performance with respect to all or any portion of this Agreement, without entitling Vendor to an adjustment in price/cost or performance schedule; (b) withhold payment to Vendor; and (c) require Vendor to re-perform the applicable Services.

13.2 Removal of Personnel. ITSC may demand immediate removal of any Vendor employee, agent, or contractor whom ITSC deems responsible for any Breach or other failure by Vendor to meet any of the defined performance requirements set forth in this Agreement, whom ITSC otherwise deems incompetent, careless, insubordinate, unsuitable, or otherwise unacceptable, or whose continued relation to this Agreement is deemed to be contrary to the public interest or the best interest of ITSC or any MRM State.

13.3 Liquidated Damages.

(a) In the event of any Breach or the failure to meet any performance requirements set forth herein, ITSC may additionally assess liquidated damages as set forth in this Section ("**Liquidated Damages**"). ITSC shall notify Vendor of amounts to be assessed as Liquidated Damages. The following table defines the standards required for Vendor's performance for the Project and the associated liquidated damages, which Vendor agrees to pay.

Requirement	Damages
The Project performance thresholds for required by _____ .	One Thousand Dollars ($1,000) per day
The Project performance thresholds for application System availability as required by _____	Ten Thousand Dollars ($10,000) per day
Failure to provide monthly Compute Utilization reports within seven (7) calendar days from the end of each month.	Five Hundred Dollars ($500) per day

Failure to make adequate progress pursuant to the Schedule required by_____ for two of the Application Vendor Agreement consecutive checkpoints during the detailed design and development phase	Ten Thousand Dollars ($10,000) per day
Data is lost because of a data redundancy failure	____ Thousand Dollars per gigabyte of data lost
Failure to correct any defects covered by the warranty in _____ within the timeframes stated in _____	Ten Thousand Dollars ($10,000) per day

(b) ITSC has the right to set off or withhold from payment hereunder any amounts due and payable to Vendor as Liquidated Damages under this Section.

(c) The parties agree that due to the complicated nature of the Vendor's obligations under this Agreement it would be impossible to specifically designate a monetary amount for a Breach by Vendor, as said amounts are likely to be uncertain and not easily proven. Vendor hereby represents and covenants it has carefully reviewed the Liquidated Damages contained in this Section, and agrees that said amounts represent a reasonable relationship between the amount and what might reasonably be expected in the event of Breach, and are a reasonable estimate of the damages that would occur from a Breach. It is hereby agreed between the parties that the Liquidated Damages represent solely the damages and injuries sustained by ITSC in losing the benefit of the bargain with Vendor and do not include any injury or damage sustained by any MRM State or other third party. Vendor agrees that the liquidated damage amount is in addition to any amounts Vendor may owe ITSC pursuant to the indemnity provision or other Section of this Agreement.

(d) ITSC may continue to assess the Liquidated Damages or a portion thereof until the Vendor attains the applicable performance requirements set forth herein or ITSC terminates the Agreement. ITSC is not obligated to assess Liquidated Damages before availing itself of any other remedy. ITSC may choose to discontinue Liquidated Damages and avail itself of any other remedy available under this Agreement or at Law or equity; provided, however, Vendor shall receive a credit for said Liquidated Damages previously withheld. Notwithstanding the foregoing table, Liquidated Damages accruing over the term of the Agreement shall not, in the aggregate exceed one million and five hundred thousand dollars ($1,500,000) per MRM State. In addition, Liquidated Damages will not be assessed against delays or performance failures attributable to ITSC, any MRM State, or third party engaged by either ITSC or any MRM State.

13.4 Partial Takeover. ITSC may, in its sole discretion, exercise a partial takeover of any Service which Vendor is obligated to perform under this Agreement, including but not limited to any Service which is the subject of a contract between Vendor and a third party, (a "**Partial Takeover**"). Such Partial Takeover shall not be deemed a Breach of Agreement by ITSC. Vendor shall be given at least 30 days prior written notice of said Partial Takeover with such notice to specify the area(s) of Service ITSC will assume and the date of such assumption. Any Partial Takeover by ITSC shall not alter in any way Vendor's other obligations under this Agreement. In addition to any other damages associated with such Partial Takeover, ITSC may thereafter withhold from the amounts due Vendor the greater of (a) amounts that would be paid Vendor to provide the Service subject to such Partial Takeover, and (b) the cost to ITSC of providing such Service (whether such Service is provided by ITSC, any MRM State(s), or any third party), as determined by ITSC in its sole discretion. The amounts may be withheld effective as of the date ITSC assumes a Partial Takeover of any such Service. Upon any Partial Takeover, Vendor shall have no right to recover from ITSC any actual, general, special, incidental, consequential, or any other damages whatsoever of any description or amount.

13.5 IPR Infringement. If the Infrastructure, Resources or any Services (or accompanying Deliverables), or any component or element thereof, or the utilization thereof or access thereto by ITSC or any MRM State or any user thereof, infringes upon, misappropriates or otherwise violates any IPR, or if ITSC reasonably believes any such infringement, misappropriation or other violation is likely to occur, Vendor shall, at the option of ITSC: (a) obtain for ITSC and each MRM State the right to utilize any of the foregoing as set forth herein; or (b) replace any of the foregoing with non-infringing alternatives or modify them so that they become non-infringing, provided, that no such replacement shall materially or adversely impact the functionality or operation of the MRM System or alter any of the performance requirements under this Agreement.

14. TRANSITION SERVICES.

14.1 Transition Services. Upon any expiration of this Agreement or termination of this Agreement for any reason, Vendor shall provide transition assistance services to ITSC and each MRM State as set forth in ***Schedule [●] (Transition Services)*** ("**Transition Services**"). Such Transition Services shall be sufficient to enable ITSC and each MRM State to accomplish the orderly transfer of the Services and any other functions, responsibilities, tasks and operations that were required to be provided by (or on behalf of) Vendor under this Agreement to ITSC, one or more of the MRM States, or an ITSC-designated third party within a period not to exceed 90 days. Without limiting the foregoing, such Transition Services shall include: (a) assisting ITSC and each MRM State or their respective designee(s) in developing a written transition plan for the transition of all applicable Services; (b) performing Services to assist in implementing such transition plans; (c) familiarizing personnel designated by ITSC and each MRM State or their respective designee(s) in the use of any work instructions and work procedures and any equipment, software, and materials used in connection with the provision of the Services; (d) cataloging all work instructions, work procedures, Deliverables, third-party contracts and tools used to provide the Services; (e) assisting in the execution of a parallel operation, data migration and testing process until the successful completion of the transition, (f) creating and providing copies of any Data in the format and on the media reasonably requested by ITSC, (g) assigning any third-party licenses and contracts to ITSC; and (h) providing other technical assistance reasonably requested by ITSC, (i) return all ITSC or MRM State Hardware and Software, (j) Perform and return all final backups of data and code, (k) provide proof of data destruction as required. Vendor shall perform the Transition Services at no additional cost to ITSC provided that such Transition Services commence and are completed within 6 months of expiration or termination of this Agreement. Vendor shall provide the Transition Services in accordance with this Section even in the event of ITSC's material breach, with or without an attendant termination for cause by Vendor.

14.2 Updates to Transition Services. Throughout the term of this Agreement, Vendor will propose updates to the Transition Services to ITSC from time to time as necessary to ensure the Transition Services continue to meet the Services and other obligations of Vendor under this Agreement. Upon the approval of ITSC, such changes proposed by Vendor shall become part of the "Transition Services" for purposes of this Agreement.

15. RECORDS, REPORTING, AND AUDIT.

15.1 Records. Vendor shall make, keep, maintain, and allow inspection and monitoring by ITSC and each MRM State of a complete file of all material records, documents, communications, notes, and other written materials, electronic media files, and communications, pertaining in any manner to the MRM System, Infrastructure, Services, Deliverables, and other obligations and responsibilities of Vendor under this Agreement, including each MRM State Addendum. Vendor shall maintain such records until the last to occur of: (a) a period of 5 years after the date this Agreement expires or is sooner terminated; (b) final payment is made hereunder; (c) the resolution of any pending matters hereunder; (d) such period required by applicable MRM State Law; or (e) if an audit is occurring or Vendor has received notice that an audit is pending, until such audit has been completed and its findings have been resolved (collectively, the "**Record Retention Period**").

15.2 Inspection. Vendor shall permit ITSC, each MRM State, and the federal government or any other duly authorized agent of a governmental agency to audit, inspect, examine, excerpt, copy and/or transcribe Vendor's records relating to this Agreement during the Record Retention Period to assure compliance with the terms hereof. Vendor shall permit any MRM State to audit, inspect, examine, excerpt, copy and/or transcribe Vendor's records pertaining to any MRM State Addendum relating to such MRM State during the Record Retention Period to assure compliance with the terms thereof.

15.3 Monitoring. Vendor shall permit ITSC, each MRM, the federal government, any state, and any governmental agency having jurisdiction, in their sole discretion, to monitor all activities conducted by Vendor pursuant to the terms of this Agreement using any reasonable procedure, including: internal evaluation procedures, examination of program data, special analyses, on-site checking, formal audit examinations, or any other procedures. All monitoring controlled by ITSC shall be performed in a manner that shall not unduly interfere with Vendor's general business operations or performance hereunder. Vendor shall permit each MRM State to monitor all activities conducted by Vendor pursuant to the terms of the Addendum relating to such MRM State, unless provided to the contrary in such Addendum.

15.4 Reports. Vendor shall provide to ITSC with all reports set forth in ***Schedule [●] (Reports)*** or any other Schedule to this Agreement in accordance with the provisions hereof, in such form as prescribed by ITSC.

15.5 Audits. Full, timely participation in scheduled and random security audits, including hosting infrastructure and/or the application vulnerability assessments. Complete compliance with all Federal and MRM state laws, regulations, statutes, policies, standards. Conduct self-audits on all software and hardware, modifications, patches applied, etc.

15.6 Notifications. Vendor shall provide ITSC and MRM States notification consistent with the failure to meet any RFP requirements, events, breaches, and agreed upon Operational Service Agreement (OSA) and Service Level Agreement (SLA) failures.

16. INDEMNIFICATION.

16.1 Indemnification. Vendor shall, at any Consortium Indemnified Party's sole discretion, defend, indemnify, and hold ITSC and each of the MRM States, as well as each of their respective elected officials, officers, agents, employees, end users, and sublicensees (collectively and individually "**Consortium Indemnified Party**"), individually and collectively, harmless, from any and all costs, losses, damages, expenses (including reasonable attorney's fees), liabilities, claims, lawsuits, proceedings, or demands (collectively "**Liability**") arising out of or resulting from and of the following (each, a "**Claim**"): (a) any claim or allegation that the Infrastructure or Services (or accompanying Deliverables), the development or operation thereof by Vendor, or the use or enjoyment thereof by any Consortium Indemnified Party infringes, misappropriates or otherwise violates any IPR of any third party; (b) any third-party claim or allegation, including any claim by any MRM State, alleging a breach by the Vendor of any of its obligations regarding confidentiality or data security or privacy hereunder; (c) any third-party claim or allegation, including any claim by any MRM State, alleging a breach by Vendor of any of its representations, warranties or covenants under this Agreement; and (iv) any claim or allegation, including, any claim by any MRM State, arising or resulting from acts, omissions, or negligence on the part of Vendor, its employees, or any person or entity acting for or on its or their behalf relating to this Agreement.

16.2 Notice of Claims. In each instance in which a Consortium Indemnified Party seeks to have Vendor indemnify such Consortium Party for or defend such Consortium Indemnified Party against any Claim or Liability, the Consortium Indemnified Party shall provide Vendor with prompt written notice of such Claim and reasonable assistance, provided that the Consortium Indemnified Party will have the right to participate in such defense and negotiations using counsel at its own expense. Vendor will obtain the Consortium Indemnified Party's consent, which will not be unreasonably withheld, prior to entering into a settlement or compromise or consenting to any injunctive relief with respect to such Claim. In instances where the Consortium Indemnified Party chooses to defend a Claim itself, the Consortium Indemnified Party shall promptly notify Vendor in writing of such choice. Vendor shall promptly reimburse the Consortium Indemnified Party for any fees for monies owed, when due, as a result of the Consortium Indemnified Party defending and resolving the claim or otherwise owed to the Consortium Indemnified Party under this Section.

16.3 Nothing contained herein shall be deemed to accord to Vendor, through its attorney(s) or otherwise, the right to represent ITSC in any legal matter, or any of the other Consortium States subject to the respective Laws of such Consortium States.

17. LIABILITY.

17.1 ITSC/Consortium Liability. Neither ITSC nor any MRM State shall have any liability to Vendor or any other third party arising out of any party's performance of this Agreement, except as expressly provided in this Agreement.

17.2 Limitation of Liability. Regardless of whether any remedy set forth herein fails of its essential purpose or otherwise, to the greatest extent permissible under applicable law, in no event will ITSC or its elected officials, affiliates, employees, agents, contractors, assigns, licensees, or successors in interest, be liable for any indirect, incidental, consequential, special, punitive or other damages other than direct damages arising out of or relating to this Agreement, whether in an action in contract, tort, strict liability or otherwise, even if ITSC has been advised of the possibility of those damages and whether or not such loss or damages are foreseeable.

17.3 Cap on Damages.

(a) The total cumulative liability of ITSC under this Agreement for any liability or damages arising out of or relating to this Agreement, whether in contract, tort, or otherwise, will not exceed the Maximum Compensation Amount, as may be amended,

(b) With the exception of liability for any indemnification obligation under this Agreement, the total cumulative liability of Vendor under this Agreement for any liability or damages arising out of or relating to this Agreement, whether in contract, tort, or otherwise, will not exceed the greater of the any actual direct damages and 3 times the Maximum Compensation Amount, as may be amended, provided that in no event shall this Section limit the liability of Vendor for its intentional torts, criminal acts, or fraudulent conduct.

17.4 Applicable Immunities. Nothing in this Agreement shall be construed or interpreted as a waiver, express or implied, of any of the immunities, rights, benefits, protection, or other provisions, of any MRM State under applicable Laws, including all applicable governmental immunity statutes.

18. CONFIDENTIALITY.

18.1 Definitions.

(a) "**Confidential Information**" means all confidential information of a Disclosing Party, whether in paper or electronic format, disclosed to a Recipient that is designated in writing as confidential at the time of disclosure or that would be reasonably understood to be proprietary and confidential. Confidential Information shall not include information received under this Agreement required to be disclosed pursuant to the open records statutes of the Laws of any MRM State.

(b) "**MRM State Confidential Information**" means all Confidential Information belonging to any MRM State.

(c) "**Disclosing Party**" means a party disclosing Confidential Information.

(d) "**ITSC Confidential Information**" means the Confidential Information of ITSC. Confidential Information of ITSC shall include the System, Infrastructure, Data, and Deliverables.

(e) "**Recipient**" means a party receiving Confidential Information.

(f) "**Vendor Confidential Information**" means all Confidential Information of Vendor.

18.2 Exceptions. Confidential Information shall not include information that: (a) was generally available to the public at the time it was disclosed, or becomes generally available to the public through no fault of the Recipient; (b) was known to the Recipient at the time of disclosure as shown by written records in existence at the time of disclosure; (c) was developed independently by the Recipient prior to the disclosure, as shown by written records in existence prior to the disclosure; (d) is disclosed with the prior written approval of the Disclosing Party; (e) becomes known to the Recipient from a source other than the Disclosing Party without breach of this Agreement, and in a manner that is otherwise not in violation of the Disclosing Party's rights; (f) is required under the open records statutes applicable to the Recipient (where the Recipient is a MRM State); or (g) is disclosed pursuant to the order or requirement of a court, administrative agency, or other governmental body, provided that the Recipient shall attempt to provide reasonable advance notice to the Disclosing Party to enable the Disclosing Party to seek a protective order or otherwise prevent such disclosure.

18.3 Obligations of the Parties. Each Recipient receiving Confidential Information of a Disclosing Party shall (a) treat as confidential all Confidential Information provided by the Disclosing Party in compliance with the laws, regulations, and state cyber-security procedures applicable to the confidentiality of information; (b) not use such Confidential Information except as expressly permitted under the terms of this Agreement under which the Confidential Information was disclosed, or as otherwise previously authorized in writing by the Disclosing Party; (c) implement reasonable procedures to prohibit the disclosure, unauthorized duplication, reverse engineering, disassembly, decompiling, misuse or removal of such Confidential Information; (d) not disclose such Confidential Information to any third party, except to employees, affiliates and contractors that require access to the Confidential Information for the performance of obligations under this Agreement and that are bound by enforceable confidentiality obligations substantially similar to

those set forth in this Agreement; and (e) except as permitted under Section 18.2. Without limiting the foregoing, each Recipient shall use at least the same degree of care to prevent the disclosure of the Confidential Information of a Disclosing Party as it uses to prevent the disclosure of its own Confidential Information, and shall in any event use no less than a reasonable degree of care.

18.4 Notification. Each Recipient of the Confidential Information of a Disclosing Party shall: (a) notify each of its agents, employees, contractors and assigns who are authorized to use or reasonably may be expected to come into contact with the Confidential Information that each is subject to the confidentiality requirements set forth herein and in any Addendum under which the disclosure is made; and (b) provide each such agent, employee, contractor, and assigns with a written explanation of such requirements before permitting such agent, employee, contractor, and assigns to access Confidential Information.

18.5 Use, Security, and Retention. Neither ITSC Confidential Information nor any MRM Confidential Information of any kind, shall be distributed or sold to any third party or used by Vendor, its contractors, or their respective employees and agents in any manner, except as approved in writing by the authorized representative of the Disclosing Party. Vendor shall provide and maintain a secure environment that ensures the confidentiality of all ITSC Confidential Information and MRM Confidential Information wherever located. Neither ITSC Confidential Information nor MRM Confidential Information shall be retained in any files or otherwise by Vendor, it contractors, or their respective employees and agents, except as approved in writing by an authorized representative of the Disclosing Party. All ITSC Confidential Information, MRM Confidential Information, and Data of any kind shall be stored, processed, or transferred only in or to facilities located within the United States.

18.6 Third Party Requests. Any request or demand by a third party for ITSC Confidential Information in the possession of Vendor shall be immediately forwarded to an authorized representative of ITSC. Any request or demand by a third party for MRM Confidential Information in the possession of Vendor shall be immediately forwarded to an authorized representative of the MRM State to which such Confidential Information belongs.

19. DATA AND DATA SECURITY.

19.1 Data. For purposes of this Agreement, "**Data**" means any data or other information collected, received, obtained, accessed, generated, processed, or provided by or through the MRM System or Infrastructure or through the performance of any Services or other obligations under this Agreement and all data and information based on such data or information. Data includes all data and information regarding individual users of the MRM System, whether or not such data or information relates to an identified or reasonably identifiable individual, including names, addresses, Social Security numbers, e-mail addresses, telephone numbers , financial profiles, credit card information, driver's license numbers, medical data, law enforcement records, agency source code or object code, agency security data, or information identifiable to an individual that relates to any of these types of information.

19.2 Data Ownership. All Data is and shall remain the sole and exclusive property of the applicable individual MRM States. Vendor agrees to and hereby does assign, transfer, and convey all right, title, and interest in and to the Data, including all IPR embodied in or arising out of the Data, to each applicable individual MRM State. Vendor shall, when directed, execute any other documents ITSC or any MRM State deems necessary or desirable to document this transfer. Vendor shall cooperate fully in all such endeavors.

19.3 Data Use and Data Privacy. Data shall not be used or accessed by Vendor for any purpose other than as expressly required to provide the Services and other obligations of Vendor under this Agreement. Except for the foregoing limited use, the Data or any part thereof shall not be used in any form, whether or not aggregated or de-identified, and may not be processed, disclosed, distributed, sold, assigned, leased, or otherwise disposed of to third parties by Vendor or exploited or otherwise utilized by or on behalf of Vendor or its officers, directors, employees, contractors or agents. Without limiting the foregoing, all use of and access to Data shall comply with all applicable Laws and all applicable requirements set forth in ***Schedule [●] (Data Security and Data Privacy)*** or otherwise provided to Vendor by ITSC or any MRM State during the term of this Agreement.

19.4 Notification of Third-Party Request for Data. Unless the notification is specifically precluded by such law, lawful order, or government authority, as applicable, Vendor shall notify Consortium in the event that Vendor is required by

Law, lawful order of a court (including any request for production of documents), or governmental authority to disclose Consortium Data. In the event that Vendor is required to produce or disclose Consortium Data, unless prohibited as set forth above, then Vendor shall provide the Consortium States with written notice of the request sufficiently in advance of the data specified for the production of the records so that the Consortium States can act to protect its data by, for example, seeking a protective order. In addition, Vendor shall not release the data pending the outcome of any measures taken by any Consortium State(s) to contest, otherwise oppose, or seek to limit disclosure by Vendor.

19.5 Data and Network Security. Vendor shall establish, implement, maintain, and enforce throughout the term of this Agreement a data and network security program providing for all reasonable and appropriate administrative, technical, environmental, and physical safeguards and security measures necessary to protect all MRM System, Infrastructure, and Data from and against unintended, unauthorized, or unlawful disclosure, processing, use, access, alteration, destruction, or loss. Vendor's program will be adequate to meet the requirements of applicable Laws and industry standards and best practices and will comply in all respects with ***Schedule [●] (Data Security and Data Privacy)***. Without limiting the foregoing, Vendor's security program will include, as applicable:

(a) Maintaining a written information security policy ("**WISP**");

(b) Conducting periodic risk assessments, and using the results of those risk assessments to update the security program and the WISP as applicable;

(c) Transmitting all Data over any public or private network in a secured and encrypted fashion;

(d) Providing dedicated storage devices for any Data, such storage devices secured against any shared access with the data of any Vendor's data or data of Vendor's other customers;

(e) Requiring that any contractors, venders, service Vendors, or other third parties to agree in writing to be bound to the security provisions in this Agreement;

(f) Processing and storing all Data only within the United States;

(g) Ensuring that Vendor's security program is audited at least annually by a qualified, objective, independent third party professional who uses procedures and standards generally accepted in the profession, and notifying ITSC within 48 hours of any Security Breach or significant deficiencies identified in Vendor's security program. Audit results must be made available to ITSC and MRM States on request at no cost;

(h) Providing ITSC and each MRM State with prompt notice (but in no case more than 24 hours) after receiving any government inquiry, complaint, lawsuit or investigation concerning the adequacy or sufficiency of its security program; and

(i) Taking such other measures as are necessary to ensure the security and confidentiality of the Data and to comply with the information security policies of ITSC and each MRM State in effect during the term of this Agreement.

Vendor will provide ITSC and each MRM State with a copy of Vendor's security program, including the WISP, and any revisions thereto. Vendor will revise and maintain its security program and the WISP at ITSC's and each MRM State's reasonable request, but will not implement any change to its security program or the WISP without ITSC's and each MRM State's prior approval.

19.6 Data Confidentiality and Privacy. Vendor hereby acknowledges that there will be confidential data being used and stored within the system. Vendor also acknowledges that they will abide by federal and state laws regarding data confidentiality and privacy including reporting and curing breaches. In addition to confidential data, there may also be federal taxpayer data being stored and used in the system. Federal Taxpayer Data will be identified by ITSC and MRM States and subject to additional data confidentiality and privacy laws as defined by the IRS (in particular publication 1075). Vendor hereby acknowledges this and agrees to support ITSC and MRM States in safeguarding, notifying and reporting of this data at no additional cost.

20. PERSONNEL AND STAFFING.

20.1 Nondiscrimination. Vendor hereby covenants and agrees that no person shall be excluded from participation in, be denied benefits of, or be otherwise subjected to discrimination in the performance of this Agreement by Vendor or in the employment practices of the Vendor on the grounds of handicap or disability, age, race, color, religion, sex, national origin, or any other classification protected by the District of Columbia or the state laws of any MRM State. Vendor shall, upon request, show proof of such nondiscrimination policies and shall post in conspicuous places, available to all employees and applicants, notices of nondiscrimination policies.

20.2 Background Checks. Vendor shall verify that all Vendor personnel, including Vendor employees and contractors: (a) are authorized to work in any country in which they are assigned to perform Services; (b) have not been convicted of a felony or a misdemeanor involving a crime that impacts their ability to perform the assigned work or that is substantially related to the assigned work; (c) have not been convicted of a felony or a misdemeanor involving a crime of theft or other moral turpitude; and (d) are not otherwise disqualified from performing the assigned work under applicable Laws. To the extent permitted under applicable Law, Vendor shall perform or have performed a reasonable background check, on all such Vendor personnel. Such check will, at a minimum, include a criminal history and background check, on all Vendor personnel assigned to work under this Agreement. In addition, Vendor shall verify that all Vendor personnel assigned to work under this Agreement have been appropriately screened in accordance with the provisions of all applicable Law against the most recent version of the "Specially Designated Nationals List" published by the Office of Foreign Assets Controls of the U.S. Department of the Treasury.

20.3 Unencumbered Personnel. All persons assigned by Vendor to perform services for ITSC under this Agreement, whether they are employees, agents, contractors, or principals of Vendor, shall not be subject to any employment contract or restrictive covenant provisions that would preclude those persons from performing the same or similar services for ITSC or any MRM State after the termination of this Agreement, either as an employee, an independent contractor, or an employee, agent, contractor or principal of another contractor with ITSC. If Vendor provides ITSC or another MRM State with the services of any person subject to a restrictive covenant or contractual provision in violation of this provision, any such restrictive covenant or contractual provision will be void and unenforceable, and the Vendor will pay the MRM States and/or ITSC all expenses, including reasonable attorneys fees and costs, associated with defending against any such claim arising out of any attempt to enforce such provisions.

20.4 Prohibition of Undocumented Workers. Vendor shall not use or employ undocumented workers in the performance of this Agreement. For purposes of this Agreement, "undocumented worker" is defined as any person who is not either a United States citizen, a Lawful Permanent Resident, or a person whose physical presence in the United States is authorized or allowed by the federal Department of Homeland Security and who, under federal immigration laws and/or regulations, is authorized to be employed in the U.S. or is otherwise authorized to provide services under the Agreement. This prohibition shall be a material provision of this Agreement, a breach of which shall be grounds for monetary and other penalties, up to and including immediate termination for cause of this Agreement without opportunity to cure.

(a) Vendor hereby attests, certifies, warrants, and assures that Vendor shall not knowingly utilize the services of undocumented workers in the performance of this Agreement and shall not knowingly utilize the services of any contractor who will utilize the services of an undocumented worker in the performance of this Agreement. Vendor shall reaffirm this attestation, in writing, by submitting to ITSC a completed and signed copy of the document at ***Schedule [●] (Attestation)*** , annually during the period of this Agreement. Such attestations shall be maintained by Vendor and made available to ITSC staff upon request.

(b) Prior to the use of any contractor in the performance of this Agreement, and semi-annually thereafter, during the period of this Agreement, Vendor shall obtain and retain a current, written attestation that the contractor shall not knowingly utilize the services of an undocumented worker to perform work relative to this Agreement, and shall not knowingly utilize the services of any contractor who will utilize the services of an undocumented worker to perform work relative to this Agreement. Attestations obtained from such contractors shall be maintained by Vendor and made available to ITSC officials upon request.

(c) Vendor shall maintain records for all personnel used in the performance of this Agreement. Said records shall be subject to review and random inspection at any reasonable time upon reasonable notice by ITSC.

20.5 Replacement. Vendor shall not, and shall not permit its contractors to, replace any personnel, including Vendor employees and contractors, who have been actively engaged in the performance of Services or the other obligations under this Agreement without ITSC's prior written consent, with the exception of circumstances where such personnel leave the employ of Vendor (e.g. through retirement or voluntary resignation). Vendor shall provide, and shall cause its contractors to provide, replacement personnel that have educational and relevant experience qualifications that meet or exceed that of the key employee being replaced. The number, classification, and qualification of key employees under this Agreement shall be material elements of Vendor's performance required und this Agreement. Positions may not be eliminated, combined, or shared with Vendor's obligations outside of this Agreement, without the prior written approval of ITSC.

20.6 Conduct. All Vendor personnel, while on the premises of ITSC or any MRM State, shall at all times (a) comply with the reasonable requests and standard rules and regulations of such state, and (b) otherwise conduct themselves in a professional and businesslike manner.

20.7 Subcontracting. Vendor shall not enter into a subcontract for any of the Services or other obligations of Vendor under this Agreement without obtaining the prior written approval of ITSC. Vendor shall submit such information in connection with its request for the approval to engage a subcontractor as deemed necessary by ITSC in its sole discretion. If ITSC consents to any such assignment or transfer, Vendor shall be (i) primarily liable for all work, activities actions and inactions of any such subcontractor, (ii) be solely responsible for all payments to such subcontractor and prohibit such parties from issuing claims directly to ITSC, and (iii) be responsible for securing written agreements for compliance by subcontractor and its personnel with the applicable terms and conditions of this Agreement. Any agreement with an approved subcontractor shall contain, at a minimum but not limited to, sections of this Agreement below pertaining to "Conflicts of Interest," "Nondiscrimination," and "Records" (as identified by the section headings), and shall provide that ITSC shall be a third-party beneficiary of any subcontract and insurance policies covered by such subcontract. Notwithstanding the foregoing, Vendor shall remain responsible for compliance by each of its subcontractors with all applicable terms and conditions of this Agreement and Vendor shall remain responsible for any and all acts or omissions of any subcontractor as if those acts or omissions were those of Vendor. Copies of all subcontracts entered into by Vendor for the purpose of performing any of the Services or other obligations of Vendor under this Agreement shall be submitted to ITSC upon request.

21. INSURANCE.

21.1 Insurance Coverage. Vendor shall carry adequate liability and other appropriate forms of insurance. Without limiting the foregoing, Vendor shall maintain, at minimum, the following insurance coverage:

(a) Workers' Compensation/ Employers' Liability (including all ITSC coverage) with a limit not less than the relevant statutory amount or one million dollars ($1,000,000) per occurrence for employers' liability whichever is greater. ITSC and the Consortium States shall be named as additional insureds and the policy (or policies) shall include a waiver of subrogation in favor of ITSC and the Consortium states.

(b) Comprehensive Commercial General Liability (including personal injury & property damage, premises/operations, independent contractor, contractual liability and completed operations/products) with a bodily injury/property damage combined single limit not less than one million dollars ($1,000,000) per occurrence and two million dollars ($2,000,000) aggregate. ITSC and the Consortium States shall be named as additional insureds, the policy (or policies) shall include a waiver of subrogation in favor of ITSC and the Consortium States and the policy (or policies) shall respond on a primary and non-contributory basis.

(c) Automobile Coverage (including owned, leased, hired, and non-owned vehicles) with a bodily injury/property damage combined single limit not less than one million dollars ($1,000,000) per occurrence. ITSC and the Consortium States shall be named as additional insureds, the policy (or policies) shall include a waiver of subrogation in favor of ITSC and the Consortium States and the policy (or policies) shall respond on a primary and non-contributory basis.

(d) Umbrella Liability Coverage (over the Workers' Compensation/ Employers' Liability, Comprehensive Commercial General Liability, and Automobile Coverage, above) in an amount not less than five million dollars ($5,000,000). ITSC and the Consortium States shall be named as additional insureds.

(e) Directors & Officers/Errors & Omissions Coverage with separate insuring clauses for management liability, management indemnification, outside director liability, professional services liability (Errors & Omissions), organization liability, each with a limit of loss of Three Million Dollars ($3,000,000) per occurrence and an aggregate limit applicable to all coverages of Five Million Dollars ($5,000,000).

(f) Intellectual Property, Cyber-Risk/Network Security/Privacy Insurance (including third-party cyber liability and first-party cyber crime/terrorism expense coverages) with a direct loss/legal liability and consequential loss and expenses resulting from cyber security/network security breaches; data loss, including protected health and personal information; intellectual property; and non-physical business interruption and extra expense, with combined single limit not less than Five Million Dollars ($5,000,000) per occurrence and Ten Million Dollars ($10,000,000.00) aggregate. ITSC and the Consortium States shall be named as additional insureds and the policy (or policies) shall include a waiver of subrogation in favor of ITSC and the Consortium states.

21.2 Certificate of Insurance. At any time ITSC or the Consortium States may require Vendor to provide a valid Certificate of Insurance detailing Coverage Description; Insurance Company & Policy Number; Exceptions and Exclusions; Policy Effective Date; Policy Expiration Date; Limit(s) of Liability; Name and Address of Insured, and any policy exemptions or exclusions. Failure to provide required evidence of insurance coverage shall be a material breach of this Agreement.

22. NOTICE.

All instructions, notices, consents, demands, or other communications required or contemplated by this Agreement shall be in writing and shall be made by (1) certified, first class mail, return receipt requested and postage prepaid; (2) overnight courier service with an asset tracking system; (3) Email; or (4) facsimile transmission with recipient confirmation. Any such communications, regardless of method of transmission, shall be addressed to the respective party at the appropriate mailing address, facsimile number, or EMAIL address as set forth below:

Vendor
Vendor Contact Name & Title
Vendor Name
Address
Email Address
Telephone # Number
FAX # Number

ITSC
ITSC Contact Name & Title
ITSC Agency Name
Address
Email Address
Telephone # Number
FAX # Number

All instructions, notices, consents, demands, or other communications shall be considered effectively given upon receipt, or recipient confirmation, as may be required, and, in the cases of email and fax, ITSC acknowledgement or constitutes notice of receipt effectively given.

23. ADDITIONAL TERMS AND CONDITIONS.

23.1 Assignment.

(a) By Vendor. Vendor's rights and obligations hereunder are personal and shall not be assigned or transferred (whether by operation of law or otherwise) without the prior written approval of ITSC. For purposes of this Agreement, a change of control of Vendor shall be considered a transfer requiring the prior written approval of ITSC. Any attempt at assignment or transfer of or under this Agreement (whether by operation of law or otherwise) without such approval shall be void. All assignments and transfers approved by ITSC under this Agreement shall be subject to all of the provisions hereof.

(b) By ITSC. ITSC may assign or transfer any or all of its rights and obligations under this Agreement to a MRM State. Upon any such transfer, ITSC shall have no further rights or obligations under this Agreement. ITSC shall provide notice to Vendor of such assignment, specifying the effective date thereof. If no MRM State accepts assignment of ITSC's right and obligations under this Agreement, ITSC may shall terminate this Agreement as provided herein.

23.2 Conflicts of Interest. Vendor warrants that no part of the Maximum Total Compensation Amount shall be paid directly or indirectly to an employee or official of ITSC as wages, compensation, or gifts in exchange for acting as an officer, agent, employee, contractor, or consultant to Vendor in connection with any work contemplated or performed relative to this Agreement. Vendor acknowledges, understands, and agrees that this Agreement shall be null and void if the Vendor is, or within the past six months has been, an agent or employee of ITSC or if the Vendor is an entity in which a controlling interest is held by an individual who is, or within the past six months has been, an employee of ITSC.

23.3 Strict Performance. Failure by any party to this Agreement to insist in any one or more cases upon the strict performance of any of the terms, covenants, conditions, or provisions of this Agreement shall not be construed as a waiver or relinquishment of any such term, covenant, condition, or provision. No term or condition of this Agreement shall be held to be waived, modified, or deleted by ITSC except by a written amendment signed by the parties.

23.4 Independent Contractor. The parties, in the performance of this Agreement, shall not act as employees, partners, joint ventures, or associates of one another. It is expressly acknowledged by the parties that such parties are independent contracting entities, and that nothing in this Agreement shall be construed to create an employer/employee relationship or to allow either to exercise control or direction over the manner or method by which the other transacts its business affairs or provides its services. The employees or agents of one party shall not be deemed or construed to be the employees or agents of the other party for any purpose whatsoever. Vendor, being an independent contractor and not an employee of ITSC, agrees to carry adequate public liability and other appropriate forms of insurance on the Vendor's employees, and to pay all applicable taxes incident to this Agreement.

23.5 Third Party Beneficiaries. Each MRM State is an intended beneficiary under this Agreement and each MRM State applicable to any MRM State Addendum is an intended beneficiary under such MRM State Addendum. Enforcement of this Agreement and all rights and obligations hereunder are reserved solely to the parties and intended beneficiaries. Other than intended beneficiaries, any services or benefits which third parties receive as a result of this Agreement are incidental to this Agreement and do not create any rights for such third parties. Enforcement of any MRM State Addendum and all rights and obligations thereunder are reserved solely to the parties to such MRM State Addendum and any intended beneficiaries, and any services or benefits which third parties receive as a result of such MRM State Addendum are incidental thereto and do not create any rights for third parties.

23.6 Governing Law and Venue. This Agreement shall be governed by and construed in accordance with the laws of the District of Columbia. Vendor agrees that: (a) it will subject itself to the exclusive jurisdiction and venue of the courts of Washington, D.C. in any cause of action that may arise under this Agreement; and (b) in any action related to or arising under this Agreement, Vendor will not oppose any motion to transfer venue to any court of appropriate jurisdiction located in any MRM State.

23.7 Severability. If any terms and conditions of this Agreement are held to be invalid or unenforceable as a matter of law, the other terms and conditions shall not be affected and shall remain in full force and effect. To this end, the terms and conditions of this Agreement are declared severable.

23.8 Headings. Section headings and subheadings of this Agreement are for reference purposes only and shall not be construed as part of this Agreement.

23.9 Counterparts. This Agreement may be executed in one or more counterparts, duplicate originals, or facsimile versions (provided that the facsimile versions are confirmed within a reasonable time by signed originals), each of which will be deemed an original, but all of which together will constitute one and the same instrument.

24. SPECIAL TERMS AND CONDITIONS.

24.1 Subject to Funds Availability. The Agreement is subject to the appropriation and availability of funds made available to ITSC via the Consortium states. In the event that the funds are not appropriated or are otherwise unavailable, ITSC reserves the right to terminate the Agreement upon written notice to Vendor. Said termination shall not be deemed a breach of Agreement by ITSC. Upon receipt of the written notice, the Vendor shall cease all work associated with the Agreement. Upon such a termination event, the Vendor shall be entitled to compensation for all satisfactory and authorized services completed as of the termination date, though the Vendor shall have no right to recover from ITSC any actual, general, special, incidental, consequential, or any other damages whatsoever of any description or amount.

24.2 Lobbying. Vendor certifies, to its knowledge and belief, that:

(a) No federally appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of an agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any federal contract, the making of any federal grant, the making of any federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any federal contract, grant, loan, or cooperative agreement.

(b) If any funds other than federally appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Agreement, grant, loan, or cooperative agreement, the Vendor shall complete and submit Standard Form-LLL, “Disclosure Form to Report Lobbying,'' in accordance with its instructions.

(c) Vendor shall require that the language of this certification be included in the award documents for all sub-awards at all tiers (including subcontracts, sub-grants, and contracts under grants, loans, and cooperative agreements) and that all subrecipients shall certify and disclose accordingly.

This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into and is a prerequisite for making or entering into this transaction imposed by section 1352, title 31, U.S. Code.

24.3 Debarment and Suspension. Vendor certifies, to its knowledge and belief, that it, its current and future principals, its current and future contractors and their principals:

(a) are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any federal or state department or agency;

(b) have not within a three (3) year period preceding this Agreement been convicted of, or had a civil judgment rendered against them from commission of fraud, or a criminal offence in connection with obtaining, attempting to obtain, or performing a public (federal, state, or local) transaction or grant under a public transaction; violation of federal or state antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification, or destruction of records, making false statements, or receiving stolen property;

(c) are not presently indicted or otherwise criminally or civilly charged by a government entity (federal, state, or local) with commission of any of the offenses detailed in subsection b. of this certification; and

(d) have not within a three (3) year period preceding this Agreement had one or more public transactions (federal, state, or local) terminated for cause or default.

The Vendor shall provide immediate written notice to ITSC and each of the other Consortium States if at any time it learns that there was an earlier failure to disclose information or that due to changed circumstances, its principals or the principals of its contractors are excluded or disqualified.

24.4 Financial Wherewithal. Quarterly, during the Term, the Vendor shall provide the Consortium States with all information reasonably requested by Consortium to assess the overall financial strength and viability of the Vendor and Vendor's ability to fully perform its obligations under this Agreement, including, but not limited to financial statements prepared in accordance with the requirements of this Agreement. In the event ITSC concludes that Vendor does not have the financial wherewithal to fully perform as required hereunder, ITSC may terminate this Agreement without further obligation or liability by providing written notice to Vendor.

24.5 Federal Funding Accountability and Transparency Act (FFATA). This Agreement requires the Vendor to provide supplies and/or services that are funded in whole or in part by federal funds that are subject to FFATA. Vendor is, therefore, responsible for ensuring that all applicable requirements, including but not limited to those set forth herein, of FFATA are met and that the Vendor provides information to the Consortium States as required by FFATA.

THE PARTIES HERETO HAVE EXECUTED THIS AGREEMENT

Persons signing for Vendor hereby swear and affirm that they are authorized to act on Vendor's behalf and acknowledge that ITSC is relying on their representations to that effect.

FOR VENDOR:	**FOR ITSC:**
Insert Vendor Legal Name	
Name: Insert-Name of Authorized Individual	Name: Insert-Name of Authorized Individual
Title: Insert-Official Title of Authorized Individual	Title: Insert-Official Title of Authorized Individual
By: _____	By: _____
Insert-Name and Title of Authorized Individual	Insert-Name and Title of Authorized Individual
Date: _____	Date: _____

Schedule [●]

Change Order Form

[To be provided in the definitive version of the Agreement.]

Schedule [●]

IaaS Services and Deliverables

[To be provided by ITSC in the definitive version of the Agreement.]

Schedule [●]

Service Levels and Additional Specifications

[Bidder's response to the RFP shall include Bidder's proposal to ITSC for reasonable and appropriate service level measurements governing the operation of the Infrastructure and Services. Such service levels shall be sufficient to ensure that the performance and operation of the Infrastructure and Services meets or exceeds all material requirements set forth in this Agreement and the RFP and to alert ITSC to any failure of the Infrastructure or Services to meet any such material requirements. Bidder's response shall also include an accompanying service level credit structure addressing deviations from applicable service levels. Failure to provide such proposed information may impact the Bidder's scoring. Final service levels and additional specifications will be provided by ITSC in the definitive version of the Agreement.]

Schedule [●]

Terms of Operational Service Agreement

[Bidder's response to the RFP shall include Bidder's proposal to ITSC for reasonable and appropriate operational terms governing the operation, support and maintenance of the Infrastructure and Services following final Acceptance by ITSC or any MRM State. Such operational terms shall include Bidder's proposal for maintenance of the Infrastructure and Services and all services necessary to support use of and access to all Infrastructure and Services by ITSC and each MRM State. Proposed operational terms shall be consistent in all respects with the terms of this Agreement and the RFP, including all service levels and credits proposed by Bidder. Failure to provide such proposed information may impact the Bidder's scoring. Final terms of the Operational Service Agreement will be provided by ITSC in the definitive version of the Agreement.]

Schedule [●]

Compensation

[To be provided by ITSC in the definitive version of the Agreement.]

Schedule [●]

Transition Services

[Bidder's response to the RFP shall include Bidder's proposal for implementing and accomplishing all transition services specified in this Agreement and the RFP. Failure to provide such proposed information may impact the Bidder's scoring. Final terms of the Operational Service Agreement will be provided by ITSC in the definitive version of the Agreement.]

Schedule [●]

Reports

[To be provided by ITSC in the definitive version of the Agreement.]

Schedule [●]

Data Security and Data Privacy

[Terms governing data security and data privacy will be consistent with the requirements of this Agreement and the RFP, including in particular Appendix D of the RFP. Final terms governing data security and data privacy will be provided by ITSC in the definitive version of the Agreement.]

Schedule [●]

Attestation

[To be provided by ITSC in the definitive version of the Agreement.]

APPENDIX D

DATA & NETWORK SECURITY

This Data & Network Security Appendix (this "**Appendix**") is subject to the terms and conditions of the Agreement.

1. DEFINITIONS. Capitalized terms not specifically defined herein shall have the meaning set forth in the Agreement.

1.1 "Data Systems" means all (a) information, computer, or communications systems; (b) Resources comprising any information, computer, or communications system; or (c) means of accessing any information, computer, or communications system.

1.2 "**MRM Data System**" means any Data System owned, controlled, or used by or for ITSC or any MRM State.

1.3 "Network Connection" means a connectivity method to the System or any other MRM Data System.

1.4 "Processing" means any operation in relation to Data, irrespective of the purposes and means applied, including access, collection, retention, storage, transfer, disclosure, use, erasure, destruction, sharing, or any other operation.

1.5 "Security Breach" means any actual, threatened or suspected:

(a) Physical or logical trespass on a facility, Data System and/or any Systems and Infrastructure;

(b) Intrusion/hacking, loss/theft of any Resource upon which Data is Processed;

(c) Unauthorized use, access, alteration, transfer, release, destruction, or other Processing with respect to any Data;

(d) Unauthorized access to or use of the System or any Infrastructure; or

(e) Reported privacy or IT security complaint (regardless of the source of the complaint) in relation to (i) any Data or access to Data, (ii) any Data System, or (iii) any Systems, Infrastructure or other Services or Deliverables.

1.6 "**Vendor Data System**" means any Data System owned, controlled, or used by or for Vendor and comprising part of the System or Infrastructure or accessed or used in the course of providing and Service or other obligation under this Agreement.

2. LOCATION AND SECURITY.

2.1 Redundancy and Location. The System shall provide a fully redundant solution that will provide full business continuity, with primary and secondary datacenters located no closer than 1,000 miles of one another within the continental United States. Vendor shall provide notice to ITSC no less than thirty days prior to any relocation of the primary or secondary data center,

2.2 Security. Vendor shall ensure that all security of Vendor Data Systems meets or exceeds the specifications of the National Institute of Standards and Technology (NIST) 800-53, Federal Information Processing Standard (FIPS) 140-2, IRS Publication 1075, and any other Laws.

2.3 Access. Vendor shall provide representatives of the State access to the primary and secondary datacenters upon reasonable request. Additionally, the secondary data center must be a third party organizationally and legally independent of the primary data center with instructions that the Data must be returned to the state upon dissolution of the organization who owns the primary data center. ITSC and the MRM States shall have access to all Data immediately upon notification presented by certified notice to the contractor, or if the primary contractor is dissolved, the Data must be delivered immediately by the secondary vendor unlocked, accessible and usable immediately by the state. The contractor is required to secure on behalf of the state, insurance to cover liability incurred in the event the Data is not returned unlocked, timely and/or in a useable manner.

3. ACCESS, USE AND DISCLOSURE.

3.1 Vendor shall Process all Data and access MRM Data Systems exclusively for the purpose of performing its obligations under the Agreement unless otherwise authorized in writing by ITSC. Any access to or use of MRM Data Systems and Data by or on behalf of Vendor for any other purpose shall be deemed a material breach of this Appendix and the Agreement by Vendor.

3.2 Vendor expressly agrees that no Data contained in any of the MRM Data Systems to which Vendor is given access under the Agreement (including this Appendix) shall be copied or removed from MRM Data Systems or otherwise disclosed by or on behalf of Vendor without ITSC's prior written consent.

3.3 Vendor shall Process all Data as Confidential Data unless otherwise required by applicable Law or authorized, designated, and/or marked by ITSC in writing.

4. PROTECTING DATA.

4.1 If Vendor is Processing Data on behalf of ITSC or any MRM State, Vendor shall:

(a) Designate in writing a primary and alternate IT security program manager to act as Vendor's contact and focal point for its obligations set out in this Appendix.

(b) Develop, implement and maintain a comprehensive information security program with commercially reasonable safeguards to protect Data and comply with the contractual obligations set out in this Appendix and the Agreement that is in writing and readily accessible to its employees.

(c) Pre-service IT Security Assessment. Prior to providing any Services, permit ITSC, or a 3rd Party chosen by ITSC and reasonably agreed to by Vendor, to perform a security assessment ("**IT Security Assessment**") of the Infrastructure and Vendor's Data Systems and work cooperatively with ITSC to determine whether additional or different security measures are required to protect the Data Processed or proposed to be Processed on behalf of ITSC or any MRM State. As part of the IT Security Assessment, Vendor shall timely disclose to ITSC all relevant information requested by ITSC in order to allow ITSC to make a security risk assessment relating to the Services to be provided by Vendor, the type of Data to be Processed by Vendor and Vendor's data security controls. Vendor agrees ITSC may perform an IT Security Assessment using industry standard tools and manual techniques. Results of an IT Security Assessment shall be treated as Vendor Confidential Information unless disclosure is otherwise required by applicable Law.

(d) Utilize commercially reasonable access control mechanisms to ensure only explicitly authorized users can access Data, including, without limitation, blocking access after multiple unsuccessful attempts to gain access and placing limitation on access to particular Data Systems or sets of Data.

(e) Maintain or establish physical, technical and administrative safeguards that provide for the following:

(f) Protection of business facilities, paper files, servers, computing equipment, including all mobile devices and other equipment with information storage capability, and backup systems containing the Data;

(g) Network, application (including databases) and platform security;

(h) Secure transmission and storage of Data (whether by encryption or other equally protective measures);

(i) Authentication and access control mechanisms; and

(j) Personnel security.

(k) Provide annual training to Vendor's employees and contingent/ temporary workers, who provide any Services, regarding compliance with physical, technical, and administrative IT security safeguards and compliance with this Appendix ("**Annual IT Security Training**").

(l) Require Vendor's subcontractors who provide Services to administer Annual IT Security Training to any of its employees and contingent/ temporary workers who provide Services.

(m) Regularly test and monitor the effectiveness of its security practices and procedures relating to Data and its compliance with the security requirements of the Agreement and this Appendix and adjust its information security program in light of the results of such testing and monitoring, any material changes to its operations or business arrangements, or any other circumstances that Vendor knows or reasonably should know may have a material effect on its information security program.

(n) Impose all security requirements imposed on Vendor under the Agreement and this Appendix on all subcontractors and third parties who have access to or Process Data and perform reasonable ongoing reviews of such subcontractors' capabilities to perform such requirements and compliance with the security requirements of the Agreement and this Appendix.

(o) Ensure all Processing of Data is in accordance with the Agreement and this Appendix and complies with any and all applicable Laws, including but not limited to data protection and privacy laws and regulations. Vendor shall ensure that, where required, Vendor has made the appropriate notifications and registrations and obtained the appropriate permits, as required by applicable Laws. Without prejudice to ITSC or any MRM State's rights and remedies, if Vendor cannot Process the Data in accordance with such applicable Laws, or becomes aware that the appropriate notifications and registrations have not been made in full or that the appropriate permits have not been obtained, then Vendor shall immediately notify ITSC of such circumstances.

(p) Prevent terminated employees from accessing records or systems containing Data.

(q) Impose disciplinary measures for violations of the Vendor's comprehensive information security program.

(r) Meet or exceed the Minimum IT Security Requirements set forth in Exhibit 1 to this Appendix.

4.2 Processing Payment Cards On Behalf of ITSC and/or Cardholder.

(a) If Vendor or any contractor or Vendor will be Processing payment card (including credit, debit card, and/or gift card) information on behalf of ITSC or any MRM State and/or any cardholder, then this Section shall apply to Vendor.

4.3 Vendor warrants that:

(a) As of the Effective Date of the Agreement, Vendor or such contractor is and shall remain fully compliant with the current version Payment Card Industry Data Security Standards ("**PCI DSS**") and any other applicable payment card data security standards, as each may be modified from time to time, at all times when Vendor or such contractor is Processing payment card information as part of the Services pursuant to the Agreement;

(b) Vendor or such contractor shall use (i) an Approved Scanning Vendor (ASV) to perform quarterly network scans (of their network) and (ii) a currently certified Qualified Security Assessor (QSA) to perform the annual onsite PCI Data Security Assessment; and

(c) Upon completion of the Services or termination or expiration of the Agreement, Vendor or such contractor will promptly remove all cardholder Data from its systems in accordance with the required process under PCI DSS or other applicable standard no later than the earlier of ninety days (90) days from cessation of the services or any required time period under PCI DSS or other applicable standard.

4.4 Vendor will give ITSC notice immediately if at any time Vendor or any such contractor is not in compliance with PCI DSS and if at any time Vendor knows or reasonably should know of any third party claim regarding PCI DSS compliance by Vendor or such contractor. If Vendor does not diligently pursue resolution of a claim nor provide ITSC with reasonable assurances that it will pursue resolution, then ITSC may, without in any way limiting its other rights and remedies, defend a third party claim at Vendor's expense.

4.5 **PCI Reporting Requirements**. All Vendor contractors that are considered to be service providers as defined by the PCI-SSC, prior to commencement of any Services, shall provide the following:

(a) A copy of the executive summary from the current Report on Compliance ("**RoC**") or a letter of attestation describing scope and services assessed signed by a PCI-SSC certified QSA and (2) Attestation of Compliance ("**AoC**") signed by a PCI-SSC certified QSA (collectively "**PCI Compliance Documents**").

(b) Thereafter, Vendor shall submit PCI Compliance Documents to ITSC annually for the Term of the Agreement sequentially following the Vendor's annual QSA assessment.

(c) PCI Compliance Documents shall be submitted to ITSC via encrypted email as directed by ITSC.

5. VULNERABILITY SCANNING & IT SECURITY AUDITS.

5.1 **Vulnerability Scanning**. During the term of the Agreement or while Data is Processed by Vendor (whichever is later), Vendor agrees ITSC or any MRM State may perform periodic vulnerability scanning using industry standard tools and manual techniques to assess the security of the System and any Data Systems used by Vendor or comprising part of the System or Infrastructure ("**Vulnerability Scanning**"). As to Vulnerability Scanning which ITSC or any MRM State may conduct, the following shall apply:

(a) Vulnerability Scanning results shall be treated as Vendor Confidential Information unless disclosure is otherwise required by applicable Law;

(b) Vulnerability Scanning performed pursuant to this Section shall comply with the scope limitations set out in this Appendix;

(c) Vulnerability Scanning will be performed by authorized ITSC cyber security professional(s);

(d) Authorized ITSC cyber security professional(s) may work with Vendor to manually validate findings on production and test systems in order to help reduce false positives. Authorized ITSC cyber security professional(s) may also contact Vendor's designated IT security program manager should any additional information or work be required as part of Vulnerability Scanning;

(e) Vendor's IT security program manager will be notified by ITSC of any major security vulnerabilities and such vulnerability notification shall be treated as Confidential Information;

(f) If Vendor utilizes a 3rd party's co-location facility to host any portion of the System or any Data Systems used by Vendor or comprising part of the System or Infrastructure, then Vendor shall be responsible (1) for informing such 3rd party of ITSC's rights under this Section and (2) for ensuring Vendor has written authorization from such 3rd party allowing ITSC or any MRM State to conduct Vulnerability Scanning;

5.2 Routine IT Security Compliance Audit. Upon at least ten (10) calendar days advanced written notice from ITSC, Vendor shall grant ITSC (or a third party on ITSC's behalf) permission to perform a routine, *non-invasive* audit of Vendor's environment in order to ensure compliance with this Appendix, the Agreement, and applicable Laws, regulations, directives, ordinances, and industry standards relative to Vendor's Processing of Data ("**Routine IT Security Compliance Audit**").

5.3 IT Security Audit – Notification of Security Breach. Notwithstanding the previous Section, ITSC (or a 3rd Party on ITSC's behalf) may, in the event of notification by Vendor of a Security Breach, perform a *non-invasive* IT security audit ("**Initial IT Security Breach Audit**") upon one (1) calendar day prior written notice. Additionally, ITSC may conduct follow up IT Security Breach Audits ("**Follow Up IT Security Breach Audit(s)**"), as required, in order to confirm Vendor's corrective actions to any findings addressed in the respective Remediation Plan. An IT Security Breach Audit (whether Initial or Follow Up) will be performed (1) during Vendor's normal business hours, (2) on a date and time mutually agreeable to Vendor and ITSC (3) pursuant to any other restrictions and/or limitations mutually agreed to by the ITSC and Vendor in writing and (4) at ITSC's expense for travel and per diem incurred by ITSC. Vendor shall document Vendor's responsive actions taken in connection with a Security Breach in accordance with all applicable Laws. Subject to the following Section, ITSC or any MRM State reserves the right to be a participant in, and Vendor shall cooperate with such participation in, any Security Breach investigations involving Data, including ITSC or any MRM State's review of forensic data relating to the Security Breach.

5.4 Scope of IT Security Audits, IT Security Assessments & Vulnerability Scanning. IT Security Audits, IT Security Assessments, and Vulnerability Scanning shall not entitle ITSC to view, or in any way access records and/or processes:

(a) Not directly related to Data Processed by Vendor;

(b) Not directly related to the System, Infrastructure, or Services or Deliverables;

(c) In violation of applicable Laws; or

(d) In violation of Vendor's confidentiality obligations owed to any 3rd party.

5.5 During an IT Security Audit, ITSC (or a 3rd Party on ITSC's behalf) may (1) inspect Vendor's facilities where Data is Processed and (2) view copies or extracts of Vendor's records and processes ("**Security Records and Processes**") resulting from Vendor's fulfillment of the requirements of the Agreement, including this Appendix. ITSC reserves the right to perform an IT Security Audit by any of the

following methods: on-site at Vendor facility where Data is Processed, questionnaires with requests for supporting documentation, conference calls, or a combination of such methods.

5.6 Remediation Plan. Any findings during an IT Security Audit will be addressed in a mutually agreed upon remediation plan and Vendor shall comply with, and complete, such remediation plan within a mutually agreeable timeframe set forth therein ("**Remediation Plan**").

6. NOTIFICATION OF INQUIRY. Except where expressly prohibited by applicable Laws, Vendor shall notify ITSC of any subpoena, judicial, administrative or arbitral order or any demand or information request from an executive or administrative agency, other governmental or self regulatory authority, or any user of the System that it receives (each, for purposes of this Appendix, an "**Inquiry**") which impacts Vendor's use or security practices affecting Data Processed on behalf of ITSC. Such notification should include any details of such subpoena, order, demand or request as known to the Vendor ("**Notification**"). Vendor shall use commercially reasonable efforts to provide ITSC with Notification within 12 hours after Vendor becomes aware of an Inquiry.

7. SECURITY BREACH.

7.1 Corrective Action. In the event of any Security Breach, Vendor will take all reasonable and appropriate steps necessary to stop such Security Breach and mitigate any actual, threatened or suspected harm or further disclosure, loss, or destruction of Data.

7.2 Notification of ITSC and Affected MRM States. Vendor will promptly notify ITSC and each affected MRM State after (but in no case more than 24 hours after) Vendor becomes aware of, or reasonably should have become aware of any Security Breach or any similar incident that has, or might have, compromised the security of any Data Processed by or otherwise in the possession or control of Vendor or led to the unauthorized or unlawful use of or access to any such Data.

7.3 Investigation and Remediation. Vendor will diligently investigate the Security Breach as instructed by ITSC and develop a corrective action plan for approval by ITSC addressing correction and remediation of the Security Breach and the effects thereof. However, notwithstanding the foregoing, if time is critical and if ITSC and/or the affected MRM States cannot be reached, Vendor will take corrective action prior to approval of such plan, including:

(a) Confirm the actual, threatened or suspected breach of security;

(b) Deny access from the source of the attack;

(c) Investigate the extent of the damage, if any;

(d) Backup the affected systems and those suspected to be affected;

(e) Strengthen defenses everywhere, not just the suspected path that the attacker used;

(f) Contact the internet service provider where the threat or attack originated and/or law enforcement to work with Vendor's security team;

(g) Produce an incident report within twenty-four (24) hours detailing Vendor's findings;

(h) Re-state the denial of access after a set time period, but continue to monitor traffic from that source until risk of further attacks is deemed by ITSC and the Consortium States to be minimized; and

(i) At the request of ITSC or any affected MRM State, provide no-cost credit monitoring services for individuals that are deemed to be part of a potential disclosure.

Following approval of Vendor's corrective action plan by ITSC, Vendor shall implement the plan and correct and remediate the effects of the Security Breach to the reasonable satisfaction of ITSC and each affected MRM State.

7.4 Notifications of Individuals. If a Security Breach requires notification to any impacted or potentially impacted individual or group under any applicable Law or in the reasonable judgment of ITSC or any MRM State, then ITSC and the applicable MRM State(s) shall have sole control over the timing, content, and method of all such notifications. Except as may be required by Law, Vendor will take no action with respect to any such notification without ITSC's express consent and instruction. Vendor acknowledges that ITSC and the affected MRM States may release any information Vendor provides to them in connection with the Security Breach as required for them to comply with applicable Law or other applicable obligations. Without operating as any limitation on potential damages caused by such breach, Vendor shall bear the cost of notification to individuals having personal identity information involved in a potential disclosure event, including individual letters and/or public notice.

7.5 Correction and Reconstruction. Vendor will, at Vendor's sole expense, promptly correct any errors or inaccuracies in any Data attributable to Vendor. Vendor will further develop and maintain procedures for the reconstruction of any lost, damaged, or corrupted Data, and Vendor will, at Vendor's sole expense, correct any errors in, or destruction, loss, corruption, or alteration of, any Data. At ITSC's request, Vendor will promptly correct any errors in, or destruction, loss or alteration of, Data.

7.6 Information and Assistance. Throughout all activity relating to any Security Breach, Vendor shall promptly provide ITSC and each MRM State with such additional information and assistance not stated herein as is requested by ITSC or any MRM State, whether or not such information and assistance is required by applicable Law.

8. NETWORK CONNECTIVITY & NETWORK SECURITY.

If Vendor is (1) utilizing a remote Network Connection or (2) utilizing a Network Connection at an ITSC facility to Process Data, this Section shall apply to Vendor.

8.1 Vendor's Use of Network Connection (either remote or at an ITSC facility).

(a) Vendor may only use only ITSC-approved Network Connections.

(b) Vendor may only use Network Connections for purposes of providing the Services and performing any other obligations of Vendor under this Agreement, as authorized by ITSC or any MRM State.

(c) Each Network Connection and any other mechanism to transmit Data between Vendor and ITSC shall be through a ITSC I/T approved secure solution and pursuant to a written agreement between the parties.

(d) Vendor's duration of access to a Network Connection shall be restricted to only when access is required.

8.2 Use of Vendor-Owned Equipment at ITSC or MRM State facilities.

(a) ITSC or an MRM State may, in ITSC's or any MRM State's sole discretion, authorize Vendor to utilize Vendor-owned equipment in ITSC or MRM State facilities ("**Vendor-Owned Equipment**").

(b) Vendor-owned equipment must conform to the applicable security standards set forth in this Appendix.

(c) Vendor-owned equipment used in ITSC or any MRM State facilities may be monitored and scanned for Appendix compliance, including vulnerability and patch scanning.

8.3 Security of ITSC and MRM State Networks.

(a) Vendor will allow only Vendor's employees who are approved in advance by ITSC ("**Authorized Vendor Employees**") to authenticate and access the ITSC's or any MRM State's Network. Vendor shall be solely responsible for ensuring that Authorized Vendor Employees are not security risks, and upon ITSC's or any MRM State's request, Vendor will provide ITSC or any MRM State with any information reasonably necessary for ITSC or that MRM State to evaluate security issues relating to any Authorized Vendor Employee.

(b) Vendor will promptly notify ITSC whenever any Authorized Vendor Employee leaves Vendor's employ or no longer requires access to ITSC's or any MRM State's Network.

(c) Each party will be solely responsible for ensuring their security procedures and policies are sufficient to ensure that (a) such party's use of the Network Connection is secure and is used only for authorized purposes, and (b) such party's business records and Data are protected against improper access, use, loss alteration or destruction.

8.4 Notifications. Vendor shall notify ITSC in writing promptly upon a change in the user base for the work performed over any Network Connection or whenever, in Vendor's opinion, a change in the connection and/or functional requirements of any Network Connection is necessary.

8.5 Upon request, Vendor shall provide ITSC with a network diagram that outlines Vendor's IT network involved in Processing access to Data.

9. DATA RETENTION.

9.1 During Agreement Term.

(a) During the term of the Agreement, Vendor shall retain and destroy Data in accordance with any data retention policy provided to Vendor by ITSC or any Member State ("**Data Retention Policy**").

(b) If Vendor cannot retain such Data for the time period agreed to in the Data Retention Policy, Vendor will regularly provide such Data to ITSC or the applicable MRM State to retain.

(c) In the absence of such Data Retention Policy, Vendor will either return or dispose of any and all Data, including without limitation any and all copies and derivatives that that are no longer needed throughout the Term of the Agreement in a manner consistent with the terms of this Agreement, applicable Law, and Vendor's internal records retention policy. Prior to any return or disposal of Data, Vendor will provide a certificate or attestation of destruction to ITSC.

9.2 Termination or Expiration of Agreement.

(a) Unless otherwise agreed to by ITSC or any MRM State, at ITSC's option and written direction, no later than 30 calendar days after the termination or expiration of the Agreement or any portion thereof, Vendor shall promptly return to ITSC and each MRM State, in the format and on the media requested by ITSC and each MRM State, all Data (or such portion as requested by ITSC or any MRM State).

(b) In addition, Vendor shall thereafter: (1) dispose of all Data, including, without limitation, any and all copies and derivatives thereof, in a manner consistent with this Agreement and applicable Laws no later than 90 calendar days after the termination or expiration of the Agreement or portion thereof; or (2) return all existing copies of all Data to ITSC or ITSC's designated recipient.

(c) Upon ITSC's request, Vendor shall present ITSC with a written and signed certification or attestation of such completion of Data return and/or disposal.

(d) If ITSC has a reasonable basis to be concerned about the unauthorized, continued retention of Data by Vendor after termination or expiration of the Agreement, upon ITSC's written request and at ITSC's expense, Vendor shall obtain an external audit to ensure total removal of Data from Vendor's systems. ITSC has the right to oversee the audit and obtain the audit results. If the audit conclusively supports Vendor's continued retention of Data after termination or expiration of the Agreement, then Vendor shall reimburse ITSC the full cost of the audit.

9.3 Data Placed on 'Legal Hold'. Occasionally, ITSC's legal department will designate certain Data as subject to a "Legal Hold." Vendor will not block, erase or dispose of any Data which Vendor has been notified it must retain in response to an ITSC "Legal Hold" unless required to do so by applicable Laws. In the event that Vendor believes it is legally required to destroy Data on Legal Hold, Vendor must notify, consult and cooperate with ITSC prior to any disposal. Vendor's obligation to retain such "Legal Hold" Data exceeds any agreed-to records or data retention policies or internal policies of Vendor. If Vendor cannot retain the "Legal Hold" Data, Vendor will provide the Data to ITSC for ITSC to retain.

10. REQUIRED USE OF CRYPTOGRAPHY.

During transit over any unsecure network or wirelessly (including but not limited to email, instant messaging and web traffic), Confidential Information must be encrypted.

10.1 Portable Devices & Removable Media. Confidential Information, stored on portable devices and/or removable media, including but not limited to laptops, PDAs, memory sticks, flash drives, portable backup drives, Compact Flash (CF) card, hot swappable disk drives, digital camera memory cards, CDs, and DVDs, must be encrypted if such Confidential Information is removed from the protections of Vendor's facilities.

10.2 Media In Transit. Confidential Information stored on portable devices or removable media in transit between Vendor's facility and another physical location must be encrypted.

11. DISASTER RECOVERY.

11.1 Unless otherwise waived by ITSC in writing, Vendor shall maintain a disaster recovery plan acceptable to ITSC for restoring its current and off-site Data files Processed pursuant to the Agreement.

11.2 Unless otherwise waived by ITSC in writing, Vendor will be responsible for backup and preservation of any Data Processed on behalf of ITSC or any MRM State. All backup copies of Data shall be treated as Confidential Information.

11.3 Unless otherwise waived by ITSC in writing, Vendor will maintain a business continuity plan acceptable to ITSC for restoring its critical business functions. Upon request, Vendor will allow ITSC or any MRM State to view such plan.

Exhibit 1 to Appendix
MINIMUM IT SECURITY REQUIREMENTS

This document sets forth minimum IT security requirements required by ITSC and the MRM States. Vendor either shall meet or exceed these requirements at all times while providing any Services.

1. SYSTEM SECURITY

1.1 System Administration

(a) Accounts with administrative privileges, such as root or administrator, must not be used unless a specifically approved administrative task is only possible with such an account. Use of the administrative account must be discontinued when the task is complete.

(b) Batch system administration activities, such as daemons, jobs, and scripts, must not run with administrative privileges unless no alternative exists.

(c) Each account with administrative privileges must be assigned to a specific, traceable and uniquely identifiable individual. Administrative tasks must be traceable to a uniquely identifiable individual.

(d) System accounts or built-in application accounts must not be used to provide generic or unauthorized access.

1.2 Account Management

(a) Only those accounts required for effective information access, ongoing operation, and maintenance of the host are permitted. All other accounts must be removed or disabled.

(b) Each account must be assigned to either a specific, traceable and uniquely identifiable individual who is a regular user of the system or to the system managers.

(c) All accounts must be reviewed at least annually to determine if they are still required. When a user's affiliation with contractor terminates, assigned accounts must be disabled or deleted immediately.

(d) All accounts that utilize passwords for authentication must use passwords that comply with the Appendix to which this Exhibit 1 is attached and are not Vendor-provided defaults.

(e) Only those services and protocols required supporting applications set out in the Agreement may be enabled. All others must be explicitly disabled.

(f) All accounts must maintain effective control of user IDs and other identifiers.

1.3 Logging, Verification, and Audit

(a) Vendor must protect the following as Confidential Data:

(i) Information related to the physical location of where the Data is stored (whether Data is stored at an ITSC or any MRM State site or at a Vendor's site);

(ii) Configuration of systems which store Data; and

(iii) Security and management practices in place to protect Data from unauthorized disclosure.

(b) Documented processes must exist to verify system configuration, detect security vulnerabilities, validate system integrity, and promptly respond to any deficiencies detected. These

documented processes must be used to log, detect, report, and resolve any events which may compromise the security of the system. This includes but is not limited to: access to critical files and successful or failed user authentication.

(c) Details of the installation of security relevant patches must be maintained; details include, but are not limited to, the following:

(i) Unique name and IP address of the system or device;

(ii) User id of the system manager who applied the patch;

(iii) The specific application, OS, middleware, etc. being patched;

(iv) Date;

(v) Time;

(vi) Vendor patch designation; and

(vii) Version information.

(d) Acceptable maintenance mechanisms include, but are not limited to, manual logs, change management logs, and configuration databases. It is also acceptable to leverage native auditing features of the system.

(e) Installation and removal of application programs or operating system must be logged.

(f) Denied access attempts to critical files must be logged.

(g) All authentication transactions must be logged.

1.4 Logical Access Control. All access to the system must be authenticated. This includes console access, individual accounts, administrative accounts, and any automated relationships with other systems.

1.5 Physical Security. The following requirements must be adhered to in Vendor's facilities where Data is located:

(a) Access to areas where ITSC-Owned Equipment is stored, regardless of whether it contains Data, must be controlled and restricted to authorized persons only and authentication controls, e.g. access control card, must be used to authorize and validate the access; an audit trail of all access, including times, must be securely maintained;

(b) The date and time of entry and departure of visitors must be recorded, and all visitors must be escorted and supervised; they must only be granted access for specific, authorized purposes and must be issued with instructions on the security requirements of the area and on emergency procedures;

(c) Access to areas where Data is Processed must have physical separation, such as cages or secured doors, and must be controlled and restricted to authorized persons only;

(d) Authentication controls, e.g. access control card, must be used to authorize and validate all access and an audit trail of all access must be securely maintained;

(e) Systems must be protected against interference with configuration or continued operation; and

(f) Video camera surveillance must not capture keyboard and/or console actions and information.

(g) Hardcopy materials must be destroyed when no longer needed for business or legal purposes in a manner which ensures that Data cannot be reconstructed. One of the following destruction methods must be used: confetti cut, cross cut shred, incineration, or pulping of the hardcopy materials. All hardcopy disposal containers must be secured with tamper proof locks.

1.6 Media Reuse and Disposal

(a) All media must be securely erased electronically, by overwriting or degaussing, or else physically destroyed prior to disposal or reassignment of the system. The media sanitization procedures must follow the procedures, particularly those in clause 5 and appendix A, contained in NIST SP 800-88, Guidelines for Media Sanitization, which can be found at http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf or any successor thereto (the "NIST Guide").

(b) The following criteria must be used for media sanitization:

(i) If the media is rewriteable, then a purge procedure recommended in the NIST Guide must be used on the media. If degaussing will render the media unusable and destruction is not the intent, then computer software purge techniques may be used where applicable. When computer software purge is not an available option, then the media must be degaussed, even when it leads to destruction.

(ii) If the media is not rewriteable, the media must be destroyed following the procedures in the NIST Guide.

1.7 Backup and Recovery

(a) Systems must have a formal backup/recovery strategy and plan that must be periodically tested, and a record of tests and results maintained for audit.

(b) Backup media must be protected against unauthorized disclosure, alteration, or destruction. Possible mechanisms include, but are not limited to, cryptographic transformation and physical controls.

1.8 Anti-Virus Configuration. Any system that stores Windows files must have current anti-virus computer software configured for automatic updates no less than once per week.

1.9 Endpoint Protection. All systems that that Access Data must have reasonable up-to-date versions of system security agent computer software which must include host firewall, malware protection and reasonably up-to-date patches and virus definitions.

2. MALICIOUS USE OF SOFTWARE OR HARDWARE

2.1 Disallowed Uses of Hardware or Software. No hardware or computer software used in or in support of the System or any Infrastructure must ever be used for any malicious purpose.

2.2 Approved Use of Diagnostic Tools

(a) Diagnostic tools may be used to support applications, computing systems, and networks. Diagnostic tools may only be used by personnel whose job function requires usage and usage must be limited to those applications, computing systems, and networks within the person's scope. Tools that might impact the performance of the services provided pursuant to the Agreement through degradation of availability or performance must receive approval from ITSC before they are used.

(b) Data gathered as a result of sniffing any network traffic, whether by placing a Network Interface Card (NIC) into promiscuous mode or by any other means, must be properly protected against

unauthorized disclosure, alteration, and destruction. Such Data must only be stored if necessary and must be immediately and securely disposed of when no longer needed.

3. PROTECTION OF PASSWORDS

3.1 Password Protection

(a) Passwords shall be stored in a protected fashion.

(b) Users must be able to change their own passwords.

(c) Each user is accountable and responsible for any action taken with that user's User ID or Username and password. No users working for Vendor should ever share or divulge their password to anyone.

(d) Passwords must be protected at all times during their lifecycle (from generation to storage, delivery, and usage), and measures must be taken to ensure no disclosure to any unauthorized person or entity. Initial passwords must be changed by the user on first use.

(e) Temporary passwords must be changed immediately upon the completion of the assigned task.

(f) The display and printing of passwords must be masked, suppressed, or otherwise obscured such that unauthorized parties will not be able to observe or subsequently recover them. Passwords must not be logged or captured as they are being entered.

(g) Passwords must be encrypted when transmitted across any network.

(h) User passwords must not be stored or used in clear text for the purpose of automating a login sequence

(i) Password change processes must not circumvent password security controls.

(j) All passwords must be promptly changed if they are suspected of being compromised or known to have been disclosed to unauthorized parties.

3.2 Password Selections

(a) Password Complexity Requirements. Password must be enabled using the capabilities provided by the specific technology being implemented. The complexity level implemented on each system must be documented, should never be less than 3 out of 4 character classes and must have character class choices such as upper case letters, lower case letters, numeric digits, or special characters (such as $, &, #, @, etc).

(b) Password Length Requirements. Password for each technology must be chosen to mitigate the risks associated with known password length vulnerabilities and must be documented. In no case may the password length be configured to be less than eight (8) characters.

(c) When provided by the specific technology being implemented, a mechanism must be in place to prevent the reuse of at least the last six (6) passwords.

3.3 Password Lockout. When provided by the specific technology being implemented, accounts must be set to lockout on not more than ten (10) consecutive failed login attempts.

3.4 Password Expiration. Passwords must be changed at regular intervals commensurate with the password length. For a password length of eight (8) characters, it is expected that the password be changed every 90 days.

4. APPROVED CRYPTOGRAPHY

4.1 Key Lifecycle

(a) Keys must be generated in a secure manner.

(b) Keys must only be available to authorized users.

(c) Keys must be protected from unauthorized use, disclosure, alteration, and destruction.

(d) If the private key associated with an asymmetric key pair is compromised for any reason, all associated certificates must be revoked.

(e) Keys must have an appropriate lifetime after which they are securely destroyed.

4.2 Approved Cryptography. Approved cryptography is set out in this Section.

5. Use of Symmetric Ciphers

(a) The AES block cipher, the triple DES block cipher, the Blowfish cipher, the Twofish cipher, the DES-X block cipher, and the RC2 block cipher are approved for all purposes except disk volume encryption and tape encryption, when used in CBC, CFB, or OFB modes.

(b) For disc volume encryption, AES-LRW, AES-XTS, and AES-CBC with the Elephant diffuser are approved.

(c) For tape encryption, AES-GCM is approved.

(d) The RC4 stream cipher is approved for all purposes except protecting stored Data.

(e) Only the TACACS+ stream cipher described here is approved for use with the TACACS+ protocol.

(f) Unless prohibited by applicable Law, symmetric ciphers must use an effective key length of at least 112 bits.

(g) If a secret key is compromised, it must be changed, and all information assets protected with that key must be protected with the new key.

6. Use of Asymmetric Ciphers

(a) The RSA algorithm is approved for performing authentication and digital signature.

(b) Unless prohibited by applicable Law, when the RSA cipher is used for authentication or digital signature, the public modulus must be at least 1024 bits.

(c) The RSA algorithm is approved for performing key transport.

(d) Unless prohibited by applicable Law, when the RSA cipher is used for key transport, the public modulus must be large enough to ensure protection of the key in transport.

(e) The US Digital Signature Standard (DSS) is approved for performing digital signatures.

(f) The Diffie-Hellman algorithm is approved for key agreement.

(g) In a Diffie-Hellman key agreement, the prime, p, must be large enough to generate sufficient bits for the intended use of the resulting key.

(h) The ElGamal algorithm is approved for use with the OpenPGP protocol. The prime, p, must be at least 1024 bits.

7. Use of Hash Algorithms

(a) The SHA-1, SHA-256, SHA-384, and SHA-512 hash algorithms are approved for performing digital signatures and HMACs.

(b) The MD5 hash algorithm is approved for HMACs.

(c) **RIPE-MD/160 Algorithm**. RIPE-MD/160 algorithm is approved for use with the OpenPGP protocol.

(d) Any other cryptography approved by ITSC.

8. NETWORK SECURITY

8.1 Network Operations and Management

(a) Vendor must provide an intrusion detection system to monitor, detect, and report misuse patterns, suspicious activities, unauthorized users, and other actual and threatened security risks to Data. Vendor shall make available, in an expedited manner if so requested, the necessary support to implement any changes required to maintain the security of the Data/information and the host and application system.

(b) Vendor's intrusion detection system must provide the ability to capture Data/information for audit purposes of all actual and suspected access exceptions and make such Data/information available to ITSC or any MRM State upon request.

(c) Vendor must create procedures describing any reconfiguration of any ITSC or MRM State Data System.

(d) Vendor's procedures for adding, changing, or removing network devices must ensure that permitted network or network device access controls are not violated. Established procedures for network reconfiguration must be followed.

8.2 Network Access Controls

(a) Networks managed on behalf of ITSC or any MRM State must have dedicated separately-defined logical domains or network compartments, each protected with suitable security perimeters and access control mechanisms. All such networks must implement bi-directional anti-spoofing filters on network boundary devices.

(b) Network access control devices between networks managed on behalf of ITSC or any MRM State and uncontrolled networks must not allow access by default; "deny all" shall be the default state. Networks, addresses, protocols, and ports must be specifically authorized before access is permitted between networks managed on behalf of ITSC or any MRM State and any other networks. Network access controls must not be circumvented.

(c) Network controls defined by network standards must be minimally met. It is permitted to implement controls that exceed the requirements of network standards.

8.3 **Third-Party Data Transit**. Third-party data transit, e.g. from one Third-Party to another Third-Party, must not take place through any network managed on behalf of ITSC or any MRM State.

9. SECURITY EVENT LOGGING

9.1 **Devices and systems requiring security event logging**. The following devices and systems when used as part of the security controls hosting or protecting ITSC or any MRM State systems or Data must provide auditable logs of security events:

(a) Network and application firewall devices Network devices that implement Network Address Translation (NAT) and proxy servers;

(b) All server platforms;

(c) Database management systems;

(d) Application middleware; and

(e) Physical Access Control Systems (badge readers, etc.).

9.2 Timestamp

(a) All systems, devices, and applications that generate or store logs of security events must maintain an accurate clock synchronized with a reliable source.

(b) Log entries must contain the date and time at which the event occurred, including appropriate time zone information. Log entries should be stored in Coordinated Universal Time (UTC).

9.3 Log Entry Content

(a) Log entries must indicate the subject, the object, and the type of transaction.

(b) Whenever possible, log entries for distributed transactions must indicate the network address of the subject.

(c) Logs stored or recorded on different systems, such as a logging server, must indicate the system generating the log entries.

9.4 Log Access Control. Logs must be labeled as "Confidential" and must be protected from unauthorized disclosure, alteration, and destruction.

9.5 Log Retention

(a) Unless otherwise specified, log entries must be retained for a period of 180 days unless provided otherwise pursuant to applicable Laws. Whenever the retention times expressed in this standard conflict with applicable Law, such as privacy law, the applicable Law takes precedence.

(b) Whenever technically feasible and practical, log entries must be retained and accessible on-line for the duration of the retention period. When log entries are stored off-line, it must be possible to retrieve an on-line copy within two (2) business days.

9.6 Log Review and Reporting. Processes must be in place for either automated or human review of security-significant events. Implementations must specify and document log review and reporting procedures.

Appendix E

MRM Consortium High Level
Deployment Schedule

Production Environment Deployment Schedule			
Task	**Start Date**	**End Date**	**Responsibility**
Cloud Infrastructure Setup	11/30/2015	3/7/2016	Cloud Vendor
Mississippi Benefits and Tax Go Live	4/11/2016	4/18/2016	Cloud Vendor, TCS, MDES
Maine Setup for Benefits Environment	4/22/2016	6/2/2016	Cloud Vendor, TCS, Maine
Maine Benefits Go Live	6/6/2016	6/10/2016	Cloud Vendor, TCS, Maine
Maine Setup for Tax Environment	6/14/2018	7/26/2018	Cloud Vendor, TCS, Maine
Maine Tax Go Live	7/29/2018	8/8/2018	Cloud Vendor, TCS, Maine
Rhode Island Setup for Benefits Environment	6/17/2016	7/29/2016	Cloud Vendor, TCS, Rhode Island
Rhode Island Benefits Go Live	8/1/2016	8/5/2016	Cloud Vendor, TCS, Rhode Island
Rhode Island Setup for Tax Environment	7/23/2017	9/3/2017	Cloud Vendor, TCS, Rhode Island
Rhode Island Tax Go Live	9/6/2017	9/16/2017	Cloud Vendor, TCS, Rhode Island

Staging Environment Deployment Schedule			
Task	**Start Date**	**End Date**	**Responsibility**
Cloud Infrastructure Setup for all 3 states	11/30/2015	2/5/2016	Cloud Vendor

Appendix F

Infrastructure Sizing Specifications

UI Applications Servers	OS Version	MS Server Count	ME Server Count	RI Server Count	Total Server Count	Avg CPU Utilization (MHz)	Peak CPU Utilization (Mhz)	Total Avg CPU Utilization (mHz)	Total Peak CPU Utilization (Mhz)	RAM GB / Svr	Total RAM GB	Disk GB / Svr	Total Disk GB
Production Environment (Separate Line Item)													
Workflow server	Linux	1	1	1	3	100	200	300	600	4	12	80	240
Single Sign-on server	Linux	2	0	0	2	200	300	400	600	8	16	80	160
IBM WebSphere App Server	Linux	2	2	2	6	2,000	3,000	12,000	18,000	8	48	100	600
IBM WorkLight server	Linux	1	1	1	3	200	300	600	900	8	24	300	900
Biz and batch server	Linux	1	1	1	3	600	2,000	1,800	6,000	8	24	230	690
IBM HTTP Server	Linux	2	2	2	6	150	300	900	1,800	4	24	80	480
DMS / Jreport Server /BIRT server	Linux	1	1	1	3	1,000	3,000	3,000	9,000	8	24	950	2,850
DB2 10.5 Server	Linux	1	1	1	3	4,000	10,000	12,000	30,000	24	72	700	2,100
Directory Server	Linux	2	2	2	6	250	600	1,500	3,600	8	48	80	480
TOP FTP Server	Windows	1	1	1	3	200	400	600	1,200	4	12	120	360
Jscape server	Linux	1	1	1	3	1,000	1,500	3,000	4,500	4	12	80	240
IBM DB2 Gateway Server	Linux	1	1	1	3	50	200	150	600	4	12	80	240
IBM SCAPM Server	Linux	1	1	1	3	300	600	900	1,800	8	24	80	240
IBM Optim Performance Mgr.	Windows	1	1	1	3	700	1,500	2,100	4,500	4	12	100	300
IBM Cognos Server	Windows	1	1	1	3	900	2,000	2,700	6,000	24	72	500	1,500
							Total	41,950	89,100		436		11,380
Production Common Environment (Separate Line Item) **Servers provide services to production environments for all states**													
Group 1 server	Linux				1	500	1000	500	1,000	2	2	80	80
Occucoder	Windows				1	100	600	100	600	2	2	80	80
							Total	600	1,600		4		160

UI Applications Servers	OS Version	MS,ME & RI Combined	Total Server Count	Avg CPU Utilization (MHz)	Peak CPU Utilization (Mhz)	Total Avg CPU Utilization (mHz)	Total Peak CPU Utilization (Mhz)	RAM GB / Svr	Total RAM GB	Disk GB / Svr	Total Disk GB
Shared Staging Environment (Separate Line Item)											
Workflow server	Linux	1	1	100	200	100	200	4	4	80	240
Single Sign-on server	Linux	2	2	200	300	400	600	8	16	90	180
IBM WebSphere App Server	Linux	2	2	2,000	3,000	4,000	6,000	8	16	100	600
IBM WorkLight server	Linux	1	1	200	300	200	300	10	10	300	900
Biz and batch server	Linux	1	1	600	2,000	600	2,000	8	8	230	690
IBM HTTP Server	Linux	2	2	150	300	300	600	8	16	80	480
DMS / Jreport /BIRT servers	Linux	1	1	1,000	3,000	1,000	3,000	8	8	950	2,850
DB2 10.5 Server	Linux	1	1	4,000	10,000	4,000	10,000	24	24	700	2,100
Directory Servers	Linux	2	2	250	600	500	1,200	8	16	80	480
Group 1 server	Linux	1	1	500	1,000	500	1,000	8	8	80	80
Occucoder	Windows	1	1	100	600	100	600	2	2	80	80
IBM Cognos server	Windows	1	1	900	2,000	900	2,000	24	24	500	500
					Total	12,600	27,500		152		9,180

Production Hardware Appliance (Separate Line Item) **- Provided by MRM Consortium**

MRM Consortium supplied appliance (hardware)	OS Version	MS Server Count	ME Server Count	RI Server Count	Total Server Count	Avg CPU Utilization (MHz)	Peak CPU Utilization (Mhz)	Total Avg CPU Utilization (mHz)	Total Peak CPU Utilization (Mhz)	RAM GB / Svr	Total RAM GB	Disk GB / Svr	Total Disk GB
Vormetric DSM - 1U	N/A	1	1	1	3	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
IBM Infosphere Guardium - 1U	N/A	1	1	1	3	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
IBM DataPower XG45 - 1U	N/A	1	1	1	3	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
							Total	0	0		0		0

N/A - Not Applicable

Note: Provide separate costs for additional virtual machines, CPU, memory and disk space by production and staging environments.

APPENDIX G

Addendum A

Request for Proposal:

Infrastructure as a Service Request for MRM Consortium

May 4, 2015

1. Introduction

This document contains the technical insight of why MRM, as part of its IaaS Vendor RFP, is requesting IaaS Vendors to deploy certain hardware and virtual appliance as part of the IaaS service. If the IaaS Vendor is not able to deploy these appliances' as highlighted in section V. Proposal Requirements; Section E. Proposal Plan; Number 5. Hardware Software on page 12, IaaS Vendor is requested to provide alternate viable solutions that can meet or exceed the MRM security requirements while remaining cost effective.

2. Background

Mississippi currently utilizes the below appliances in their production center:

1. Vormetric DSM
2. Guardium
3. DataPower (procured but not deployed)

These appliances are used to satisfy certain security requirements as published in IRS Publication 1075.

The below table describes the major security requirements fulfilled by these appliances. Mississippi and the MRM Consortium would prefer to leverage these investments and use them as part of the IaaS Vendor's solution.

S No	Appliance	Appliance Type	Major Security Requirements
1.	Vormetric Data Security Manager (DSM) - 1 Appliance along with a failover option, Per State	Hardware (1 Unit)	• Data at rest encryption e.g. for DB2 database, data files with FTI (Federal Tax Information) data and etc. • Encryption must be using FIPS 140-2 cryptographic modules. NIST maintains a list of validated cryptographic modules on its website at http://csrc.nist.gov/ . Vormetric DSM is on this list. • Control of the encryption keys will be with the MRM i.e. at each state level.
2.	IBM Guardium – 1 Virtual Appliance, Per State	Virtual	• Recipients of FTI are allowed to use a shared facility but only in a manner that does not allow access to FTI by employees, agents, representatives or contractors of other agencies using the shared facility.

S No	Appliance	Appliance Type	Major Security Requirements
			• It is recommended that FTI be kept separate from other information to the maximum extent possible to avoid inadvertent disclosures. To fulfil the above set of requirements of having secure access to the database which contains both the UI (unemployment insurance) and FTI data, Mississippi makes use of the Guardium appliance to manage the ACL (access control list). Security policies are added to the appliance and it not only audits and reports access to the sensitive FTI data but actively blocks and quarantines unauthorized users and access until administrators can determine their intentions.
3.	IBM DataPower (XG45) – MRM Consortium is evaluating IBM DataPower. 1 Appliance along with a failover option, Per State	Hardware (1 Unit)	• Hardened appliance purpose-built Service Gateway and load balancer. • Load Balancer with a capability to terminate SSL sessions and encrypt FTI data elements before forwarding to the backend application servers • Hardware based SSL accelerator providing much better throughput • Configurable ciphers such as AES 256 • With additional Application Optimization (AO) module, it can easily integrate with IBM WebSphere Application Server for direct load balancing the request among the members of the application server cluster.

3. Proposal Requirements

3.1 FedRAMP certified IaaS Vendor Requirement

One of the mandatory requirements of the RFP is for the IaaS Vendor is to be FedRAMP certified. If the FedRAMP certification restricts the IaaS Vendor to not host any customer owned appliances, IaaS Vendors are requested to provide alternate solutions that meet the above requirements and be cost effective.

3.1.1 Assumption

FedRAMP may restrict customer owned hardware appliances and not virtual appliances. Alternate solutions may only be proposed for Vormetric DSM and DataPower gateway and load balancer.

3.2 Load Balancer Security Requirements

IaaS Vendor must explain how they will secure FTI data elements on the Load Balancer and data in transit from the Load Balancer to the Application Server as per IRS Publication 1075.

3.3 MRM Proposed Alternate Solution for Vormetric

IaaS Vendor will support the VPC (virtual private cloud) where the Vormetric DSM is hosted at the agencies' (each state's own) data center. The state's data center will connect to IaaS data center via secure VPN or other private and secure direct connection.

3.4 Managed Service Partner, Subcontractor or Agent

IaaS Vendors and Managed Service Providers may propose and partner with one another in response to this RFP. Proposals must identify which vendor will be the prime and sub-contractor. Additionally, Vendors must specifically address their and the proposed partner's role and duties. Pricing should be broken out by prime and sub-contractor costs. Copies of agreements to be executed between the Vendor and partner must be included in the IaaS Vendor's proposal. ITSC and MRM consortium has the option of selecting either partnered or IaaS Vendor bids.