Addendum A

Request for Proposal:
Infrastructure as a Service Request for MRM Consortium

May 5, 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. • It is recommended that FTI be kept separate from other information to the maximum extent possible to avoid inadvertent disclosures.

S No	Appliance	Appliance Type	Major Security Requirements
			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.