

Memorandum

To: State Entity IT Directors and Purchasing Agents

From: David L. Litchliter 

Date: January 8, 2010

Re: Payment Card Industry (PCI) Compliance Audit Services - Instructions for Use

CC: ITS Project File Number 37081

The Mississippi Department of Information Technology Services (ITS), in conjunction with the Mississippi Department of Finance and Administration (DFA), has established a procurement vehicle for use in obtaining PCI compliance audit services. The services on this list were procured by ITS on behalf of state entities via Request for Proposal (RFP) No. 3532 and meet Mississippi requirements for legal purchases.

Instructions for Use

- **Agency Required Use**

State agencies that process, transmit, and/or store cardholder information are required to use RFP No. 3532 to obtain PCI compliance audit services as outlined in *DFA Administrative Rule for Payment by Credit Card, Charge Card, Debit Cards or Other Forms of Electronic Payment of Amounts Owed to State Agencies* in accordance with §27-104-33, Mississippi Code of 1972. PCI compliance is required, regardless of the payment channel used (mail, telephone or e-commerce) or transaction volume. Audit results will be supplied to DFA and ITS as proof of compliance.

- **Scope**

RFP No. 3532 includes self assessment questionnaire, scanning, and remediation planning services required to meet PCI Data Security Standard (DSS) compliance in both internet and customer facing (card present) environments. This procurement does not include the remediation work required to satisfy/resolve any audit findings. If remediation services are required, procurement of those services should follow established policy for procurement of IT services. Refer to the Procurement Handbook via the ITS Web Site (www.its.ms.gov) for further information or call the ITS Procurement Help Desk at 601 576-HELP.

The detailed scope of services is listed below.

- The awarded vendor, Coalfire Systems, Inc. (Coalfire), will conduct an initial meeting with each entity to clarify any questions or requirements and to review each entity's payment card environment (PCE). These meetings will allow Coalfire to gain knowledge of each entity's specific environment and provide each entity with the guidance required to complete their self-assessment questionnaire (SAQ).
- Coalfire will assist entities in completing their annual SAQs. Completion of the SAQ will be facilitated by Coalfire's proprietary platform, RapidSAQ. RapidSAQ is a web-based tool that allows each entity to evaluate, document, and generate its SAQ. Each entity will have its own RapidSAQ environment. Each entity will provide a list of users who will be responsible for completing the SAQ and these users will be given credentials to access their entity's RapidSAQ environment. After completing their responses, entities have the ability to generate an electronic version of the SAQ (exact format and look of the paper-based form required by the PCI Security Standards Council) that they can print out, sign, and forward to DFA and/or the entity's acquiring bank as appropriate.
- Coalfire will review each entity's SAQ to ensure completeness and accuracy.
- After each entity completes its SAQ, Coalfire will prepare and deliver a remediation plan (electronic copy) to the entity, DFA, and ITS identifying any compliance gaps and including the following components.
 - Associated PCI requirement
 - Risk rating
 - Reason for deficiency
 - Recommended remediation action
 - Cost estimate for remediation activities
- Coalfire will perform quarterly external PCI scans required as part of the State's validation of PCI compliance. These scans will occur on a defined schedule. As part of the initiation of the RapidSAQ process, each entity will be asked to provide a list of all public facing IP addresses used by the entity. If the entity's application(s) is hosted and managed by ITS, then this information will be provided by ITS and no action is required by the entity. The scan service includes the following:
 - Downloadable reports in .pdf format, available electronically within 2 business days after completion of the scan. The reports include:
 - A prioritized list of all vulnerabilities identified, and
 - Recommended remediation actions for each vulnerability including references to sources of information and/or security patches that help to resolve the vulnerability.
 - In the event of a failing scan, follow-up scans after remediation has been completed, to verify that remediation activity results in a passing scan.

- Coalfire is required to provide copies of all audit results to the ITS PCI Compliance Representative, DFA Chief Systems Information Officer, and each entity contact person. Electronic delivery of the audit results must be performed in a secure manner. Coalfire will deploy a Project Portal that provides role-based security access for named project members and incorporates alerting tools based on daily, weekly or activity-based criteria. The portal helps streamline communication and provides a secure means of transferring sensitive project data and reports, because connection is secured via SSL. Each entity will have a dedicated area within the portal to facilitate secure exchange of information with Coalfire audit staff and each such area will only be accessible to named personnel.

For more information regarding the PCI DSS and its associated requirements (including the SAQ), please visit the PCI SSC's website at <https://www.pcisecuritystandards.org/>.

- **Effective Dates**

PCI compliance audit services may be acquired from this RFP No. 3532 through June 30, 2011.

- **Dollar Limitations of Use**

There is no maximum dollar limitation for services obtained from RFP No. 3532.

- **Vendor Contact Information for Requesting Services under RFP No. 3532**

Coalfire Systems, Inc.
361 Centennial Parkway, Suite 150
Louisville, Colorado 80027-1283

Name: Alan Ferguson, Vice President
Phone: (303) 554-6333 ext 7002
e-mail: alan.ferguson@coalfiresystems.com

- **Scheduling Services**

- ITS and DFA, in consultation with Coalfire, will determine which entities will be required to participate in the PCI compliance process. Those entities will be notified by ITS/DFA and will be asked to provide a list of staff responsible for completing the SAQ along with a primary point of contact (POC) for the project. When Coalfire receives the agency information, Coalfire will prepare a project quote for each entity and deliver it to the entity POC. The quote will detail the costs for participating in the PCI Compliance process. The project quote must also be sent to DFA and ITS for review and approval before any work can be scheduled.
- Entities desiring consulting services to scope and define their cardholder data environments, their validation type(s) and corresponding SAQ type(s), and/or guidance on how the applicable PCI DSS control requirements apply to their

environment should contact DFA to initiate the process of obtaining these services. Once DFA, Coalfire, ITS, and the entity understand the scope of services desired, Coalfire will submit to the entity, DFA, and ITS a Statement of Work which provides a not-to-exceed price for the services.

- **Contractual Terms and Conditions**

ITS has executed a Professional Services Agreement on behalf of the state. State entities do not need to execute an additional agreement for services.

- **Cost of Services**

The costs for annual PCI compliance services listed below are based on an entity’s need to complete one SAQ. If an entity’s business process employs multiple channels resulting in the need for multiple SAQs, then the cost for annual PCI compliance audit services is derived by multiplying the number of SAQs required by the cost listed below.

The not-to-exceed annual cost of PCI compliance audit services by entity or SAQ, as applicable, is \$2,941.50, for the first 18 audits provided to the state. Beginning with the 19th audit, the not-to-exceed annual cost per agency or SAQ is \$3,126.50.

The project quote prepared by Coalfire will include some combination of the line items listed below, with a maximum total cost as noted above.

Audit Services	Cost
Regular Project Status Calls	
Face-to-Face Interviews for Data Gathering and Assistance	
Offsite Support on Rapid Self Assessment Questionnaire	
SAQ Review	
Develop Compliance Roadmap	
Develop Remediation Plans based on Findings	
Provide ISO-compliance Policy Templates Aligned to PCI Requirements	
Not-to-Exceed Contract Cost per Entity*	\$2,941.50
One Time Setup for Entities / Merchant Ids beyond First 18	\$185.00

** In addition to the costs shown above, each entity requesting an audit after the first 18 have been performed will be assessed a \$185.00 configuration and setup charge. The quote you receive from Coalfire will detail the actual amount you will be charged.*

In order to assist agencies in acquiring the necessary PCI DSS services, DFA and ITS have established fee payment tiers for requesting services under the Professional Services Agreement between Coalfire Systems, Inc. and the Mississippi Department of Information Technology Services, on behalf of the Agencies and Institutions of the State of Mississippi. The fee schedule is based upon

risk levels for intrusions and access to customer card information, and the additional, enterprise-level protections provided through the state’s payment service for those agency applications hosted at ITS.

Tier I - All agency payment processes are hosted within the State Data Center and use the State’s payment service, and are developed and managed by ITS. Agencies in this tier are not responsible for costs associated with the necessary PCI DSS services.

Tier II – Agency has Tier I application(s), and has credit card processes outside of the State’s payment process, or has applications hosted within the State’s payment infrastructure that are not developed by ITS. Agencies in this tier will be responsible for fifty percent of the costs associated with the necessary PCI DSS services.

Tier III – Agency uses standalone dial-out terminals not connected to any other system, and has low transaction volume. ITS, DFA, and Coalfire Systems will determine qualifications for this tier after reviewing the agency’s processes and risks. Necessary PCI DSS services will be provided at no cost to the state.

Tier IV – Agency uses a 3rd party process in a national consortium, and collects the per transaction EOC fee. Agencies in this tier are not responsible for costs associated with the necessary PCI DSS services.

Tier V – Agency uses the State’s payment service, but developed and hosts their application in the agency environment, or the agency uses a 3rd party agreement for other payment services, or the agency solely uses a 3rd party payment service (not a national consortium). Agencies in this tier are responsible for all costs associated with the necessary PCI DSS services.

Entities requiring planning assistance or more detailed advisory services may use this procurement vehicle to obtain those services as well. All agencies are responsible for the costs associated with this type of assistance. Note that these consulting services do not include remediation work required to satisfy or resolve any audit findings.

Consulting Services	
As identified by individual Statements of Work based on a not-to-exceed effort estimate in hours	\$185.00 per hour

• **Paying for Services: Object Codes**

ITS, in conjunction with DFA and the Office of the State Auditor, requests that all state entities carefully code purchases with the correct Minor Object Codes. State agencies that utilize the Statewide Automated Accounting System (SAAS) should use the following expenditure account code on purchase order documents for services from this RFP No. 3532.

Object Code	Category	Use
61902	IS Professional	Payments to an outside vendor for information systems

	Fees – Outside Vendor	consulting services such as consulting studies; project management; facilities/staff management; and analysis, design, development/enhancement of <u>non-telecommunications software</u>
--	-----------------------	--

- **What Goes in Your Purchase / Audit File?**

A copy of this “Instructions for Use” memo, along with the project quote provided by Coalfire and the approval document from DFA/ITS.

- **To Report Problems and/or Request Assistance**

Renee Murray, ITS PCI Compliance Representative
601.359-2742 renee.murray@its.ms.gov

Jim Hurst, DFA/OFM PCI Compliance Representative
601.359-3011 hurstj@dfa.state.ms.us

Clyde Murrell, DFA/MMRS PCI Compliance Representative
601.359-1490 murrellc@dfa.state.ms.us