State of Oklahoma

Office of Management and Enterprise Services

ADDENDUM 1 TO
STATE OF OKLAHOMA CONTRACT WITH COALFIRE SYSTEMS, INC.
RESULTING FROM STATEWIDE CONTRACT 1042

This Addendum 1 ("Addendum") is an Amendment to the Contract awarded to Coalfire Systems, Inc. in connection with Statewide 1042 ("Solicitation") and is effective October 2, 2017.

Recitals

Whereas, the State issued a Solicitation for proposals to provide information technology risk, security and compliance products and services to state agencies and to ensure compliance with all industry and regulatory data security standards, as more particularly described in the Solicitation;

Whereas, Coalfire Systems, Inc. submitted a proposal which contained various other Contract Documents; and

Whereas, the State and Coalfire Systems, Inc. have negotiated the final terms under which Coalfire Systems, Inc. will perform the Services under the Contract.

Now, therefore, in consideration of the foregoing and the mutual promises set forth herein, the receipt and sufficiency of which are hereby acknowledged the parties agree as follows:

1. **Addendum Purpose.**

   This Addendum memorializes the agreement of the parties with respect to negotiated terms of the Contract that is being awarded to Coalfire Systems, Inc. as of even date with execution of this Addendum. The parties agree that Supplier has not yet begun performance of work contemplated by the Solicitation.

2. **Negotiated Documents of the Contract**.

   2.1. The parties have negotiated certain terms of the Contract as follows:

i. certain additional negotiated terms to the Solicitation as contained in Attachment A to this Addendum titled Negotiated Additional Terms;
ii. revisions to Coalfire Systems, Inc.'s Master Agreement as contained in Attachment B to this Addendum titled, Master Agreement; and
iii. revisions to the service order initially proposed by Coalfire Systems, Inc. as contained in Attachment C to this Addendum titled Service Order.

2.2. The Contract is amended to include the above-described, negotiated documents which are attached hereto and incorporated herein and which, for the avoidance of doubt, shall have the following order of precedence:

i. Negotiated Additional Terms, Attachment A;
ii. Master Agreement, Attachment B; and
iii. Service Order, Attachment C.

Contract Documents shall be read to be consistent and complementary. Any conflict among these documents shall be resolved by giving priority to these documents in the order listed above.

2.3. Accordingly, any reference to a Contract Document refers to such Contract Document as it may have been amended. If and to the extent any provision is in multiple documents and addresses the same or substantially the same subject matter but does not create an actual conflict, the more recent provision is deemed to supersede earlier versions.

State of Oklahoma

By: _____

Name: James L. Reese, II

Title: Chief Information Officer

Date: 10-6-17

Coalfire Systems, Inc.

By: DocuSigned by: Alan Ferguson BE266259B3A64D8...

Name: Alan Ferguson

Title: Exec. Vice President

Date: 10/4/2017 | 10:19 AM MDT

APPROVED BY LEGAL

DS CD

Attachment A to
Addendum 1 to
STATE OF OKLAHOMA CONTRACT WITH COALFIRE SYSTEMS, INC.
RESULTING FROM STATEWIDE CONTRACT 1042

Negotiated Exceptions and Additional Terms

The Solicitation is hereby amended as set forth below and supersedes all prior Exceptions submitted by Coalfire Systems, Inc. or discussed by the parties.

Solicitation, Section A General Provisions, Subsection A.18 is hereby deleted in its entirety and replaced with the following:

A. Vendor may terminate the Contract in the event (**i.)** it has provided the State with written notice of material breach and (**ii.)** the State fails to cure such material breach within thirty (30) days of receipt of written notice. The State may terminate the Contract in whole or in part in the event (**i.)** it has provided Vendor with written notice of material breach, and (**ii.)** Vendor fails to cure such material breach within thirty (30) days of receipt of written notice. Similarly, a Customer may terminate its obligations, in whole or in part, to Vendor if it has provided Vendor with written notice of material breach and Vendor fails to cure such material breach within thirty (30) days of receipt of written notice.

B. The State may terminate the Contract in whole or in part immediately without a thirty (30) day written notice to Vendor, only if Vendor's material breach is reasonably determined (**i.)** to be an impediment to the function of the State and detrimental to the State, (**ii.)** when conditions preclude the thirty (30) day notice, or (**iii.)** or when the State determines that an administrative error occurred prior to Contract performance.

C. If the Contract or certain obligations under the Contract are terminated, the Customer shall be liable only for payment for Products delivered and accepted or Services rendered prior to the date of such termination. Products shall be deemed accepted if Customer fails to provide notice of rejections of the Product within 15 calendar days of receipt of the Product. To the extent State disputes an invoice for Services due to performance or otherwise, State shall pay the invoice costs for the undisputed costs. If the disputed costs are owed, Customer shall remit payment for the disputed costs within 45 days of resolution. Such termination shall not be an exclusive remedy but shall be in addition to any other rights and remedies provided for by law. In no event shall a Customer be liable to the Vendor for compensation for any Products neither requested nor accepted by the Customer or for any Services requested by the Customer. In no event shall the State's exercise of its right to

terminate the Contract for cause relieve the Vendor of any liability to the State or a Customer for claims arising under the Contract.

Solicitation, Section B Special Provisions, Subsection B.12 is hereby added:

Vendor marked the following as confidential: LABS-Sample Penetration Test Report, Pricing Proposal; and the Cyber Security Services Proposal. After review, the state advised Vendor it was not in compliance with Oklahoma Administrative Code 260:115-3-9. The State advised Vendor could specifically identify the information in these documents that is confidential and enumerate the specific grounds based on applicable laws which support treatment of these documents as exempt from disclosure for state's further review or withdraw Vendor's confidentiality claim. Vendor confirmed on letterhead it agreed to withdraw its claim of confidentiality on the LABS – Sample Penetration Test Report, Pricing Proposal; and the Cyber Security Services Proposal.

Attachment B to
Addendum 1 to
STATE OF OKLAHOMA CONTRACT WITH COALFIRE SYSTEMS, INC.
RESULTING FROM STATEWIDE CONTRACT NO. 1042

The Master Agreement is hereby amended as set forth below and supersedes all prior documents submitted by Coalfire Systems, Inc. or discussed by the parties.

COALFIRE℠

THIS MASTER AGREEMENT ("Agreement") is effective [Month], [Date], 2017 ("Effective Date") by and between Coalfire Systems, Inc., on behalf of its affiliates ("Coalfire"), and Client, on behalf of its affiliates, (each, a "Party," and together, the "Parties") and sets forth the general terms and conditions pursuant to which Coalfire will provide services ("Service(s)") and reports ("Deliverable(s)") to Client.

1. SERVICE ORDERS. During the term of this Agreement, the Parties may execute certain documents more fully describing the Service(s) provided by Coalfire to Client ("Service Order(s)"). In the event of a conflict between the terms of this Agreement and a Service Order, the terms of this Agreement will govern except where the terms of a Service Order specifically state otherwise.

2. INVOICING; TAXES

2.1 Invoicing. Coalfire will invoice Client on a monthly basis for fees and expenses incurred, and payment is due in accordance with Oklahoma law, If Client fails to pay timely, Coalfire reserves the right to charge interest on the amount past due at the lesser of 1.5% per month or the maximum allowed by Oklahoma law.

3. TERM & TERMINATION. The term of this Agreement begins on the Effective Date and continues until terminated as set forth in this Agreement or State of Oklahoma Statewide Contract 1042 with Coalfire. Additionally, either Party may terminate a Service Order due to the other Party's breach of any of its obligations that remain uncured after thirty (30) days' written notice from the non-breaching Party. Termination for cause will not preclude the non-breaching Party from pursuing any and all remedies available to it at law or in equity. Upon expiration or termination of this Agreement or a Service Order for any reason: (a) Except for a situation of non-appropriations, Client shall pay Coalfire for all Services and Deliverables accepted by Client in accordance with applicable Oklahoma law.

4. INDEMNIFICATION

[Intentionally omitted]

5. ACKNOWLEDGEMENTS; WARRANTIES

5.1 By Coalfire. Coalfire represents that the Services will be performed in a workmanlike and professional manner by individuals who have skill and experience commensurate with the requirements of the Services.

5.2 By Client. Client agrees that Coalfire will not be responsible for nonconformities or any errors in work papers or Deliverables resulting from Coalfire's reliance on inaccurate, inauthentic or incomplete data or information provided by Client. Client will cooperate with Coalfire and take actions reasonably necessary to enable Coalfire to perform the Services. To that end, Client will provide, on a timely basis, all information, as well as access to systems, locations and personnel, reasonably requested by Coalfire to enable Coalfire to provide the Services or will timely provide an explanation as to why it cannot confirm to Coalfire's responsible requests. If Coalfire is required to reschedule the delivery of Service due to the foregoing, then Client understands that such rescheduling will be dependent upon Coalfire's resource availability and may result in additional charges. Client further acknowledges and agrees that (a) any outcome of the Services involving security assessment is limited to a point-in-time examination consistent with the Engagement Scope set forth in the applicable Service Order, (b) the outcome of any audits, assessments or testing by, and the opinions, advice, recommendations and/or certification of, Coalfire does not constitute any form of representation, warranty or guarantee that Client's systems are secure from every form of attack, even if fully implemented, (c) in examining Client's compliance or non-compliance status, Coalfire relies upon accurate, authentic and complete information provided by Client as well as use of certain sampling techniques, and (d) Client's management is solely responsible for the scope, goals and overall direction of the Services, as well as the implementation of any course of action based on such Services.

5.3 No Implied Warranties. Other than those expressly contained in this Section, neither Party makes any other representations or warranties, implied, statutory or otherwise, with respect to the Services or Deliverables. Coalfire EXPRESSLY DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

6. LIMITATIONS ON LIABILITY. Neither Client nor its employees, officers and directors, on the one hand, nor Coalfire and its employees, officers and directors and licensors, on the other hand will be liable to the other Party under the Agreement for lost profits or any consequential, incidental, indirect, punitive or special damages, or any other similar damages under any theory of liability whether in contract, tort or strict liability, however caused and regardless of legal theory or foreseeability, directly or indirectly, arising under this Agreement. In no event shall liability under this Agreement of Coalfire exceed those fees payable to Coalfire by Client under the applicable Service Order. For the avoidance of doubt, this limitation of liability set forth in this Section 6 shall not apply to (a) any claims or actions arising from or related to a breach of confidentiality or (b) infringement of third party intellectual rights by seller.

7. INTELLECTUAL PROPERTY RIGHTS

7.1 Of Coalfire. Client understands that Coalfire is engaged to use its existing knowledge, training, experience and proprietary methodologies ("Coalfire Methodologies") to perform the Services set forth in the applicable Service Order, which may include an assessment of Client's information technology system and certain security aspects thereof, and in some cases, to provide a written report regarding such Services. Client will not acquire, and Coalfire will not assign, any right, title or interest in or to the Coalfire Methodologies or any text, data or other materials that were owned by, or licensed to, Coalfire prior to Coalfire's performance of Services under the applicable Service Order ("Pre-existing Intellectual Property") or to any new knowledge, techniques and methodologies developed by Coalfire in the performance of the Services and the creation of the Deliverables. As between Coalfire and Client, Coalfire is and will remain the owner of all Pre-existing Intellectual Property and Coalfire Methodologies and all processes, know-how, methodologies and technology used in connection with providing the Services.

7.2 Of Client. Coalfire will not acquire, and Client does not assign, any right, title or interest in or to confidential information or other materials provided by Client that were owned by or licensed to Client prior to Coalfire's performance of Service under the applicable Service Order ("Client Pre-existing Intellectual Property"). As between Coalfire and Client, Client is and will remain the owner of all Client Pre-existing Intellectual Property.

7.3 License Grant. Subject to the terms of this Agreement, the Deliverables provided to Client will be owned by Client. If a Deliverable includes any Pre-existing Intellectual Property, Coalfire hereby grants to Client a perpetual, non-exclusive, royalty-free license to use such Deliverable for Client's business purposes. If such use involves disclosure of the Deliverable to a third party, Client agrees: (i) that such disclosure will be in furtherance of a legitimate business need of Client, (ii) the Deliverable will not be altered in any way, and (iii) such disclosure will be non-public

in nature and subject to confidentiality terms at least as restrictive as those specified herein.

8. DISPUTE RESOLUTION. This Agreement will be interpreted and construed in accordance with the substantive laws of the State of Oklahoma, without regard to any provisions of its choice of law rules. Coalfire has no liability for actions by Visa U.S.A., PCI or PCI's member organizations, their employees, officers, consultants, subcontractors or affiliates with respect to Client's confidential information contained in the any formal compliance attestation report subject to standards published by the PCI SSC (including, but not limited to, Report on Compliance, Report on Validation, ASV Vulnerability Scan Report, and other developed materials).

9. PERFORMANCE OF SERVICES. The location from which Coalfire will provide the Services will be specified in the Service Order; however, Coalfire may conduct sampling in connection with the Services from any sites that Coalfire deems appropriate.

10. ADDITIONAL PROVISIONS REGARDING CERTAIN COALFIRE SERVICES

10.1 Security Assessment Services. If the Services include technical security testing, penetration testing (including physical, application, ethical or network penetration assessment and testing) or computer forensic services, Coalfire will use various commercial, open source, freely distributed or proprietary testing tools, techniques and monitoring methods to evaluate the devices, software or resources (collectively "Systems") identified by the Client, and verified by Coalfire, as within scope. Coalfire may also use tools that meet the definition of malware by anti-virus platforms. Coalfire is not responsible for adverse consequences resulting from inaccurate information, including inaccurate IP Addresses, furnished by Client with respect to any System.

11. GENERAL TERMS. No amendments or other variation to this Agreement will be effective unless in writing and signed by an authorized person on behalf of each Party. Except as set forth in Oklahoma Statewide Contract 1042, Neither Party may assign nor transfer any of its rights or obligations under this Agreement to any third party without the express written consent of the other Party. For the purposes of this Agreement, the assignment of Contract or rights under the Contract to successor by merger or consolidation is not considered an assignment for purposes of this provision. Either party shall be temporarily excused from performance to the extent delayed as a result of unforeseen causes beyond its reasonable control including fire or other casualty, act of God, strike or labor dispute, way or other violence, or any law, order or requirement of any governmental agency or authority provided the party experiencing the force majeure event has prudently and promptly acted to take any and all steps within the party's control to ensure continued performance and to shorten duration of the event. In the event that a party's performance of its obligations is materially hindered as a result of a force majeure event, such party shall promptly notify the other party of its best reasonable assessment of the nature and duration of the force majeure event and steps it is taking, and plans to take, to mitigate the effects of the force majeure event. The party shall use commercially reasonable best efforts to continue performance to the extent possible during such event and resume full performance as soon as reasonably practicable. Subject to the condition set forth above, such non-performance shall not be deems a default. However, Client may terminate a purchase order if Coalfire cannot cause delivery of Products or services in a timely manner to meet the business needs of the Client. Coalfire will perform its obligations under this Agreement as an independent contractor and not as an agent or joint venture partner of Client. No term or provision of this Agreement is intended to be, nor will be, for the benefit of any person, firm, organization or corporation not a party hereto, and no such third party will have any right or cause of action hereunder. Notices required under this Agreement will be in writing and delivered in person or sent by overnight courier addressed to the addresses in the applicable Service Order with copies to the following:

Chief Information Officer
3115 North Lincoln Blvd
Oklahoma City, OK 73105

Information Services Deputy General Counsel
3115 North Lincoln Blvd
Oklahoma City, OK 73105

State Purchasing Director
5005 N. Lincoln Blvd, Suite 300
Oklahoma City, OK 73105

Central Purchasing Deputy General Counsel
5005 N. Lincoln Blvd, Suite 300
Oklahoma City, OK 73105

Notice will be effective when sent by overnight courier or upon delivery if delivered in person. If any provision of this Agreement is determined to be unenforceable or invalid, the remaining provisions of this Agreement will remain in full force and effect.

Attachment C to
Addendum 1 to
STATE OF OKLAHOMA CONTRACT WITH COALFIRE SYSTEMS, INC.
RESULTING FROM STATEWIDE CONTRACT NO. 1042

The Service Order is hereby amended as set forth below and supersedes all prior documents submitted by Coalfire Systems, Inc. or discussed by the parties. The parties agree to use this Service Order or a document substantially in the form of this Service Order.

COALFIRE

TEMPLATE

TITLE

SERVICE ORDER

Submitted to:

Name
Title
Address
City, State ZIP
Phone
Email

Submitted by:
Coalfire Systems, Inc.
Name
Title
Address
City, State ZIP
Phone
Email

TABLE OF CONTENTS

PROJECT OVERVIEW

Coalfire Systems, Inc. (“Coalfire”) is pleased to provide _____("Client") with this Service Order to provide_____

This Service Order is entered into between Coalfire and Client in connection with the State of Oklahoma Agreement, Statewide Contract No. 1042 with Coalfire Systems. Inc. (“Agreement”).

The tasks detailed in this Service Order are specific to Client and intended to meet these objectives:

- XXXX
- XXXX
- XXXX

The services and scope defined in this Service Order constitute the extent of services Coalfire will provide to Client with the understanding that services not specified in this Service Order are out of scope for this engagement. Services and deliverables listed in this document will be provided on a mutually agreeable schedule.

ENGAGEMENT SCOPE

The following table describes the scope of Coalfire’s engagement, and Coalfire and the Client agree that a change in scope may result in a Change Order to reflect the increase or decrease in Coalfire’s level of effort to meet Client’s objectives.

Scope Category	Client Detail for the Engagement Scope
General Company Information HQ/Data Centers/Call Center/Locations	**Overview:** • Headquarters (city, state): • # of Employees: • X Data Centers (locations, cities, states, regions, countries) • X Call Center (locations, City, State) • X Locations (cities, states, regions, countries) • Services covered for the assessment activities include: –
Technical Environment	The following asset types are in-scope for assessment activities: • # of Network Devices (firewalls, routers, switches, IDS/IPS) • # of Servers (specify physical vs virtual and specify server operating system(s)) • # of Workstations (specify function and workstation operating system) • # of Telephony Devices • # Applications • # Databases with CHD • Other
Technical Testing	The following technical testing assumptions are in-scope. Any assumption not listed herein are considered out of scope for the engagement: Scanning Assumptions • External scanning for up to ____ IPs. • Internal scanning for up to ___ IPs.

	Penetration Testing Assumptions
	• External Penetration Testing for X external IPs
	• Internal Penetration Testing and Segmentation Testing
	  – INSERT Bid Sheet Assumptions
	• Web-Application reviews for X Externally Facing Applications
	  – Application and Description of complexity/ testing (black box and single user credential) Coalfire assumes all testing will be conducted during normal business hours
	• Coalfire assumes all internal testing may be done remotely using a drone connected to the internal corporate network.
	• Coalfire assumes project activities are not required to commence sooner that 6-8 weeks following contract signature.
	• The Client is responsible for facilitation of proper approvals for testing related to third party service providers and colocations.
	• Coalfire assumes all penetration testing takes place during Coalfire's normal business hours (Monday to Friday / 6 AM to 6 PM Mountain time).

SERVICES AND PRICING

Services & Pricing	
The following services are provided as a fixed fee budget	
XXXXX: • XXXX	$
XXXXX: • XXXX	$
XXXXX: • XXXX	$
Total fixed fee budget	**$**

	Hourly Rate
Assessment Remediation & Retesting	$

Payment Terms

PCI DSS Assessment Services	
Invoice 1	• 25% of the fixed fee upon Project Charter
Invoice 2	• 25% of the fixed fee upon completion of Pre-Assessment Analysis
Invoice 3	• 25% of the fixed fee upon completion of Onsite Assessment
Invoice 4	• 25% of the fixed fee upon delivery of a draft report
Technical Testing Services	
Invoice 1	• 50% of the fixed fee upon Project Charter
Invoice 2	• 50% of the fixed fee upon delivery of a draft report
Vulnerability Scanning Subscription Services	
Invoice 1	• CoalfireOne services are billed in full for an annual subscription upon execution of this Service Order.

- Services delivered on a T&M basis under this Service Order are invoiced monthly based upon actual work completed.

REQUIREMENTS AND ASSUMPTIONS

PRICING REQUIREMENTS & ASSUMPTIONS

- The prices listed in this Service Order are valid for 30 days from the Service Order date.
- For Fixed Fee Services, invoices are issued per the terms of the Agreement.
- Fixed Fee Services purchased hereunder apply to the Service(s) delivered within the Engagement Scope and may not be used toward any other Service provided to Client by Coalfire.

  The number of Advisory Services hours set forth in the table above may not be sufficient to provide the Services in the Engagement Scope. In the event Coalfire believes at its reasonable discretion additional hours are required to perform such services, Coalfire will notify Client in writing and the parties agree to work in good faith to negotiate and execute a Change Order or new Service Order providing for additional hours at an additional charge.

  Advisory Services, remediation support or re-testing that are not expressly identified herein will be delivered subject to written agreement between the parties.
- Additional external IP addresses beyond those described in the Service Order will be billed at $15 each.
- Additional internal IP addresses beyond those described in the Service Order will be billed at $8 each.
- CoalfireOne™ Lighthouse™ Return Policy - In the event Client's CoalfireOne™ internal scanning service is terminated, the CoalfireOne™ Lighthouse™ equipment provided by Coalfire should be returned to Coalfire promptly as Client will continue to be billed the monthly rental fee for the equipment until it is returned. If the CoalfireOne™ Lighthouse™ appliance is lost, damaged or are otherwise unable to be returned in working condition, Coalfire will invoice Client for the full replacement cost.
- Timing of Services:

  Services are provided as set forth in the charter document, subject to the terms of the Agreement and this Service Order.

  All testing activities performed by Coalfire Labs are conducted between 6:00AM and 6:00PM Mountain Time, Monday thru Friday, national holidays excepted. Any testing required outside of this timeframe and not specified in this Service Order shall be set forth in a Change Order and subject to an additional charge of 20% of the total amount due for Penetration Testing.
- Change Orders:

  As part of the fixed-fee budget, Coalfire assumes evidence review, including onsite and remote review of documentation and observations, will be completed during a single, one-time work activity by Coalfire. Client understands and agrees that any additional reviews of evidence needed based on additional evidence provided by Client may necessitate a Change Order and budget modification.
- The Client acknowledges and agrees that:

  Any outcome of the Services involving security assessment is limited to a point-in-time examination of Client's security status with the applicable standards or industry best practices set forth in the Service Order.

The outcome of any audits, assessments or testing by, and the opinions, advice, recommendations and/or certification of, Coalfire does not constitute any form of representation, warranty or guarantee that Client's systems are secure from every form of attack, even if fully implemented.

In examining Client's compliance or non-compliance status, Coalfire relies upon accurate, authentic and complete information provided by Client as well as use of certain sampling techniques.

Client will cooperate with Coalfire and take all actions reasonably necessary to enable Coalfire to perform the Services. To that end, Client will provide, on a timely basis, all information, as well as access to systems, locations and personnel, reasonably requested by Coalfire to enable Coalfire to provide the Services.

- If applicable and to the extent reasonably necessary, Client shall provide to Coalfire the following to enable Coalfire's delivery of Service:

  Reasonable access to business staff, documentation, and facilities

  Office space with web access for on-site activities

  Necessary safety equipment and training while on Client's, or Client's customers or service provider's, site

  Timely input and review of progress as reasonably requested by Coalfire

  Introductions to, and facilitated discussion with, Client's service providers and/or third-party business partners

  Access to corporate and hosted computer systems (if any) and network connections

  A single point of contact throughout the engagement:
  - With the technical knowledge about the in-scope systems, devices and networks - or with access to such subject-matter experts within the Client's organization
  - To provide notice in the event Coalfire discovers high-risk vulnerabilities or other similar findings

  - Except as identified to Coalfire in writing, Client represents that it is unaware of any on-going or previous data breach or compromise, or indications of such potential compromise, involving its business processes or systems it owns or manages that are subject to the Services.

- Except as identified to Coalfire in writing, Client represents that it periodically examines systems for retention or transmission of unencrypted credit card data, including track data, and Client represents that it does not store such unencrypted data.
- The parties acknowledge that changes to the Payment Card Industry (PCI) Data Security Standard (DSS) or Payment Application Data Security Standard (PA-DSS) implemented subsequent to the date of this Service Order may affect testing and reporting activities required for the Services described herein. If such changes occur, the parties agree to jointly review the changes and make the appropriate adjustments to the activities, deliverables, and associated budget(s).
- Any Coalfire services performed around undocumented cardholder data flows will constitute additional out-of-scope work and is not covered by the fees section of this Service Order.
- During the course of this engagement, Coalfire may identify third-party entities connecting to the Client's network. Data flows transferred over these connections are in-scope, but assessments of vendor networks or systems on the other end of these connections are not included in this Service Order.
- Notwithstanding anything in any agreement between the parties to the contrary, Coalfire may submit the scan report, along with any clarifying notes, documents, or verbal input, to the card brands or Client's acquiring bank/processor in accordance with practices adopted by the PCI SSC.

- The Results include a Report on Compliance and, without limitation, any associated working papers, notes, and other materials and information generated in connection with this project, including a copy of this Agreement.
- Client agrees that, without further permission from Client and notwithstanding anything in any agreement between the parties to the contrary, Coalfire may submit project "Results" to a "Requesting Organization," as those terms are defined by the PCI Security Standards Validation Requirements for Qualified Security Assessors.
- The Results include a Report on Validation and, without limitation, any associated working papers, notes, and other materials and information generated in connection with this project, including a copy of this Agreement.
- Client must complete an assessment using CoalfireOne™ Rapid PA-DSS. Per PCI DSS guidelines, the Implementation Guide must be complete before the PA-DSS Assessment Phase can be started.
- Client represents that it periodically examines systems for retention or transmission of unencrypted personal health information, and Client represents that it does not store such unencrypted information except as identified to Coalfire in writing.
- All healthcare assessment testing will be completed within 90 days.

ACCEPTANCE

This Service Order and the Appendices attached hereto (and hereby incorporated by reference) are effective as of the last date of signature below ("Effective Date"). THE TERMS OF STATE OF OKLAHOMA STATEWIDE CONTRACT NO. 1042 ("AGREEMENT") WITH COALFILE SYSTEMS, INC., INCLUDING THE THE MASTER AGREEMENT CONTROL THIS SERVICE ORDER.

Service Order: YY-MMDD-CLIENT	
_____	**Coalfire Systems, Inc.**
Signed:	Signed:
Name:	Name: Alan Ferguson
Title:	Title: Executive Vice President, Sales
Date:	Date:

Kindly return signed Service Order to the attention of NAME@coalfire.com

INVOICING

- To be completed by Client:

  Please send invoices to:
  Name: _____
  Email Address: _____

Phone Number: _____
Accounts Payable Email Address: _____
Required invoicing instructions if applicable:
_____
_____
PO #, if required: _____
Please send a copy of the PO to invoices@coalfiresystems.com and NAME@coalfire.com

APPENDICES

APPENDIX - METHODOLOGY

Client Project Charter

The Client Project Charter takes place in person, via conference call, or a combination of both to support participation of all stakeholders. This meeting serves to get project participants introduced, roles and responsibilities communicated, key dates and timelines established, and project methodologies and tools reviewed. There is no preparation on the Client's part for this session, and only attendance by key stakeholders is required.

Activity	Activity Description
Introduction	Introduce project stakeholders to foster good communications and coordination among key members of the project team, including Coalfire, Client, and any third-party personnel.
Roles and Responsibilities	Establish and agree on roles and responsibilities for project team members and identify points of contact for project activities and specific subject matter expertise. At a minimum, Project Stakeholders include: **Coalfire** • Managing Director • Project Director • Coalfire Labs Director • Project Manager • Senior Auditor and staff **Client** • Executive Sponsor • Project Leader/Liaison • Various Project Support Staff
Timelines & Milestones	Establish and agree on timelines, milestones, status meeting dates, and target deliverable timeframes.
Review and Approve Methodologies and Tools	Align stakeholders to the project management process and establish overall project management roles. Review pertinent methodologies and tools with Client.
Definition of Risk and Approval Processes	A written rules of engagement memorandum will be finalized and agreed upon by Client and Coalfire.
Access Rights	Identify approved team members to be granted access rights to the secure project portal, established to create a central place for all participants to store and retrieve working documents.
Required Document Forms	Prior to the Charter Meeting, Coalfire will provide Client with a "Required Documents Form" listing documents that the Coalfire project team will review to prepare for the Charter.

Deliverables and Requirements

The deliverables from this task include the initial version of the project charter document and subsequent versions as amended for adjustments to project scope, timelines, or objectives.

The Coalfire Project Manager is responsible for maintaining changes to the charter document. Updated versions, if any, will be uploaded by the Coalfire Project Manager to the portal as approved by the parties.

Coalfire and the Client will mutually agree to any changes and adjustments to the charter document in writing.

Task 1:

APPENDIX – PROJECT MANAGEMENT PROGRAM

Activity	Activity Description
Engagement Project Management	It is important for all parties to understand the Timeline and Milestone dates set in the Client Project Charter that define the overall project plan. Coalfire will assign a **Project Manager** to this engagement to communicate milestone status to all team members (Coalfire and the Client). The **Project Manager** will provide ***ALL*** Project Stakeholders with status updates with the following items: • Clearly state that the Project is "On Schedule" or "Project Constrained". Any constraints on both the Client and/or Coalfire are described. • Clearly state where the Project is on the timeline. • Clearly state Project Milestones that are pending in the following two weeks. • Clearly state whether any additional discussion is required. Missed milestones by the Client or Coalfire will create an immediate Project Constraint that will be communicated to the entire team and escalated to the Project Director and/or Managing Director for immediate action. The Client stakeholders should expect a description of the constraint, the potential impact to the project, and next step recommendations. **Deliverables:** • Secure Project Portal • Project manager • Project Management Status Reports
Project Portal	Coalfire supports secure communications throughout the project's life cycle. All project processes are managed through a web-based portal that maintains the project chartering, budgeting, scoping, project plans, status reports, task assignments, stakeholders and communication channels, milestone tracking, reports, and deliverables. This portal is a living tool for managing the project from our perspective and it helps Client staff remain informed on project progress. The secure portal provides a centralized repository for: • Final reports, work-in-progress reports, and raw data. • Coalfire controls access for critical information. • Contact information for all team members. Coalfire manages the secure portal for the duration of our relationship. As our relationship continues and develops, Coalfire will add folders and sub-portals to the portal to separate multiple years, other projects, etc. Coalfire manages security on a per-portal basis allowing us to enforce authorized user access control. Coalfire and Client can manage security differently to any project portal level, allowing us to better control access to project data. It should be noted that only authorized Coalfire personnel, such as your project delivery team, have access to your information through a specific user authorization and access control procedure. Sales, marketing, and administration do not have access to your information or reports. Coalfire can, at Client's option, archive the project materials and close the portal.