

STATE OF NEW HAMPSHIRE

DEPT. OF ADMINISTRATIVE SERVICES
BUREAU OF PURCHASE AND PROPERTY

INTER-DEPARTMENT COMMUNICATION

DATE: September 16, 2013

FROM: Robert B. Lawson, Purchasing Agent
Bureau of Purchase & Property

TO: Rudolph W. Ogden
Robert D. Stowell
Michael P. Connor
Linda M. Hodgdon

SUBJECT: AWARD OF CONTRACT FOR CATEGORY 2 – NETWORK & APPLICATION PENETRATION TESTING SERVICES

Attached for your approval are the contract documents for three Statewide contracts for Category 2, Network & Application Penetration Testing Services, which we are recommending. These contracts will run for a period of approximately 39 months until 1/31/17. This bid allows for the award of up to three contracts.

This recommendation is based on an evaluation of responses to State's RFB #1560-14.

Commissioner's signature is requested on the attached documents as indicated by signature arrows.

Vendors Contracts for Approval:

Coalfire

UHY

Enterprise Risk Management

STATE OF NEW HAMPSHIRE APPROVAL SIGNATURE PAGE

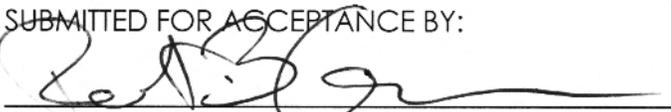
VENDOR COALFIRE SYSTEMS, INC.

CONTRACT FOR AWARD OF BID 1560-14 FOR CATEGORY 2 – NETWORK & APPLICATION PENETRETION TESTING SERVICES

EFFECTIVE THROUGH JANUARY 31, 2017

* * * * *

SUBMITTED FOR ACCEPTANCE BY:


ROBERT LAWSON, PURCHASING AGENT
BUREAU OF PURCHASE AND PROPERTY

DATE 9/16/13

REVIEWED BY:


RUDOLPH W. OGDEN, ADMINISTRATOR
BUREAU OF PURCHASE AND PROPERTY

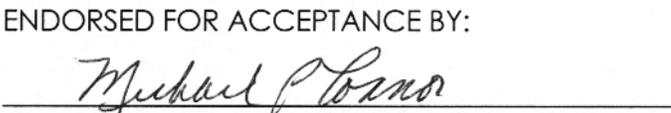
DATE 9/16/13

RECOMMENDED FOR ACCEPTANCE BY:


ROBERT STOWELL, ADMINISTRATOR
BUREAU OF PURCHASE AND PROPERTY

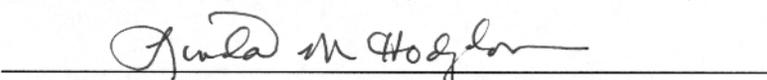
DATE 9/18/13

ENDORSED FOR ACCEPTANCE BY:


MICHAEL P. CONNOR, DEPUTY COMMISSIONER,
DEPARTMENT OF ADMINISTRATIVE SERVICES

DATE 9/18/13

ACCEPTED FOR THE STATE OF NEW HAMPSHIRE UNDER THE AUTHORITY GRANTED TO ME BY NEW HAMPSHIRE REVISED STATUTES, ANNOTATED 21-I:14, XII.


LINDA M. HODGDON, COMMISSIONER
DEPARTMENT OF ADMINISTRATIVE SERVICES

DATE 9/23/13

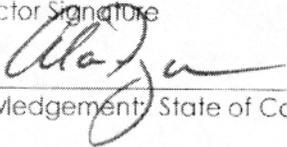
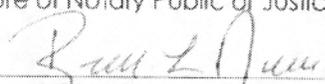
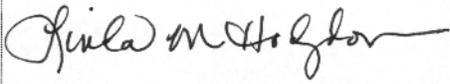
Subject: CATEGORY 2 – NETWORK & APPLICATION PENETRATION TESTING SERVICES

AGREEMENT

The State of New Hampshire and the Contractor hereby mutually agree as follows:

GENERAL PROVISIONS

1. IDENTIFICATION.

1.1 State Agency Name State of New Hampshire Administrative Services		1.2 State Agency Address 25 Capitol Street, Room 102 Concord, NH 03301	
1.3 Contractor Name Coalfire Systems Inc.		1.4 Contractor Address 361 Centennial Parkway, Ste. 150, Louisville, CO 80027	
1.5 Contractor Phone Number 877 224-8077	1.6 Account Number	1.7 Completion Date January 31, 2017	1.8 Price Limitation \$360,000.00
1.9 Contracting Officer for State Agency Robert Lawson, Purchasing Agent		1.10 State Agency Telephone Number 603-271-3147	
1.11 Contractor Signature 		1.12 Name and Title of Contractor Signatory Alan Ferguson, Executive Vice President	
1.13 Acknowledgement: State of Colorado County of Boulder On <u>Sept 13, 2013</u> , before the undersigned officer, personally appeared the person identified in block 1.12, or satisfactorily proven to be the person whose name is signed in block 1.11, and acknowledged that s/he executed this document in the capacity indicated in block 1.12.			
1.13.1 Signature of Notary Public or Justice of the Peace [Seal] 		<div style="border: 2px solid black; padding: 5px; text-align: center;"> REBECCA L NAVARRO NOTARY PUBLIC STATE OF COLORADO </div>	
1.13.2 Name and Title of Notary or Justice of the Peace <u>Rebecca L Navarro</u>			
1.14 State Agency Signature 		1.15 Name and Title of State Agency Signatory Linda M. Hodgdon, Commissioner Administrative Services	
1.16 Approval by the N.H. Department of Administration, Division of Personnel (if applicable) By: _____ Director, On: _____			
1.17 Approval by the Attorney General (Form, Substance and Execution) By: _____ On: _____			
1.18 Approval by the Governor and Executive Council By: _____ On: _____			

2. EMPLOYMENT OF CONTRACTOR/SERVICES TO BE PERFORMED. The State of New Hampshire, acting through the agency identified in block 1.1 ("State"), engages contractor identified in block 1.3 ("Contractor") to perform, and the Contractor shall perform, the work or sale of goods, or both, identified and more particularly described in the attached EXHIBIT A which is incorporated herein by reference ("Services").

3. EFFECTIVE DATE/COMPLETION OF SERVICES.

3.1 Notwithstanding any provision of this Agreement to the contrary, and subject to the approval of the Governor and Executive Council of the State of New Hampshire, this Agreement, and all obligations of the parties hereunder, shall not become effective until the date the Governor and Executive Council approve this Agreement ("Effective Date").

3.2 If the Contractor commences the Services prior to the Effective Date, all Services performed by the Contractor prior to the Effective Date shall be performed at the sole risk of the Contractor, and in the event that this Agreement does not become effective, the State shall have no liability to the Contractor, including without limitation, any obligation to pay the Contractor for any costs incurred or Services performed. Contractor must complete all Services by the Completion Date specified in block 1.7.

4. CONDITIONAL NATURE OF AGREEMENT. Notwithstanding any provision of this Agreement to the contrary, all obligations of the State hereunder, including, without limitation, the continuance of payments hereunder, are contingent upon the availability and continued appropriation of funds, and in no event shall the State be liable for any payments hereunder in excess of such available appropriated funds. In the event of a reduction or termination of appropriated funds, the State shall have the right to withhold payment until such funds become available, if ever, and shall have the right to terminate this Agreement immediately upon giving the Contractor notice of such termination. The State shall not be required to transfer funds from any other account to the Account identified in block 1.6 in the event funds in that Account are reduced or unavailable.

5. CONTRACT PRICE/PRICE LIMITATION/ PAYMENT.

5.1 The contract price, method of payment, and terms of payment are identified and more particularly described in EXHIBIT B which is incorporated herein by reference.

5.2 The payment by the State of the contract price shall be the only and the complete reimbursement to the Contractor for all expenses, of whatever nature incurred by the Contractor in the performance hereof, and shall be the only and the complete compensation to the Contractor for the Services. The State shall have no liability to the Contractor other than the contract price.

5.3 The State reserves the right to offset from any amounts otherwise payable to the Contractor under this Agreement those liquidated amounts required or permitted by N.H. RSA 80:7 through RSA 80:7-c or any other provision of law.

5.4 Notwithstanding any provision in this Agreement to the contrary, and notwithstanding unexpected circumstances, in no event shall the total of all payments authorized, or actually made hereunder, exceed the Price Limitation set forth in block 1.8.

6. COMPLIANCE BY CONTRACTOR WITH LAWS AND REGULATIONS/ EQUAL EMPLOYMENT OPPORTUNITY.

6.1 In connection with the performance of the Services, the Contractor shall comply with all statutes, laws, regulations, and orders of federal, state, county or municipal authorities which impose any obligation or duty upon the Contractor, including, but not limited to, civil rights and equal opportunity laws. In addition, the Contractor shall comply with all applicable copyright laws.

6.2 During the term of this Agreement, the Contractor shall not discriminate against employees or applicants for employment because of race, color, religion, creed, age, sex, handicap, sexual orientation, or national origin and will take affirmative action to prevent such discrimination.

6.3 If this Agreement is funded in any part by monies of the United States, the Contractor shall comply with all the provisions of Executive Order No. 11246 ("Equal Employment Opportunity"), as supplemented by the regulations of the United States Department of Labor (41 C.F.R. Part 60), and with any rules, regulations and guidelines as the State of New Hampshire or the United States issue to implement these regulations. The Contractor further agrees to permit the State or United States access to any of the Contractor's books, records and accounts for the purpose of ascertaining compliance with all rules, regulations and orders, and the covenants, terms and conditions of this Agreement.

7. PERSONNEL.

7.1 The Contractor shall at its own expense provide all personnel necessary to perform the Services. The Contractor warrants that all personnel engaged in the Services shall be qualified to perform the Services, and shall be properly licensed and otherwise authorized to do so under all applicable laws.

7.2 Unless otherwise authorized in writing, during the term of this Agreement, and for a period of six (6) months after the Completion Date in block 1.7, the Contractor shall not hire, and shall not permit any subcontractor or other person, firm or corporation with whom it is engaged in a combined effort to perform the Services to hire, any person who is a State employee or official, who is materially involved in the procurement, administration or performance of this Agreement. This provision shall survive termination of this Agreement.

7.3 The Contracting Officer specified in block 1.9, or his or her successor, shall be the State's representative. In the event of any dispute concerning the interpretation of this Agreement, the Contracting Officer's decision shall be final for the State.

8. EVENT OF DEFAULT/REMEDIES.

8.1 Any one or more of the following acts or omissions of the Contractor shall constitute an event of default hereunder ("Event of Default"):

8.1.1 failure to perform the Services satisfactorily or on schedule;

8.1.2 failure to submit any report required hereunder; and/or

8.1.3 failure to perform any other covenant, term or condition of this Agreement.

8.2 Upon the occurrence of any Event of Default, the State may take any one, or more, or all, of the following actions:

8.2.1 give the Contractor a written notice specifying the Event of Default and requiring it to be remedied within, in the absence of a greater or lesser specification of time, thirty (30) days from the date of the notice; and if the Event of Default is not timely remedied, terminate this Agreement, effective two (2) days after giving the Contractor notice of termination;

8.2.2 give the Contractor a written notice specifying the Event of Default and suspending all payments to be made under this Agreement and ordering that the portion of the contract price which would otherwise accrue to the Contractor during the period from the date of such notice until such time as the State determines that the Contractor has cured the Event of Default shall never be paid to the Contractor;

8.2.3 set off against any other obligations the State may owe to the Contractor any damages the State suffers by reason of any Event of Default; and/or

8.2.4 treat the Agreement as breached and pursue any of its remedies at law or in equity, or both.

9. DATA/ACCESS/CONFIDENTIALITY/ PRESERVATION.

9.1 As used in this Agreement, the word "data" shall mean all information and things developed or obtained during the performance of, or acquired or developed by reason of, this Agreement, including, but not limited to, all studies, reports, files, formulae, surveys, maps, charts, sound recordings, video recordings, pictorial reproductions, drawings, analyses, graphic representations, computer programs, computer printouts, notes, letters, memoranda, papers, and documents, all whether finished or unfinished.

9.2 All data and any property which has been received from the State or purchased with funds provided for that purpose under this Agreement, shall be the property of the State, and shall be returned to the State upon demand or upon termination of this Agreement for any reason.

9.3 Confidentiality of data shall be governed by N.H. RSA chapter 91-A or other existing law. Disclosure of data requires prior written approval of the State.

10. TERMINATION. In the event of an early termination of this Agreement for any reason other than the completion of the Services, the Contractor shall deliver to the Contracting Officer, not later than fifteen (15) days after the date of termination, a report ("Termination Report") describing in detail all Services performed, and the contract price earned, to and including the date of termination. The form, subject matter, content, and number of copies of the Termination Report shall be identical to those of any Final Report described in the attached EXHIBIT A.

11. CONTRACTOR'S RELATION TO THE STATE. In the performance of this Agreement the Contractor is in all respects an independent contractor, and is neither an agent nor an employee of the State. Neither the Contractor nor any of its officers, employees, agents or members shall have authority to bind the State or receive any benefits, workers' compensation or other emoluments provided by the State to its employees.

12. ASSIGNMENT/DELEGATION/SUBCONTRACTS. The Contractor shall not assign, or otherwise transfer any interest in this Agreement without the prior written consent of the N.H. Department of Administrative Services. None of the Services shall be subcontracted by the Contractor without the prior written consent of the State.

13. INDEMNIFICATION. The Contractor shall defend, indemnify and hold harmless the State, its officers and employees, from and against any and all losses suffered by the State, its officers and employees, and any and all claims, liabilities or penalties asserted against the State, its officers and employees, by or on behalf of any person, on account of, based or resulting from, arising out of (or which may be claimed to arise out of) the acts or omissions of the Contractor. Notwithstanding the foregoing, nothing herein contained shall be deemed to constitute a waiver of the sovereign immunity of the State, which immunity is hereby reserved to the State. This covenant in paragraph 13 shall survive the termination of this Agreement.

14. INSURANCE.

14.1 The Contractor shall, at its sole expense, obtain and maintain in force, and shall require any subcontractor or assignee to obtain and maintain in force, the following insurance:

14.1.1 comprehensive general liability insurance against all claims of bodily injury, death or property damage, in amounts of not less than \$250,000 per claim and \$2,000,000 per occurrence; and

14.1.2 fire and extended coverage insurance covering all property subject to subparagraph 9.2 herein, in an amount not less than 80% of the whole replacement value of the property.

14.2 The policies described in subparagraph 14.1 herein shall be on policy forms and endorsements approved for use in the State of New Hampshire by the N.H. Department of Insurance, and issued by insurers licensed in the State of New Hampshire.

A.P.
9/13/13

14.3 The Contractor shall furnish to the Contracting Officer identified in block 1.9, or his or her successor, a certificate(s) of insurance for all insurance required under this Agreement. Contractor shall also furnish to the Contracting Officer identified in block 1.9, or his or her successor, certificate(s) of insurance for all renewal(s) of insurance required under this Agreement no later than fifteen (15) days prior to the expiration date of each of the insurance policies. The certificate(s) of insurance and any renewals thereof shall be attached and are incorporated herein by reference. Each certificate(s) of insurance shall contain a clause requiring the insurer to endeavor to provide the Contracting Officer identified in block 1.9, or his or her successor, no less than ten (10) days prior written notice of cancellation or modification of the policy.

15. WORKERS' COMPENSATION.

15.1 By signing this agreement, the Contractor agrees, certifies and warrants that the Contractor is in compliance with or exempt from, the requirements of N.H. RSA chapter 281-A ("Workers' Compensation").

15.2 To the extent the Contractor is subject to the requirements of N.H. RSA chapter 281-A, Contractor shall maintain, and require any subcontractor or assignee to secure and maintain, payment of Workers' Compensation in connection with activities which the person proposes to undertake pursuant to this Agreement. Contractor shall furnish the Contracting Officer identified in block 1.9, or his or her successor, proof of Workers' Compensation in the manner described in N.H. RSA chapter 281-A and any applicable renewal(s) thereof, which shall be attached and are incorporated herein by reference. The State shall not be responsible for payment of any Workers' Compensation premiums or for any other claim or benefit for Contractor, or any subcontractor or employee of Contractor, which might arise under applicable State of New Hampshire Workers' Compensation laws in connection with the performance of the Services under this Agreement.

16. WAIVER OF BREACH. No failure by the State to enforce any provisions hereof after any Event of Default shall be deemed a waiver of its rights with regard to that Event of Default, or any subsequent Event of Default. No express failure to enforce any Event of Default shall be deemed a waiver of the right of the State to enforce each and all of the provisions hereof upon any further or other Event of Default on the part of the Contractor.

17. NOTICE. Any notice by a party hereto to the other party shall be deemed to have been duly delivered or given at the time of mailing by certified mail, postage prepaid, in a United States Post Office addressed to the parties at the addresses given in blocks 1.2 and 1.4, herein.

18. AMENDMENT. This Agreement may be amended, waived or discharged only by an instrument in writing signed by the parties hereto and only after approval of such amendment, waiver or discharge by the Governor and Executive Council of the State of New Hampshire.

19. CONSTRUCTION OF AGREEMENT AND TERMS. This Agreement shall be construed in accordance with the laws of the State of New Hampshire, and is binding upon and inures to the benefit of the parties and their respective successors and assigns. The wording used in this Agreement is the wording chosen by the parties to express their mutual intent, and no rule of construction shall be applied against or in favor of any party.

20. THIRD PARTIES. The parties hereto do not intend to benefit any third parties and this Agreement shall not be construed to confer any such benefit.

21. HEADINGS. The headings throughout the Agreement are for reference purposes only, and the words contained therein shall in no way be held to explain, modify, amplify or aid in the interpretation, construction or meaning of the provisions of this Agreement.

22. SPECIAL PROVISIONS. Additional provisions set forth in the attached EXHIBIT C are incorporated herein by reference.

23. SEVERABILITY. In the event any of the provisions of this Agreement are held by a court of competent jurisdiction to be contrary to any state or federal law, the remaining provisions of this Agreement will remain in full force and effect.

24. ENTIRE AGREEMENT. This Agreement, which may be executed in a number of counterparts, each of which shall be deemed an original, constitutes the entire Agreement and understanding between the parties, and supersedes all prior Agreements and understandings relating hereto.

EXHIBIT A
SCOPE OF SERVICES

1. INTRODUCTION

Coalfire Systems, Inc. (hereinafter referred to as the "Contractor") hereby agrees to provide the State of New Hampshire with CATEGORY 2 – Network Application Penetration Testing Services in accordance with NH State Bid #1560-14 and as described herein.

2. CONTRACT DOCUMENTS

This Contract consists of the following documents ("Contract Documents") in order of precedence:

- a. State of New Hampshire Terms and Conditions, General Provisions Form P-37
- b. EXHIBIT A Scope of Services
- c. EXHIBIT B Payment Schedule
- d. EXHIBIT C Special Provisions
- e. EXHIBIT D RFB 1560-14

3. TERM OF CONTRACT

This contract shall commence upon the approval of Commissioner of the Department of Administrative Services through January 31, 2017, a period of approximately thirty nine (39) months. The contract may be extended for additional periods of time thereafter under the same terms, conditions and pricing structure upon the mutual agreement between the Contractor and the Bureau of Purchase and Property, subject to the approval of the Commissioner of the Department of Administrative Services; however the contract shall not exceed a period of more than five (5) years.

4. CONTRACTOR RESPONSIBILITY

Contractor shall be solely responsible for meeting all terms and conditions specified in this Contract.

5. TERMINATION

The State of New Hampshire shall have the right to terminate the Contract at any time by giving the Contractor a thirty (30) day written notice.

6. OBLIGATIONS AND LIABILITY OF THE CONTRACTOR

Contractor shall complete all work to the satisfaction of the State and in accordance with the specifications herein mentioned, at the price herein agreed upon and fixed therefore. All the work, labor and equipment to be done and furnished under this Contract, shall be done and furnished strictly pursuant to, and in conformity with the specifications described herein, and the directions of the State representatives as given from time to time during the progress of the work, under the terms of this Contract.

The Contractor shall take all responsibility for the work under this Contract. They shall in no way be relieved of their responsibility by any right of the State to give permission or issue orders relating to any part of the work; or by any such permission given on orders issued or by failure of the State to give such permission or issue such orders.

7. GENERAL REQUIREMENTS

Contractor shall provide CATEGORY 2 – Network & Application Penetration Testing Services to meet ongoing Payment Card Industry Data Security Standard (PCI DSS) security and monitoring requirements as established by the Security Standards Council. These services include, but are not limited to: network penetration testing and application penetration testing services. This Contract may be used by the State of New Hampshire agencies and institutions during the term of the Contract.

Services shall be consistent with all the terms and conditions set forth in this Contract.

Contractor shall be solely responsible for meeting all terms and conditions in this Contract.

8. SCOPE OF SERVICES

Contractor shall be certified by the PCI Security Standards Council for PCI DSS compliance services by Visa, MasterCard, American Express and Discover as a Qualified Security Assessor (QSA). Contractor shall be required to continue to be PCI certified as required while performing PCI services for the State.

All testing must be done from locations within the United States of America. Access will not be provided to foreign IP addresses.

Services shall be provided as needed for Agency Merchants throughout the term of the Contract.

During the term of the Contract the State may add or delete locations as needed. Any location deleted during the term of the Contract will only be responsible for payment for services received up to that point.

During the term of the Contract locations may be added by requesting the Contractor to provide a quotation for that new location. Pricing quotations submitted for new locations shall be in line with the pricing structure in this Contract.

Services shall be completed in a reasonable time frame as mutually agreed upon with agency and Contractor. The Contractor shall submit a proposed schedule to the state agency requesting services at each facility at least ten (10) days prior to each period.

Penetration Testing Services

Contractor shall be a Qualified Security Assessor (QSA) who can provide services that allow agencies to comply with PCI Security Standards Council PCI DSS Requirements 6.6 and 11.3 for network penetration and application penetration testing. Services shall include:

TABLE 1 PENETRATION TESTING SERVICES

Network-layer penetration tests (PCI DSS Requirement 11.3.1) PCI DSS requirement 11 requires that penetration tests be conducted at least annually or after any significant change to your network. The Contractor shall provide a service designed to satisfy these requirements and include the following
--

<u>Enumeration</u> : A list of targeted and authorized IP addresses shall be
--

<p>developed based on State provided data (domain names, network blocks and individual IP addresses). This includes intelligent domain name resolution in which dynamic, periodic name resolution is employed in order to discover load-balancing architectures that utilize multiple public IP addresses</p>
<p><u>Inventory</u>: The Contractor shall determine which of the enumerated IP addresses are actually running, available and offering network services. Host inventory uses a number of techniques, including ICMP pings, common TCP service probes, and protocol-specific UDP service probes. In local, LAN-based scans, ARP queries also reveal active systems. Open services shall be probed by the Contractor for any information that can be used to verify the actual application layer protocol (e.g., HTTP), as well as Contractor applications (e.g. Apache, IIS, Netscape, Domino) and version</p>
<p><u>System Discovery</u>: The Contractor attempts to identify other IP addresses associated with the target IP addresses. Typical discovery methods include DNS record lookups and various dynamic port mapping techniques (e.g., DCE Endpoint Mapping and Java RMI Registry probes)</p>
<p><u>Vulnerability Checks</u>: The Contractor shall perform specific checks for vulnerabilities on all accessible host IP addresses and services</p>
<p><u>Manual Analysis and Verification</u>: The Contractor shall perform manual verification and analysis of the discovered vulnerabilities on Internet facing systems to identify security holes and eliminate false positives. Upon completion of the testing, a report shall be provided by the Contractor documenting the findings and include high-level recommendations. All testing phases shall be coordinated with the State to minimize any adverse impact that may occur as a result of the services</p>
<p>Application-layer penetration tests (PCI DSS Requirements 6.6 and 11.3.2) PCI DSS require that application reviews and penetration tests be conducted at least annually or after any significant change to your application. The Contractor shall provide a service designed to satisfy these requirements and include the following</p>
<p><u>Manual Analysis and Verification</u>: Contractor shall perform manual web application vulnerability assessment based on PCI DSS Requirements 6.5 and 11.3.1</p>
<p><u>Vulnerability Checks</u>: Contractor shall perform specific checks for vulnerabilities on all accessible host IP addresses and services</p>

Guarantee of Business Volume

There is no minimum amount of business guaranteed under this Contract. Agencies will use this Contact as necessary. Contractor shall have adequate personnel to fulfill contract requirements but should have sufficient existing business to sustain those personnel without relying on business from the State.

9. AGENCIES AS MERCHANTS

Below is a list of Merchant agencies that are processing credit cards with their annual sales and transaction volume as of 2012.

Ref#	Agency / Boards Accepting Merchant Cards	Locations Processing Merchant Card Transactions	Totals	
			Gross Sales	Gross Transactions
1	Administration of the Courts	82	\$ 5,382,241.39	26,798
2	Agriculture Department	1	\$ 22,892.00	847
3	Corrections Department	1	\$ 152,364.29	678
4	Education Department	1	\$ 945,445.00	8,270
5	Environmental Services Department	1	\$ 152,852.96	592
6	Fish & Game Department	1	\$ 239,567.25	3,475
7	Health and Human Services Department	1	\$ 255,228.16	830
8	Joint Board of Licensure	1	\$ 1,269,910.37	7,788
9	Liquor Commission	82	\$ 337,381,899.79	5,824,069
10	Lottery Commission ³	1	\$ 373,100.00	2,944
11	Nursing, Board of	1	\$ 1,386,445.00	16,977
12	Pease Development Authority	2	\$ 749,699.26	3,330
13	Resources & Economic Development	19	\$ 7,019,664.53	311,056
14	Safety Department	28	\$ 18,072,311.63	233,001
15	Secretary of State	1	\$ 7,059,484.00	65,342
16	Transportation Department	1	\$ 315,004.00	13,392
	Total	224	\$ 380,778,109.63	6,519,389

Contractor Initials *G.F.*
 Date *9/13/13*

10. CONTRACTOR PERSONNEL QUALIFICATIONS

As required by PCI DSS, the Contractor shall assign certified consultants to validate the State's compliance with the data security requirements.

In the event the Contractor proposes a foreign national to perform the testing, the Contractor shall provide the State with copies of all security checks and clearance reports as well as documentation of their foreign labor certification.

11. SUBCONTRACTOR

Contractor shall be solely responsible for meeting all terms and conditions specified in this Contract. Any subcontractor shall first be approved by the State. The Contractor shall remain wholly responsible for performance under the Contract and will be considered the sole point of contact with regard to all contractual matters, including payment of any and all charges.

Subcontractors will only be considered if they have a minimum of three years of successful experience providing the required services.

12. CONFIDENTIALITY & CRIMINAL RECORD

If Applicable, by the using agency, the Contractor shall have signed by each of employees or its approved sub-contractor(s), if any, working in the office or externally with the State of New Hampshire records a Confidentiality form and Criminal Record Authorization Form. These forms shall be returned to the individual using agency prior to the start of any work.

13. PRE-ENGAGEMENT CHECKLIST

Contractor shall agree to use the Pre-Engagement Checklists found in **Attachment 1** of this Contract.

This form will be used by a requesting agency to convey to all the Contractors the services they are requesting. The Contractor shall use this Checklist to generate a quote to the Agency based on their contracted hourly rates. All Contractors will have the opportunity to submit such a quote and a Purchase Order, if issued, will go to the Contractor submitting the lowest priced quotation.

Agencies shall provide the pre-engagement checklist to the Contractors to ensure they provide the adequate details as to the scope of each individual engagement.

14. PRICING QUOTATIONS

Agencies may request quotations from all Contractors by providing a Statement of Work (SOW) describing the services required as well as the Pre-Engagement Checklist. If appropriate, the Contractors may be allowed to view code or facilities after the execution of confidentiality agreements. Contractors shall return pricing quotations within five (5) business days. If additional information has been circulated to all Contractors, they will have one (1) extra business day to revise their quotation. The specified hourly rates shall not exceed the rates quoted under this Contract.

15. ORDERING PROCEDURE FOR SERVICES

Agencies shall process purchase orders complete with attached quote for services procured under this contract. The Bureau of Purchase and Property will issue purchase orders in excess of \$500 on behalf of the State agencies.

ATTACHMENT 1

Network Penetration Testing: Pre-Engagement Checklist

These questions are intended to help the Contractor understand your agency's needs for an assessment to validate your compliance with the Payment Card Industry Data Security Standard (PCI DSS0 v1.2).

Agency Information

Contact Name		
Name of Organization		
Mailing Address		
City, State, Zip Code		
Telephone Number		
Fax Number		
E-mail Address		
Policy and Procedures		
Do information security policies and procedures currently exist?	Yes	No
Can these documents be made available to contractor analysts?	Yes	No

Network Penetration Testing – Automated and manual attacks. Comprehensive but will not exploit identified vulnerabilities.

Question	Answer
How large is the IP space to be assessed? Please provide the subnets/IP addresses.	
How many hosts are in scope as part of this assessment?	
Are any systems or devices in scope hosted by a third party?	
Are brute-force attacks and password cracking in scope?	
Are there any timing restrictions on the testing?	
Provide logical diagrams showing system and/or subnet boundaries, location of protection devices (firewall, IDS, IPS) and of interconnections with other systems, flow/locations of cardholder data.	

Internal Network Characteristics (Please provide the following information about your internal network to accurately determine your assessment needs.)

Deployed Critical applications (For each deployed critical application, please provide the following information)

Name of Application		Purpose of Application	
Deployed Internal Servers (For each deployed internal server, please provide the following information)			
Type of Server		Number of Servers	
Deployed End-User Workstations (For each type of deployed end-user workstation, please provide the following information)			
Type of Workstation		Number of Workstations	
Number of End-Users			
Total number of End-Users			
Type of Physical Network			
Wired		Yes	No
Wireless		Yes	No

Security Devices within the Internal Network (Please indicate with a check mark which security devices are deployed within your organization's internal network; then provide the additional requested information about the types and numbers of devices.

Device			Type(s) of Devices	Number of Devices
Firewalls	Yes	No	Type(s)	Number
Intrusion Detection or Prevention System			Type(s)	Number
Host based	Yes	No		
Network based	Yes	No		
Logging			Type(s)	Number
Host based	Yes	No		
Network based	Yes	No		
Are log analysis tools used to generate reports?			Yes	No
SPAM Filter	Yes	No	Type(s)	Number
Encryption/VPN	Yes	No	Type(s)	Number
Authentication (e.g., tokens, biometrics)	Yes	No	Type(s)	Number
Anti-Virus			Type(s)	Number
Host based	Yes	No		
Network based	Yes	No		
Gateway based	Yes	No		

Application Penetration Testing: Pre-Engagement Checklist

These questions are intended to help the Contractor understand your agency's needs for an assessment to validate your compliance with the Payment Card Industry Data Security Standard (PCI DSS0 v1.2).

Agency Information

Contact Name			
Name of Organization			
Mailing Address			
City, State, Zip Code			
Telephone Number			
Fax Number			
E-mail Address			
Policy and Procedures			
Do information security policies and procedures currently exist?		Yes	No
Can these documents be made available to Contractor analysts?		Yes	No

Application Penetration Testing: Automated and manual attacks.

Question	Answer
Written description of the Cardholder Data Environment (CDE) – e.g. CDE system boundaries, description of how the CDE is segregated from the rest of the agency's systems, major components and/or subnets, interconnections with other systems (including ISPs and any other information system to which this system is connected, such as business partners and separately-managed information systems within the organization), flow/locations of cardholder data, etc.	
What applications are in scope and what are their names/URLs?	
What is the type of application (Web, Thick-client, etc.)?	
Is the application available over the Internet? If not, what location does the testing team need to be at in order to test?	
How many URLs are required to access the application components (basic application functions, administration)?	
Is the application in a test or production environment?	

Does the application provide both a web interface and a web services interface?	
What is the web application/web services platform?	
What other technologies are involved in the web application's n-Tier architecture?	
Is a current application design diagram available for the application architecture including platforms, locations of customer data, network-based controls, etc.? If so, please provide.	
Was the application purchased from a vendor, developed in-house or the result of an outsourced development project?	
What is the total number and type of authorization levels in scope for this assessment (anonymous, admin, workflow)?	
What type of authentication is required (password, OTP token, certificate)?	
How many form fields exist or how many dynamic pages exist and what is the average inputs per page?	
What languages are used (C, C++, Java)?	
What is the development platform (.Net, J2EE, ColdFusion)?	
Which application server or middleware is used (Weblogic, Websphere)?	
What database server is used (Oracle, MS SQL, DB2)?	

EXHIBIT B
PAYMENT TERMS

The contract price limitation for this contract is \$360,000.00. The following pricing and payment terms apply:

INVOICING:

Invoices shall be submitted after completion of work to the requesting agency.

No reimbursement by the State for travel time or mileage shall be allowed.

PAYMENTS:

Payment shall be paid in full within thirty (30) days after receipt of invoice and acceptance of the work to the State's satisfaction. Said payments shall be made electronically or by a check mailed to the address in Section 1.4 of this Contract.

COST TABLES

COST OF SERVICES:

Table 1 –
 PENETRATION
 TESTING PRICING
 COMBINED RATE

Tasks	
10/13/2013 – 10/12/2014	<u>Hourly Rate</u>
Network-layer Penetration Tests / Hourly Rate	\$ 165.00
Application-layer Penetration Tests / Hourly Rate	\$ 165.00

10/13/2014 – 10/12/2015	
Network-layer Penetration Tests / Hourly Rate	\$ 165.00
Application-layer Penetration Tests / Hourly Rate	\$ 165.00

10/13/2015 – 10/12/2016	
Network-layer Penetration Tests / Hourly Rate	\$ 165.00
Application-layer Penetration Tests / Hourly Rate	\$ 165.00

EXHIBIT C
SPECIAL PROVISIONS

1. Delete Paragraph 14.1.1 and substitute the following: comprehensive general liability insurance against all claims of bodily injury, death or property damage, in amounts of not less than \$250,000 per claim and \$1,000,000 per incident and no less than \$1,000,000 in excess/umbrella liability each occurrence; and
2. There are no other special provisions for this contract.

EXHIBIT D

RFB 1560-14 is incorporated herewith.

Contractor Initials A.F.
Date 9/13/13

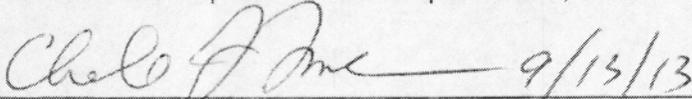
CERTIFICATE OF VOTE OF AUTHORIZATION

September 13, 2013

I, Charles J. Friedman, hereby do represent and certify that:

- (1) I am Corporate Secretary of Coalfire Systems, Inc., a Delaware corporation (the "Corporation").
- (2) I am familiar with the books and records and minutes of the Corporation.
- (3) I am duly authorized to issue certificates with respect to the contents of such books and records.
- (4) The following statements are true and accurate based on the resolutions adopted by the Board of Directors of the Corporation on February 7, 2011 in accordance with Delaware law and the current by-laws of the Corporation.
 - (a) The signature of Alan Ferguson, Vice President of this Corporation, affixed to any contract instrument or document shall bind the Corporation to the terms and conditions of the contract instrument or document.
 - (b) The foregoing signature authority has not been revoked, annulled or amended in any manner whatsoever, and remains in full force and effect as of the date hereof.

IN WITNESS WHEREOF, I have hereunto set my hand as Corporate Secretary of the Corporation and have affixed its corporate seal this September 13, 2013.

 9/13/13

Charles J. Friedman, Corporate Secretary, September 13, 2013

(SEAL)

STATE OF COLORADO

BOULDER COUNTY

On this 13th day of September, 2013, before me, Rebecca Navarro, personally appeared Charles J. Friedman and acknowledged himself to be the Corporate Secretary of Coalfire Systems, Inc., a Delaware corporation, and that he, as such being authorized to do so, executed the foregoing instrument.

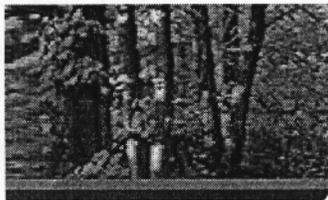
IN WITNESS WHEREOF, I hereunder set my hand and official seal.


Notary Public

My Commission Expires:

8/14

REBECCA L NAVARRO
NOTARY PUBLIC
STATE OF COLORADO



NEW HAMPSHIRE

Corporation Division

Search
 By Business Name
 By Business ID
 By Registered Agent
 Annual Report
 File Online

Date: 8/14/2013 **Filed Documents**
 (Annual Report History, View Images, etc.)

Business Name History

Name	Name Type
Coalfire Systems, Inc.	Legal
Coalfire Systems, Inc.	Home State

Corporation - Foreign - Information

Business ID:	616727
Status:	Good Standing
Entity Creation Date:	7/16/2009
State of Business.:	DE
Principal Office Address:	361 Centennial Parkway Suite 150 Louisville CO 80027
Principal Mailing Address:	No Address
Last Annual Report Filed Date:	1/7/2013
Last Annual Report Filed:	2013

Registered Agent

Agent Name:	Business Filings Incorporated
Office Address:	9 Capitol Street Concord NH 03301

Mailing Address:

Important Note: The status reflected for each entity on this website only refers to the status of the entity's filing requirements with this office. It does not necessarily reflect the disciplinary status of the entity with any state agency. Requests for disciplinary information should be directed to agencies with licensing or other regulatory authority over the entity.

DESCRIPTIONS (Continued from Page 1)

WC Policy Limit: \$1,000,000

WC Each Employee Limit: \$1,000,000

Coalfire

STATE OF NEW HAMPSHIRE BID TRANSMITTAL LETTER

Date: August 2, 2013

Company Name: Coalfire Systems, Inc.

Address: 361 Centennial Parkway, Ste. 150

Louisville, CO 80027

To, Point of Contact: ROBERT LAWSON
Telephone: (603) 271-3147
Email: prcnweb@inn.gov

RFP Bid Invitation Name: CATEGORY 2 - Network & Application Penetration Testing Services
Bid Number: RFB 1560-14
Bid Opening Date and Time: 8/5/13 @ 11:30 AM

[Insert name of signor] Alan Ferguson, on behalf of Coalfire Systems, Inc. [insert name of entity submitting bid (collectively referred to as "Vendor")] hereby submits an offer as contained in the written bid submitted herewith ("Bid") to the State of New Hampshire in response to BID # 1560-14 for CATEGORY 2 - Network & Application Penetration Testing Services or the price(s) quoted herein in complete accordance with the bid.

Vendor attests to the fact that:

1. The Vendor has reviewed and agreed to be bound by the Bid.
2. The Vendor has not altered any of the language or other provisions contained in the Bid document.
3. The Bid is effective for a period of 180 days from the Bid Opening date as indicated above.
4. The prices Vendor has quoted in the Bid were established without collusion with other vendors.
5. The Vendor has read and fully understands this Bid.
6. Further, in accordance with RSA 214:11-c, the undersigned Vendor certifies that neither the Vendor nor any of its subsidiaries, affiliates or principal officers (principal officers refers to individuals with management responsibility for the entity or association):
 - a. Has, within the past 2 years, been convicted of, or pleaded guilty to, a violation of RSA 356:2, RSA 356:4, or any state or federal law or county or municipal ordinance prohibiting specified bidding practices, or involving antitrust violations, which has not been annulled.
 - b. Has been prohibited, either permanently or temporarily, from participating in any public works project pursuant to RSA 638:20.
 - c. Has previously provided false, deceptive, or fraudulent information on a vendor code number application form, or any other document submitted to the state of New Hampshire, which information was not corrected as of the time of the filing a bid, proposal, or quotation.
 - d. Is currently debarred from performing work on any project of the federal government or the government of any state.
 - e. Has, within the past 2 years, failed to cure a default on any contract with the federal government or the government of any state.
 - f. Is presently subject to any order of the department of labor, the department of employment security, or any other state department, agency, board, or commission, finding that the applicant is not in compliance with the requirements of the laws or rules that the department, agency, board, or commission is charged with implementing.
 - g. Is presently subject to any sanction or penalty finally issued by the department of labor, the department of employment security, or any other state department, agency, board, or commission, which sanction or penalty has not been fully discharged or fulfilled.
 - h. Is currently serving a sentence or is subject to a continuing or unfulfilled penalty for any crime or violation noted in this section.
 - i. Has failed or neglected to advise the division of any conviction, plea of guilty, or finding relative to any crime or violation noted in this section, or of any debarment, within 30 days of such conviction, plea, finding, or debarment; or
 - j. Has been placed on the debarred parties list described in RSA 214:11-c within the past year.

Authorized Signor's Signature [Signature] Authorized Signor's Title Exec. VP, Sales

NOTARY PUBLIC/JUSTICE OF THE PEACE

COUNTY: Boulder STATE: CO ZIP: 80027

On the 2nd day of August, 2013, personally appeared before me, the above named Alan Ferguson, in his/her capacity as authorized representative of Coalfire Systems known to me or satisfactorily proven, and took oath that the foregoing is true and accurate to the best of his/her knowledge and belief.

In witness thereof, I hereunto set my hand and official seal.

[Signature: Mary S. Nelson]
(Notary Public/Justice of the Peace)



My commission expires: 04/08/2015 (Date)

Form P32-A

1.21 OBLIGATIONS and LIABILITY OF THE VENDOR:

Vendor shall complete the entire work to the satisfaction of the State and in accordance with the specifications herein mentioned, at the price herein agreed upon and fixed therefore. All the work, labor and equipment to be done and furnished under this contract(s) shall be done and furnished strictly pursuant to, and in conformity with the specifications described herein, and the directions of the State representatives as given from time to time during the progress of the work, under the terms of this contract(s) and also in accordance with contract(s) drawings.

The Vendor shall take all responsibility for the work under this contract(s). They shall in no way be relieved of their responsibility by any right of the State to give permission or issue orders relating to any part of the work; or by any such permission given on orders issued or by failure of the State to give such permission or issue such orders.

1.22 PERFORMING SERVICES:

The Vendor will perform all services according to the requirements and specifications of this bid.

1.23 SCHEDULE OF EVENTS:

EVENT DESCRIPTION	DATE	TIME
BID Released (On or About)	7/17/13	
Questions Must Be Submitted No Later Than	7/26/13	4:00 PM
Responses To Questions Will Be Posted By	7/31/13	4:00 PM
Bid Opening Date (Due Date)	8/5/13	11:30 AM

BIDDER CONTACT INFORMATION:

The following information is for this office to be able to contact a person knowledgeable of your bid response, and who can answer questions regarding it:

Jim Fish

Contact Person

303-872-4151

Fax Number

303-554-6333

Telephone Number

jim.fish@coalfire.com

E-mail Address

1-877-224-8077

Toll Free Telephone Number

www.coalfire.com

Company Website

ATTACHMENT 1

PRICE RESPONSE SHEETS

Prices for the specified services **MUST** be entered in the following Price Response sheets. Vendors **MUST** provide pricing for **ALL required services** to be considered for award. Vendors may **NOT** submit pricing in any format other than the tables provided. Bid prices must be FOB Destination. Bid rates are fully loaded and include all additional charges including but not limited to: meals, travel, and lodging. A maximum of three individual contracts shall be awarded to the vendors with the lowest priced compliant bids.

Normal Business Hours – 8:00 AM to 5:00 PM EST Monday through Friday, excluding State of New Hampshire Holidays. State Holidays are: New Years Day, Martin Luther King Day, President's Day, Memorial Day, July 4th, Labor Day, Veterans Day, Thanksgiving Day, the day after Thanksgiving Day and Christmas Day. Specific Dates will be provided.

PENETRATION TESTING – Vendors are asked to submit hourly rates for providing both network-layer testing and application-layer penetration testing. Contracts will be awarded based on these hourly rates.

Once the contract has been awarded, agencies may request quotations from all contracted vendors by providing a Statement of Work (SOW) describing the services required as well as the Pre-Engagement Checklist. If appropriate, the vendors may be allowed to view code or facilities after the execution of confidentiality agreements. Vendors must return pricing quotations within five (5) business days. If additional information has been circulated to all vendors, vendors will have one extra business day to revise their quotation. The specified hourly rates quoted shall not exceed the rates offered in the Vendor's bid response. A Maximum of three (3) contracts will be awarded to the vendors with the lowest Total Bids.

OFFER: The undersigned hereby offers to perform the services to the State of New Hampshire as specified at the prices quoted below, in complete accordance with general and detailed specifications included herewith.

Table 1 – PENETRATION TESTING PRICING COMBINED RATE

Tasks	Hourly Rate			Total
	10/13/2013 – 10/12/2014	10/13/2014 – 10/12/2015	10/13/2015 – 10/12/2016	
Network-layer Penetration Tests	\$165	\$165	\$165	\$165
Application-layer Penetration Tests	\$165	\$165	\$165	\$165
Total	\$165	\$165	\$165	\$165

EXHIBIT 2
REFERENCE CHECKLIST FORMAT

EXHIBIT 2
REFERENCE CHECKLIST FORMAT

All vendors must provide, as **ATTACHMENT 2**, at least 3 (three) references for which they currently hold similar contracts with multiple delivery locations. For each reference the vendor must provide customer name, contact name, contact telephone number, a description of the service provided and service time period (start to finish dates). **Ensure that all Reference names and phone numbers are current and can be contacted easily.**

Ref. No.	Customer Name, Address and Contact	Customer Contact Telephone Number	Dates of Service From-To	Products and Services Provided
1	State of Massachusetts One Ashburton Place, 9th Floor; Boston, MA 02108	Patricia Davis Comptroller's Office – PCI Liasion, Ecommerce Program Coordinator Office of the State Comptroller Phone: (617) 973-2332 Email: Patricia.Davis@massmail.state.ma.us	2008 to the present	Coalfire has provided PCI compliance services including network scans, gap assessment, validation and application testing to over 30 entities within the Commonwealth of MA since 2008. Entities included under the statewide blanket contract for PCI services include Universities, Colleges and Departments
2	State of Colorado 601 East 18 th Avenue, Suite 250; Denver, CO 80203	Jonathan Trull Chief Information Security Officer Governor's Office of Information Technology Phone: 303-764-7994 Email: jonathan.trull@state.co.us	2004 to the present	Coalfire has worked with various departments since 2004. Recently, following a competitive bid process, Coalfire was contracted by the Colorado State Auditor to provide statewide penetration test services for 26 departments Following the guidelines contained in OSSTMM, NIST 800-42 and OWASP, Coalfire testing focused on State systems collecting, processing, and storing sensitive and confidential data such as tax records, social security numbers, criminal histories, and personal health information. The goal was to quickly identify exploitable systems, including high profile web sites. Tasks included:

				<ul style="list-style-type: none"> • No-Disclosure External Assessment • External / Internal Vulnerability Scans • External and Onsite Penetration Testing • Password Audit • Wireless Assessment and War Dialing • Application Vulnerability Testing • Social Engineering
3	<p>State of Oklahoma 525 Central Park Drive, Suite 600; Oklahoma City, OK 73105</p>	<p>Ken Ontko VP of Information Technology</p> <p>Phone: (405) 556-9203 Email: kontko@osla.org</p>	<p>2004 to the present</p>	<p>Coalfire has worked on numerous State project since 2004. The State of Oklahoma has a number of initiatives to improve the IT security posture for State agencies designed to better serve constituents, comply with emerging regulations, improve homeland security and prepare for potential e-government programs. As part of these initiatives, the State, through a competitive bid process managed by the Office of State Finance (OSF) and Department of Human Services (OKDHS), selected Coalfire to conduct a comprehensive IT security assessment for selected state agencies. Mr. Ontko was the Information Security Officer for the Office of State Finance.</p>

ATTACHMENT 3 – COMPANY PROFILE AND VENDOR MINIMUM REQUIREMENTS

COALFIRE OVERVIEW:

Coalfire has been independently ranked as North America's largest IT security GRC (Governance, Risk, and Compliance) firm. From our founding in 2001, we have been a vendor neutral and platform agnostic firm focused exclusively on IT audit and compliance to the exclusion of other IT security product related services.

Corporate Video:

<http://www.coalfire.com/Video/October-2011/Coalfire-Company-Overview>

Securing Emerging Technologies

Coalfire has earned a reputation for being on the forefront of emerging technologies:

	<p>Mobile Security</p> <p>Coalfire has led the validation of some of the industry's most innovative mobile solutions available. Coalfire participates on 5 major mobile standards bodies and was one of only 3 QSA's to participate on the PCI SSC's mobile security task force. Coalfire has supports global merchants in security advisory role for mobile solutions.</p>
	<p>EMV and Contactless Payments</p> <p>Coalfire leverages our broad industry expertise and participation working with mobile security, global acquirers, card brands, terminal manufactures and EMVCo to help guide our clients in selecting appropriate EMV and contactless payment solutions.</p>
	<p>Virtualization and Cloud Security</p> <p>Coalfire is one the world's leading firms on Cloud Security and Compliance and has been selected by both VMWare and HP to help design and validate their cloud security reference architectures. Coalfire has led many industry special interest groups working on virtualization security including the PCI SSC virtualization SIG and has published many white papers and regularly presents on cloud security challenges and solutions.</p>
	<p>P2PE – Point-to-Point Encryption</p> <p>The use of encryption has always been one of the most challenging security tools for the retailer. Coalfire is established as the leader in these emerging technology trends. Coalfire is the selected independent validation firm for almost every retail encryption solution vendor including VeriFone, Voltage, Magtek and RSA. Coalfire was used as the technical reference firm by the PCI SSC as they formulated their approach to P2PE and was a founding participant of the PCI SSC P2PE SIG.</p>
	<p>Cloud Computing and VMware</p> <p>Coalfire is currently the only assessor in the country certified to conduct Cloud assessments for PCI, FedRAMP (3PAO) and HITRUST. Our independence as an assessor puts us in a unique position which has allowed us to provide strategic services for cloud providers and vendors. Coalfire is the only assessor which has created a dedicated team of VMware and virtualization experts and is endorsed through the VMware TAP Elite program. With over 1,000 assessments conducted last year, we have the experience and knowledge about the cloud which no others can match.</p>

Coalfire Labs

Coalfire Labs offers services that are pre-emptive and immediate. We also provide post-incident support when needed. From start to finish, through forensic e-discovery processes, we follow a standard methodology that promotes knowledge transfer and a thorough understanding of your needs.

Our services are delivered by the brightest minds in IT security with technical experts that are industry-certified and well-versed in regulations, digital forensics, threat mitigation, electronic discovery, vulnerability risks, and incident response.

Services:

- Penetration Testing
- Vulnerability Scanning & Assessments
- Social Engineering
- Application Security
- Incident Response Planning
- Electronic Discovery support
- Forensics and Litigation Support

Lab Professional Credentials:

- AccessData Certified Examiner (ACE)
- AccessData Mobile Examiner (AME)
- CCNA Security
- Certified Disaster Recovery Planner (CDRP)
- Certified in Risk and Information Systems Control (CRISC)
- Certified Information Systems Auditor (CISA)
- Certified Information Systems Security Professional (CISSP)
- Certified VISA and ABA Encryption Auditor (TG3)
- Certified Ethical Hacker (CEH)
- Certified TACLANE Operator (General Dynamics NSA Type 1 Encryptor Certification)
- Cisco Certified Network Associate (CCNA)
- CompTIA A+, Network+, Linux+
- CompTIA Advanced Security Practitioner (CASP)
- GIAC Certified Incident Handler (GCIH)
- GIAC Certified Web Application Penetration Tester (GWAPT)

- GIAC Penetration Tester (GPEN)
- GIAC Certified Forensic Analyst (GCFA)
- GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)
- Holistic Information Security Practitioner (HISP) – HISPI
- ITIL Foundationsv3
- Microsoft Certified System Engineer (MCSE)
- Microsoft Certified Technology Specialist (MCTS)
- Offensive Security Certified Expert (OSCE)
- Offensive Security Certified Professional (OSCP)
- Offensive Security Wireless Professional (OSWP)
- PA-QSA (P2PE)
- QSA (P2PE)
- Red Hat Certified Engineer (RHCE)

NUMBER OF EMPLOYEES: 150+ Coalfire
22 Labs

LENGTH OF TIME IN BUSINESS: Coalfire Has Been In Continuous Operation Since 2001.

ATTACHMENT 4 - CONTRACTOR CERTIFICATIONS

Client: 23086

COALSYS

ACORD CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)
3/21/2012

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an **ADDITIONAL INSURED**, the policy(ies) must be endorsed. If **SUBROGATION IS WAIVED**, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER Hanney Team Mesitrow Insurance Services 353 N. Clark Street Chicago, IL 60654	CONTACT Malinda Romanowski Phone (US, Int. Dial): 312 593-6259 Fax: 312 593-6807 E-Mail: mromanowski@mesitrow.com																	
	<table border="1"> <tr> <th>INSURER A</th> <th>INSURER B</th> <th>INSURER C</th> <th>INSURER D</th> <th>INSURER E</th> <th>INSURER F</th> </tr> <tr> <td>National Fire Ins Co. of Harfo</td> <td>Continental Casualty</td> <td>American Casualty Co of Reading</td> <td>Liberty Mutual</td> <td>Continental Ins. Co.</td> <td></td> </tr> <tr> <td>30478</td> <td>30443</td> <td>30437</td> <td></td> <td>30280</td> <td></td> </tr> </table>	INSURER A	INSURER B	INSURER C	INSURER D	INSURER E	INSURER F	National Fire Ins Co. of Harfo	Continental Casualty	American Casualty Co of Reading	Liberty Mutual	Continental Ins. Co.		30478	30443	30437		30280
INSURER A	INSURER B	INSURER C	INSURER D	INSURER E	INSURER F													
National Fire Ins Co. of Harfo	Continental Casualty	American Casualty Co of Reading	Liberty Mutual	Continental Ins. Co.														
30478	30443	30437		30280														

COVERAGES **CERTIFICATE NUMBER:** **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

TYPE	TYPE OF INSURANCE	INSURER	POLICY NUMBER	POLICY EFF. DATE (MM/DD/YYYY)	POLICY EXP. DATE (MM/DD/YYYY)	LIMITS
A	GENERAL LIABILITY <input checked="" type="checkbox"/> COMMERCIAL GENERAL LIABILITY <input type="checkbox"/> CLEARANCE <input checked="" type="checkbox"/> OCCUP <input type="checkbox"/> AUTO <input type="checkbox"/> AIRCRAFT <input type="checkbox"/> RAILROADS <input type="checkbox"/> PAPER PRODUCTS <input type="checkbox"/> POLLUTANTS <input type="checkbox"/> PRODUCTS <input type="checkbox"/> CONTRACTORS <input checked="" type="checkbox"/> LIEN		4032914629	08/18/2011	08/18/2012	EACH OCCURRENCE: \$1,000,000 PRODUCTS (No deductibles): \$1,000,000 MED EXP (By one person): \$15,000 PERSONAL & ADV INURY: \$1,000,000 UTILITY ACCIDENTS: \$2,000,000 POLLUTANTS - COMPROP AGG: \$2,000,000 AIRCRAFT: \$0 RAILROADS: \$0 PAPER PRODUCTS: \$0 POLLUTANTS: \$0 PRODUCTS: \$0
E	AUTOMOBILE LIABILITY <input type="checkbox"/> ANY AUTO <input type="checkbox"/> ALL OWNED AUTOS <input checked="" type="checkbox"/> HYBRID AUTOS <input type="checkbox"/> SCHEDULED AUTOS <input checked="" type="checkbox"/> NON-COMMERCIAL AUTOS		4032914613	08/18/2011	08/18/2012	AUTOMOBILE LIABILITY (Per accident): \$1,000,000 BODILY INJURY (Per person): \$0 BODILY INJURY (Per accident): \$0 PROPERTY DAMAGE (Per accident): \$0 UNINSURED: \$0
B	UMBRELLA & EXCESS LIABILITY <input checked="" type="checkbox"/> EXCESS LIABILITY <input type="checkbox"/> OCCUP <input type="checkbox"/> CONTRACTORS <input checked="" type="checkbox"/> PRODUCTS <input checked="" type="checkbox"/> POLLUTANTS LIMIT: \$1,000,000		4032914646	08/18/2011	08/18/2012	EACH OCCURRENCE: \$5,000,000 AUTOMOBILE: \$5,000,000 AIRCRAFT: \$0 RAILROADS: \$0 PAPER PRODUCTS: \$0 POLLUTANTS: \$0 PRODUCTS: \$0
C	WORKERS COMPENSATION AND EMPLOYERS LIABILITY ANY EMPLOYER/EMPLOYEE/INDEPENDENT CONTRACTOR/RENTAL & RELEASED (Statutory in WA) 90 days, benefits under applicable workers compensation laws		4032914601	08/18/2011	08/18/2012	WC STAT: \$0 EMP: \$0 B.L. EACH OCCURRENCE: \$1,000,000 B.L. DAMAGE - EA EMPLOYE: \$1,000,000 B.L. DAMAGE - POLICY LIMIT: \$1,000,000
A	Professional Lib		4032914629	08/18/2011	08/18/2012	\$3,000,000 Aggregate
D	Crime		PCCHCU003012	01/30/2012	01/30/2013	\$1,000,000

DESCRIPTION OF OPERATIONS, LOCATIONS, VEHICLES (Attach ACORD 41 - Additional Remarks Schedule if more space is required):
Blanket Waiver of Subrogation applies to the General Liability policy.

CERTIFICATE HOLDER Proof of Insurance	CANCELLATION SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.
	AUTHORIZED REPRESENTATIVE 

ATTACHMENT 5 – PROPOSED SUBCONTRACTORS

Not Applicable

STATE OF NEW HAMPSHIRE

BUREAU OF PURCHASE AND PROPERTY
STATE HOUSE ANNEX
25 CAPITOL STREET
CONCORD, NEW HAMPSHIRE 03301-6398

ADDENDUM # 1

TO RFB INVITATION # 1560-14

DATE OF BID OPENING: 8/5/13

TIME OF BID OPENING: 11:30 AM

FOR: CATEGORY 2 – Network & Application Penetration Testing Services

QUESTIONS AND ANSWERS

QUESTION #1

I was speaking to our technical architect, and he said we would be able to complete the services requested in this bid. We were wondering how important QSA is as a requirement for an award. Here is a short description of QSA and how it doesn't impact our ability to perform the services required.

"QSA ("Qualified Security Assessor") is a certification bestowed by the PCI Security Standards Council for organizations who are permitted to prepare official Report On Compliance (ROC) documentation (i.e., they can perform official 3rd party PCI audits). That certification is not required for performing penetration testing for PCI under section 11.3, and it has nothing to do with the ability to perform penetration testing-- it's about auditing against the PCI DSS. CDW is not a QSA, but we are expert penetration testers."

After reviewing that information will you allow us to respond and be awarded the business assuming our proposal is chosen?

ANSWER #1

Services provided by a Qualified Security Assessor (QSA) is a mandatory requirement.

QUESTION #2

Am I correct in thinking as per Section 2.3 only US companies may respond?

ANSWER #2

We assume you are referring to the following bid language:

The State requires that all testing must be done from locations within the United States of America. Access will not be provided to foreign IP addresses.

This does not prevent foreign companies from bidding but it does require that the testing be done from locations within the United States.

QUESTION #3

PCI does not require a company to be a QSA in order to perform the testing that the State of New Hampshire is requesting. Would the State allow a non-QSA who is qualified to perform the requested tests?

ANSWER #3

Services provided by a Qualified Security Assessor (QSA) is a mandatory requirement.

QUESTION #4

Would we be able to get the RFB in an editable form? (to allow completion of the forms)

ANSWER #4

You may have the response portion of the bid by sending a request to Robert.lawson@nh.gov

QUESTION #5

Section 5 – Response Format, 5.2.3 Price Response Sheets – There is a statement that says “Attachment 1 must remain in its original location in the RFB.” Since the Original RFB is to be printed in the previous section (5.2.2 Original RFB) would the State like us to complete the price sheets within section 5.2.2 and just make reference to the completed price sheets in section 5.2.3?

ANSWER #5

We are just looking for all the bids to have all the items in the same sequence so we don't have to go looking for all the materials we need to review. Please sort the materials in the requested order.

QUESTION #6

Would the State entertain alternative language to Section 13 of the General Provisions?
a. The extensiveness of the provisions as proposed in Section 13 precludes bidders from evaluating or pricing the associated risk in the penetration testing environment. The provision requires bidders to assume an uncapped and uninsured liability.

ANSWER #6

Sorry, we cannot modify the existing language.

QUESTION #7

How many externally facing web applications are in scope?

ANSWER #7

Please see the table at the end of this document for the requested addresses.

QUESTION #8

How many externally facing web applications are internally developed custom applications?

ANSWER #8

Please see the table at the end of this document for the requested addresses.

QUESTION #9

How many internal hosts are in scope?

ANSWER #9

The number of internal servers in scope varies by each agency's application and cardholder flow. Details on each is provided as part of the Scope of Work and Pre-Engagement Checklist submitted to the vendor for pricing prior to conducting any work

QUESTION #10

How many internal network segments are there?

ANSWER #10

The number of internal servers in scope varies by each agency's application and cardholder flow. Details on each is provided as part of the Scope of Work and Pre-Engagement Checklist submitted to the vendor for pricing prior to conducting any work

QUESTION #11

How many external IP addresses/hosts are there?

ANSWER #11

Please see the table at the end of this document for the requested addresses.

QUESTION #12

How many virtual hosts exist that would only respond to a host name?

ANSWER #12

None

QUESTION #13

Is there a pre-established budget for this project? Could you please provide the budget figure?

ANSWER #13

Sorry, there is no pre-established budget for this project.

QUESTION #14

Is there a set-aside and/or any special considerations for this opportunity to prefer small disadvantaged businesses, woman-owned businesses, economically disadvantaged woman owned small businesses, and/or minority-owned businesses?

ANSWER #14

Sorry, No.

QUESTION #15

Is this the first time that the State will contract a vendor for a project with this (or similar) scope?

ANSWER #15

No, there are currently contracts in place that were established in 2010.

QUESTION #16

Could you please name the previous successful contractor(s) and the "not to exceed" hourly rates proposed by said contractor(s)?

ANSWER #16

This information is available at nh.gov. All current contracts are posted for public view.

QUESTION #17

Further, if there is an incumbent, what is the reason that the State is looking to contract a new vendor(s) for this requirement (e.g. poor performance by previous vendor, conflict of interest issues, etc.)?

ANSWER #17

Current contracts are expiring and procedure requires that we provide a new bidding opportunity.

QUESTION #18

During evaluation of proposals received, will any preference/points be awarded for vendors that submit references from government organizations? Is it preferred that the contractor have government experience?

ANSWER #18

Please review the bid requirements. No preference/points will be given but vendors must meet the requirements in the bid or they will be considered non-compliant.

QUESTION #19

At the bidding stages, would a "Summary of Insurance Coverage" document that shows compliance with the requirements stated in Section 1.20 of the RFB document suffice? Or is the State looking for a bidder to submit a proper insurance certificate with the State as the beneficiary?

ANSWER #19

We will need a proper Insurance Certificate. This will be needed to be able to proceed with any potential contract.

QUESTION #20

Is there a preference for a local firm (or one that is more accessible)? Will this go against a vendor who is not local or not more accessible, in the scoring process? If so, please specify the point deductions applicable.

ANSWER #20

Please review the bid requirements. The only preference would be for a New Hampshire company if there were a tie.

QUESTION #21

Since all scope activities can be performed remotely, is it acceptable to the State that a vendor hold all meetings over GoTo Meeting or a similar remote collaboration platform, in order to keep costs low and offer the best value to the State?

ANSWER #21

Yes, this would be acceptable if provided at vendor's expense.

QUESTION #22

Is the State looking for a bidder to provide any other material beyond the completed attachments (e.g. a technical proposal or such)? Or will the completed attachments provided as part of the RFB suffice?

ANSWER #22

The information requested as part of the RFB is sufficient to allow the state to select vendors for possible award.

QUESTION #23

It is our understanding that at the time of bidding, a vendor need not be registered nor have a certificate of Good Standing with the State, but that once awarded a vendor would have to obtain said certificate. Can you please confirm if this understanding is correct?

ANSWER #23

Per Section 1.9; On submitting a bid any vendor should already be registered with the Bureau of Purchase and Property to do business with the State.

Although you need not be registered with the Secretary of State at the time of submitting a bid it can take some time to get registered such that if we were to be ready to offer you a contract you may not be able to get registered in time and the contract would have to be awarded to another bidder.

QUESTION #24

Please confirm that a bid response may be submitted over e-mail (to prchweb@nh.gov) and that this mode of submission is acceptable to the State.

ANSWER #24

Section 1.16 shows the manner in which bids may be submitted and via e-mail is one of the options.

QUESTION #25

As part of the final result announcement on this RFB, will the names of all selected bidders be announced?

ANSWER #25

As per Section 1.19; bid results will be posted on the web site for public view.

QUESTION #26

Please confirm that a QSA audit (typical QSA audit followed by a report on compliance) is not in scope and only network and application layer penetration testing is in scope.

ANSWER #26

The Scope of this RFB is for services to meet PCI DSS 11.3.

QUESTION #27

Based on the RFB document, it appears that the methodology that will be used in network and application penetration tests is not being evaluated currently. Can you please confirm that this is the case? Or is the vendor expected to provide the methodologies used as a separate document (or as part of a technical proposal)?

ANSWER #27

The vendor is not required to provide the methodologies used in their response to this Bid request. This information is required, however, whenever the vendor performs work under this Bid.

QUESTION #28

Will any of the penetration testing (external or internal) involved systems or applications that are hosted by a 3rd party (vendor) service provider?

ANSWER #28

Not at this time but it is conceivable that this may change over the course of this contract.

QUESTION #29

Is there a preference for:

- a. Uninformed testing ("black box"),
- b. Informed testing ("white box"), or
- c. A combination of uninformed and informed testing?

ANSWER #29

The State does not have a stated preference beyond the requirements under PCI 11.3.

QUESTION #30

Do any of the agencies have systems with modems that will require war-dialing as part of the external penetration testing?

ANSWER #30

None of the current applications have modems in place however; it is conceivable that this may change over the course of the contract. Vendors must be capable of handling this type of situation.

QUESTION #31

For internal network penetration testing, is remote testing permissible?

ANSWER #31

Yes.

QUESTION #32

Does the state intend to include wireless infrastructure in the scope of internal network penetration testing?

ANSWER #32

Not at this time because wireless is not part of any of the existing applications. It is conceivable that this may change over the course of this contract.

+++++

QUESTION #33

Who is driving your PCI requirement or is this an internal exercise?

ANSWER #33

PCI DSS 11.3 requires all merchants to have network and application penetration tests done on an annual basis or when there is a significant change to the environment. The State has determined the best way to accomplish this is using a qualified external third party.

QUESTION #34

How many externally/internally facing IPs do you have for each department?

1. Education Dept.
2. Fish & Game Dept.
3. Joint Board of Licensure

4. Liquor Commission
5. Lottery Commission
6. Nursing, Board
7. Pease Development Authority
8. Resources & Economic Development
9. Safety Dept.
10. Secretary of State
11. Transportation Department

For External Pen Testing:

1. How many Edge Router(s) / Switch(es)?
2. Education Dept.
3. Fish & Game Dept.
4. Joint Board of Licensure
5. Liquor Commission
6. Lottery Commission
7. Nursing, Board
8. Pease Development Authority
9. Resources & Economic Development
10. Safety Dept.
11. Secretary of State
12. Transportation Department

ANSWER #34

Please see the table at the end of this document.

QUESTION #35

2. How many Firewall(s)?
 1. Education Dept.
 2. Fish & Game Dept.
 3. Joint Board of Licensure
 4. Liquor Commission
 5. Lottery Commission
 6. Nursing, Board

7. Pease Development Authority
8. Resources & Economic Development
9. Safety Dept.
10. Secretary of State
11. Transportation Department

ANSWER #35

The number of firewalls in scope varies by each agency's application and cardholder flow. Details on each are provided as part of the Scope of Work and Pre-Engagement Checklist submitted to the vendor for pricing prior to conducting any work. For security purposes, the State does not provide details about the networking and application environments.

QUESTION #36

3. How many VPNs/ Remote Access?
 1. Education Dept.
 2. Fish & Game Dept.
 3. Joint Board of Licensure
 4. Liquor Commission
 5. Lottery Commission
 6. Nursing, Board
 7. Pease Development Authority
 8. Resources & Economic Development
 9. Safety Dept.
 10. Secretary of State
 11. Transportation Department

ANSWER #36

Whether there is VPN in scope varies by each agency's application and cardholder flow. Details on each are provided as part of the Scope of Work and Pre-Engagement Checklist submitted to the vendor for pricing prior to conducting any work. For security purposes, the State does not provide details about the networking and application environments.

QUESTION #37

4. IP address spaces are exposed?
1. Education Dept.
 2. Fish & Game Dept.
 3. Joint Board of Licensure
 4. Liquor Commission
 5. Lottery Commission
 6. Nursing, Board
 7. Pease Development Authority
 8. Resources & Economic Development
 9. Safety Dept.
 10. Secretary of State
 11. Transportation Department

ANSWER #37

The full network scope and IP addressing varies by each agency's application and cardholder flow. Details on each are provided as part of the Scope of Work and Pre-Engagement Checklist submitted to the vendor for pricing prior to conducting any work. For security purposes, the State does not provide details about the networking and application environments.

QUESTION #38

5. How many web servers? SOAP, XML, dynamic content?
- a. What is the physical number of web servers that you have in your environment to be tested?
 - 1) Education Dept.
 - 2) Fish & Game Dept.
 - 3) Joint Board of Licensure
 - 4) Liquor Commission
 - 5) Lottery Commission
 - 6) Nursing, Board
 - 7) Pease Development Authority
 - 8) Resources & Economic Development
 - 9) Safety Dept.
 - 10) Secretary of State
 - 11) Transportation Department

ANSWER #38

The number of servers in scope varies by each agency's application and cardholder flow. Details on each are provided as part of the Scope of Work and Pre-Engagement Checklist submitted to the vendor for pricing prior to conducting any work. For security purposes, the State does not provide details about the networking and application environments.

QUESTION #39

b. How many different applications reside amongst the web servers? (Web applications can include web sites or full blown applications)

1. Education Dept.
2. Fish & Game Dept.
3. Joint Board of Licensure
4. Liquor Commission
5. Lottery Commission
6. Nursing, Board
7. Pease Development Authority
8. Resources & Economic Development
9. Safety Dept.
10. Secretary of State
11. Transportation Department

ANSWER #39

Details about each application varies by each agency's application and cardholder flow. Details on each are provided as part of the Scope of Work and Pre-Engagement Checklist submitted to the vendor for pricing prior to conducting any work. For security purposes, the State does not provide details about the networking and application environments.

QUESTION #40

c. What are the applications? (Static Web Pages or Dynamic)

1. Education Dept.
2. Fish & Game Dept.
3. Joint Board of Licensure

4. Liquor Commission
5. Lottery Commission
6. Nursing, Board
7. Pease Development Authority
8. Resources & Economic Development
9. Safety Dept.
10. Secretary of State
11. Transportation Department

ANSWER #40

Details about each application varies by each agency's application and cardholder flow. Details on each are provided as part of the Scope of Work and Pre-Engagement Checklist submitted to the vendor for pricing prior to conducting any work. For security purposes, the State does not provide details about the networking and application environments.

QUESTION #41

- d. What languages are web applications developed in?
1. Education Dept.
 2. Fish & Game Dept.
 3. Joint Board of Licensure
 4. Liquor Commission
 5. Lottery Commission
 6. Nursing, Board
 7. Pease Development Authority
 8. Resources & Economic Development
 9. Safety Dept.
 10. Secretary of State
 11. Transportation Department

ANSWER #41

Details about each application varies by each agency's application and cardholder flow. Details on each are provided as part of the Scope of Work and Pre-Engagement Checklist submitted to the vendor for pricing prior to conducting any work. For security purposes, the State does not provide details about the networking and application environments.

QUESTION #42

e. How many forms are present in your web application?

1. Education Dept.
2. Fish & Game Dept.
3. Joint Board of Licensure
4. Liquor Commission
5. Lottery Commission
6. Nursing, Board
7. Pease Development Authority
8. Resources & Economic Development
9. Safety Dept.
10. Secretary of State
11. Transportation Department

ANSWER #42

Details about each application varies by each agency's application and cardholder flow. Details on each are provided as part of the Scope of Work and Pre-Engagement Checklist submitted to the vendor for pricing prior to conducting any work. For security purposes, the State does not provide details about the networking and application environments.

QUESTION #43

f. How many pages make up your web app?

1. Education Dept.
2. Fish & Game Dept.
3. Joint Board of Licensure
4. Liquor Commission
5. Lottery Commission
6. Nursing, Board
7. Pease Development Authority
8. Resources & Economic Development
9. Safety Dept.
10. Secretary of State
11. Transportation Department

ANSWER #43

Details about each application varies by each agency's application and cardholder flow. Details on each are provided as part of the Scope of Work and Pre-Engagement Checklist submitted to the vendor for pricing prior to conducting any work. For security purposes, the State does not provide details about the networking and application environments.

QUESTION #44

For Internal Penetration Testing:

1. Number of datacenter locations
 1. Education Dept.
 2. Fish & Game Dept.
 3. Joint Board of Licensure
 4. Liquor Commission
 5. Lottery Commission
 6. Nursing, Board
 7. Pease Development Authority
 8. Resources & Economic Development
 9. Safety Dept.
 10. Secretary of State
 11. Transportation Department

ANSWER #44

Details about State data centers vary by each agency's application and cardholder flow. Details on each is provided as part of the Scope of Work and Pre-Engagement Checklist submitted to the vendor for pricing prior to conducting any work. For security purposes, the State does not provide details about the networking and application environments.

QUESTION #45

2. Number of retail/store locations (if any)?

ANSWER #45

See Exhibit 1.

QUESTION #46

3. Are all the locations accessible from a single site?

If we are going to do a penetration test (internal); is your network segmented in a manner that allows us to either access it from one point or do we need to access it from multiple geographic locations.

ANSWER #46

VPN accounts will be provided as necessary to allow the vendor to access the specific network locations required for penetration testing.

QUESTION #47

4. How many IP addresses per location would need to be scanned?
1. Education Dept.
 2. Fish & Game Dept.
 3. Joint Board of Licensure
 4. Liquor Commission
 5. Lottery Commission
 6. Nursing, Board
 7. Pease Development Authority
 8. Resources & Economic Development
 9. Safety Dept.
 10. Secretary of State
 11. Transportation Department

ANSWER #47

The full network scope and IP addressing varies by each agency's application and cardholder flow. Details on each are provided as part of the Scope of Work and Pre-Engagement Checklist submitted to the vendor for pricing prior to conducting any work. For security purposes, the State does not provide details about the networking and application environments.

QUESTION #48

5. Your internal systems that process, transmit, store or handle credit card data, are they on a segmented network of their own with no other systems (servers, desktops etc) present?

1. Education Dept.
2. Fish & Game Dept.
3. Joint Board of Licensure
4. Liquor Commission
5. Lottery Commission
6. Nursing, Board
7. Pease Development Authority
8. Resources & Economic Development
9. Safety Dept.
10. Secretary of State
11. Transportation Department

ANSWER #48

The full network scope and cardholder flow varies by each agency's application. Details on each are provided as part of the Scope of Work and Pre-Engagement Checklist submitted to the vendor for pricing prior to conducting any work. For security purposes, the State does not provide details about the networking and application environments.

QUESTION #49

6. This can be accomplished with either a firewall, router and acl's or VPN's with acl's that restrict
access to only systems that need access and is not open to all.
 - a. If yes, how many physical computers are present?

ANSWER #49

The full network scope and cardholder flow varies by each agency's application. Details on each are provided as part of the Scope of Work and Pre-Engagement Checklist submitted to the vendor for pricing prior to conducting any work. For security purposes, the State does not provide details about the networking and application environments.

QUESTION #50

- i. Many organizations will have a standard process for building production servers. Typically windows and unix / linux web servers, database servers etc will each have their own process often referred to as a template to ensure consistency.

Are these systems built using such a process? If yes, how many different templates are present in these network segments that are considered in scope for PCI?

If no, how many systems are there total? i.e.: servers, desktops devices, etc.

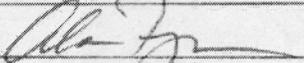
ANSWER #50

The State has standard build configurations based on purpose and operating system. Details about how this is done for each agency is provided as part of the Scope of Work and Pre-Engagement Checklist submitted to the vendor for pricing prior to conducting any work. For security purposes, the State does not provide details about the networking and application environments.

PURCHASING AGENT: ROBERT LAWSON
TEL. NO: 603/271-3147

NOTE IN THE EVENT THAT YOUR BID INVITATION HAS BEEN SENT TO THIS OFFICE PRIOR TO RECEIVING THIS ADDENDUM, RETURN ADDENDUM WITHIN THE SPECIFIED TIME WITH ANY CHANGES YOU MAY WISH TO MAKE AND MARK ON THE REMITTANCE ENVELOPE BID INVITATION NUMBER AND OPENING DATE. RETURNED ADDENDA WILL SUPERSEDE PREVIOUSLY SUBMITTED BID.

BIDDER Coalfire Systems, Inc. ADDRESS 361 Centennial Parkway, Ste. 150

BY  Louisville, CO 80027

(this document must be signed)

Alan Ferguson, Exec. VP. Sales TEL. NO. 303-554-6333

(please type or print name)

