

STATE OF NEW HAMPSHIRE  
BUREAU OF PURCHASE AND PROPERTY  
STATE HOUSE ANNEX - ROOM 102  
25 CAPITOL ST  
CONCORD NH 03301-6398

DATE: 5/16/2018  
CONTRACT #: 8002314 NIGP CODE: 920-0000  
CONTRACT FOR: Security Compliance, Testing & Remediation Services (Merchant Cards)  
CONTRACTOR: Coalfire Systems Inc. VENDOR CODE #: 221845

SUBMITTED FOR ACCEPTANCE BY:  
  
\_\_\_\_\_  
MATHEW STANTON, ADMINISTRATOR III  
BUREAU OF PURCHASE AND PROPERTY

DATE 5/16/18

\*\*\*\*\*  
APPROVED FOR ACCEPTANCE BY:  
  
\_\_\_\_\_  
GARY LUNETTA, DIRECTOR  
DIVISION OF PROCUREMENT & SUPPORT SERVICES

DATE 5/16/18

ACCEPTED FOR THE STATE OF NEW HAMPSHIRE UNDER THE AUTHORITY GRANTED TO ME BY NEW HAMPSHIRE REVISED STATUTES, ANNOTATED 21-I:14, XII.  
  
\_\_\_\_\_  
CHARLES M. ARLINGHAUS, COMMISSIONER  
DEPARTMENT OF ADMINISTRATIVE SERVICES

DATE 5/17/18

.....

This is one of 6 contracts to be awarded

Subject: SECURITY COMPLIANCE, TESTING AND REMEDIATION - FORENSIC INVESTIGATION SERVICES

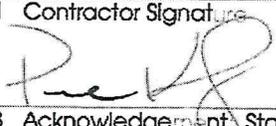
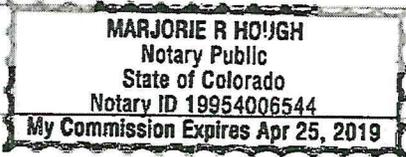
**Notice:** This agreement and all of its attachments shall become public upon submission to Governor and Executive Council for approval. Any information that is private, confidential or proprietary must be clearly identified to the agency and agreed to in writing prior to signing the contract.

**AGREEMENT**

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

**GENERAL PROVISIONS**

**1. IDENTIFICATION.**

1.1 State Agency Name Department of Administrative Services		1.2 State Agency Address 25 Capitol Street Concord, NH 03301	
1.3 Contractor Name Coalfire Systems, Inc.		1.4 Contractor Address 11000 Westmoor Circle Suite 450 Westminster, CO 80021	
1.5 Contractor Phone Number 303-554-6333	1.6 Account Number Various	1.7 Completion Date 2/28/2021	1.8 Price Limitation \$300,000.00
1.9 Contracting Officer for State Agency Jeffery Haley		1.10 State Agency Telephone Number 603-271-2202	
1.11 Contractor Signature 		1.11 Name and Title of Contractor Signatory Paul Kleinschnitz, Executive Vice President	
1.13 Acknowledgement, State of Colorado, County of Adams On <u>APRIL 24 2018</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) 			
1.13.2 Name and Title of Notary or Justice of the Peace MARJORIE R. HOUGH			
1.14 State Agency Signature 		1.15 Name and Title of State Agency Signatory Charles M. Arlinghaus, Commissioner	
Date: <u>5/17/18</u>			
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) (if applicable) By: _____ On: _____			
1.18 Approval by the Governor and Executive Council (if applicable) 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, if applicable, this Agreement, and all obligations of the parties hereunder, shall become effective on the date the Governor and Executive Council approve this Agreement as indicated in block 1.18, unless no such approval is required, in which case the Agreement shall become effective on the date the Agreement is signed by the State Agency as shown in block 1.14 ("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. This may include the requirement to utilize auxiliary aids and services to ensure that persons with communication disabilities, including vision, hearing and speech, can communicate with, receive information from, and convey information to the Contractor. 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 notice and consent of the State. None of the Services shall be subcontracted by the Contractor without the prior written notice and 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 \$1,000,000 per occurrence and \$2,000,000 aggregate; and

14.1.2 special cause of loss coverage form 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.

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 thirty (30) 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 provide the Contracting Officer identified in block 1.9, or his or her successor, no less than thirty (30) 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 unless no such approval is required under the circumstances pursuant to State law, rule or policy.

**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 (hereinafter referred to as the "State"), Department of Administrative Services, with Security Compliance, Testing And Remediation - Forensic Investigation Services in accordance with the bid submission in response to State Request for Bid # 2075-18 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 Terms
- d. EXHIBIT C      Special Provisions
- e. EXHIBIT D      RFB 2075-18
- f. EXHIBIT E      Pre-Engagement Checklist
- g. EXHIBIT F      Glossary of Terms
- h. EXHIBIT G      Additional Terms

**3. TERM OF CONTRACT**

This contract shall commence upon the approval of the Commissioner of Administrative Services and terminate on February 28, 2021, a period of approximately two (2) years and ten (10) 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, with the approval of the Commissioner of the Department of Administrative Services, but shall not exceed five (5) years in total.

**4. SCOPE OF WORK**

All services performed under this Contract(s) shall be performed between the hours of 8:00 A.M. and 4:00 P.M. unless other arrangements are made in advance with the State. Any deviation in work hours shall be pre-approved by the Contracting Officer. The State requires ten-day advance knowledge of said work schedules to provide security and access to respective work areas. No premium charges will be paid for any off-hour work.

The State shall require correction of defective work or damages to any part of a building or its appurtenances when caused by the Contractor's employees, equipment or supplies. The Contractor shall replace in satisfactory condition all defective work and damages rendered thereby or any other damages incurred. Upon failure of the Contractor to proceed promptly with the necessary corrections, the State may withhold any amount necessary to correct all defective work or damages from payments to the Contractor.

The work staff shall consist of qualified persons completely familiar with the products and equipment they shall use. The Contracting Officer may require the Contractor to dismiss from the work such

employees as deems incompetent, careless, insubordinate, or otherwise objectionable, or whose continued employment on the work is deemed to be contrary to the public interest or inconsistent with the best interest of security and the State.

The Contractor or their personnel shall not represent themselves as employees or agents of the State.

While on State property, employees shall be subject to the control of the State, but under no circumstances shall such persons be deemed to be employees of the State.

All personnel shall observe all regulations or special restrictions in effect at the State Agency.

The Contractor's personnel shall be allowed only in areas where services are being performed. The use of State telephones is prohibited.

**SUBCONTRACTING:**

In addition to the provisions of Section 12 of the P-37 related to assignment and subcontracting of contractual rights and obligations, the Contractor shall be responsible to the State for the acts and omissions of all subcontractors or agents and of persons directly or indirectly employed by such subcontractors, and for the acts and omissions of persons employed directly by the Contractor. No contractual relationships exist between any subcontractor and the State.

**STAFFING REQUIREMENTS:**

Employment of Undocumented Workers Prohibited – Contractor shall not employ any employee without obtaining documentation showing the employee's eligibility to work in the United States. The employer shall maintain such documentation for the period required by federal law. Acceptable documentation of eligibility to work in the United States shall include documents required by federal law or supporting documentation that satisfies the requirement of federal law.

**Bankruptcy or Receivership**

Voluntary or involuntary bankruptcy or receivership by the Contractor may be cause for termination at the election of the State.

**Material Breach**

The non-breaching party may terminate the contract in whole or in part after thirty (30) days written notice, as described in the Form P-37 General Terms and Conditions Section 8, in the event of the breaching party's failure to perform a material obligation of the contract.

**LIAISON AND SERVICE OF NOTICES:**

All project management and coordination on behalf of the State shall be through a single point of contact designated as the State's liaison. The Contractor shall designate a liaison that shall provide the single point of contact for management and coordination of Contractor's work. All work performed pursuant to this Contract shall be coordinated between the State's liaison and the Contractor's liaison.

**DISPUTE RESOLUTION:**

Prior to the filing of any formal proceedings with respect to a dispute (other than an action seeking Injunctive relief with respect to intellectual property rights or Confidential Information), the party believing itself aggrieved (the "Invoking Party") shall call for the progressive management involvement in the dispute negotiations by written notice to the other party. Such notice shall be without prejudice to the invoking party's right to any other remedy permitted by this Contract.

## SECTION II: FORENSIC INVESTIGATION SERVICES (ALL DATA BREACHES)

Contractor shall be certified by the PCI Security Standards Council for PCI DSS compliance services by Visa, MasterCard, American Express and Discover as a PCI Forensic Investigators (PFI). PCI Forensic Investigators must work for a Qualified Security Assessor (QSA) company that has been qualified by the PCI Security Standards Council. Only Approved PFIs can perform PCI forensic investigations. QSAs are also qualified to provide forensic investigation services for non-PCI related compliance incidents.

PCI Forensic Investigators provide an independent investigation related to a data breach and the security vulnerabilities that enabled it. A PFI is retained to investigate the security issue, determine root cause and provide recommendations on mitigation and remediation efforts. In addition to investigations of the State's PCI cardholder environment, the PFI services can also be used for other data breaches and security events that compromise personally identifiable information (PII) and other sensitive data such as personal health information (PHI) or federal tax information (FTI).

The Contractor's servers and their workers must be located within the United States of America.

The Contractor must be in good standing for the Contract duration. The Contract shall be terminated immediately if the Contractor is dropped from the PCI SSC listings of QSA companies or is placed on remediation status.

### **PCI Forensic Investigators:**

Contractor, as a PFI Company, responsibilities include (without limitation) the following:

Driving and performing all aspects of PFI Investigations

- Adhere to all procedures, guidelines and evidence handling as identified in the PCI Security Standards Council's (PCI SSC) Forensic Investigator Program Guide, under the current version;
- Determine the scope of the investigation and the relevant sources of evidence
- Make recommendations on how the State should prioritize containment and secure sensitive data;
- Provide Investigation reporting and delivery of applicable PFI Reports as further described below; and
- For cardholder incidents governed by PCI security requirements, provide a feedback form as described in Appendix D of the PCI SSC's Forensic Investigator Program Guide, under the current version

### **Investigation Reporting:**

The Contractor, as a PFI Company, will have all requisite authority to provide materials and information (including but not limited to final and draft PFI Reports and work papers as described above. Before beginning each PFI Investigation engagement, Contractor must inform the State that it shall be required to disclose the same as herein described and must obtain clear, unqualified permission and consent from the State to make such disclosures.

The following reports must be produced as part of each PFI Investigation:

**Preliminary Incident Response Report:** Each completed Preliminary Incident Response Report must be delivered to the applicable State agency no later than five (5) business days after beginning PFI Investigation review.

At a minimum, the preliminary incident response report shall include a description of the scope of the:

- Identity of the reporting agency
- Identify of the lead investigator
- Identity of all third parties included in the investigation
- Date of the start of the investigation
- Date of report
- Breach evidence
- First confirmed date that the intruder or malware entered the network
- Scope of the forensic investigation
- Type of data
- Initial thoughts on attacker
- If contained, how was it contained and when was it contained
- Estimated date of investigation completion

**Final Incident Response Report:**

The completed Final PFI Report must be delivered to each affected Participating Payment Brand, the applicable State agency, and such State of New Hampshire's affected acquirer(s) (if the State is a merchant), in each case no later than ten (10) business days after completion of the corresponding PFI Investigation of such:

- Identity of the reporting agency
- Identify of the lead investigator
- Identity of all third parties included in the investigation
- Date of the start of the investigation
- Date of report
- Breach evidence
- First confirmed date that the intruder or malware entered the network
- Scope of the forensic investigation
- Descriptive list of items submitted for examination
- Executive Summary of the results and conclusions, including short term and long term recommendations to prevent future events
- Description of steps taken during the examination including search parameters and recovered files
- Detailed report of the results and conclusions along with supporting evidence.

**5. TERMINATION**

The State of New Hampshire has the right to terminate the contract at any time by giving the Contractor thirty (30) days advance written notice.

**6. OBLIGATIONS AND LIABILITY OF THE CONTRACTOR**

The Contractor shall provide all services strictly pursuant to, and in conformity with, the specifications described in State RFB # 2075-18, as described herein, and under the terms of this Contract.

The Contractor shall agree to hold the State of NH harmless from liability arising out of injuries or damage caused while performing this work. The Contractor shall agree that any damage to building(s), materials, equipment or other property during the performance of the service shall be repaired at its own expense, to the State's satisfaction.

Contractor Initials PIL  
Date 4/21/18

**7. DEBARMENT, SUSPENSION, INELIGIBILITY AND VOLUNTARY EXCLUSION LOWER TIER COVERED TRANSACTIONS**

The Contractor certifies, by signature of this contract, that neither It nor Its principals is presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction by any Federal Department or Agency.

**8. INSURANCE**

Certificate of insurance amounts must be met and maintained throughout the term of the contract and any extensions as per the P-37, section 14 and cannot be cancelled or modified until the State receives a 10 day prior written notice.

In addition, the following coverage shall be required by the Contractor along with proof of coverage:

- Minimum coverage level of \$5,000,000 for Professional Errors and Omissions
- Cyber Theft Liability in the amount of \$2,000,000 per occurrence
- Electronic Data Loss (EDL) in the amount of \$2,000,000 per occurrence

**9. CONFIDENTIALITY & CRIMINAL RECORD**

If requested by the using agency, the Contractor and Its employees, and Sub-Contractors (if any), shall be required to sign and submit a Confidential Nature of Department Records Form and a Criminal Authorization Records Form. These forms shall be submitted to the individual using agency prior to the start of any work.

**EXHIBIT B  
PAYMENT TERMS**

**1. CONTRACT PRICE**

The Contractor hereby agrees to provide security compliance, testing and remediation services in complete compliance with the terms and conditions specified in Exhibit A for an amount up to and not to exceed a price of \$300,000.00; this figure shall not be considered a guaranteed or minimum figure; however it shall be considered a maximum figure from the effective date of through the expiration date set as February 28, 2021.

**2. PRICING STRUCTURE**

<b>Service Description</b>	<b>Hourly Rate (Onsite)</b>	<b>Hourly Rate (Offsite)</b>
Data Breach Investigative Services	\$350	\$350

**3. PRICING QUOTATIONS FOR INDIVIDUAL PROJECTS**

State agencies shall request quotations from all contractors awarded in the section of services being requested by providing a Statement of Work (SOW) describing the services required as well as the Pre-Engagement Checklist (Exhibit E). If appropriate, the contractors may be allowed to view code or facilities after the execution of confidentiality agreements. Contractor must return pricing quotations within five (5) business days. If additional information has been circulated to all contractors, Contractor shall have one (1) extra business day to revise the quotation. The quoted hourly rates shall not exceed the rates listed herein.

**4. INVOICE**

Itemized invoices shall be submitted to the individual agency after the completion of the job/services and shall include a brief description of the work done along with the location of work.

Contractor shall be paid within 30 days after receipt of properly documented invoice and acceptance of the work to the State's satisfaction.

The invoice shall be sent to the address of the using agency under agreement.

**5. PAYMENT**

Payments shall be made via ACH. Use the following link to enroll with the State Treasury for ACH payments: <https://www.nh.gov/treasury>

**EXHIBIT C  
SPECIAL PROVISIONS**

There are no special provisions of this contract.

Contractor Initials PK  
Date 9/24/18

**EXHIBIT D**

RFB # 2075-18 is incorporated here within.

Contractor Initials *PK*  
Date *4/27/18*

**EXHIBIT E**

**Pre-Engagement Checklist (EXAMPLE)**

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 DSS current version) or Federal, State or Industry standards

**Agency Information**

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

Check which of the following performance categories are included under this SOW:

- PCI – Penetration Testing, or Remediation efforts
- Non-PCI – Security and compliance assessments, code reviews, penetration testing and reviews for general information management and security compliance

1. **Identify details of the engagement and project schedule.**  
(Provide narrative that outlines purpose of the engagement. If non-PCI, identify what security standards are in scope)
  
2. **Details about the environment in scope for the engagement.**  
(Provide business processes, policies and procedures, network diagrams, data flow diagrams, IP address and application credentials and any other information about the engagement needed by the Contractor to assess the level of effort)
  
3. **What are the rules of engagement?**  
(This includes project timeline, success criteria, toolset identification, testing behaviors)

Contractor Initials PK  
Date 9/20/10

**EXHIBIT F  
GLOSSARY OF TERMS**

TERM	DEFINITION
Acquirer	Also referred to as "merchant bank," "acquiring bank," or "acquiring financial institution". Entity, typically a financial institution that processes payment card transactions for merchants and is defined by a payment brand as an acquirer. Acquirers are subject to payment brand rules and procedures regarding merchant compliance.
Agency	Any entity that utilizes or seeks to utilize payment card processing services under contracts secured by DAS
AOC	Attestation of Compliance
BAMS	Bank of America Merchant Services
Chase	J.P. Morgan Chase Merchant Services
Administrative Safeguards	Administrative safeguards are administrative actions, policies, and procedures to prevent, detect, contain, and correct security violations. Administrative safeguards involve the selection, development, implementation, and maintenance of security measures to protect e-PHI and to manage the conduct of workforce members in relation to the protection of that information. A central requirement is that you perform a security risk analysis that identifies and analyzes risks to e-PHI and then implement security measures to reduce the identified risks.
Audit	An independent examination of security controls associated with a representative subset of organizational information systems to determine the operating effectiveness of system controls; to ensure compliance with established policy and operational procedures; and to recommend changes in controls, policy, or procedures where needed.
Audit trail	A chronological record of system activities sufficient to enable the reconstruction, review, and examination of security events related to an operation, procedure, or event in a transaction from its inception to final results.
Authentication	Verification of the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Banner	Display of an information system, which outlines the parameters for system or information use.
CDE	Acronym for "cardholder data environment." The people, processes and technology that store, process, or transmit cardholder data or sensitive authentication data.
Certification in Health Information Security	Healthcare Information and Management Systems Society (HIMSS) and the American Health Information Management Association (AHIMA) are two organizations that offer certifications upon successful completion of an exam.
Certified in Healthcare Privacy and Security (CHPS)	This credential is designated to professionals who are responsible for safeguarding patient information. This credential signifies expertise in planning, executing, and administering privacy and security protection programs in health care organizations and competence in a specialized skill set in the privacy and security aspects of health information management.
Certified Professional in Healthcare Information and Management Systems (CPHIMS)	CPHIMS is a professional certification program for health care information and management systems professionals.

CISA	Certified Information Systems Auditor (CISA)
CISSP	Certified Information Systems Security Professional (CISSP)
Classified	National security information classified pursuant to Executive Order 12958.
CMS	Centers for Medicare and Medicaid Services
Compensating Controls	Compensating controls may be considered when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other controls. Compensating controls must:
Compromise	Also referred to as "data compromise," or "data breach." Intrusion into a computer system where unauthorized disclosure/theft, modification, or destruction of cardholder data is suspected.
Configuration management	A structured process of managing and controlling changes to hardware, software, firmware, communications, and documentation throughout the system development life cycle.
Contractor	The company and/or consultants providing the services.
Cross-Site Request Forgery (CSRF)	Vulnerability that is created from insecure coding techniques, resulting in improper input validation. Often used in conjunction with CSRF and/or SQL injection.
Cross-Site Scripting (XSS)	Vulnerability that is created from insecure coding methods that allows for the execution of unwanted actions through an authenticated session. Often used in conjunction with XSS and/or SQL injection.
Cryptography	The process of rendering plain text information unreadable and restoring such unreadable information to a readable form.
Decryption	The process of converting encrypted information into a readable form. This term is also referred to as deciphering.
De-Identified Information	Records that have had enough PII removed or obscured such that the remaining information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual.
De-Identified PHI	The Privacy Rule does not restrict the use or disclosure of de-identified health information. De-identified health information neither identifies nor provides a reasonable basis to identify an individual. If data is de-identified in the manner prescribed by HIPAA, it is not PHI. Increasingly researchers are seeking and using de-identified clinical data for health system improvement activities.
Discretionary access control	A method of restricting logical access to information system objects (e.g., files, directories, devices, permissions, rules) based on the identity and need-to-know of users, groups, or processes.
Distinguishable Information	Information that can be used to identify an individual.
DMZ	Abbreviation for "demilitarized zone." Physical or logical sub-network that provides an additional layer of security to an organization's internal private network. The DMZ adds an additional layer of network security between the Internet and an organization's internal network so that external parties only have direct connections to devices in the DMZ rather than the entire internal network.
DNS	Acronym for "domain name system" or "domain name server." A system that stores information associated with domain names in a distributed database to provide name-resolution services to users on networks such as the Internet.
EHR	Electronic Health Record
EMV	Europay, MasterCard and Visa which stands for a global standard for cards equipped with computer chips and the technology used to authenticate chip-card transactions.

Entity Under Investigation	A merchant, service provider, financial institution or other entity that processes, stores, or transmits cardholder data is required to comply with any PCI Standard, and is at the time in question required pursuant to Industry Rules to undergo a PFI investigation of a specific Security Issue by a PFI.
Event	Refers to a single event of a known or suspected data compromise. It is used interchangeably with the term "incident."
Forensics	Also referred to as "computer forensics." As it relates to information security, the application of investigative tools and analysis techniques to gather evidence from computer resources to determine the cause of data compromises.
HIPAA	Health Insurance Portability and Accountability Act as updated by the HIPAA Omnibus Final Rule <sup>2</sup> in 2013, set forth how certain entities, including most health care providers, must protect and secure patient information. They also address the responsibilities of Business Associates (BAs), which include EHR developers working with health care providers.
Incident	Refers to each single occurrence of known or suspected data compromise. It is used interchangeably with the term "event."
Information Security: Encryption	Per the HIPAA Security Rule, a CE, such as a health care provider, must use encryption if, after implementing its security management process, it determines that encryption is a reasonable and appropriate safeguard in its practice environment to safeguard the confidentiality, integrity, and availability of e-PHI.
Information system security	The protection of information systems and information against unauthorized access, use modification, or disclosure to ensure the confidentiality, integrity, and availability of information systems and information.
Integrity	The protection of information systems and information from unauthorized modification to ensure the quality, accuracy, completeness, nonrepudiation, and authenticity of information.
Key	Information used to establish and periodically change the operations performed in cryptographic devices for the purpose of encrypting and decrypting information.
Key Staff	The Contractor's vital staff assigned to the project (for example: QSA's)
Management controls	Security controls focused on managing organizational risk and information system security and devising sufficient countermeasures or safeguards to mitigate risk to acceptable levels. Management control families include risk assessment, security planning, system and services acquisition, and security assessment.
Masking	In the context of PCI DSS, it is a method of concealing a segment of data when displayed or printed. Masking is used when there is no business requirement to view the entire PAN. Masking relates to protection of PAN when displayed or printed. See Truncation for protection of PAN when stored in files, databases, etc.
Merchant	For the purposes of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services. Note that a merchant that accepts payment cards as payment for goods and/or services can also be a service provider, if the services sold result in storing, processing, or transmitting cardholder data on behalf of other merchants or service
MO/TO	Mail-Order/Telephone-Order

Network Segmentation	Also referred to as "segmentation" or "isolation." Network segmentation isolates system components that store, process, or transmit cardholder data from systems that do not. Adequate network segmentation may reduce the scope of the cardholder data environment and thus reduce the scope of the PCI DSS assessment. See the Network Segmentation section in the PCI DSS Requirements and Security Assessment Procedures for guidance on using network segmentation. Network segmentation is not a PCI DSS requirement.
Obscured Data	Data that has been distorted by cryptographic or other means to hide information. It is also referred to as being masked or obfuscated.
Operational controls	Security controls focused on mechanisms primarily implemented by people as opposed to systems. These controls are established to improve the security of a group, a specific system, or group of systems. Operational controls require technical or specialized expertise and often rely on management and technical controls. Operational control families include personnel security, contingency planning, configuration management, maintenance, system and information integrity, incident response, and awareness and training.
Organizational Standards	These standards require a CE to have contracts or other arrangements with BAs that will have access to the CE's e-PHI. The standards provide the specific criteria required for written contracts or other arrangements.
PA-DSS	Payment Application Data Security Standard
PAN	Acronym for "primary account number" and also referred to as "account number." Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder
Payment Application	In the context of PA-DSS, a software application that stores, processes, or transmits cardholder data as part of authorization or settlement, where the payment application is sold, distributed, or licensed to third parties.
Payment Processor	Sometimes referred to as "payment gateway" or "payment service provider (PSP)". Entity engaged by a merchant or other entity to handle payment card transactions on their behalf. While payment processors typically provide acquiring services, payment processors are not considered acquirers unless defined as such by a payment card brand.
PCI	Payment Card Industry
PCI Forensic Investigator, PFI, or PFI Company	Refers to a company, organization, or other legal entity that is in compliance with all PFI Company Requirements (defined in the PFI Qualification Requirements) and has been qualified as a PFI Company and/or PFI Employee by PCI SSC (or another Approving Organization, if applicable) as a PFI. A list of PFIs can be obtained at <a href="http://www.pcisecuritystandards.org">www.pcisecuritystandards.org</a>
PCI-DSS	Payment Card Industry Data Security Standard
Penetration Test	Penetration tests attempt to identify ways to exploit vulnerabilities to circumvent or defeat the security features of system components. Penetration testing includes network and application testing as well as controls and processes around the networks and applications, and occurs from both outside the environment (external testing) and from inside the environment.
Personally Identifiable Information	Any information about an individual maintained by an agency with respect to, but not limited to, education, financial transactions, medical history, and criminal or employment history, and information that can be used to distinguish or trace an individual's identity (e.g., name, Social Security Number, date and place of birth, mother's maiden name, biometric records) including any other personal information linked or linkable to an individual.

PFI Investigation	Refers to the forensic investigation of a Security Issue for an Entity Under Investigation pursuant to applicable Industry Rules for PFI Program
PFI Portal	The secure web portal designated by PCI SSC for the applicable purpose in connection with the PFI Program.
Physical Safeguards	These safeguards are physical measures, policies, and procedures to protect electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion. These safeguards are the technology and the policies and procedures for its use that protect e-PHI and control access to it.
PII Confidentiality Impact Level	The PII confidentiality impact level—low, moderate, or high—indicates the potential harm that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.
PMP	Project Management Professional
POI	Acronym for "Point of Interaction," the initial point where data is read from a card. An electronic transaction-acceptance product, a POI consists of hardware and software and is hosted in acceptance equipment to enable a cardholder to perform a card transaction. The POI may be attended or unattended. POI transactions are typically integrated circuit (chip) and/or magnetic-stripe card-based payment
Point of Compromise	Refers to the location where account number data was obtained by unauthorized third parties.
Policies and Procedures	These standards require a CE to adopt reasonable and appropriate policies and procedures to comply with the provisions of the Security Rule. A CE must maintain, until six years after the date of their creation or last effective date (whichever is later), written security policies and procedures and written records of required actions, activities, or assessments. A CE must periodically review and update its documentation in response to environmental or organizational changes that affect the security of e-PHI.
Privacy Impact Assessment (PIA)	*An analysis of how information is handled that ensures handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; determines the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and examines and evaluates protections and alternative processes for handling information to mitigate potential privacy risks.
Project	The Payment Card Industry Data Security Standard PCI Compliance Assessment provide to the State of New Hampshire
Project Leads	The Contractor's main staff that will direct the project through to completion (for example: Project Managers)
Project Staff	All of the Contractor's Staff assigned to complete the PCI Assessments and/or Remediation efforts, including project leads, management and key staff.
QSA	Qualified Security Assessor

Risk Analysis	The risk analysis requirement in the HIPAA Security Rule is much more expansive. It requires you to assess the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all the electronic Protected Health Information (e-PHI) that an organization creates, receives, maintains, or transmits — not just the e-PHI maintained in Certified EHR Technology (CEHRT). This includes e-PHI in other electronic systems and all forms of electronic media, such as hard drives, floppy disks, compact discs (CDs), digital video discs (DVDs), and smart cards or other storage devices, personal digital assistants, transmission media, or portable electronic media. In addition, you will need to periodically review your risk analysis to assess whether changes in your environment necessitate updates to your security measures.
ROC	Report on Compliance
Security Issue	Refers to an actual or suspected compromise or other incident that, in accordance with applicable Industry Rules, requires forensic investigation by a PFI.
Service Provider	Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity. This also includes companies that provide services that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, IDS and other services as well as hosting providers and other entities. If an entity provides a service that involves only the provision of public network access—such as a telecommunications company providing just the communication link—the entity would not be considered a service provider for that service (although they may be considered a service provider for other services).
SoNH	State of New Hampshire
SQL Injection	Form of attack on database-driven web site. A malicious individual executes unauthorized SQL commands by taking advantage of insecure code on a system connected to the Internet. SQL Injection attacks are used to steal information from a database from which the data would normally not be available and/or to gain access to an organization's host computers through the computer that is hosting the database.
State	Refers to the State of New Hampshire
System of Records	"A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."
System Security Plan	An official document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements (NIST SP 800-18).
Technical controls	Security controls executed by the computer system through mechanisms contained in the hardware, software, and firmware components of the system. Technical security control families include identification and authentication, access control, audit and accountability, and system and communications protection.
Traceable	Information that is sufficient to make a determination about a specific aspect of an individual's activities or status.
Voice over Internet Protocol (VoIP)	A methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet protocol networks, such as the Internet.

Vulnerability assessment	Systematic examination of an information system to determine its security posture, identify control deficiencies, propose countermeasures, and validate the operating effectiveness of such security countermeasures after implementation.
Work Plan	Schedule and description of the elements of the Statement of Work

Contractor Initials PK  
Date 4/24/18

**EXHIBIT G  
ADDITIONAL TERMS**

Notwithstanding anything else to the contrary in the Agreement, the RFB, or otherwise, the following terms shall apply to the provision of Services hereunder. In the event of a conflict between the terms of the Agreement or RFB and this Exhibit, this Exhibit shall govern.

- (1) **Consequential Damages Waiver.** Notwithstanding anything to the contrary contained in the Agreement or RFB, in no event will either party, or its suppliers, be liable to the other, whether in contract or in tort or under any other legal theory (including, without limitation, strict liability and negligence), for lost profits or revenues, loss of use or loss of data, or for any indirect, special, exemplary, punitive, multiple, incidental, consequential or similar damages, hereunder, even if advised of the possibility of such damages. Notwithstanding this language, this limitation shall not apply to any of the Contractor's obligations under any indemnity clauses in this Agreement.
- (2) **Limitation of Vendor's Liability.** Contractor, Contractor's employees', agents', officers' and directors' total liability under the Agreement, RFB, and in connection with any services provided by Contractor be limited to 2x the amount of fees paid by the State of New Hampshire hereunder. Notwithstanding this language, this limitation shall not apply to any of the Contractor's obligations under any indemnity clauses in this Agreement. Further, in no event shall Contractor's aggregate liability for all claims under the Agreement, RFB, and in connection with any services provided by Contractor, including Contractor's indemnification obligations herein, exceed the greater of one million dollars (\$1,000,000) or the applicable limits of insurance stated in Exhibit A, Section 8 – Insurance.
- (3) **Ownership of Deliverables.** The parties agree that, except as specifically provided herein or the applicable statement of work, all deliverables provided in connection with the services are the property of the State of New Hampshire. Notwithstanding the foregoing, the parties agree that Contractor Intellectual Property (defined below) shall not be considered "work for hire" and shall remain the exclusive property of Contractor. In the event Contractor Intellectual Property is incorporated into any deliverables, Contractor grants the State of New Hampshire an irrevocable, nonexclusive, royalty-free, limited license for the State of New Hampshire to use Contractor Intellectual Property to the extent necessary to use such deliverable for its internal purposes only. "Contractor Intellectual Property" means any know-how, processes, techniques, concepts, methodologies, tools, ideas, designs, inventions, patents, copyrights, improvements, computer programs, software, source code, object code, graphics, intellectual property, information, and/or pictorial representations that (i) Contractor developed prior to responding to this RFB and/or prior to entering into the applicable statement of work with the State of New Hampshire; (ii) is or are developed separate and apart from the RFB, statement of work, and/or services at any time by Contractor; or (iii) led to or produced the results of the services or were otherwise used by Contractor to provide the services.
- (4) **Warranty Disclaimer.** Except for the warranties set forth in the RFB, Contractor hereby disclaims all other warranties, express or implied, including, without limitation, the implied warranties of merchantability and fitness for a particular purpose.

## Business Information

### Business Details

Business Name: COALFIRE SYSTEMS, INC.	Business ID: 616727
Business Type: Foreign Profit Corporation	Business Status: Good Standing
Business Creation Date: 07/16/2009	Name in State of Incorporation: COALFIRE SYSTEMS, INC.
Date of Formation in Jurisdiction: 07/16/2009	
Principal Office Address: 11000 Westmoor Circle, Suite 450 Attn Tax Dept, Westminster, CO, USA	Mailing Address: 11000 Westmoor Circle, Suite 450 Attn Tax Dept, Westminster, CO, USA
Citizenship / State of Incorporation: Foreign/Delaware	
	Last Annual Report Year: 2018
	Next Report Year: 2019
Duration: Perpetual	
Business Email: taxmb@coalfire.com	Phone #: 303-554-6333
Notification Email: NONE	Fiscal Year End Date: NONE

### Principal Purpose

S.No	NAICS Code	NAICS Subcode
1	OTHER / IT Consultants for SAS 70 IT Audits for private businesses.	

Page 1 of 1, records 1 to 1 of 1

### Registered Agent Information

Name: Business Filings Incorporated

Registered Office Address: 9 Capitol Street, Concord, NH, 03301, USA

Registered Mailing Address: 9 Capitol Street, Concord, NH, 03301, USA

### Trade Name Information

---

No Trade Name(s) associated to this business.

---

### Trade Name Owned By

---

No Records to View.

---

### Trademark Information

---

Trademark Number	Trademark Name	Business Address	Mailing Address
------------------	----------------	------------------	-----------------

No records to view.

---

[Filing History](#)     [Address History](#)     [View All Other Addresses](#)     [Name History](#)  
[Shares](#)     [Businesses Linked to Registered Agent](#)     [Return to Search](#)     [Back](#)

NH Department of State, 107 North Main St. Room 204, Concord, NH 03301 -- [Contact Us \(/online/Home/ContactUS\)](#)

Version 2.1 © 2014 PCC Technology Group, LLC, All Rights Reserved.

