

STATE OF NEW HAMPSHIRE
Dept. of Administrative Services
Div. of Procurement and Support Services
Bureau of Purchase and Property
State House Annex
Concord, New Hampshire 03301

Date: January 30, 2019

NOTICE OF CONTRACT – REVISED
(NEW CONTACT)

COMMODITY: SECURITY COMPLIANCE, TESTING AND REMEDIATION SERVICES

CONTRACT NO.: 8002314

NIGP: 920-0000

VENDOR: Coalfire Systems, inc. **VENDOR # :** 221845
11000 Westmoor Circle Suite 450
Westminster, CO 80021

CONTACT PERSON(S): Gil Urena
Tel. No.: 720.259.4222
E-Mail: gil.urena@coalfire.com

EFFECTIVE FROM: May 16, 2018 through February 28, 2021

SCOPE OF WORK: Forensic Investigation Services (All Data Breaches)

PFI Companies 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, the PFI Company must inform the State of New Hampshire that it shall be required to disclose the same as herein described and must obtain clear, unqualified permission and consent from the State of New Hampshire 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 of New Hampshire agency no later than five (5) business days after beginning PFI Investigation review of such State of New Hampshire.

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

- Identity of the reporting agency
- Identity 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 of New Hampshire, and such State of New Hampshire's affected acquirer(s) (if the State of New Hampshire is a merchant), in each case no later than ten (10) business days after completion of the corresponding PFI Investigation of such State of New Hampshire.

- Identity of the reporting agency
- Identity 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.

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

QUESTIONS: Direct any questions to Heather Kelley, 603-271-3147 or Heather.Kelley@NH.Gov

INVOICING, PAYMENTS & DELIVERY:

Invoices shall be submitted after completion of work to the requesting agency. Payment shall be paid in full within thirty (30) days after receipt of invoice and acceptance to the State's satisfaction.

PRICING QUOTATIONS:

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. 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. **The Contractor that provides the lowest bid will be the one that will be selected. Agencies are required to submit a copy of all Contractor quotes to the Department of Administrative Services – Merchant Card Services as proof of bidding out the service to all applicable contractors.**

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	
Policy and Procedures	
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)

NOTE: State of NH PCI DSS Inventory which contains details of the cardholder environment. ***That is part of the checklist.***