

STATE OF NEW HAMPSHIRE
BUREAU OF PURCHASE AND PROPERTY
25 CAPITOL STREET - ROOM 102
CONCORD NEW HAMPSHIRE 03301-6398

DATE: JANUARY 25, 2016

NOTICE OF CONTRACT
REVISION

COMMODITY: CATEGORY 2 - NETWORK & APPLICATION PENETRATION TESTING SERVICES

CONTRACT#: 8001452

NIGP CODE: 920-0000

CONTRACTOR: COALFIRE SYSTEMS, INC. #221845
361 CENTENNIAL PARKWAY, SUITE 150
LOUISVILLE, CO 80027

CONTACT PERSON: HASSAN MAHMOUD
TEL: OFFICE (646) 459-7340 CELL: (848) 219-4516
E-MAIL: Hassan.Mahmoud@coalfire.com

CONTRACT PERIOD: SEPTEMBER 23, 2013 THROUGH JANUARY 31, 2017

TERMS: NET 30 DAYS

ORDERING: SEE ATTACHED PAGES

PRICES AND ITEMS COVERED BY THIS CONTRACT: SEE ATTACHED PAGES

QUESTIONS: DIRECT ANY QUESTIONS TO ROBIN PARKHURST AT 603 271-7410
OR BOB LAWSON AT 603 271-3147

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.

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 shall be done from locations within the United States of America. Access shall 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 shall 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 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
<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
<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)
<u>Vulnerability Checks</u> : The Contractor shall perform specific checks for vulnerabilities on all accessible host IP addresses and services
<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
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
<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
<u>Vulnerability Checks</u> : Contractor shall perform specific checks for vulnerabilities on all accessible host IP addresses and services

PRE-ENGAGEMENT CHECKLIST

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

This form shall 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 shall have the opportunity to submit such a quote and a Purchase Order, if issued, shall 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.

PRICING QUOTATIONS

Agencies shall 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 shall have one (1) extra business day to revise their quotation. The specified hourly rates shall not exceed the rates quoted under this Contract.

ORDERING PROCEDURE FOR SERVICES

Agencies shall process purchase orders complete with attached quote for services procured under this contract. The Contractor providing the lowest priced quote shall be used. The Bureau of Purchase and Property shall 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 shall 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				Type(s)	Number
	Yes		No		
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
	Yes		No		
SPAM Filter				Type(s)	Number
	Yes		No		
Encryption/VPN				Type(s)	Number
	Yes		No		
Authentication (e.g., tokens, biometrics)				Type(s)	Number
	Yes		No		
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 Contractor, 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)?	

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.

PRICING

Table 1 – PENETRATION TESTING PRICING COMBINED RATE

Tasks	Hourly Rate
10/13/2013 – 10/12/2014	
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