

STATE OF NEW HAMPSHIRE APPROVAL SIGNATURE PAGE

VENDOR UHY ADVISORS, TX, LLC

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

EFFECTIVE THROUGH JANUARY 31, 2017

* * * * *

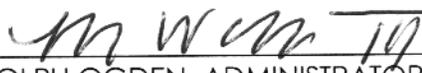
SUBMITTED FOR ACCEPTANCE BY:



ROBERT LAWSON, PURCHASING AGENT
BUREAU OF PURCHASE AND PROPERTY

DATE 9/16/13

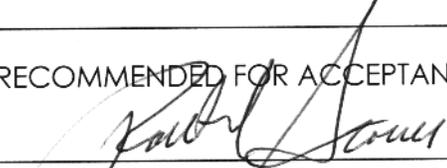
REVIEWED BY:



RUDOLPH OGDEN, ADMINISTRATOR
BUREAU OF PURCHASE AND PROPERTY

DATE 9/16/13

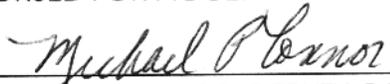
RECOMMENDED FOR ACCEPTANCE BY:



ROBERT STOWELL, ADMINISTRATOR
BUREAU OF PURCHASE AND PROPERTY

DATE 9/18/13

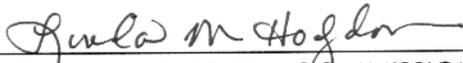
ENDORSED FOR ACCEPTANCE BY:



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

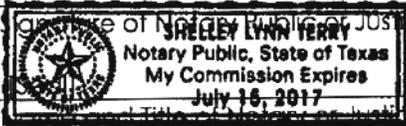
Subject: CATEGORY 2 – NETWORK & APPLICATION PENETRATION TESTING SERVICES

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 UHY Advisors, TX, LLC		1.4 Contractor Address 2929 Allen Parkway, 20 th Floor, Houston, TX 77019	
1.5 Contractor Phone Number 800 949-1706	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 <i>Robert Lawson</i>		1.12 Name and Title of Contractor Signatory <i>Norman Comstock Managing Director</i>	
1.13 Acknowledgement: State of _____, County of _____ On <u>September 9, 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 		1.13.2 Title of Notary Public or Justice of the Peace <i>Shelley Terry</i> <u>9/9/2013</u>	
1.14 State Agency Signature <i>Linda M. Hodgdon</i>		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.

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

UHY Advisors TX, LLC (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
--

Enumeration: 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

Guarantee of Business Volume

There is no minimum amount of business guaranteed under this Contract. Agencies will use this Contract 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	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

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	<input type="checkbox"/>	Yes	<input type="checkbox"/>
Wireless	<input type="checkbox"/>	Yes	<input type="checkbox"/>

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	<input type="checkbox"/>	Yes	<input type="checkbox"/>	No	Type(s)	Number
Intrusion Detection or Prevention System			Type(s)	Number		
Host based	<input type="checkbox"/>	Yes	<input type="checkbox"/>	No		
Network based	<input type="checkbox"/>	Yes	<input type="checkbox"/>	No		
Logging			Type(s)	Number		
Host based	<input type="checkbox"/>	Yes	<input type="checkbox"/>	No		
Network based	<input type="checkbox"/>	Yes	<input type="checkbox"/>	No		
Are log analysis tools used to generate reports?			Yes	<input type="checkbox"/>	No	<input type="checkbox"/>
SPAM Filter	<input type="checkbox"/>	Yes	<input type="checkbox"/>	No	Type(s)	Number
Encryption/VPN	<input type="checkbox"/>	Yes	<input type="checkbox"/>	No	Type(s)	Number
Authentication (e.g., tokens, biometrics)	<input type="checkbox"/>	Yes	<input type="checkbox"/>	No	Type(s)	Number
Anti-Virus			Type(s)	Number		
Host based	<input type="checkbox"/>	Yes	<input type="checkbox"/>	No		
Network based	<input type="checkbox"/>	Yes	<input type="checkbox"/>	No		
Gateway based	<input type="checkbox"/>	Yes	<input type="checkbox"/>	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?	

STATE OF NEW HAMPSHIRE
 Department of Administrative Services
 CATEGORY 2 – Network Application Penetration Testing Services

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	Hourly Rate
Network-layer Penetration Tests / Hourly Rate	\$ 149.00
Application-layer Penetration Tests / Hourly Rate	\$ 149.00

10/13/2014 – 10/12/2015	
Network-layer Penetration Tests / Hourly Rate	\$ 149.00
Application-layer Penetration Tests / Hourly Rate	\$ 149.00

10/13/2015 – 10/12/2016	
Network-layer Penetration Tests / Hourly Rate	\$ 149.00
Application-layer Penetration Tests / Hourly Rate	\$ 149.00

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.

UHY ADVISORS TX, LLC
Certificate of Corporate Authority

RON MARTIN, being duly sworn, deposes and says:

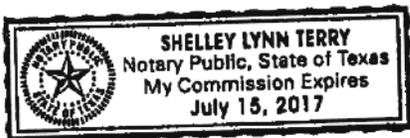
1. I am a duly designated Manager, and the duly elected CEO, of UHY Advisors TX, LLC, a Texas limited liability company (the "Company"), and I am familiar with the provisions and terms of the Company Agreement of the Company dated as of June 30, 2007.

2. Norman Comstock is a duly designated and acting Managing Director of the Company, and has requisite power and authority to execute a contract for RFB #1560-14 with the State of New Hampshire on the Company's behalf, and to execute and deliver such other documents, and do and perform such other things, as he may deem necessary or appropriate in connection therewith.

IN WITNESS WHEREOF, I have caused the Company to execute this Certificate on
September 9, 2013

UHY ADVISORS TX, LLC

By *Ronald W. Martin*
CEO



Shelley Terry
September 9, 2013

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

Filed Documents

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

Business Name History

Name	Name Type
UHY Advisors TX, LLC	Legal
UHY Advisors TX, LLC	Home State

Limited Liability Company - Foreign - Information

Business ID: 636808
Status: Good Standing
Entity Creation Date: 9/29/2010
State of Business.: TX
Principal Office Address: 2929 Allen Parkway, 20th Floor
 Houston TX 77019
Principal Mailing Address: 2929 Allen Parkway, 20th Floor
 Houston TX 77019
Last Annual Report Filed Date: 4/23/2013
Last Annual Report Filed: 2013

Registered Agent

Agent Name: National Registered Agents, Inc.
Office Address: Sulloway & Hollis
 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.



CERTIFICATE OF LIABILITY INSURANCE

UHYAD-1

OP ID: SH

DATE (MM/DD/YYYY)

08/01/13

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 Cambridge Underwriters Ltd. P.O. Box 511077 Livonia, MI 48151-7077 Shauna L. McFarlane, AAI, LIC	734-525-0927	CONTACT NAME:		FAX (A/C, No):	
	734-525-0612	PHONE (A/C, No, Ext):			
		E-MAIL ADDRESS:			
		INSURER(S) AFFORDING COVERAGE		NAIC #	
		INSURER A: Federal Insurance Company		20281	
		INSURER B: Great Northern Insurance Co.		20303	
		INSURER C:			
		INSURER D:			
		INSURER E:			
		INSURER F:			

INSURED
UHY Advisors TX, LLC
Attn: Gerald Burger
2929 Allen Parkway, 20th Floor
Houston, TX 77019-7100

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.

INSR LTR	TYPE OF INSURANCE	ADGL INSR	BUSR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
A	GENERAL LIABILITY <input checked="" type="checkbox"/> COMMERCIAL GENERAL LIABILITY <input type="checkbox"/> CLAIMS-MADE <input checked="" type="checkbox"/> OCCUR			35765238	07/15/13	07/15/14	EACH OCCURRENCE	\$ 1,000,000
	GENL AGGREGATE LIMIT APPLIES PER: <input type="checkbox"/> POLICY <input type="checkbox"/> PRO-JECT <input type="checkbox"/> LOC						DAMAGE TO RENTED PREMISES (Ea occurrence)	\$ 1,000,000
A	UMBRELLA LIAB EXCESS LIAB			79798398	07/15/13	07/15/14	MED EXP (Any one person)	\$ 10,000
	<input checked="" type="checkbox"/> OCCUR <input checked="" type="checkbox"/> CLAIMS-MADE						PERSONAL & ADV INJURY	\$ 1,000,000
B	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below		N/A	71648195	07/15/13	07/15/14	GENERAL AGGREGATE	\$ 2,000,000
							PRODUCTS - COMPROP AGG	\$ 2,000,000
	AUTOMOBILE LIABILITY ANY AUTO ALL OWNED AUTOS HIRED AUTOS						COMBINED SINGLE LIMIT (Ea accident)	\$
							BODILY INJURY (Per person)	\$
							BODILY INJURY (Per accident)	\$
							PROPERTY DAMAGE (Per accident)	\$
								\$
							EACH OCCURRENCE	\$ 25,000,000
							AGGREGATE	\$ 25,000,000
								\$
							<input checked="" type="checkbox"/> WC STATU-TORY LIMITS	OTH-ER
							E.L. EACH ACCIDENT	\$ 1,000,000
							E.L. DISEASE - EA EMPLOYEE	\$ 1,000,000
							E.L. DISEASE - POLICY LIMIT	\$ 1,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (Attach ACORD 101, Additional Remarks Schedule, if more space is required)
RE: RFB 1560-14: Category 2 - Network & Application Penetration Testing Services

CERTIFICATE HOLDER

BUOFCNH

Bureau of Purchase and
Property c/o Robert Lawson
State House Annex, Room 102
25 Capitol Street
Concord, NH 03301

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
Shauna L. McFarlane, AAI, LIC

© 1988-2010 ACORD CORPORATION. All rights reserved.

STATE OF NEW HAMPSHIRE

CATEGORY 2 – NETWORK & APPLICATION PENETRATION TESTING
SERVICES

AUGUST 5, 2013



ADDENDUM #1

RFB INVITATION #1560-14

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?

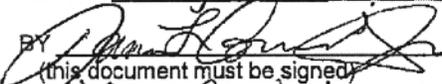
If no, how many systems are there total? i.e.: servers, desktops devices, etc.

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 UHY ADVISORS TX, LLC ADDRESS 2929 Allen Parkway, 20th Floor.
BY  Houston, TX 77019
(this document must be signed)
Norman Comstock TEL. NO. (713) 960-1706
(please type or print name)

Agency	Application	URL	Development
Board of Nursing	Online Licensing for Nursing Professionals	https://nhlicenses.nh.gov/MyLicenseEnterprise/	COTS
Liquor Commission	Online Licensing for Onsite/Offsite Liquor Permittees	https://nhlicenses.nh.gov/MyLicenseEnterprise/	COTS
Joint Board of Licensure and Certification	Online Licensing for Accounting Professionals	https://www4.egov.nh.gov/MyLicenseMLO/Login.aspx	COTS
Joint Board of Licensure and Certification	Online Professional Licensing	https://nhlicenses2.nh.gov/professional/	Custom - Vendor
Department of Education	Educator Information System	https://my.doe.nh.gov/NHEIS	Custom - Vendor
Department of Safety	Online Driver License Renewal	https://www4.egov.nh.gov/odlr/	Custom - In House
Department of Safety	Online Ticket Payment	https://www4.egov.nh.gov/OTP/default.aspx?type=1	Custom - In House
Department of Transportation	Online Oversize/Overweight Permitting	https://nhlicenses2.nh.gov/cc-cl-bin/osow/login.cgi	Custom - Vendor
Liquor Commission	ICE/Gift Card E-Commerce Solution	http://ca.liquor.nh.gov/	Custom - In House
Lottery Commission	Online Lottery Subscription	https://www4.egov.nh.gov/LotterySubscriptions/HomePage.aspx	Custom - In House
Secretary of State's Office	SystemWorks - UCC Online Services	https://ccrp.sos.nh.gov/	Custom - Vendor
Secretary of State's Office	Annual Report Online Filing	https://www.sos.nh.gov/corporate/annualreport/	Custom - Vendor

SIGNED TRANSMITTAL LETTER

RFB INVITATION #1560-14

STATE OF NEW HAMPSHIRE BID TRANSMITTAL LETTER

Date: 8/5/13

Company Name: UHY Advisors TX, LLC
Address: 2929 Allen Parkway, 20th Floor, Houston, TX 77019

To: Point of Contact: ROBERT LAWSON
Telephone: (603)-271-3147
Email: prchweb@nh.gov

RE: 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] Norman Comstock on behalf of UHY Advisors TX, LLC [insert name of entity submitting bid] 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 at 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 21-I: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 21-I:11-c within the past year.

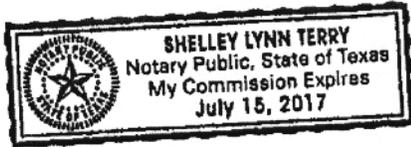
Authorized Signor's Signature [Signature] Authorized Signor's Title Managing Director

NOTARY PUBLIC/JUSTICE OF THE PEACE

COUNTY: Harris STATE: TX ZIP: 77019

On the 5 day of August, 2013, personally appeared before me, the above named Norman Comstock, in his/her capacity as authorized representative of UHY Advisors 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]
(Notary Public/Justice of the Peace)



My commission expires: July 15, 2017 (Date)

**REQUEST FOR BID FOR - CATEGORY 2 - NETWORK & APPLICATION PENETRATION TESTING SERVICES FOR
THE STATE OF NEW HAMPSHIRE**

SECTION 1 – GENERAL INSTRUCTIONS

1.1 INSTRUCTIONS TO VENDOR:

Read the entire bid invitation prior to filling it out. Complete the pricing information in **ATTACHMENT 1 – PRICE RESPONSE SHEET** and all other required information on your offer. Also complete the "Vendor Contact Information" Page 6. Finally, complete the company information on the "Bid Transmittal Letter" page of this bid invitation, then sign the bid in the space provided on that page.

1.2 SPECIFICATIONS:

Complete specifications required are detailed in **SECTION 2 - SPECIFICATIONS**. In responding to the bid, the vendor shall address all requirements for information as outlined.

1.3 VENDOR RESPONSIBILITY:

The successful Vendor shall be solely responsible for meeting all terms and conditions specified in the bid, and any resulting contract(s).

1.4 TERMS OF SUBMISSION:

All material received in response to this bid shall become the property of State and will not be returned to the Vendor. Regardless of the Vendors selected, State reserves the right to use any information presented in a bid response. The content of each Vendor's bid shall become public information once a contract(s) has been awarded.

Complete bids shall be filled out on original bid format. Vendors may submit additional paperwork with pricing, but all pricing shall be on bid and in the State's format.

1.5 LIABILITY:

The State shall not be held liable for any costs incurred by the vendor in the preparation of their bid or for work performed prior to contract(s) issuance.

1.6 CONTRACT(S) TERMS AND CONDITIONS:

The vendor's signature on a bid submitted in response to this bid guarantees that all of the State of New Hampshire's Terms and Conditions are accepted by the Vendor

The form contract(s) P-37 attached hereto shall be part of this bid and the basis for the contract(s). The successful Vendor and the State, following notification, shall promptly execute this form of contract(s), which is to be completed by incorporating the service requirements and price conditions established by the vendor's offer.

1.7 PUBLIC DISCLOSURE OF BID SUBMISSIONS:

Generally, all bids and proposals (including all materials submitted in connection with them, such as attachments, exhibits and addenda) become public information upon the effective date of a resulting contract or purchase order. However, to the extent consistent with applicable state and federal laws and regulations, as determined by the State, including, but not limited to, RSA Chapter 91-A (the "Right-to-Know" Law), the State will attempt to maintain the confidentiality of portions of a bid that are clearly and properly marked by a Vendor as confidential. Any and all information contained in or connected to a bid or proposal that a Vendor considers confidential must be clearly designated in a manner that draws attention to the designation. The State shall have no obligation to maintain the confidentiality of any portion of a bid, proposal or related material, which is not so marked. Marking an entire bid, proposal, attachment or sections thereof confidential without taking into consideration the public's right to know will neither be accepted nor honored by the State. Notwithstanding any provision of this RFP/RFB to the contrary, pricing will be subject to public disclosure upon the effective date of all

resulting contracts or purchase orders, regardless of whether or not marked as confidential. If a bid or proposal results in a purchase order or contract, whether or not subject to approval by the Governor and Executive Council, all material contained in, made part of, or submitted with the contract or purchase order shall be subject to public disclosure.

If a request is made to the State by any person or entity to view or receive copies of any portion of a bid or proposal, and if disclosure is not prohibited under RSA 21-I: 13-a, Vendors acknowledge and agree that the State may disclose any and all portions of the bid, proposal or related materials which is not marked as confidential. In the case of bids, proposals or related materials that contain portions marked confidential, the State will assess what information it believes is subject to release; notify the Vendor that the request has been made; indicate what, if any, portions of the bid, proposal or related material will not be released; and notify the Vendor of the date it plans to release the materials. The State is not obligated to comply with a Vendor's designation regarding confidentiality.

By submitting a bid or proposal, the Vendor agrees that unless it obtains and provides to the State, prior to the date specified in the notice described in the paragraph above, a court order valid and enforceable in the State of New Hampshire, at its sole expense, enjoining the release of the requested information, the State may release the information on the date specified in the notice without any liability to the Vendor.

1.8 TERMINATION:

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

1.9 VENDOR CERTIFICATIONS:

ALL Vendors **SHALL** be duly registered as a Vendor authorized to conduct business in the State of New Hampshire. Vendors shall comply with the certifications below at the time of submission and through the term of any contract which results from said bid. Failure to comply shall be grounds for disqualification of bid and/or the termination of any resultant contract:

- **STATE OF NEW HAMPSHIRE VENDOR APPLICATION:** Vendor **SHALL** have a completed Vendor Application and Alternate W-9 Form which **SHALL** be on file with the NH Bureau of Purchase and Property. See the following website for information on obtaining and filing the required forms (no fee): <http://admin.state.nh.us/purchasing/Contractor.asp>
- **NEW HAMPSHIRE SECRETARY OF STATE REGISTRATION:** A bid award, in the form of a contract(s), will **ONLY** be awarded to a Vendor who is registered to do business **AND** in good standing with the State of New Hampshire. Please visit the following website to find out more about the requirements for registration with the NH Secretary of State: <http://www.sos.nh.gov/corporate>.
- **CONFIDENTIALITY & CRIMINAL RECORD:** If Applicable, by the using agency, the Vendor will 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.

1.10 INVOICING:

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 of the work to the State's satisfaction.

1.11 BID INQUIRIES:

All questions regarding this bid, including clarifications and proposed specification changes shall be submitted to Robert Lawson Purchasing Agent, Bureau of Purchase and Property, at bob.lawson@nh.gov, or Telephone number: 603-271-3147. All requests shall be submitted five business days prior to bid opening date.

Vendor shall include complete contact information including the vendor's name, telephone number and fax number and e-mail address.

1.12 BID DUE DATE:

All bid submissions shall be received at the Bureau of Purchase and Property no later than the date and time shown on transmittal letter of this bid. Submissions received after the date and time specified will be marked as "Late" and will not be considered in the evaluation process.

All offers shall remain valid for a period of one hundred and eighty (180) days from the bid due date. A vendor's disclosure or distribution of Bids other than to DAS, Bureau of Purchase and Property may be grounds for disqualification.

1.13 VENDOR'S RESPONSIBILITY:

Read the entire bid invitation prior to filling it out. Complete the pricing information in **ATTACHMENT 1 – PRICE RESPONSE SHEET** and all other required information on your offer. Also complete the "Bidder Contact Information" Page 7. Finally, complete the company information on the "Bid Transmittal Letter" page of this bid invitation, then sign the bid in the space provided on that page. All State of New Hampshire bid invitations and addenda to these bid invitations are advertised on our website at: <http://admin.state.nh.us/purchasing/index2.asp>

It is a prospective Vendor's responsibility to access our website to determine any bid invitation under which they wish to participate. It is also the Vendor(s)'s responsibility to access our website for any posted addendum.

The website is update several times per day; it is the responsibility of the prospective Vendor(s) to access the website frequently to ensure no bidding opportunity or addenda are overlooked.

It is the prospective Vendor's responsibility to forward a signed copy (if the form has a signature block) of any addenda to the Bureau of Purchase and Property with the bid response.

1.14 INSTRUCTIONS TO VENDOR(S):

Read the entire bid invitation prior to filling it out. In the preparation of your bid response you shall:

- Complete the pricing information in **ATTACHMENT 1 – PRICE RESPONSE SHEET**
- Complete all other required information on your offer
- Complete the "Vendor(s) Contact Information" section
- Complete the company information on the Bid Transmittal Letter page, and sign the bid in the space provided on that page.

1.15 IF AWARDED A CONTRACT, The Vendor must complete the following sections of the attached agreement State of New Hampshire Form #P-37;

Section 1.3 Contractor(s) Name

Section 1.4 Contractor(s) Address

Section 1.11 Contractor(s) Signature

Section 1.12 Name & Title of Contractor(s) Signor

Section 1.13 Acknowledgement

Section 1.13.1 Signature of Notary Public or Justice of the Peace

Section 1.13.2 Name & Title of Notary or Justice of the Peace

- Provide certificate of insurance with the minimum limits required as described in **Section 1.20**.
- Provide a certificate of good standing from the NH Secretary of State or proof of your completion of and payment for the start of the registration process.
- Provide a Corporate Resolution or Certificate of Authority. This document provides evidence that the person signing the Contract has the corporate authority to sign such agreements.

1.16 BID SUBMISSION:

This bid may have been delivered to you in a facsimile or web based format. Vendor shall return their signed complete hard copy or complete fax copy offers to the Bureau of Purchase and Property before the date and time above in "Bid Submission".

Submission of bid in its entirety via mail, fax (603-271-7564) or email (prchweb@nh.gov) to:
Robert Lawson, Purchasing Agent
NH Bureau of Purchase and Property
25 Capitol Street - Room 102
Concord NH 03301

Bid responses shall be marked as:

State of New Hampshire RFB 1560-14

Due Date: 8/5/13 @ 11:30 AM

CATEGORY 2 – Network & Application Penetration Testing Services

1.17 BID RESPONSE PREPARATION AND REJECTION RIGHTS:

The State reserves the right to waive any irregularities or information in any Vendor's bid. A bid may be rejected if it is conditional, incomplete, or if it contains irregularities of any kind.

If a bidder has altered, modified, deleted or taken exception to the contents of this bid the bidder will be required to withdraw such alterations, modifications, deletions or exceptions to be considered for award.

1.18 AWARD:

The award shall be made to the responsible Vendor(s) meeting the criteria established in this RFB and providing the lowest cost in total. The State reserves the right to reject any or all bids or any part thereof and add/delete locations to the contract price. If an award is made it shall be, in the form of a State of New Hampshire Contract(s).

Any resulting contract(s) shall become effective on the date approved by the Commissioner of Department of Administrative Services for the State of New Hampshire.

The term of the contract shall be from the date of award through January 31, 2017. 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 successful Vendor and the Bureau of Purchase and Property, with the approval of the Commissioner of the Department of Administrative Services. In no event, however, shall the total term of the contract and any extensions thereof exceed five (5) years in total.

1.19 NOTIFICATION AND AWARD OF CONTRACT(S):

Bid results will not be given by telephone. For Vendors wishing to attend the bid opening: only the names of the vendors submitting responses will be made public. Specific response information will not be given out. Bid results will be made public after final approval of the contract(s).

Bid results may also be viewed on our website at <http://www.state.nh.us/purchasing/bld.asp>.

1.20 CERTIFICATE OF INSURANCE:

Prior to performing any services for the State, vendors awarded a contract shall be required to:

- Submit proof of comprehensive general liability insurance. The coverage shall have appropriate riders against all claims of bodily injury, death or property damage, in amounts of not less than \$250,000.00 per claim and \$2,000,000.00 per occurrence or \$1,000,000.00 per occurrence with \$1,000,000.00 umbrella.
- Certify compliance with, or exemption from, the requirements of NH RSA 281-A, Workers' Compensation.

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:

<u>RICHARD PETERS</u>	<u>713) 407-3870</u>	<u>(800) 949-1706</u>
Contact Person	Telephone Number	Toll Free Telephone Number
<u>713) 960-9549</u>	<u>RPETERS@UTHY-US.COM</u>	<u>WWW.UTHY-US.COM</u>
Fax Number	E-mail Address	Company Website

SECTION 2 – SPECIFICATIONS

2.1 **PURPOSE:**

The purpose of this bid invitation is to establish Statewide Contracts to provide 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. Any contract(s) resulting from this solicitation may be used by the State of New Hampshire agencies and institutions during the term of the contract(s), in accordance with the requirements of this bid invitation and any resulting contract(s).

2.2 **BACKGROUND:**

Eleven (11) State agencies accept merchant cards at more than one hundred (100) locations (see **Exhibit 1**). The majority of agency business offices that support these locations are headquartered in Concord, New Hampshire but the merchandising locations are geographically located throughout the state.

The State's acceptance of credit cards has grown significantly over time currently numbering almost 6.5 million transactions and \$374 million in sales annually. Agencies use a variety of methods to accept credit cards including standalone swipe devices, point of sale terminals, and e-commerce applications. The State currently has a contract with Bank of America Merchant Card Services to process its credit card transactions.

2.3 **SCOPE OF SERVICES:**

Contracts will be awarded to up to three (3) vendors who are 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). Vendors shall be required to continue to be PCI certified as required while performing PCI services for the state.

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.

The scope of work shall include **CATEGORY 2 - Network & Application Penetration Testing Services** for all locations included in this bid in **Exhibit 1** and other locations that may be added 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 contracted vendor to provide a quotation for that new location. Pricing quotations submitted for new locations shall be in line with the pricing structure as submitted in this bid.

CATEGORY 2 - Network & Application Penetration Testing Services shall be completed in a reasonable time frame as mutually agreed upon with agency and vendor. The Vendor 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

The State of New Hampshire will award contracts to a maximum of three (3) QSA vendors.

The contracts will be awarded to Qualified Security Assessor (QSA) vendors 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. These contracts shall require:

TABLE 1 PENETRATION TESTING SERVICES

<p>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 vendor shall provide a service designed to satisfy these requirements and include the following</p>
<p><u>Enumeration</u>: A list of targeted and authorized IP addresses will 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</p>
<p><u>Inventory</u>: The vendor determines 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 are probed by the Vendor for any information that can be used to verify the actual application layer protocol (e.g., HTTP), as well as vendor applications (e.g. Apache, IIS, Netscape, Domino) and version</p>
<p><u>System Discovery</u>: The vendor 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 vendor performs specific checks for vulnerabilities on all accessible host IP addresses and services</p>
<p><u>Manual Analysis and Verification</u>: The vendor performs 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 vendor documenting the findings and include high-level recommendations. All testing phases must 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 vendor shall provide a service designed to satisfy these requirements and include the following</p>
<p><u>Manual Analysis and Verification</u>: Contractor performs manual web application vulnerability assessment based on PCI DSS Requirements 6.5 and 11.3.1</p>
<p><u>Vulnerability Checks</u>: Contractor performs specific checks for vulnerabilities on all accessible host IP addresses and services</p>

Guarantee of Business Volume

Vendors should note that there is no minimum amount of business guaranteed in this bid solicitation. Agencies will use these contacts as their needs develop. Vendors responding to this bid should have adequate personnel to fulfill contract requirements but should have sufficient existing business to sustain those personnel without relying on business from the State.

2.4 AGENCIES AS MERCHANTS:

The agencies listed on the **EXHIBIT 1, AGENCIES AS MERCHANTS** provide a representation of the types of agencies that process credit cards and their annual sales and transaction volume.

2.5 VENDOR PERSONNEL QUALIFICATIONS:

As required by PCI DSS. The contractor shall assign certified consultants to validate the State's compliance with the data security requirements listed in this RFB.

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

Responses to qualification requirements will be recorded in **ATTACHMENT 3, COMPANY PROFILE AND VENDOR MINIMUM REQUIREMENTS** of the Response.

2.6 SUBCONTRACTOR:

The successful Vendor shall be solely responsible for meeting all terms and conditions specified in this solicitation, their bid, and any resulting contract. Any subcontracted vendor shall first be approved by the State. The Vendor 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 resulting from any contract.

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

Vendors must provide, as **ATTACHMENT 5, PROPOSED SUBCONTRACTORS as described below.**

- The name, address and phone number of any proposed subcontractor.
- Number of years they have provided these types of services
- References of customers for whom they have provided similar services
- A company profile including a description of staff, # of employees, position held, qualifications, number of years in industry etc.

2.7 PRE-ENGAGEMENT CHECKLIST:

Vendors shall agree to use the Pre-Engagement Checklists found in **Exhibits 3 and 4** of this bid.

This form will be used by a requesting agency to convey to all the awarded contractors the services they are requesting. Contracted vendors will use this Checklist to generate a quote to the Agency based on the hourly rates they are submitting in this response. All contracted vendors will have the opportunity to submit such a quote and a Purchase Order, if issued, will go to the contracted vendor submitting the lowest priced quotation.

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

2.8 PRICING QUOTATIONS

Once the contract has been awarded, agencies may request quotations from all awarded 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 shall not exceed the rates quoted under this Contract. A Maximum of three (3) contracts will be awarded to the vendors with the lowest Total Bids.

2.9 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 to vendors on behalf of the State agencies.

SECTION 3 – BID RESPONSE PROCEDURES

3.1 PRICE RESPONSE SHEETS:

Vendors must provide, as **ATTACHMENT 1, PRICE RESPONSE SHEETS**, pricing as specified within this RFB. **All Pricing must be submitted as Fully Loaded (all expenses included) and FOB Destination.** Vendors must submit pricing using the table format provided.

Table 1 - Table 1 lists the rate for each scanning service category in each of three contract years as well as a three year total.

3.2 REFERENCES:

All vendors must provide, as **ATTACHMENT 2**, at least three (3) business references, to which they have supplied related services of a comparable magnitude. Vendors should use the Vendor Reference Checklist format included as **Exhibit 2**.

For each reference the vendor must provide:

- A description of the service provided
- The service time period (start date to finish date)
- Required reference contact information

Ensure that all Reference names and phone numbers are current and can be contacted easily.

3.3 COMPANY PROFILE AND VENDOR MINIMUM REQUIREMENTS:

The vendor shall provide the following information in **ATTACHMENT 3**,

COMPANY PROFILE

The vendor shall complete a Company Profile which includes, as a minimum, the following:

- Company overview/background
- Number of employee's
- Length of time business has been in existence

VENDOR COMPANY MINIMUM REQUIREMENTS

Vendor must show evidence that they have successfully completed engagements of a similar nature with government organizations of similar size. Vendor must demonstrate a minimum of three years of performing this type of work.

Vendor must include credentials of personnel meeting the certification requirements and place them in **ATTACHMENT 3** of the Vendor Response. All QSA employees must have valid QSA certification as verified by the PCI Standards Security Council (https://www.pcisecuritystandards.org/approved_companies_providers/verify_qsa_employee.php)

3.4 CONTRACTOR CERTIFICATIONS:

All vendors must provide, as **ATTACHMENT 4**, the following:

- Certificate of Insurance, demonstrating that the vendor has the insurance necessary to provide the services required by the contract as detailed in **Section 1.20**.

Vendors may also be required to provide the following, but need not submit them with the bid response:

- Certificate of Corporate, or Organizational Authority, demonstrating that the officer signing the contract has been duly authorized to do so.
- Certificate of Good Standing/Authority from the New Hampshire Secretary of State.

SECTION 4 – BID EVALUATION, SELECTION & AWARD PROCESS

4.1 **AWARD:**

A Maximum of three (3) contracts will be awarded to the vendors with the lowest Total Bids. Responses must meet or exceed all of the requirements of this RFB.

4.2 **EVALUATION:**

Responses will be reviewed by the Bureau of Purchase and Property and the Department of Information Technology. When the evaluation is complete recommendations for contract awards, if any, will be made to the Commissioner of Administrative Services for final approval.

4.3 **EVALUATION SCREENING PROCESS AND CRITERIA:**

All submissions will be passed through three levels of screening, an Initial Screening Process, an Intermediate Evaluation and a Final Selection process.

4.3.1 Initial Screening Process

The initial screening of will verify full compliance with all mandatory-filing requirements specified in this RFB. Submissions that do not comply may be rejected. Submissions meeting all the requirements will proceed to the Intermediate Evaluation Process.

Each vendor response must be:

- Complete, fulfilling all requirements of the RFB.
- Clear and understandable
- In the format specified in **Section 5; RESPONSE FORMAT.**

4.3.2 Intermediate Evaluation

ATTACHMENT 2 (REFERENCES), and **ATTACHMENT 3 (COMPANY PROFILE AND VENDOR MINIMUM REQUIREMENTS)** will be reviewed and evaluated on a pass/fail basis. Only those responses with a "passing" evaluation in all categories will proceed to the **FINAL SELECTION** stage.

4.3.3 Final Selection

A Maximum of three (3) contracts will be awarded to those vendors whose submissions successfully reach the **FINAL SELECTION** stage, and who have the lowest Total Bids in **ATTACHMENT 1 (PRICE RESPONSE SHEETS).**

BID RESULTS

Bid results will not be given over the telephone. Bid results may be viewed on our web site at: <http://admin.state.nh.us/purchasing/bids.htm>

SECTION 5 - RESPONSE FORMAT

5.1 **FORMAT REQUIREMENTS FOR RESPONSE TO RFB:**

The following format was developed to ensure a comprehensive evaluation of the vendor's offering. This format is not an attempt to limit the content of the response or in any way inhibit a presentation. Submissions not conforming to the format described below may be excluded from further consideration. The vendor's response will consist of the following items, presented in the order in which the explanations appear in this section. If the vendor's response is presented in a tabbed notebook, each tab must have the headings from the following sections.

- Printouts of complete original **Addenda** (if any issued) in numerical sequence, and signed.
- Original printout of **RFB**
- Price Response Sheets (**ATTACHMENT 1**).
- References (**ATTACHMENT 2**).
- Company Profile and Vendor Minimum Requirements (**ATTACHMENT 3**).
- Contractor Certifications (**ATTACHMENT 4**).
- Proposed Subcontractor(s) (**ATTACHMENT 5**)

5.2 **EXPLANATION OF RESPONSE SECTIONS:**

5.2.1 **Original Addenda**

Addenda may be issued for the purpose of change or clarification to the original RFB. Each Addendum must be printed, filled out, signed and inserted in the order in which they were issued.

5.2.2 **Original RFB**

Printout of the Original RFB in its original order with signed and completed Transmittal Letter.

5.2.3 **Price Response Sheets**

The vendor must complete the appropriate table or tables in **ATTACHMENT 1**, as detailed in **Section 3.1; PRICE RESPONSE SHEETS**, providing price information for all services listed. **ATTACHMENT 1** must remain in its original location in the RFB.

5.2.4 **References**

The vendor must provide References in **ATTACHMENT 2**, as detailed in **Section 3.2; References**.

5.2.5 **Company Profile And Vendor Minimum Requirements,**

The vendor must provide in **ATTACHMENT 3**, information as detailed in **Section 3.3, COMPANY PROFILE AND VENDOR MINIMUM REQUIREMENTS**.

5.2.6 **Contractor Certifications**

The vendor must provide in **ATTACHMENT 4**, information as detailed in **Section 3.4, Contractor Certifications**.

5.2.7 **Proposed Subcontractors**

The vendor must provide in **ATTACHMENT 5**, information as detailed in **Section 2.8, Proposed Subcontractor**.

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				
Application-layer Penetration Tests				
Total				

ATTACHMENT 2

REFERENCES

(REFER TO SECTION 3.2 FOR SUBMISSION REQUIREMENTS)

Ensure that all Reference names and phone numbers are current and can be contacted easily.

ATTACHMENT 3

COMPANY PROFILE AND VENDOR MINIMUM REQUIREMENTS

(REFER TO SECTION 2.6 AND 3.3 FOR SUBMISSION REQUIREMENTS)

ATTACHMENT 4

CONTRACTOR CERTIFICATIONS

(REFER TO SECTION 3.4 FOR SUBMISSION REQUIREMENTS)

ATTACHMENT 5

PROPOSED SUBCONTRACTORS

(REFER TO SECTION 2.7 FOR SUBMISSION REQUIREMENTS)

EXHIBIT 1

Agencies as merchants

Sales and transaction data by State Agency for calendar year 2012

Ref#	Agency / Boards Accepting Merchant Cards	Locations Processing Merchant Card Transactions	Totals	
			Gross Sales	Gross Transactions
1	Education Department	1	\$ 945,445.00	8,270
2	Fish & Game Department	1	\$ 239,567.25	3,475
3	Joint Board of Licensure	1	\$ 1,269,910.37	7,788
4	Liquor Commission	82	\$ 337,381,899.79	5,824,069
5	Lottery Commission ^a	1	\$ 373,100.00	2,944
6	Nursing, Board of	1	\$ 1,386,445.00	16,977
7	Pease Development Authority	2	\$ 749,699.26	3,330
8	Resources & Economic Development	19	\$ 7,019,664.53	311,056
9	Safety Department	28	\$ 18,072,311.63	233,001
10	Secretary of State	1	\$ 7,059,484.00	65,342
11	Transportation Department	1	\$ 315,004.00	13,392
	Total	138	\$ 374,812,530.83	6,489,644

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				
2				
3				

EXHIBIT 3

Network Penetration Testing: Pre-Engagement Checklist

These questions are intended to help the vendor 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 vendor 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					
Host based	Yes	No		Type(s)	Number
Network based	Yes	No			
Logging					
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					
Host based	Yes	No			
Network based	Yes	No			
Gateway based	Yes	No			

EXHIBIT 4

Application Penetration Testing: Pre-Engagement Checklist

These questions are intended to help the vendor 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 vendor 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)?	

Subject: _____

1.0 AGREEMENT

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

GENERAL PROVISIONS

1. IDENTIFICATION.

1.1 State Agency Name		1.2 State Agency Address	
1.3 Vendor Name		1.4 Vendor Address	
1.5 Vendor Phone #	1.6 Account Number	1.7 Completion Date	1.8 Price Limitation
1.9 Contract(s)ing Officer for State Agency		1.10 State Agency Telephone Number	
1.11 Vendor Signature		1.12 Name and Title of Vendor Signatory	
1.13 Acknowledgement: State of _____, County of _____ On _____, 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			
1.14 State Agency Signature		1.15 Name and Title of State Agency Signatory	
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 VENDOR/SERVICES TO BE PERFORMED. The State of New Hampshire, acting through the agency identified in block 1.1 ("State"), engages Vendor identified in block 1.3 ("Vendor") to perform, and the Vendor 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 Vendor commences the Services prior to the Effective Date, all Services performed by the Vendor prior to the Effective Date shall be performed at the sole risk of the Vendor, and in the event that this Agreement does not become effective, the State shall

have no liability to the Vendor, including without limitation, any obligation to pay the Vendor for any costs incurred or Services performed. Vendor shall 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 Vendor 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(S) PRICE/PRICE LIMITATION/ PAYMENT.

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

5.3 The State reserves the right to offset from any amounts otherwise payable to the Vendor 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 VENDOR WITH LAWS AND REGULATIONS/ EQUAL EMPLOYMENT OPPORTUNITY.

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

6.2 During the term of this Agreement, the Vendor 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 Vendor 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 Vendor further agrees to permit the State or United States access to any of the Vendor'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 Vendor shall at its own expense provide all personnel necessary to perform the Services. The Vendor 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 Vendor shall not hire, and shall not permit any subvendor 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 Contract(s)ing 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 Contract(s)ing 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 Vendor 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 Vendor 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 Vendor notice of termination;

8.2.2 give the Vendor 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(s) price which would otherwise accrue to the Vendor during the period from the date of such notice until such time as the State determines that the Vendor has cured the Event of Default shall never be paid to the Vendor;

8.2.3 set off against any other obligations the State may owe to the Vendor 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 Vendor shall deliver to the Contract(s)ing 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(s) 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. VENDOR'S RELATION TO THE STATE. In the performance of this Agreement the Vendor is in all respects an independent Vendor, and is neither an agent nor an employee of the State. Neither the Vendor 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/SUBCONTRACT(S). The Vendor 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 subcontract(s)ed by the Vendor without the prior written consent of the State.

13. INDEMNIFICATION. The Vendor 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 Vendor. 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 Vendor shall, at its sole expense, obtain and maintain in force, and shall require any subvendor 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.

14.3 The Vendor shall furnish to the Contract(s)ing Officer identified in block 1.9, or his or her successor, a certificate(s) of insurance for all insurance required under this Agreement. Vendor shall also furnish to the Contract(s)ing 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 Contract(s)ing 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 Vendor agrees, certifies and warrants that the Vendor is in compliance with or exempt from, the requirements of N.H. RSA chapter 281-A ("Workers' Compensation").

15.2 To the extent the Vendor is subject to the requirements of N.H. RSA chapter 281-A, Vendor shall maintain, and require any subVendor or assignee to secure and maintain, payment of Workers' Compensation in connection with activities which the person proposes to undertake pursuant to this Agreement. Vendor shall furnish the Contract(s)ing 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 Vendor, or any subVendor or employee of Vendor, 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 Vendor.

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.

ATTACHMENT 1 – COST/PRICE RESPONSE SHEET

The hourly rates below are fully loaded and include all additional charges including but not limited to: meals, travel and lodging.

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	\$149/hr	\$149/hr	\$149/hr	
Application-layer Penetration Tests	\$149/hr	\$149/hr	\$149/hr	
Total	\$149/hr	\$149/hr	\$149/hr	

ATTACHMENT 2 - REFERENCES

Below are three references for which UHY currently holds similar contracts with multiple delivery locations. As a business courtesy to all parties involved, please coordinate with the UHY engagement team lead before contacting any of these references.

Ref. No.	Customer Name, Address and Contact	Customer Contact Telephone Number	Dates of Service From-To	Products and Services Provided
1	Chicago Bridge & Iron One CB&I Plaza 2103 Research Forest Dr. The Woodlands, TX 77380 Mr. Todd Freeman Director, Internal Audit	(832) 513-1842		Attack and Penetration Testing and Vulnerability Scanning
2	CITGO Petroleum 1293 Eldridge Parkway Houston, TX 77077 Mrs. Jamie DuBray General Auditor	(832) 486-4924		Attack and Penetration Testing and PCI DSS Assessment
3	Transocean, Inc. P.O. Box 2765 Houston, Texas 77252 Mr. John Truschinger Senior Vice President, Support Services, and CIO	(713) 232-7500		Attack and Penetration Testing

ATTACHMENT 3 – COMPANY PROFILE AND VENDOR MINIMUM REQUIREMENTS

COMPANY PROFILE

GLOBAL REACH

We are a member firm of UHY International, a global leader in tax and business consultancy services with a high standard of professionalism and service quality with more than 250 independent member firms.

With a significant presence in our two founding member countries, the U.S. and the UK, we now have the depth and breadth to help our clients compete effectively and successfully internationally.

Our national capabilities are enhanced by our global resources and attentive personal service. We can do this because we know each other personally, we know about each firm's specialist sector knowledge and about each other's individual expert experience. But, more than that, we know each other as people through meeting and working together regularly. Our member firms' drive to provide clients with quality services, coupled with an active participation in independent quality assurance programs enabling them to deliver a competitive advantage for clients.

That is why clients like working with us: we provide in-country expertise where required by mid-market clients, and when those clients, as well as established multinationals, seek our services we are able to provide cohesive, cross-border teams, sharing clients' aspirations and delivering customized and timely services to help them make the right decisions.

We achieve sustainable success that generates long-term and loyal client relationships. Our drive for professionalism, quality, integrity and innovation combined with this global reach has enabled us to achieve substantial growth for both



- International organization of tax and business consulting firms
- 6,800 staff in over 250 independent member firms in more than 80 countries
- Global resources and capabilities to assist you with all of your local, national and international service requirements

OUR SERVICE VALUES AND CORE PRINCIPLES

- **Sector Expertise** – Our firm provides access to a pool of highly skilled professionals to meet your specific sector requirements.
- **Responsive and Personal Service** – Our firm believes our clients are best served with a proactive, passionate and technically superior team of professionals with an emphasis placed on continuity of the service team. Our key account executives are available throughout the engagement to review and supervise the team members, meet with management, and to respond to questions as they arise.
- **Value Received for Fees** – We offer efficient and effective service. We also commit to be transparent in our fee communications with the Company.
- **Independence and Integrity** – Our firm adheres to a strict Code of Conduct at every level of service requiring independence in fact and appearance of every partner, principal, employee, and any related party.
- **Thought Leadership** – We offer a client experience beyond the engagement. We believe our clients appreciate thought provoking articles and dialogue opportunities about the issues impacting their business. As a catalyst for discussion, our professionals actively publish points of view on relevant issues. The purpose is to stimulate thinking and discussion. Our mission is to bring you the latest thinking on topics and share best practices. We actively support forums and roundtable discussions that encourage conversation on relevant topics.



PROFESSIONAL SERVICES

- **Audit & Assurance Services** – over 130 professionals offering a broad range of assurance services which are designed to meet rigid compliance requirements and yet provide value in the form of insight into your business. These services include: financial statement audits, reviews and compilations, agreed-upon procedures, SEC registrations, pension and benefit plan audits, due-diligence procedures, and attestation of internal control standards (for Sarbanes-Oxley legislation).
- **Transaction Services** – UHY Advisors is an acknowledged practice leader in providing services to the investment community. Our seasoned professionals can facilitate your strategic investment decisions with their considerable expertise in tax structuring, financial due diligence and valuations.
- **Tax Planning & Compliance Services** – over 130 professionals providing a complete range of tax consulting and compliance services on local, state, national and international issues. Consulting services include tax minimization strategies, structuring of transactions, business formation, and IRS controversy representation.
- **Advisory Services** – with over 90 professionals, our team has deep experience in services that help companies maximize their value, such as Risk Management Consulting, Governance, Compliance and Technology Consulting. Our services include internal/IT audit, operational reviews, cost recovery, construction and joint interest audits, Sarbanes-Oxley documentation and testing, business process improvement, IT security, project management office, software selection and pre and post implementation reviews. This team also consists of certified consultants who partner with clients to assist in the identification and implementation of achieving business objectives; as well as to provide support in acquiring, implementing or developing IT solutions to be integrated into the business process. Our highly certified (QSA, CPA, CISA, CITP, CGEIT, CISSP) trained technology auditors and consultants understand company financial reporting and internal controls requirements, and can readily assess your information risk management and operational effectiveness. We also provide recruiting services for finance, accounting and IT resources throughout the nation and finance, accounting and IT resources on a project or interim basis to help companies complete any project accurately and on time.
- **Forensic, Litigation and Valuation**– more than 30 professionals offering fraud and accounting, forensic litigation/damage analysis, valuation and transactional services, including eDiscovery, FCPA, international arbitration and energy litigation. Across the country and around the world, law firms rely on this group's broad knowledge base, decades of experience and excellent judgment.

ADVISORY SERVICES

UHY's Advisory Services has over 90 professionals, with deep experience in services that help companies maximize their value, such as Risk Management Consulting, Governance, Compliance and Technology Consulting. Our services include internal/IT audit, operational reviews, cost recovery, construction and joint interest audits, Sarbanes-Oxley documentation and testing, business process improvement, IT security, project management office, software selection and pre and post implementation reviews.

Internal Audit, Risk and Compliance Services

GOVERNANCE & PROCESSES

- Establish an Internal Audit Function
- Internal Audit Quality Assessments & Improvements
- Business Process Improvement
- Regulatory Compliance Reviews
- Management & Audit Committee Training
- Industry & Best Practice Benchmarking

RISK & CONTROLS

- Internal Audit Outsourcing & Co-Sourcing
- Sarbanes-Oxley Documentation & Testing
- Fraud, Corruption & Money Laundering Assessments
- IA Quality Assurance Reviews & Best Practices Implementation
- Control Self-Assessment Facilitation & Implementation
- Enterprise Risk Management
- Process Documentation & Improvement

RECOVERIES & CONCERNS

- Joint Interest Audits
- Contract Audits
- Construction Audits
- Foreign Corrupt Practices Act
- Fraud
- Due Diligence
- Special Projects

FINANCIAL EFFECTIVENESS

- People & Organization (Review the finance function & advise on organization structure, skill requirements & the development of competencies)
- Standardization & Simplification of Processes (Conduct assessments of finance controls, processes, data, organization structure, people, systems & benchmark against best practices)
- Support the Implementation of Simplified & Standardized Operating Models & Processes

INFORMATION TECHNOLOGY

- Monitor & Evaluate (IT Audit, IT SOX, Risk Assessments, Payment Card Industry [PCI], SSAE 16s*, Data Mining, Vulnerability Assessments)
- Deliver & Support (Data Management, Security)
- Acquire & Implement (Software Selection, Segregation of Duties (SoD) Implementations, Pre/Post Implementation Reviews)
- Plan & Organize (IT Governance, Project Management)

*Provided exclusively by UHY LLP, an independent licensed CPA and PCAOB registered firm.

Management and Technology Consulting Services

INFORMATION RISK

MANAGEMENT

- Agreed Upon Procedures*
- Co-Sourcing
- Encryption Advisory
- Enterprise-Wide Risk Assessment
- Operational Audits
- Outsourcing
- Payment Card Industry (PCI) DSS
- Readiness Assessment
- Statement on Standards for Attestation Engagements (SSAE-16)
- Technology Audits

PRIVACY & COMPLIANCE

- Compliance Function Assessments
- HIPAA
- HITECH
- NERC Compliance
- PCI DSS – QSA & ASV
- Policies & Procedures
- Privacy & Regulatory Compliance
 - Gramm-Leach-Bliley Act (Privacy)
 - ISO Assistance
 - Sarbanes-Oxley Act (Internal or External)*
 - Application Specific IT Controls
 - General IT Controls

OPERATIONAL EFFECTIVENESS

- IT Governance
- Performance Monitoring
 - Infrastructure Monitoring & Analysis
 - Metrics – IT & Operational
 - Service Level Agreements
- Process Improvement
 - Application Controls Reviews
 - Business Process Reviews
 - Policies, Procedures & Documentation
- Project Management Office (PMO)
 - PMO Accounting
 - PMO Audits
 - PMO Extension
 - PMO Installation
 - PMO Support
 - System & Process Implementation

TECHNOLOGY CONSULTING

- Attack & Penetration Testing
- Business Continuity & Disaster Recovery Planning
- Cloud Provider Vendor Selection
- Cloud Security
- Enterprise Security Architecture Design & Implementation
- ERP Selection & Implementation Assistance
- Network Design, Implementation & Maintenance
- Security Strategy & IT Strategy
- Software Selection

INFRASTRUCTURE

- Infrastructure Diagnostic
- Virtualization
- Infrastructure Design and Build
- VOIP
- SAP
- Oracle

IT OPERATIONS

- ITIL
- ISO 27002 Certification
- Data Management

CIO ADVISORY

- IT Governance
- IT Strategy & Alignment
- IT Transformation

FLEXIBLE SOLUTIONS

- Infrastructure as a Service (IAAS)
- Flex-IT
- Staffing

*Provided exclusively by UHY LLP, an independent licensed CPA and PCAOB registered firm.

GENERAL INFORMATION

Official Registered Name	UHY Advisors TX, LLC
Dun & Bradstreet Number	78-435-3638
Primary SIC Number	541211 – Professional Services
Secondary SIC Number	No Secondary SIC Number
Address	2929 Allen Parkway, 20 th Floor Houston, Texas 77019
Main Phone Number	713-960-1706
Toll Free Number	1-888-276-7080
Fax Number	713-572-4681

KEY CONTACT / AUTHORIZED PARTY

The key contact for this RFP is Managing Director Norman Comstock. His office address is the same as above. His direct line is 713-407-3191; his fax number is 713-572-4681.

Norman is authorized to contractually bind the organization for any proposal against this RFP.

BRIEF HISTORY

In July 2000, six leading regional tax and business advisory firms, with tenures dating back to the early 1970s, merged to form a national professional services entity known as UHY Advisors, Inc. They came together in the pursuit of a shared vision: to deliver the service of a local/regional firm and the services of a national firm to the dynamic middle market.

The Management & Technology Consulting practice within the UHY Advisors TX, LLC Advisory Services division has been offering information security testing since 2001. Further details regarding our strengths and services follow on the next few pages and conclude this response.

OUR APPROACH

Our approach is to deliver relevant and intelligent solutions to our clients. We listen to our clients' needs and take the time to understand their expectations.

We pride ourselves on delivering the highest standard of professional services to our clients in a timely, professional and intelligent manner. We have professional relationships with suppliers that share our values to assist our clients if required.

- We work in collaboration with our clients to ensure they achieve their objectives.
- Our services focus on our clients' requirements with a good understanding of their needs.
- Our client portfolio is broad and consists of publicly listed corporations, large and medium-sized companies, privately owned businesses, not-for-profit and public organizations.
- As a member of UHY, our firm is able to offer specialist sector and country knowledge to the same high quality professional standards in major international business centers.
- We share our clients' aspirations and deliver customized, timely advice to help you make the right business decisions.
- Our drive for professionalism, quality, integrity and innovation combined with global reach has realized substantial growth in our longstanding history for both clients and member firms.

OUR COMMITMENT TO QUALITY

Quality is one of our main values; because it is so very important to us, we strive to achieve this in everything we do.

- Leadership
- Client acceptance procedures
- Compliance with ethical obligations set out by the International Federation of Accountants in its global standard Code of Ethics for Professional Accountants
- Human resources policies and procedures (such as education and training)
- Quality control procedures in accordance with internationally recognized standards

Our firm has signed a Quality Charter committing to the adoption and achievement of performance and service objectives considered essential to delivering this quality promise to clients.

It is our belief in quality as a value and the successful implementation of that value across all of our service areas that make us even more dedicated to quality.

OUR CREDENTIALS

The majority of our practitioners hold professional designations such as certified public accountant (cpa), certified information systems auditor (cisa), certified information systems security professional (cissp), certified information security manager (cism), certified internal auditor (cia), certified in the governance of enterprise it (cgeit) and qualified security assessor (qsa). UHY is committed to hiring and training the best professionals to respond to the needs of our clients.

OUR BENCH STRENGTHS

- Independent member of Urbach Hacker Young International Limited, an international network with 250 independent member firms in over 80 countries.
- 5th largest⁽¹⁾ professional services firm with over 450 professionals, next to the "Big 4," in Texas.
- Hands-on, proactive transaction service professionals providing expertise in financial due diligence, valuation and tax structuring.
- Top 20⁽²⁾ professional services firm in the United States with nearly 1,000 professionals in 13 offices.

⁽¹⁾ Source – *Houston Business Journal*, 2012

⁽²⁾ Source – *Accounting Today*, 2013

NUMBER OF EMPLOYEES & LENGTH OF TIME IN BUSINESS

UHY Advisors TX, LLC has over 1,000 professionals in over 15 offices in the United States. The company has been in business since 1971.

U.S. LOCATIONS

GEORGIA

ATLANTA

Five Concourse Parkway
Suite 2450
Atlanta, GA 30328
Telephone: 678-602-4400
Fax: 678-602-4300

ILLINOIS

CHICAGO

30 S. Wacker Dr.
Suite 2850
Chicago, IL 60606
Telephone: 312-578-9600
Fax: 312-346-6500

MARYLAND

COLUMBIA

6851 Oak Hall Lane
Suite 300
Columbia, MD 21045
Telephone: 410-720-5220
Fax: 410-381-2524

MICHIGAN

Metropolitan Detroit

SOUTHFIELD

26200 American Drive
Suite 500
Southfield, MI 48034
Telephone: 248-355-1040
Fax: 248-355-1084

STERLING HEIGHTS

12900 Hall Road
Suite 500
Sterling Heights, MI 48313
Telephone: 586-254-1040
Fax: 586-254-1805

MISSOURI

ST. LOUIS

15 Sunnen Drive
Suite 100
St. Louis, MO 63143
Telephone: 314-615-1200
Fax: 314-647-8304

NEW JERSEY

OAKLAND

169 Ramapo Valley Road
Oakland, NJ 07436
Telephone: 201-337-0009
Fax: 201-337-1391

NEW YORK

ALBANY

66 State Street
Albany, NY 12207
Telephone: 518-449-3166
Fax: 518-449-5832

NEW YORK

UHY Advisors NY, Inc.
19 West 44th Street
New York, NY 10036
Telephone: 212-381-4700
Fax: 212-354-6445

-and-

UHY Advisors FLVS, Inc.
555 Fifth Avenue
3rd Floor
New York, NY 10017
Telephone: 646-746-1120
Fax: 646-746-1125

WHITE PLAINS

800 Westchester Avenue
Suite North 641
Rye Brook, NY 10573
Telephone: 914-697-4954
Fax: 914-697-7583

TEXAS

DALLAS

1717 Main
Suite 2400
Dallas, TX 75201
Telephone: 214-243-2900
Fax: 214-243-2929

HOUSTON

UHY Advisors TX, LLC
2929 Allen Parkway, 20th Floor
Houston, TX 77019
Telephone: 713-960-1706
Fax: 713-960-9549
Toll-free: 800-949-1706

WASHINGTON D.C.

WASHINGTON

1325 G Street NW
Suite 500
Washington, D.C. 20005
Telephone: 202-609-6100

VENDOR COMPANY MINIMUM REQUIREMENTS

The UHY information security attack and penetration testing team consists of five personnel, locally. The testing team is skilled in information security offensive (attack) and defensive security skills, which serve to provide clients with a complete view of their information security posture. The UHY team is very experienced having performed industry-wide security work and numerous PCI assessments. The UHY team is also experienced in evaluating vulnerability assessments and penetration tests with respect to PCI. UHY has performed this type of work for multiple government agencies in New Hampshire since 2010. Three team members are active Qualified Security Assessors (QSA).

The main UHY office performing the assessment is located at 2929 Allen Parkway, 20th Floor; Houston, Texas 77019. The Houston main office number is 713-960-1706. Norman Comstock, Richard Peters and Kenneth Sayles are based out of the Houston office.

Our supporting office for this project is located at 1717 Main Street, Suite 2400; Dallas, Texas 75201. The Dallas main office number is 214-243-2900. Ty Coffee and Colin Travis are based out of the Dallas office.

The UHY security testing team will coordinate with the designated Company personnel to define the 'Rules of Engagement' for the overall project, as well as establish communication channels for ongoing testing. It is the intention of the UHY security testing team to communicate daily via email on the current status as well as the planned scanning or activity for that day/evening. Additionally, an onsite meeting or conference call will be set up weekly to quickly discuss plans, actions and milestones.

Please see the team resumes that follow on the next few pages.

Norman Comstock, MBA, MIB, CIA, CGEIT, CISA, CISSP, CCSA, CSOXP, QSA, CCSFP, managing director, has over 20 years of IT audit and consulting experience.

Throughout his career, Norman has led and supported the execution of all activities necessary to complete comprehensive auditing processes, application reviews, IT security reviews, hands-on quality assurance reviews, and numerous business process improvement projects. His broad expertise includes IT governance and risk management, with an emphasis on risk assessment and control design.

Prior to joining UHY, Norman was President of GCRM Solutions, LLC a firm that specialized in IT governance, compliance and risk management solutions. His clients have included Academy Sports + Outdoors, GlobalSantaFe, Houston Casualty Company, Spinnaker Exploration, Houston Exploration, Mountaineer Gas, Willbros USA, Marathon Oil Company, Centerpoint Energy, Meridian Resources, Teppco, Duke Energy Field Services, Maxxam, Ultra Petroleum, Core Laboratories and American Physicians.

Norman is nationally recognized as a business intelligence (BI) professional, and is also proficient in data warehousing, OLAP and reporting solutions. He is an authority on advanced analytics, data strategy, program planning, information architecture and project management.

Norman graduated from the University of Houston with a B.B.A in Accounting. He has a Masters of International Business and an M.B.A. in Marketing, both from the Cameron School of Business, University of St. Thomas.

Professional Affiliations, Licenses or Certifications

- President, Information Systems Audit and Control Association (ISACA)
- Vice President of Technology, Internal Auditors Association (IIA)
- Chair-Elect, Audit Committee, Information Systems and Security Association
- Leadership Council, Open Compliance and Ethics Group
- Adjunct Professor, Business Ethics, Advanced Internal Audit
- Microsoft's Business Intelligence Advisory Council in 2001 and 2002
- Alumnus instructor of The Data Warehousing Institute
- Certified Information Systems Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)
- Qualified Security Assessor (QSA)
- Certified Internal Auditor (CIA)
- Certified in the Governance of Enterprise IT (CGEIT)
- Checkpoint Certified Security Administrator (CCSA)
- Certified Sabanes-Oxley Professional (CSOXP)
- Certified Common Security Framework Practitioner (CCSFP)

Project Responsibilities

- Executive Leadership and Debriefing

Richard Peters CISSP, CISA, CCSFP, QSA senior manager, specializes in Information Security and Payment Card Industry (PCI) Compliance. He brings over 13 years of experience managing, performing and delivering cost effective Internal Controls and Information Security solutions.

His experience includes technology risk management, IT auditing, IT Security Assessments, Internal Auditing, Vulnerability Assessments, Attack and Penetration Testing services and security analysis in domestic and global entities in the energy, technology, financial and manufacturing industries.

Richard is skilled in designing, assessing, and testing against multiple security standards and frameworks including ISO 17799, ISO 27001, PCI DSS, COBIT and NIST. He is a professor at the University of Houston instructing tomorrow's leaders in the areas of information security. He is a frequent speaker and leader at major security conventions around the country.

Richard graduated from the University of Texas at Austin with a B.B.A. in Finance.

Professional Affiliations, Licenses or Certifications

- Information Systems Audit and Control Association (ISACA)
- Information Systems Security Association (ISSA)
- Institute of Internal Auditors (IIA)
- National Information Security Group (NAISG)
- Open Web Application Security Project (OWASP)
- Certified Information Systems Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)
- Qualified Security Assessor (QSA)
- Certified Common Security Framework Practitioner (CCSFP)

Qualifications and Relevant Experience (Similar Projects)

- Performed attack and penetration testing and vulnerability assessments on some of the largest organizations including attacks against network, application, and wireless technologies.
- Completed multiple security audits and ISO 17799 compliance tests for multiple organizations. Checked for compliance to established security policies and advised on any gaps found. Created and delivered substantial reports based upon data collected.
- Audited security policies for multi-billion dollar global enterprise - developed security control objectives, testing procedures and remediation efforts.
- Supervised as well as lead several security assessments on supervisory control and data acquisition systems (SCADA) within petrochemical industry, as well as international port and canal operations.
- Past experience has included auditing and assessing security policies for multi-billion dollar global enterprises, assessing PCI Compliance for global oil & gas corporations, performing attack and penetration testing and vulnerability assessments on some of the largest organizations, creating security plans and performing risk analysis for NASA contractors, and supervised as well as leading several security assessments on supervisory control and data acquisition systems (SCADA) within the petrochemical industry, as well as international port and canal operations.

Project Responsibilities

- Project Manager/Owner; Security Assessor

Ty Coffee, CISA, CCSFP, QSA senior IT security and audit manager, has nine years of experience managing, performing and delivering cost effective Internal Controls and Information Technology (IT) solutions.

His experience includes technology risk management, Penetration Testing, Physical Security, IT auditing, IT Security Assessments, Internal Auditing, business analysis, accounting and systems analysis in domestic and global entities in the energy, technology, financial, federal and manufacturing industries.

Ty graduated from Texas A & M University with a B.A. in Accounting and an M.S. in Management Information.

Professional Affiliations, Licenses or Certifications

- Information Systems Audit and Control Association (ISACA) - National Capital Area Chapter
- Information Systems Audit and Control Association (ISACA) - North Texas Chapter
- Greater Washington Society of Certified Public Accountants (GWSCPA)
- Certified Information Systems Auditor (CISA)
- Qualified Security Assessor (QSA)
- Certified Common Security Framework Practitioner (CCSFP)

Qualifications and Relevant Experience (Similar Projects)

- He has over nine years of experience in managing, supervising and performing Information Technology internal control reviews, system audits and consulting for large/complex federal governmental entities and private and public companies.
- Performed quantitative and qualitative IT risk assessments for large/complex Federal agencies, as well as private and public companies. Assessments identified numerous risks due to inappropriate use of assets as well as security vulnerabilities. Risk Assessments were used to develop audit plans and prioritize remediation activities to address critical risks not controlled or adequately mitigated due to weak control design.
- Defined and managed IT risk assessments for clients to ensure compliance to regulations (e.g., HIPAA, FISMA, PCI DSS, Sarbanes-Oxley (SOX)).
- Managed and conducted security assessments (Vulnerability Scanning and Penetration Testing included) for both governmental and commercial entities using various methodologies including DoD 8500 series and NIST criteria in various countries.
- Performed numerous analysis and assessments of key physical and logical controls over information system integrity and reliability for both governmental and commercial entities.

Project Responsibilities

- Security Assessor

Kenneth Sayles III, CISSP, C|EH, CEPT, CISA, CISM, manager, has over seven years of experience in information security.

In the course of his career, he has supported various aspects of information security, including tool development, modeling and simulation, code analysis, compliance testing, vulnerability assessments and penetration testing.

In addition to having technical competency, Kenneth is a strong communicator with experience briefing to various audiences and management levels. Outside of information security, Kenneth is a freelance philosophy writer with specific attention towards technological concerns.

Kenneth graduated from the University of Texas at El Paso with a Master of Science in Computer Science and Master of Arts in Philosophy.

Professional Affiliations, Licenses or Certifications

- Certified Information Systems Security Professional (CISSP)
- Certified Ethical Hacker (C|EH)
- Certified Expert Penetration Tester (CEPT)
- Certified Information Systems Auditor (CISA)
- Certified Information Security Manager (CISM)

Qualifications and Relevant Experience (Similar Projects)

- Coordinated vulnerability assessments for networks as large as 2,000 systems.
- Conducted vulnerability scans for multiple proprietary networks, including networks interconnected with multiple companies and networks with mainly mobile assets.
- Coordinated penetration tests for both small networks (<10 systems) and large networks (>100 systems) in various time frames.
- Experience in both web application and network infrastructure penetration testing.
- Experience with a wide variety of systems, included embedded systems, standard desktops, and network devices.

Project Responsibilities

- Security Assessor

Colin Travis has four years of experience maintaining Level 1 PCI compliance in a large retail organization, as well as four years of experience with the composition and implementation of technical and procedural documentation related to PCI and organizational security standards. Colin led the development of a company-wide security plan for the System Development Life Cycle; monitored and maintained access to HIPAA and PCI controlled environments; designed and implemented a media destruction initiative in accordance with PCI regulations; monitored and remediated the configuration of Windows, Linux, Unix, and IBM i-Series systems for financial and PCI audits; participated in architecting and implementing an in-house based eCommerce initiative while maintaining PCI compliance and audited and participated in remediation of wireless systems in accordance with NIST Standards while adhering to PCI regulations.

Colin is adept at project management related to Information Security with a strong ability to meet deadlines while under pressure, and he is skilled in providing organizations with guidance on confidentiality, integrity and availability of data issues.

Professional Affiliations, Licenses or Certifications

- National Information Security Group – (NAISG)

Qualifications and Relevant Experience (Similar Projects)

- Colin has worked on numerous engagements in relation to security analysis, security standards and security plans for organizations. He is currently working on an ISO 27002 implementation initiative at a multi-national oil field service company.

Project Responsibilities

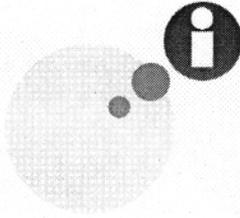
- Security Assessor

ATTACHMENT 4 – CONTRACTOR CERTIFICATIONS

ATTACHMENT 5 – PROPOSED SUBCONTRACTORS

PRE-ENGAGEMENT CHECKLIST

UHY will not be using subcontractors on this engagement.



THE NEXT LEVEL OF SERVICE

In July, 2000, six leading regional tax and business advisory firms, with tenures dating back to the early 1970s, merged to form a national professional services entity known as UHY Advisors, Inc. They came together in the pursuit of a shared vision: to deliver the service of a local/regional firm and the services of a national firm to the dynamic middle market.

UHY Advisors
2929 Allen Parkway, 20th Floor
Houston, TX 77019-7100

Phone: 713 960 1706
Fax: 713 572 4681
www.uhy-us.com

UHY Advisors, Inc. provides tax and business consulting services through wholly owned subsidiary entities that operate under the name of "UHY Advisors." UHY Advisors, Inc. and its subsidiary entities are not licensed CPA firms.

UHY LLP is a licensed independent CPA firm that performs attest services in an alternative practice structure with UHY Advisors, Inc. and its subsidiary entities. UHY Advisors, Inc. and UHY LLP are U.S. members of Urbach Hacker Young International Limited, a UK company, and form part of the international UHY network of legally independent accounting and consulting firms.

"UHY" is the brand name for the UHY international network. Any services described herein are provided by UHY Advisors and/or UHY LLP (as the case may be) and not by UHY or any other member firm of UHY. Neither UHY nor any member of UHY has any liability for services provided by other members.