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

Date: August 22, 2019

NOTICE OF CONTRACT – REVISED
(UPDATED PRE-ENGAGEMENT CHECKLIST)

COMMODITY: **Qualified Security Assessor Services (All Security Assessments)**
Security Testing and Remediation Services (Includes Penetration Testing)

CONTRACT NO.: **8002130**

NIGP: 920-0000

VENDOR: Control Case LLC
10615 Judicial Drive
Fairfax, VA 22030

VENDOR # : 287049

CONTACT PERSON(s): Afy Merchant
Tel. No.: (703) 488-0480
Fax No.: # (703) 991-5341
E-Mail: amerchant@controlcase.com

EFFECTIVE FROM: April 27, 2018 **through** February 28, 2021

SCOPE OF WORK:

Qualified Security Assessor Services (All security Assessments)

Perform both PCI DSS Audits and Non-PCI Audits for all State Agencies. State agencies have a responsibility to safeguard data deemed to contain PII, PHI, FTI as well as any other data requiring protection mandated by other state and federal statutes and regulations for other types of confidential data. The duties to protect this sensitive data apply equally to both PCI covered data (credit card holder data) and non-PCI covered data (bank accounts, ACH, health information and all other personally identifiable information (PII)). At this time, the Payment Card Industry Council mandates a formal PCI Compliance process to validate DSS for all merchants. The services available under this Statewide Contract can be used for audits and assessments for any of these data types.

Security Testing and Remediation Services (Includes Penetration Testing)

Agencies shall submit a pre-engagement checklist to all qualified Contractors. The checklist shall clearly identify whether the services are for PCI or non-PCI security engagement. Agencies hall award the work to the lowest cost Contractor in conformance with Pricing Quotations.

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

Security compliance, testing and remediation results shall be provided in both an executive and summary report that provides a written assessment of the vulnerabilities found as well detailed technical information related for each vulnerability identified during the engagement. The technical report shall include the following for each vulnerability:

- A vulnerability rating in accordance with a mutually acceptable risk rate methodology to indicate the severity of the problem;
- Details about the specific methods about how and the extent that the vulnerability can be exploited; and
- Information about potential remediation steps.

All results that include identified vulnerabilities shall include follow-up testing after the agency has completed remediation of any identified vulnerabilities. Detailed technical information shall be available to the State in a spreadsheet or CSV format.

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

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

INVOICING, PAYMENTS & DELIVERY:

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

The Contractor shall be paid in five Installments based on Deliverables for Section 1:

Deliverable	Description	Expected Due Date	% of Fee
Work Plan & Schedule	For each year during the term of the Contract, the Contractor shall submit a detailed work plan according to the Specifications in Exhibit A	15 days after the effective date of the contract and mutually agreeable in subsequent year during the term of the Contract	10%
Preliminary Report on Compliance	For each year during the term of the Contract the Contractor shall submit a preliminary Report on Compliance according to the Specifications in Exhibit A	After initial assessment, Contractor will draft and present a preliminary Report on Compliance for the State. Along with this, the State will complete all necessary remediation steps to ensure Compliance. This will include remediation support services from the Contractor. This must be done 30 days prior to the Final Report on Compliance.	40%
Final Report on Compliance	On an Annual basis	After the Preliminary Report on Compliance and remediation steps are completed, the Contractor will re-evaluate to ensure that the State is Compliant. The Contract will prepare and deliver the Final Report on Compliance and Attestation of Compliance to the State.	35%
Post Assessment Executive Report and Oral Presentation	For each year during the term of the Contract, the Contractor shall submit a Post Assessment Executive Report and will present this report according to specifications in Exhibit A.	This report should include but is not limited to: High level overall State Compliance, summary of strengths & weaknesses, summary of applied compensating controls that were put in place to address areas of non-compliance and recommend long term changes and summary of short and long term changes the State should consider to reduce overall exposure and future costs.	10%
Contractor Authored Documents	For each year during the term of the Contract, the Contractor shall provide copies of the Contractor Authored Documents according to the specifications in Exhibit A.	A copy of all documentation created by the Contractor in the course of its services under this contract shall be provided to the State in hard and/or electronic copy.	5%

PRICING QUOTATIONS:

State agencies **shall request quotations from all contractors awarded in the section of services** being requested by providing a Statement of Work (SOW) describing the services required as well as the Pre-Engagement Checklist. If appropriate, the contractors may be allowed to view code or facilities after the execution of confidentiality agreements. Contractor must return pricing quotations within five (5) business days. If additional information has been circulated to all contractors, Contractor shall have one (1) extra business day to revise the quotation. The quoted hourly rates shall not exceed the rates listed herein. The contractor that provides the lowest bid will be the one that will be selected**. The Contractor that provides the lowest bid will be the one that will be selected. Agencies are required to submit a copy of all Contractor quotes to the Department of Administrative Services – Merchant Card Services as proof of bidding out the service to all applicable contractors. For the Annual Statewide PCI DSS Audit, DAS Merchant Card Services will submit the SOW to all applicable contractors and select the lowest bid.**

PRE-ENGAGEMENT CHECKLIST:

Agencies shall submit a pre-engagement checklist to all qualified contractors. The checklist shall clearly identify whether the services are for PCI or non-PCI security engagement. Along with the pre-engagement checklist, agencies will submit State of NH PCI DSS CDE Inventory which specifies all hardware and software in scope for the services that are being requested. Agencies shall award the work to the lowest cost contractor in conformance with Pricing Quotations. Pricing Quotation shall be listed as a fixed price based unless otherwise agreed to by the State.

Procedure: Request for Quotations Security Testing and Remediation Services	
	New Hampshire Department of Administrative Services Merchant Card Program
	Effective Date: August 21, 2019 Last Revision: August 20, 2019 Version: 2.0

Overview

Agencies shall submit a pre-engagement checklist to all qualified contractors. The checklist shall clearly identify whether the services are for a PCI or non-PCI Security engagement. Along with the pre-engagement checklist, agencies will submit the State of NH PCI DSS CDE Inventory, if applicable, which specifies all hardware and software in scope for the services that are being requested. Agencies shall submit all quotations to the Merchant Card Administrator for review and approval. Award will be made to the lowest cost Contractor in conformance with pricing quotations. Pricing quotations shall be listed as a fixed price based unless otherwise agreed to by the State.

Agencies will also provide the Contractor with the appropriate Quotation Form for the Contractor. There is a Quotation Form for each Contractor with their contracted rates. The Contractors should be complete the hours of work need to perform the security testing and remediation services. The Contractor must submit this Quotation Form along with any other documentation.

Rules of Engagement

Prior to the commencement of any testing, agencies are to document and agree upon the conditions in which testing is to be performed and the degree of exploitation, if any, that is permitted. This will authorize the Contractor to test the environment and ensure that agency knows what to expect from the testing.

For penetration testing, agencies will need to outline the following tasks and information:

- What timeframe does testing to be performed;
- Are there any legacy systems that have known issue with automated scanning and if so, how should testing be performed against these systems;
- How is the scope and issues encountered during the engagement communicated;
- If updates are required during the testing;
- If there are security controls that would detect or prevent testing. Determine whether these should be disabled or configured to not interfere during testing;
- If passwords or sensitive data is compromised during testing, how should this be disclosed;
- If IP addresses from which testing originates needs to be provided;
- If equipment owned by the tester is allowed to be connected to the network and if so, what steps must be taken to ensure that this equipment does not pose a threat to the environment;
- If sensitive data shown to be accessible during the test be retained by the tester during and after the test; and
- What steps are to be taken if an active or previous compromise is detected.

Testing results

The results of the security compliance, testing, and remediation shall be provided in both an executive summary report that provides a written assessment of the vulnerabilities found as well as detailed technical information related for each vulnerability identified during the engagement.

The technical report shall include the following:

- A vulnerability rating in accordance with a mutually acceptable risk rating methodology to indicate the severity of the problem;
- Details about the specific methods about how and the extent that the vulnerability can be exploited; and
- Information about potential remediation steps.

All results that includes identified vulnerabilities shall include follow-up testing after the agency has completed remediation of any identified vulnerabilities. Detailed technical information shall be available to the State in a spreadsheet or CSV format.

REQUEST FOR QUOTATION
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-DSS current version) or Federal, State or industry standards.

All testing will shall be done in compliance with PCI-DSS Requirement 11.3 of the current version, for network penetration and application testing.

AGENCY INFORMATION

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

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

☐ PCI – Penetration Testing or Remediation efforts.
*If agencies need external penetration testing, agencies must include the IP address and the URL.

☐ Non-PCI -- Security and compliance assessments, code reviews, penetration testing and reviews for general information management and security compliance.

1. **Identify details of the engagement and project schedule.**
   (Provide narrative that outlines purpose of the engagement. If non-PCI, identify what security standards are in scope)

2. **Details about the environment in scope for the engagement.**
   (Provide business processes, policies and procedures, network diagrams, data flow diagrams, IP address and application credentials and any other information about the engagement needed by the Contractor to assess the level of effort)

3. **What are the rules of engagement?**
   (This includes project timeline, success criteria, toolset identification, testing behaviors)

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

AWARD

Award will be made to the bidder offering the lowest total cost.

By submitting a quotation, the Contractor agrees that the State of New Hampshire terms and conditions, contained in Form P-37 of the master Contracts shall form the basis of any Agreement resulting from this RFQ.

The Contract Documents consist of the documents listed below. In the event of conflict or ambiguity among any of the text of the Contract Documents, the following Order of Precedence shall govern:

1. Master Agreement for Security Compliance Testing, and Remediation Services Contracts 8002297, 8002306, and 8002314, and the State of New Hampshire Terms and Conditions, Form P-37 Contract Agreement.
2. Request for Quotation.
3. RFB 2075-18 Security Compliance Testing, and Remediation Services Dated March 8, 2018, with any addenda incorporated; then
4. The Vendor quote in response to RFB 2075-18.

BIDDER INFORMATION AND SIGNATURE:

Name of Company (please print)	**Street/ PO Box Address**	**Telephone No**
Authorized Signature.	**City/Town/State/Zip**	**E-mail Address**

STATE OF NEW HAMPSHIRE
QUOTATION FORM

CONTROL CASE, LLC

Date	
Quotation Number	

Vendor Information

Vendor Name	
Vendor Contact	
Contact Phone Number	
Contact E-mail Address	

Agency Information

Contact Name	
Agency	
Contact Phone Number	
Contact E-mail Address	

Pricing Table(s)

The tables below are embedded excel files with the contracted rate(s) for the Contractor. The Contractor is to complete the 'Description of Service' and 'Hour(s)' fields. The contracted rate, price, and total price are protected fields and will calculate the total price based on the figure entered in the 'Hour(s)' field.

The Contractor does not need to complete both the onsite and offsite table, just the table in which it prefers to provide services.

Onsite Service

DESCRIPTION OF SERVICE	CONTRACTED RATE	HOUR(S)	PRICE
	$185		$0
		TOTAL PRICE	$0

Offsite Service

DESCRIPTION OF SERVICE	CONTRACTED RATE	HOUR(S)	PRICE
	$150		$0
		TOTAL PRICE	$0

This quotation conforms with all the terms and conditions of the State of New Hampshire Contract 8002130.

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

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

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

Per Bid # 2075-18