

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: June 19, 2018

NOTICE OF CONTRACT – REVISED
(NEW CONTACT)

COMMODITY: SECURITY COMPLIANCE, TESTING AND REMEDIATION SERVICES

CONTRACT NO.: 8002295

NIGP: 920-0000

VENDOR: Citrin Cooperman & Company, LLP
10 Weybosset Street, Suite 700
Providence, RI 02902
VENDOR # : 285665

CONTACT PERSON(S): Suzanne Miller, Ph.D.
Tel. No.: 401-421-4800 ext. 273
Cell No.: 321-282-8516
Fax No.: # 401-421-0643
E-Mail: smiller@citrincooperman.com

EFFECTIVE FROM: April 13, 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.

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.

Pre-Engagement Checklist (EXAMPLE)

These questions are intended to help the Contractor understand your agency's needs for an assessment to validate your compliance with the Payment Card Industry Data Security Standard (PCI DSS current version) or Federal, State or industry standards

Agency Information

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

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

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

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

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

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

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