

STATE OF NEW HAMPSHIRE
BUREAU OF PURCHASE AND PROPERTY

STATE HOUSE ANNEX - ROOM 102
25 CAPITOL ST
CONCORD NH 03301-6398

DATE: 4/9/2018

CONTRACT #: 8002297

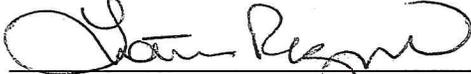
NIGP CODE: 920-0000

CONTRACT FOR: Security Compliance, Testing & Remediation Services (Merchant Cards)

CONTRACTOR: Enterprise Risk Management Inc

VENDOR CODE #: 252311

SUBMITTED FOR ACCEPTANCE BY:



LORETTA RAZIN, PURCHASING MANAGER
BUREAU OF PURCHASE AND PROPERTY

DATE 4/10/18

APPROVED FOR ACCEPTANCE BY:



GARY LUNETTA, DIRECTOR
DIVISION OF PROCUREMENT & SUPPORT SERVICES

DATE 4/10/18

ACCEPTED FOR THE STATE OF NEW HAMPSHIRE UNDER THE AUTHORITY GRANTED TO ME BY NEW HAMPSHIRE REVISED STATUTES, ANNOTATED 21-I:14, XII.



CHARLES M. ARLINGHAUS, COMMISSIONER
DEPARTMENT OF ADMINISTRATIVE SERVICES

DATE 4/10/18

This is one of 6 contracts to be awarded

Subject: SECURITY COMPLIANCE, TESTING AND REMEDIATION SERVICES

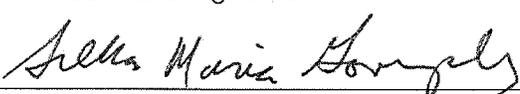
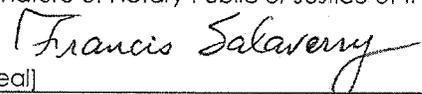
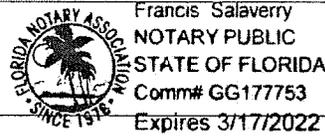
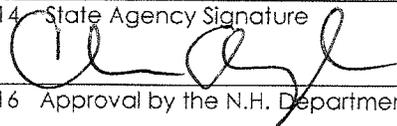
Notice: This agreement and all of its attachments shall become public upon submission to Governor and Executive Council for approval. Any information that is private, confidential or proprietary must be clearly identified to the agency and agreed to in writing prior to signing the contract.

AGREEMENT

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

GENERAL PROVISIONS

1. IDENTIFICATION.

1.1 State Agency Name Department of Administrative Services		1.2 State Agency Address 25 Capitol Street, Concord, NH 03301	
1.3 Contractor Name Enterprise Risk Management Inc VC 252311		1.4 Contractor Address 800 South Douglas Road, #940N Coral Gables FL 33134	
1.5 Contractor Phone # 305-447-6750	1.6 Account Number	1.7 Completion Date 02/28/2021	1.8 Price Limitation \$1,230,000.00
1.9 Contracting Officer for State Agency Robin Parkhurst, Administrator		1.10 State Agency Telephone Number 603-271-7410	
1.11 Contractor Signature 		1.12 Name and Title of Contractor Signatory SILKA MARIA GONZALEZ, PRESIDENT	
1.13 Acknowledgement: State of <u>Florida</u> , County of <u>Miami Dade</u> On <u>04/06/2018</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  [Seal]			
1.13.2 Name and Title of Notary or Justice of the Peace Francis Salaverry, Office Manager			
1.14 State Agency Signature 		1.15 Name and Title of State Agency Signatory Charles M. Arlinghaus, Commissioner Date: <u>4/11/18</u>	
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) (if applicable) By: _____ On: _____			
1.18 Approval by the Governor and Executive Council (if applicable) 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, if applicable, this Agreement, and all obligations of the parties hereunder, shall become effective on the date the Governor and Executive Council approve this Agreement as indicated in block 1.18, unless no such approval is required, in which case the Agreement shall become effective on the date the Agreement is signed by the State Agency as shown in block 1.14 ("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. This may include the requirement to utilize auxiliary aids and services to ensure that persons with communication disabilities, including vision, hearing and speech, can communicate with, receive information from, and convey information to the Contractor. 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 notice and consent of the State. None of the Services shall be subcontracted by the Contractor without the prior written notice and 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 \$1,000,000 per occurrence and \$2,000,000 aggregate; and

14.1.2 special cause of loss coverage form 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 thirty (30) 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 provide the Contracting Officer identified in block 1.9, or his or her successor, no less than thirty (30) 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 unless no such approval is required under the circumstances pursuant to State law, rule or policy.

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

Enterprise Risk Management Inc (hereinafter referred to as the "Contractor") hereby agrees to provide the State of New Hampshire (hereinafter referred to as the "State"), Department of Administrative Services, with Security Compliance, Testing And Remediation Services in accordance with the bid/proposal submission in response to State Request for Bid #2075-18 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 Terms
- d. EXHIBIT C Special Provisions
- e. EXHIBIT D RFB 2075-18

3. TERM OF CONTRACT

This contract shall commence upon the approval of the Commissioner of Administrative Services and terminate on February 28, 2021, a period of approximately two (2) years and ten (10) 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, with the approval of the Commissioner of the Department of Administrative Services, but shall not exceed five (5) years in total.

4. SCOPE OF WORK

Provide services to meet ongoing Payment Card Industry Data Security Standard (PCI DSS) security and monitoring requirements as established by the PCI Security Standards Council. In addition to PCI compliance, the services can also be used for other information security audits, compliance reviews of standards, and systems and controls to protect personally identifiable information and other sensitive data.

These services include, but are not limited to: network and application layer penetration testing, compliance and quality assurance reviews and testing for information and data management systems (paper or electronic), security compliance, PCI compliance, physical and electronic security of records, PII (personally identifiable information), PHI (personal health information), FTI (federal tax information) and confidential information, E-discovery, data breach forensics investigations and remediation, or other audits and compliance reviews related to data management systems and security.

Section I: Qualified Security Assessor Services (All security Assessments)

Section II: Forensic Investigation Services (All Data Breaches)

Section III: Security Testing and Remediation Services (All Environments)

Section IV: External Vulnerability Scanning and Self-Assessment Questionnaire

S.M. D.
04/06/2018

SUBCONTRACTING:

In addition to the provisions of Section 12 of the P-37 related to assignment and subcontracting of contractual rights and obligations, the Contractor shall be responsible to the State for the acts and omissions of all subcontractors or agents and of persons directly or indirectly employed by such subcontractors, and for the acts and omissions of persons employed directly by the Contractor. No contractual relationships exist between any subcontractor and the State.

STAFFING REQUIREMENTS:

Employment of Undocumented Workers Prohibited – Contractor shall not employ any employee without obtaining documentation showing the employee's eligibility to work in the United States. The employer shall maintain such documentation for the period required by federal law. Acceptable documentation of eligibility to work in the United States shall include documents required by federal law or supporting documentation that satisfies the requirement of federal law.

Bankruptcy or Receivership

Voluntary or involuntary bankruptcy or receivership by the Contractor may be cause for termination at the election of the State.

Material Breach

The non-breaching party may terminate the contract in whole or in part after thirty (30) days written notice, as described in the Form P-37 General Terms and Conditions Section 8, in the event of the breaching party's failure to perform a material obligation of the contract.

LIAISON AND SERVICE OF NOTICES:

All project management and coordination on behalf of the State shall be through a single point of contact designated as the State's liaison. The Contractor shall designate a liaison that shall provide the single point of contact for management and coordination of Contractor's work. All work performed pursuant to this Contract shall be coordinated between the State's liaison and the Contractor's liaison.

DISPUTE RESOLUTION:

Prior to the filing of any formal proceedings with respect to a dispute (other than an action seeking injunctive relief with respect to intellectual property rights or Confidential Information), the party believing itself aggrieved (the "Invoking Party") shall call for the progressive management involvement in the dispute negotiations by written notice to the other party. Such notice shall be without prejudice to the invoking party's right to any other remedy permitted by this Contract.

5. TERMINATION

The State of New Hampshire has the right to terminate the contract at any time by giving the Contractor thirty (30) days advance written notice.

6. OBLIGATIONS AND LIABILITY OF THE CONTRACTOR

The Contractor shall provide all services strictly pursuant to, and in conformity with, the specifications described in State RFB #2075-18, as described herein, and under the terms of this Contract.

The Contractor shall agree to hold the State of NH harmless from liability arising out of injuries or damage caused while performing this work. The Contractor shall agree that any damage to

Contractor Initials D.M.H.
Date 09/06/2018

building(s), materials, equipment or other property during the performance of the service shall be repaired at its own expense, to the State's satisfaction.

7. DEBARMENT, SUSPENSION, INELIGIBILITY AND VOLUNTARY EXCLUSION LOWER TIER COVERED TRANSACTIONS

The Contractor certifies, by signature of this contract, that neither it nor its principals is presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction by any Federal Department or Agency.

8. INSURANCE

Certificate of insurance amounts must be met and maintained throughout the term of the contract and any extensions as per the P-37, section 14 and cannot be cancelled or modified until the State receives a 10 day prior written notice.

In addition, the following coverage shall be required by the Contractor along with proof of coverage:

- Minimum coverage level of \$5,000,000 for Professional Errors and Omissions
- Cyber Theft Liability in the amount of \$2,000,000 per occurrence
- Electronic Data Loss (EDL) in the amount of \$2,000,000 per occurrence

9. SUBCONTRACTING:

In addition to the provisions of Section 12 of the P-37 related to assignment and subcontracting of contractual rights and obligations, the Contractor shall be responsible to the State for the acts and omissions of all subcontractors or agents and of persons directly or indirectly employed by such subcontractors, and for the acts and omissions of persons employed directly by the Contractor. No contractual relationships exist between any subcontractor and the State.

SCOPE OF SERVICES:

SECTION I
QUALIFIED SECURITY ASSESSOR (QSA)

GENERAL / OBJECTIVES

In addition, 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.

Good Standing with the PCI Security Standards Council

The Contractor must be in good standing with the PCI Security Standards Council ("PCI SSC") as a QSA for the project duration; the Contract may, at the State's discretion be terminated immediately if the Vendor is dropped from the PCI SSC listing of QSA companies or is placed on remediation status.

The Vendors' servers must be located within the "USA" and their workers located in the "USA"

Contractor Initials A.M.H.
Date 04/06/2018

The Contractor shall validate what system components are in scope for the audit or assessment by gaining a complete understanding of the State's environment including, but not limited to, all system components, network components, servers (web, application, database, authentication, mail, proxy, network time protocol, domain name server), firewalls, switches, routers, wireless access points, network appliances, security appliances, applications (purchased, custom, internal and external/internet), applicable manual and automated business processes, and in-house and contracted personnel duties.

The Contractor shall determine what security requirements are applicable to the State.

The Contractor shall verify all technical information provided by the State.

The Contractor shall identify and analyze the State's current information security protocols including a review of the policies, processes and procedures (to include documentation, system and network device configuration details, and network and application architecture guidelines.)

The Contractor shall, in accordance with the appropriate Security Assessment Procedures; perform any necessary examinations and sampling of system components and compensating controls deemed in scope and subject to compliance requirements.

The Contractor shall provide any and all necessary guidance to the State as required in order to achieve compliance with the appropriate security standards while using independent judgment to confirm the standards have been complied with.

The Contractor shall determine all areas where the State may be non-compliant with standards, and the extent of non-compliance (critical, important, and minor).

The Contractor shall identify issues of concern, communicate potential deficiencies or lack of controls that may result in failure to comply with the standards or which may present a general security risk. Each area of concern must be documented with its level of non-compliance.

The Contractor shall have an internal QA/QC mechanism that will ensure the quality of the QSA's work product prepared in support of the PCI Requirements and Security Assessment Procedures.

The Contractor shall provide any and all necessary on-going consultant services to support annual compliance requirements.

The Contractor shall assist the State in strengthening its data environment by consulting on remediation and/or compensating controls to address all discovered areas of non-compliance and control weaknesses during the assessment.

The Contractor shall prepare any and all necessary documentation required to demonstrate compliance that the State will in turn submit to the acquiring bank and payment card brands or regulatory authority on an annual basis.

At any time during this contract, The State may request and the Contractor shall provide a Security Assessment for: (i) a new State agency; (ii) an existing State agency who proposes to modify their current system/application; and (iii) network or other infrastructure changes that impact the data environment. The purpose of the Security Assessment shall be to validate the merchant/State is fully compliant with the security standards prior to beginning /or modifying their existing system/application. Upon request to said services from the State, the Contractor shall prepare and

Contractor Initials J. N. J.
Date 04/06/2018

submit a detailed cost proposal (utilizing the per hour rates as detailed in section 7 Cost Proposal) to the State within 7 business days.

EXPECTED PROJECT DELIVERABLES

WORK PLAN & SCHEDULE

As part of their Bid the Contractor shall provide a preliminary project schedule / Work Plan demonstrating how the elements of the Scope of Work will be completed to meet required deadlines.

Within fifteen (15) calendar days of the award of the contract, the Contractor shall submit a final detailed Work Plan for accomplishing the tasks described in the Scope of Work for the first year of the contract. The Contractor shall submit Work Plans for the subsequent years of the contract on or before the anniversary date of the contract for each subsequent year. The Work Plan shall include all of the Contractor's major work activities and shall address all major tasks and subtasks. Sufficiently detailed milestones dates and responsibilities for meeting the major tasks and subtasks shall be identified. The Work Plan shall also indicate the manpower efforts and commitments of time needed from the State's staff in order to facilitate the Contractor's work.

In performing the task described above, the Contractor is expected to define the level of specificity needed to accomplish the work. Implementation of the Work Plan by the Contractor shall commence upon authorization by the State.

REPORT ON COMPLIANCE

The Report on Compliance must be a formal report that is prepared in accordance with the PCI Security Standards Council's security audit procedures, containing:

- Contact Information and Report Date
- Executive Summary
- Description of Scope of Work and Approach Taken
- Findings and Observations

The Report on Compliance shall be written to encompass all State Agencies accepting payment cards. A single Statewide Report on Compliance shall be presented to the State's acquiring banks.

The Contractor shall provide and an Executive Officer of the State shall sign a completed Attestation of Compliance (AOC) form that shall accompany the Report on Compliance for filing with the State's Acquirers. The AOC shall include such assertions as are required by card brands to ensure that accuracy and completeness of the Report on Compliance. The Confirmation of Report Accuracy declaration format shall be of the Contractor's choosing and shall be included with the Bids sample deliverables.

PRELIMINARY REPORT ON COMPLIANCE

After the initial assessment, the Contractor will prepare a Preliminary Report on Compliance that will be presented to the State. If required, the State will complete any necessary remediation before a final Report on Compliance is presented. The State may if necessary request remediation support services from the Contractor, this will solely be at the discretion of the State.

FINAL REPORT ON COMPLIANCE

After the preliminary Report on Compliance has been reviewed by the State team and any necessary remediation is completed by the State; the requested changes and/or edits will be

submitted to the Contractor. Once the accuracy of the report is agreed upon, the updates to the report will be made by the Contractor. The final Report of Compliance will be prepared by the Contractor and presented to the State at least five (5) days prior to being presented to the State's acquiring banks and the payment card brands.

POST ASSESSMENT EXECUTIVE REPORT

After all Agency assessments have been completed the Contractor will be requested to draft a Post Assessment Executive Report that will be presented to the contracting agency.

The report shall include, but, is not limited to:

- High level summary of overall State compliance
- High level summary of control strengths and weaknesses
- High level summary of applied compensating controls that were put in place to address areas of non-compliance and recommended long term solutions.
- High level summary of short and long term changes the State should consider (and fund) to reduce overall PCI exposure and future costs.

MEETINGS AND DELIVERABLES

There shall be regular weekly status meetings between the Contractor and State staff during the course of the compliance assessment to measure progress against the Work Plan and related milestones.

The Contractor Project Manager shall submit weekly status reports. All status reports shall be prepared in formats approved by the State, unless otherwise agreed by the parties in writing.

Status reports shall include, at a minimum the following:

- Project status related to the Project Work Plan and Milestones
- Accomplishment during the week being reported
- Planned activities for the upcoming weekly period
- Future activities
- Issues and concerns requiring resolution: e.g.
 - a) Summary of issues logged with Contractor's recommendations on issues;
 - b) Summary of risks logged, with Contractor's recommendations on the risks;

The Contractor shall prepare and submit the preliminary Report on Compliance after the preliminary assessment and the final Report on Compliance after all remediation processes have been implemented and validated.

On or about the time of submission of the final Report on Compliance, the Contractor may be required at the State's sole discretion to make an oral presentation(s) to the Agencies included in the audit along with senior executive staff.

DATA ENVIRONMENT DETAILS

Details of the Data Environment will only be released to the Contractor(s) awarded this bid. In Addition, upon request the awarded Contractor may be provided with, but, not limited to the following project data sources.

- Network Diagrams
- Application Penetration Tests
- Network Penetration Tests
- External Vulnerability Scanning
- Internal Vulnerability Scanning

- Internal Reports / Configuration documentation

ACCESS AND RETENTION OF RECORDS

Access to Records

The Contractor shall provide the State, or any authorized agents, access to any records, or copies of said records, necessary to determine contract compliance.

Retention Period

The Contractor shall retain records for a period of three years after either the completion date of this contract or the conclusion of any claim, litigation or exception relating to this contract taken by the State or a third party. Such records shall be available for any PCI reviews as part of its normal QSA Quality Assurance review process.

APPROACH TO SCOPE OF WORK

All Contractors shall provide, as, a detailed description of their PCI Security Assessment approach with a heterogeneous environment. The Contractor shall demonstrate a clear understanding of the nature of the work to be performed under the proposed Contract by describing its approach to meeting the RFB's overall and specific requirements and why this methodology is optimal for this project. The Contractor shall provide a complete and detailed response addressing the following items:

Overview

The Contractor must present a narrative description of its proposed overall plan for providing PCI DSS consultant services that will ultimately result in Contractor signed compliance reports that will be submitted to the acquiring bank and card brands the State does business with. This section should also describe the plan for providing ongoing consulting services in support of annual compliance requirements as well as the Contractor's general approach to handling interpretations of the PCI DSS standards and how the Contractor handles disagreements with these interpretations.

Detailed Approach

The Contractor must describe its detailed approach to meeting the elements of the Scope of Work. The Contractor shall articulate specific methodologies that demonstrate a clear understanding of the nature of the work to be performed including any on-line tools such as SharePoint and details on any software applications employed. This would include but not limited to assumptions, constraints and risks that could impede the completion of this project.

Disclosure of User Agreements and/or Indemnification Requirements

The Contractor shall disclose and provide a copy of any and all electronic and written user agreements that may require State staff to indemnify and/ or changes or adds additional requirements beyond those defined in an established contract, when granted access to any on-line tools or software applications provided by the Contractor. The State reserves the right to reject and or request amendments to such agreements and proposals.

PRELIMINARY PROJECT WORK PLAN & SCHEDULE

All Contractors shall provide, a preliminary Work Plan that ties into the detailed approach and shall include a detailed project schedule indicating services and deliverables, (e.g., Report on Compliance) that demonstrates how the elements of the Scope of Work will be completed to meet the deadlines as outlined. The Work Plan must take into consideration the expected milestones outlined in It is anticipated the project milestone dates may be adjusted based on the Contractor's final approved Work Plan and Schedule.

All services performed under this Contract shall be performed between the hours of 8:00 A.M. and 5:00 P.M unless other arrangements are made in advance with the State. Any deviation in work hours shall be pre-approved by the Contracting Officer. The State requires ten-day advance knowledge of said work schedules to provide security and access to respective work areas. No premium charges will be paid for any off-hour work.

Contractor shall not commence work until a conference is held with each agency, at which representatives of the Contractor and the State are present. The conference will be arranged by the requesting agency (State).

The Contractor shall not commence work until a conference is held with each agency, at which representatives of the Contractor and the State are present. The conference shall be arranged by the requesting agency (State).

The State shall require correction of defective work or damages to any part of a building or its appurtenances when caused by the Contractor's employees, equipment or supplies. The Contractor shall replace in satisfactory condition all defective work and damages rendered thereby or any other damages incurred. Upon failure of the Contractor to proceed promptly with the necessary corrections, the State may withhold any amount necessary to correct all defective work or damages from payments to the Contractor.

The work staff shall consist of qualified persons completely familiar with the products and equipment they shall use. The Contracting Officer may require the Contractor to dismiss from the work such employees as deems incompetent, careless, insubordinate, or otherwise objectionable, or whose continued employment on the work is deemed to be contrary to the public interest or inconsistent with the best interest of security and the State.

The Contractor or their personnel shall not represent themselves as employees or agents of the State.

While on State property, employees shall be subject to the control of the State, but under no circumstances shall such persons be deemed to be employees of the State.

All personnel shall observe all regulations or special restrictions in effect at the State agency.

The Contractor's personnel shall be allowed only in areas where services are being performed. The use of State telephones is prohibited.

SECTION II

Forensic Investigation Services (All Data Breaches)

PCI Forensic Investigators:

PFI Company responsibilities include (without limitation) the following:

Driving and performing all aspects of PFI Investigations

- Adhere to all procedures, guidelines and evidence handling as identified in the PCI Security Standards Council's (PCI SSC) Forensic Investigator Program Guide, under the current version;
- Determine the scope of the investigation and the relevant sources of evidence
- Make recommendations on how the State of New Hampshire should prioritize containment and secure sensitive data;
- Provide Investigation reporting and delivery of applicable PFI Reports as further described below; and

- For cardholder incidents governed by PCI security requirements, provide a feedback form as described in Appendix D of the PCI SSC's Forensic Investigator Program Guide, under the current version.

Good Standing with the PCI Security Standards Council

The Contractor must be in good standing with the PCI Security Standards Council ("PCI SSC") as a PFI for the project duration; the Contract may, at the State's discretion be terminated immediately if the Vendor is dropped from the PCI SSC listing of PFI companies or is placed on remediation status.

The Contractors' servers and their workers must be located within the United States of America.

Investigation Reporting:

PFI Companies have all requisite authority to provide materials and information (including but not limited to final and draft PFI Reports and work papers as described above. Before beginning each PFI Investigation engagement, the PFI Company must inform the State of New Hampshire that it shall be required to disclose the same as herein described and must obtain clear, unqualified permission and consent from the State of New Hampshire to make such disclosures.

The following reports must be produced as part of each PFI Investigation:

Preliminary Incident Response Report: Each completed Preliminary Incident Response Report must be delivered to the applicable State of New Hampshire agency no later than five (5) business days after beginning PFI Investigation review of such State of New Hampshire.

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

- Identity of the reporting agency
- Identify of the lead investigator
- Identity of all third parties included in the investigation
- Date of the start of the investigation
- Date of report
- Breach evidence
- First confirmed date that the intruder or malware entered the network
- Scope of the forensic investigation
- Type of data
- Initial thoughts on attacker
- If contained, how was it contained and when was it contained
- Estimated date of investigation completion

Final Incident Response Report:

The completed Final PFI Report must be delivered to each affected Participating Payment Brand, the applicable State of New Hampshire, and such State of New Hampshire's affected acquirer(s) (if the State of New Hampshire is a merchant), in each case no later than ten (10) business days after completion of the corresponding PFI Investigation of such State of New Hampshire.

- Identity of the reporting agency
- Identify of the lead investigator
- Identity of all third parties included in the investigation
- Date of the start of the investigation
- Date of report
- Breach evidence
- First confirmed date that the intruder or malware entered the network
- Scope of the forensic investigation

Contractor Initials S.A.W.
Date 04/26/2018

- Descriptive list of items submitted for examination
- Executive Summary of the results and conclusions, including short term and long term recommendations to prevent future events
- Description of steps taken during the examination including search parameters and recovered files
- Detailed report of the results and conclusions along with supporting evidence.

SECTION III
Security Testing and Remediation Services

Security Compliance, Testing and Remediation Services all State Agencies
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 shall 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 Contractors' servers must be located within the "USA" and their workers located in the "USA".

Security compliance, testing and remediation results shall be provided in both an executive 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 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
- 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.

SECTION IV
EXTERNAL VULNERABILITY SCANNING AND SELF ASSESSMENT QUESTIONNAIRE

VULNERABILITY SCANNING SERVICES

Provide services that allow agencies to comply with the current version of PCI Security Standards Council PCI DSS Requirement 11.2 for external quarterly scans of IP addresses on its network.

Good Standing with the PCI Security Standards Council

The Contractor must be in good standing with the PCI Security Standards Council ("PCI SSC") as an ASV for the project duration; the Contract may, at the State's discretion be terminated immediately if the Vendor is dropped from the PCI SSC listing of PFI companies or is placed on remediation status.

The Vendors' servers must be located within the "USA" and their workers located in the "USA".

Monthly External Scanning of all Merchants to include:

- i. Automatically scanning the list of external IP addresses and/or domains for

- known vulnerabilities and configuration issues
 - ii. Providing an executive summary and compliance report
 - iii. Providing a detailed findings report with various levels of detail. It shall include: compliance status, prioritized vulnerabilities, policy weaknesses and remediation recommendations.
 - iv. Providing a secure web portal that allows each agency to review its findings and reports as well as consolidate all agency scans at a State level
 - v. Ability for the State to download all detailed findings results in a csv or excel spreadsheet format to use for internal remediation efforts. Individual finding shall be listing in its own row.
 - vi. State has the ability to setup and modify scan schedules.
- b) Compliance Questionnaire that allows each agency to respond to the appropriate current PCI Security Standards Council's Self-Assessment Questionnaire (SAQ) based on information provided about its credit card environment
- c) State has the ability to setup, modify and disable users within both the external scanning and SAQ modules.
- d) Compliance Certification indicating whether the agency, based on the external vulnerability scanning and responses to the Compliance Questionnaire, meets the current version of PCI DSS compliance.

**EXHIBIT B
PAYMENT TERMS**

1. CONTRACT PRICE

The Contractor hereby agrees to provide security compliance, testing and remediation services in complete compliance with the terms and conditions specified in Exhibit A for an amount up to and not to exceed a price of \$1,230,000.00; this figure shall not be considered a guaranteed or minimum figure; however it shall be considered a maximum figure from the effective date of through the expiration date set as February 28, 2021.

2. PRICING STRUCTURE

Section 1		
Services - not limited to, but may include	Hourly Rate (Onsite)	Hourly Rate (Offsite)
PCI DSS Audit Assessment	\$160	\$150

Section 2		
Services - not limited to, but may include	Hourly Rate (Onsite)	Hourly Rate (Offsite)
Data Breach Investigative Services	\$160	\$150

Section 3		
Services - not limited to, but may include	Hourly Rate (Onsite)	Hourly Rate (Offsite)
Remediation Services	\$160	\$150
Security Assessment	\$160	\$150
Risk/Audit Assessment	\$160	\$150
Security Compliance	\$160	\$150
Security Testing	\$160	\$150
Reconnassance & Discovery	\$160	\$150
Social Engineering	\$160	\$150
Security Policy Creation & Review	\$160	\$150
Application & Network Penetration Testing	\$160	\$150

Section 4	
Services - not limited to, but may include	Fixed Rate
External Vulnerability Scanning	\$21
Self-Assessment Questionnaires	\$60

3. PRICING QUOTATIONS FOR INDIVIDUAL PROJECTS

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 (Exhibit E). 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.

4. PAYMENT

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

5. 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 to the State's satisfaction.

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 Contractor will prepare and deliver the Final Report on Compliance and Attestation of Compliance to the State.	35%
Post Assessment Executive Report	For each year during the term of the Contract, the	This report should include but is not limited to: High level overall	10%

Contractor Initials D.M.H.
 Date 04/06/2018

and Oral Presentation	Contractor shall submit a Post Assessment Executive Report and will present this report according to specifications in Exhibit A.	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.	
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%

Contractor Initials D.M.A.
Date 04/01/2018

**EXHIBIT C
SPECIAL PROVISIONS**

There are no special provisions of this contract.

Contractor Initials A.M.H.
Date 09/26/2018

EXHIBIT D

RFB 2075-18 is incorporated here within.

Contractor Initials D.M.G.
Date 04/06/2018

EXHIBIT E

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.**

Contractor Initials ANN
Date 04/06/2018

**EXHIBIT F
GLOSSARY OF TERMS**

TERM	DEFINITION
Acquirer	Also referred to as "merchant bank," "acquiring bank," or "acquiring financial institution". Entity, typically a financial institution that processes payment card transactions for merchants and is defined by a payment brand as an acquirer. Acquirers are subject to payment brand rules and procedures regarding merchant compliance.
Agency	Any entity that utilizes or seeks to utilize payment card processing services under contracts secured by DAS
AOC	Attestation of Compliance
BAMS	Bank of America Merchant Services
Chase	J.P. Morgan Chase Merchant Services
Administrative Safeguards	Administrative safeguards are administrative actions, policies, and procedures to prevent, detect, contain, and correct security violations. Administrative safeguards involve the selection, development, implementation, and maintenance of security measures to protect e-PHI and to manage the conduct of workforce members in relation to the protection of that information. A central requirement is that you perform a security risk analysis that identifies and analyzes risks to e-PHI and then implement security measures to reduce the identified risks.
Audit	An independent examination of security controls associated with a representative subset of organizational information systems to determine the operating effectiveness of system controls; to ensure compliance with established policy and operational procedures; and to recommend changes in controls, policy, or procedures where needed.
Audit trail	A chronological record of system activities sufficient to enable the reconstruction, review, and examination of security events related to an operation, procedure, or event in a transaction from its inception to final results.
Authentication	Verification of the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Banner	Display of an information system, which outlines the parameters for system or information use.
CDE	Acronym for "cardholder data environment." The people, processes and technology that store, process, or transmit cardholder data or sensitive authentication data.
Certification in Health Information Security	Healthcare Information and Management Systems Society (HIMSS) and the American Health Information Management Association (AHIMA) are two organizations that offer certifications upon successful completion of an exam.
Certified in Healthcare Privacy and Security (CHPS)	This credential is designated to professionals who are responsible for safeguarding patient information. This credential signifies expertise in planning, executing, and administering privacy and security protection programs in health care organizations and competence in a specialized skill set in the privacy and security aspects of health information management.
Certified Professional in Healthcare Information & Mgmt. Systems (CPHIMS)	CPHIMS is a professional certification program for health care information and management systems professionals.
CISA	Certified Information Systems Auditor (CISA)
CISSP	Certified Information Systems Security Professional (CISSP)

Classified	National security information classified pursuant to Executive Order 12958.
CMS	Centers for Medicare and Medicaid Services
Compensating Controls	Compensating controls may be considered when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other controls. Compensating controls must:
Compromise	Also referred to as "data compromise," or "data breach." Intrusion into a computer system where unauthorized disclosure/theft, modification, or destruction of cardholder data is suspected.
Configuration management	A structured process of managing and controlling changes to hardware, software, firmware, communications, and documentation throughout the system development life cycle.
Contractor	The company and/or consultants providing the services.
Cross-Site Request Forgery (CSRF)	Vulnerability that is created from insecure coding techniques, resulting in improper input validation. Often used in conjunction with CSRF and/or SQL injection.
Cross-Site Scripting (XSS)	Vulnerability that is created from insecure coding methods that allows for the execution of unwanted actions through an authenticated session. Often used in conjunction with XSS and/or SQL injection.
Cryptography	The process of rendering plain text information unreadable and restoring such unreadable information to a readable form.
Decryption	The process of converting encrypted information into a readable form. This term is also referred to as deciphering.
De-identified Information	Records that have had enough PII removed or obscured such that the remaining information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual.
De-Identified PHI	The Privacy Rule does not restrict the use or disclosure of de-identified health information. De-identified health information neither identifies nor provides a reasonable basis to identify an individual. If data is de-identified in the manner prescribed by HIPAA, it is not PHI. Increasingly researchers are seeking and using de-identified clinical data for health system improvement activities.
Discretionary access control	A method of restricting logical access to information system objects (e.g., files, directories, devices, permissions, rules) based on the identity and need-to-know of users, groups, or processes.
Distinguishable Information	Information that can be used to identify an individual.
DMZ	Abbreviation for "demilitarized zone." Physical or logical sub-network that provides an additional layer of security to an organization's internal private network. The DMZ adds an additional layer of network security between the Internet and an organization's internal network so that external parties only have direct connections to devices in the DMZ rather than the entire internal network.
DNS	Acronym for "domain name system" or "domain name server." A system that stores information associated with domain names in a distributed database to provide name-resolution services to users on networks such as the Internet.
EHR	Electronic Health Record
EMV	Europay, MasterCard and Visa which stands for a global standard for cards equipped with computer chips and the technology used to authenticate chip-card transactions.

Entity Under Investigation	A merchant, service provider, financial institution or other entity that processes, stores, or transmits cardholder data is required to comply with any PCI Standard, and is at the time in question required pursuant to Industry Rules to undergo a PFI Investigation of a specific Security Issue by a PFI.
Event	Refers to a single event of a known or suspected data compromise. It is used interchangeably with the term "incident."
Forensics	Also referred to as "computer forensics." As it relates to information security, the application of investigative tools and analysis techniques to gather evidence from computer resources to determine the cause of data compromises.
HIPAA	Health Insurance Portability and Accountability Act as updated by the HIPAA Omnibus Final Rule2 in 2013, set forth how certain entities, including most health care providers, must protect and secure patient information. They also address the responsibilities of Business Associates (BAs), which include EHR developers working with health care providers.
Incident	Refers to each single occurrence of known or suspected data compromise. It is used interchangeably with the term "event."
Information Security: Encryption	Per the HIPAA Security Rule, a CE, such as a health care provider, must use encryption if, after implementing its security management process, it determines that encryption is a reasonable and appropriate safeguard in its practice environment to safeguard the confidentiality, integrity, and availability of e-PHI.
Information system security	The protection of information systems and information against unauthorized access, use modification, or disclosure to ensure the confidentiality, integrity, and availability of information systems and information.
Integrity	The protection of information systems and information from unauthorized modification to ensure the quality, accuracy, completeness, nonrepudiation, and authenticity of information.
Key	Information used to establish and periodically change the operations performed in cryptographic devices for the purpose of encrypting and decrypting information.
Key Staff	The Contractor's vital staff assigned to the project (for example: QSA's)
Management controls	Security controls focused on managing organizational risk and information system security and devising sufficient countermeasures or safeguards to mitigate risk to acceptable levels. Management control families include risk assessment, security planning, system and services acquisition, and security assessment.
Masking	In the context of PCI DSS, it is a method of concealing a segment of data when displayed or printed. Masking is used when there is no business requirement to view the entire PAN. Masking relates to protection of PAN when displayed or printed. See Truncation for protection of PAN when stored in files, databases, etc.
Merchant	For the purposes of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services. Note that a merchant that accepts payment cards as payment for goods and/or services can also be a service provider, if the services sold result in storing, processing, or transmitting cardholder data on behalf of other merchants or service
MO/TO	Mail-Order/Telephone-Order

Network Segmentation	Also referred to as "segmentation" or "isolation." Network segmentation isolates system components that store, process, or transmit cardholder data from systems that do not. Adequate network segmentation may reduce the scope of the cardholder data environment and thus reduce the scope of the PCI DSS assessment. See the Network Segmentation section in the PCI DSS Requirements and Security Assessment Procedures for guidance on using network segmentation. Network segmentation is not a PCI DSS requirement.
Obscured Data	Data that has been distorted by cryptographic or other means to hide information. It is also referred to as being masked or obfuscated.
Operational controls	Security controls focused on mechanisms primarily implemented by people as opposed to systems. These controls are established to improve the security of a group, a specific system, or group of systems. Operational controls require technical or specialized expertise and often rely on management and technical controls. Operational control families include personnel security, contingency planning, configuration management, maintenance, system and information integrity, incident response, and awareness and training.
Organizational Standards	These standards require a CE to have contracts or other arrangements with BAs that will have access to the CE's e-PHI. The standards provide the specific criteria required for written contracts or other arrangements.
PA-DSS	Payment Application Data Security Standard
PAN	Acronym for "primary account number" and also referred to as "account number." Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder
Payment Application	In the context of PA-DSS, a software application that stores, processes, or transmits cardholder data as part of authorization or settlement, where the payment application is sold, distributed, or licensed to third parties.
Payment Processor	Sometimes referred to as "payment gateway" or "payment service provider (PSP)". Entity engaged by a merchant or other entity to handle payment card transactions on their behalf. While payment processors typically provide acquiring services, payment processors are not considered acquirers unless defined as such by a payment card brand.
PCI	Payment Card Industry
PCI Forensic Investigator, PFI, or PFI Company	Refers to a company, organization, or other legal entity that is in compliance with all PFI Company Requirements (defined in the PFI Qualification Requirements) and has been qualified as a PFI Company and/or PFI Employee by PCI SSC (or another Approving Organization, if applicable) as a PFI. A list of PFIs can be obtained at www.pcisecuritystandards.org
PCI-DSS	Payment Card Industry Data Security Standard
Penetration Test	Penetration tests attempt to identify ways to exploit vulnerabilities to circumvent or defeat the security features of system components. Penetration testing includes network and application testing as well as controls and processes around the networks and applications, and occurs from both outside the environment (external testing) and from inside the environment.
Personally identifiable information	Any information about an individual maintained by an agency with respect to, but not limited to, education, financial transactions, medical history, and criminal or employment history, and information that can be used to distinguish or trace an individual's identity (e.g., name, Social Security Number, date and place of birth, mother's maiden name, biometric records) including any other personal information linked or linkable to an individual.
PFI Investigation	Refers to the forensic investigation of a Security Issue for an Entity Under Investigation pursuant to applicable Industry Rules for PFI Program

PFI Portal	The secure web portal designated by PCI SSC for the applicable purpose in connection with the PFI Program.
Physical Safeguards	These safeguards are physical measures, policies, and procedures to protect electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion. These safeguards are the technology and the policies and procedures for its use that protect e-PHI and control access to it.
PII Confidentiality Impact Level	The PII confidentiality impact level—low, moderate, or high—indicates the potential harm that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.
PMP	Project Management Professional
POI	Acronym for "Point of Interaction," the initial point where data is read from a card. An electronic transaction-acceptance product, a POI consists of hardware and software and is hosted in acceptance equipment to enable a cardholder to perform a card transaction. The POI may be attended or unattended. POI transactions are typically integrated circuit (chip) and/or magnetic-stripe card-based payment
Point of Compromise	Refers to the location where account number data was obtained by unauthorized third parties.
Policies and Procedures	These standards require a CE to adopt reasonable and appropriate policies and procedures to comply with the provisions of the Security Rule. A CE must maintain, until six years after the date of their creation or last effective date (whichever is later), written security policies and procedures and written records of required actions, activities, or assessments. A CE must periodically review and update its documentation in response to environmental or organizational changes that affect the security of e-PHI.
Privacy Impact Assessment (PIA)	"An analysis of how information is handled that ensures handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; determines the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and examines and evaluates protections and alternative processes for handling information to mitigate potential privacy risks.
Project	The Payment Card Industry Data Security Standard PCI Compliance Assessment provide to the State of New Hampshire
Project Leads	The Contractor's main staff that will direct the project through to completion (for example: Project Managers)
Project Staff	All of the Contractor's Staff assigned to complete the PCI Assessments and/or Remediation efforts, including project leads, management and key staff.
QSA	Qualified Security Assessor
Risk Analysis	The risk analysis requirement in the HIPAA Security Rule is much more expansive. It requires you to assess the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all the electronic Protected Health Information (e-PHI) that an organization creates, receives, maintains, or transmits — not just the e-PHI maintained in Certified EHR Technology (CEHRT). This includes e-PHI in other electronic systems and all forms of electronic media, such as hard drives, floppy disks, compact discs (CDs), digital video discs (DVDs), and smart cards or other storage devices, personal digital assistants, transmission media, or portable electronic media. In addition, you will need to periodically review your risk analysis to assess whether changes in your environment necessitate updates to your security measures.
ROC	Report on Compliance

Security Issue	Refers to an actual or suspected compromise or other incident that, in accordance with applicable Industry Rules, requires forensic investigation by a PFI.
Service Provider	Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity. This also includes companies that provide services that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, IDS and other services as well as hosting providers and other entities. If an entity provides a service that involves only the provision of public network access—such as a telecommunications company providing just the communication link—the entity would not be considered a service provider for that service (although they may be considered a service provider for other services).
SoNH	State of New Hampshire
SQL Injection	Form of attack on database-driven web site. A malicious individual executes unauthorized SQL commands by taking advantage of insecure code on a system connected to the Internet. SQL injection attacks are used to steal information from a database from which the data would normally not be available and/or to gain access to an organization's host computers through the computer that is hosting the database.
State	Refers to the State of New Hampshire
System of Records	"A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.¶
System Security Plan	An official document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements (NIST SP 800-18).
Technical controls	Security controls executed by the computer system through mechanisms contained in the hardware, software, and firmware components of the system. Technical security control families include identification and authentication, access control, audit and accountability, and system and communications protection.
Traceable	Information that is sufficient to make a determination about a specific aspect of an individual's activities or status.
Voice over Internet Protocol (VoIP)	A methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet protocol networks, such as the Internet.
Vulnerability assessment	Systematic examination of an information system to determine its security posture, identify control deficiencies, propose countermeasures, and validate the operating effectiveness of such security countermeasures after implementation.
Work Plan	Schedule and description of the elements of the Statement of Work

State of New Hampshire

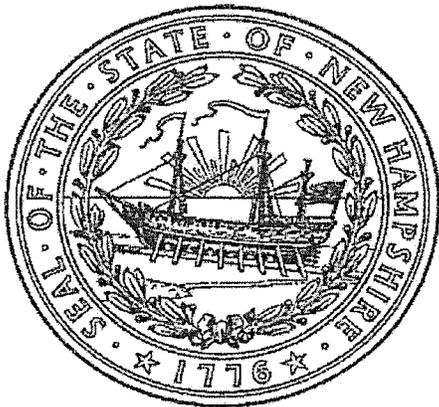
Department of State

CERTIFICATE

I, William M. Gardner, Secretary of State of the State of New Hampshire, do hereby certify that ENTERPRISE RISK MANAGEMENT, INC. is a Florida Profit Corporation registered to transact business in New Hampshire on March 08, 2016. I further certify that all fees and documents required by the Secretary of State's office have been received and is in good standing as far as this office is concerned.

Business ID: **740251**

Certificate Number: **0004076676**



IN TESTIMONY WHEREOF,
I hereto set my hand and cause to be affixed
the Seal of the State of New Hampshire,
this 6th day of April A.D. 2018.

A handwritten signature in black ink, appearing to read "William M. Gardner".

William M. Gardner
Secretary of State

CORPORATE RESOLUTION
OF
ENTERPRISE RISK MANAGEMENT, INC.

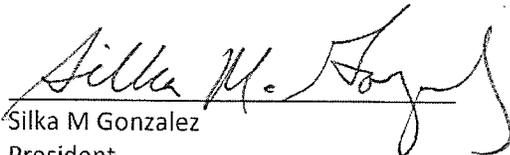
We, the undersigned, being all Directors of Enterprise Risk Management Inc., in the form prescribed by the Florida Financial Services Commission and Chapter 517 of the Florida Statutes, organized and existing under the laws of Florida, and having its principal place of business at 800 S. Douglas Road, Suite 940 North Tower, Coral Gables, Florida 33134 (the "Corporation"), hereby certify that the following is a true and correct copy of a resolution duly adopted at a meeting of Directors of the Corporation duly held and convened on April 06, 2018, at which a quorum of the Board of Directors was present and voting throughout, and that such resolution has not been modified, rescinded or revoked, and is at present in full force and effect:

Therefore, it is resolved:

We have accepted the award for NH Bid 2075-18, which the completion date should be by 02/28/2021 and the price should not go over \$1,230,000.

By affirmative votes noted as signatures below, a majority vote of the Directors of Enterprise Risk Management, Inc. with authority to bind the Company approves the form and content of this resolution, to be effective immediately.

DIRECTORS



Silka M Gonzalez
President

04/06/2018
Date

ATTEST (SECOND OFFICER)



Esteban O Farao
Director of Consulting Services

4/6/2018
Date



CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)

04/06/18

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 have ADDITIONAL INSURED provisions or 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 Aon Risk Services, Inc of Florida 1001 Brickell Bay Drive, Suite #1100 Miami, FL 33131-4937	CONTACT NAME: Aon Risk Services, Inc of Florida
	PHONE (A/C, No, Ext): 800-743-8130 FAX (A/C, No): 800-522-7514
EMAIL ADDRESS: ADP.COI.Center@Aon.com	
INSURER(S) AFFORDING COVERAGE	
INSURER A: Illinois National Insurance Co NAIC # 23817	
INSURER B:	
INSURER C:	
INSURER D:	
INSURER E:	
INSURER F:	

COVERAGES **CERTIFICATE NUMBER:** 1880813 **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. LIMITS SHOWN ARE AS REQUESTED.

INSR LTR	TYPE OF INSURANCE	ADDL INSR	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
	COMMERCIAL GENERAL LIABILITY <input type="checkbox"/> CLAIMS-MADE <input type="checkbox"/> OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: <input type="checkbox"/> POLICY <input type="checkbox"/> PROJECT <input type="checkbox"/> LOC <input type="checkbox"/> OTHER						EACH OCCURRENCE \$ DAMAGE TO RENTED PREMISES (Ea occurrence) \$ MED EXP (Any one person) \$ PERSONAL & ADV INJURY \$ GENERAL AGGREGATE \$ PRODUCTS - COMP/OP AGG \$ \$	
	AUTOMOBILE LIABILITY <input type="checkbox"/> ANY AUTO OWNED AUTOS ONLY <input type="checkbox"/> HIRED AUTOS ONLY <input type="checkbox"/> SCHEDULED AUTOS <input type="checkbox"/> NON-OWNED AUTOS ONLY						COMBINED SINGLE LIMIT (Ea accident) \$ BODILY INJURY (Per person) \$ BODILY INJURY (Per accident) \$ PROPERTY DAMAGE (Per accident) \$ \$	
	<input type="checkbox"/> UMBRELLA LIAB <input type="checkbox"/> OCCUR <input type="checkbox"/> EXCESS LIAB <input type="checkbox"/> CLAIMS-MADE DEC RETENTION \$						EACH OCCURRENCE \$ AGGREGATE \$	
A	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	WC 026160313 FL	01/01/18	07/01/18	<input checked="" type="checkbox"/> PER STATUTE <input type="checkbox"/> OTH-ER E.L. EACH ACCIDENT \$ 2,000,000 E.L. DISEASE - EA EMPLOYEE \$ 2,000,000 E.L. DISEASE - POLICY LIMIT \$ 2,000,000	

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)
 All worksite employees working for ENTERPRISE RISK MANAGEMENT INC, paid under ADP TOTALSOURCE, INC.'s payroll, are covered under the above stated policy. ENTERPRISE RISK MANAGEMENT INC is an alternate employer under this policy.

CERTIFICATE HOLDER

CANCELLATION

State of New Hampshire, Administrative Services ATTN: Loretta Razin, Purchasing Manager 25 Capitol Street, Room 102 Concord, NH 03301	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 <i>Aon Risk Services, Inc of Florida</i>
--	---

STATE OF NEW HAMPSHIRE BID TRANSMITTAL LETTER

Date: March 13, 2018

Company Name: Enterprise Risk Management, Inc.
Address: 800 S. Douglas Road, #940N,
Coral Gables, FL 33134.

To: Point of Contact: Jeff Haley
Telephone: (603) 271-2202
Fax: (603) 271-7564
Email: prchweb@nh.gov

RE: Bid Invitation Name: **SECURITY COMPLIANCE, TESTING AND REMEDIATION SERVICES**
Bid Number: **BID 2075-18**
Bid Posted Date (on or by): **3/8/2018**
Bid Closing Date and Time: **3/16/2018 @ 1:30 PM (EST)**

Dear Jeff Haley:

[Insert name of signor] Silka M. Gonzalez, on behalf of Enterprise Risk Management, Inc. [insert name of entity submitting bid (collectively referred to as "Vendor")] hereby submits an offer as contained in the written bid submitted herewith ("Bid") to the State of New Hampshire in response to BID # 1988-18 for security compliance, testing and remediation 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 21-1:11-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 21-1:11-c within the past year.

Authorized Signor's Signature *Silka M. Gonzalez* Authorized Signor's Title President

NOTARY PUBLIC/JUSTICE OF THE PEACE

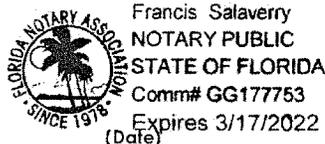
COUNTY: Miami-Dade STATE: Florida ZIP: 33134

On the 13th day of March, 2018, personally appeared before me, the above named Silka M. Gonzalez, in his/her capacity as authorized representative of Vendor, 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.

Francis Salaverry
(Notary Public/Justice of the Peace)

My commission expires: 03/17/2022



Social Engineering	\$160	\$150		See "ATTACHMENT - Methodologies.pdf"	
Security Policy Creation & Review	\$160	\$150		See "ATTACHMENT - Methodologies.pdf"	
Other (Please Specify)	THESE WILL BE FOR EVALUATION PURPOSES ONLY AND NOT INCLUDED IN THE LOWEST HOURLY RATE(S) IN TOTAL CONSIDERED FOR AWARD				
Other (Please Specify)					
ERMPProtect Pilot	Free 1 Month Pilot			See "ATTACHMENT - Methodologies.pdf"	
Other Cybersecurity Services and Support	Hourly rates and/or fixed fees can be provided upon mutual discussion and agreement.			Any other cybersecurity services required but not listed herein.	

***HOURLY RATE FOR COMPARISON PURPOSES; HOWEVER AT THE TIME OF THE QUOTE THE STATE NEEDS A FIXED PRICE**

VENDOR 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:

Silka M. Gonzalez	305-447-6750	N/A
Contact Person	Telephone Number	Toll Free Telephone Number
305-447-6752	sgonzalez@emrisk.com	www.emrisk.com
Fax Number	E-mail Address	Company Website
Enterprise Risk Management, Inc.	610144201	
Vendor Company Name	DUNS #	

ATTACHMENTS:

The following attachments are an integral part of this bid invitation:

Attachment #1: Reference Checklist

Attachment #2: Glossary of Terms

Note: To be considered, bid shall be signed and notarized on front cover sheet in the space provided.