

9B  
24



**STATE OF NEW HAMPSHIRE**  
**DEPARTMENT OF INFORMATION TECHNOLOGY**  
 27 Hazen Dr., Concord, NH 03301  
 Fax: 603-271-1516 TDD Access: 1-800-735-2964  
 www.nh.gov/doit

**Denis Goulet**  
 Commissioner

August 21, 2019

His Excellency, Governor Christopher T. Sununu  
 and the Honorable Executive Council  
 State House  
 Concord, NH 03301

**REQUESTED ACTION**

Authorize the Department of Information Technology to enter into a contract with NuHarbor Security, Inc. of Essex Junction, VT, (VC# 273554) in the amount not to exceed \$499,000.00 for the purpose of providing a comprehensive cybersecurity risk assessment of the Executive Branch information technology enterprise, effective upon Governor and Executive Council approval through June 30, 2020, with an option to renew up to (1) one time for (1) one year upon consent of both parties and Governor and Executive Council approval.

**100% Capital Funds:** Funding is available in the Department of Information Technology accounts as follows. 100% Capital Funds.

CAT#-DEPT#-AGENCY#-ACTIVITY#- ACCOUNTING UNIT #- DEPT NAME- AGENCY NAME -ACCOUNTING UNIT NAME CLASS- OBJECT - DESC	ACTIVITY CODE	FY 20
01-03-03-030030-17030000 – DoIT Cyber Security Program Enhancement 034-500099 Capital Project	N/A	\$499,000.00

**EXPLANATION**

As a public entity, the State of New Hampshire is exposed to the full range of cyber threats on a continual basis: malware, botnets, ransomware, and denial of service attacks do not discriminate – any network connected to the Internet is exposed to these threats. The old boundaries of cybersecurity and cyberattacks are disappearing — from the network perimeter, to distinct types of malware, to nation-state tactics vs. that of the cybercriminal. The attacker's advantage lies in this fluidity, exploiting endpoint vulnerabilities and inadequate security

controls; reshaping attacks to evade detection; and repurposing tactics, techniques and procedures for their own use. It has been said that "You don't know what you don't know" and to that end, the State of New Hampshire is pursuing an independent, comprehensive cybersecurity risk assessment in order to focus cybersecurity resources on the biggest risks and gaps in our security posture. The contract with NuHarbor Security, Inc. will assist with comprehensive cybersecurity risk assessment of the Executive Branch information technology enterprise. In addition to determining gaps or shortfalls in the State's cybersecurity posture, a key outcome of this assessment will be a roadmap to improve the security, readiness and effectiveness of the State of New Hampshire's cybersecurity posture.

The alternative - without this contract - would leave DoIT and the state Executive Branch agencies with minimal ability to assess cybersecurity gaps and vulnerabilities across our enterprise networks, servers and applications that contain sensitive and confidential citizen and state data. The state does not possess the resources, expertise or time to conduct a comprehensive and independent cybersecurity assessment of this scope and depth, so the state will continue to be at significant cyber risk of unknown magnitude.

This contract is the result of a competitive solicitation under DoIT 2018-111 Comprehensive Cyber Security Risk Assessment issued on January 08, 2019. The scoring committee consisted of (5) five state employees, each with expertise in the RFP review process and expertise in the required areas. The scoring team determined NuHarbor Security, Inc. met the minimum qualifications and received the highest overall score of all proposals to the RFP. The Department of Information Technology recommends NuHarbor Security, Inc. be awarded this contract.

The Department of Information Technology respectfully requests approval of this contract.

Respectfully submitted,



Denis Goulet

DG/kaf  
DoIT #2018-111  
RID: 43666

	Vendor Name	Proposal Cost	Technical points	Price points	Total points	Invited to Present
1	NuHarbor	\$259,000.00	625	96	721	yes
2	Cyber Defense Technology	\$393,400.00	625	63	688	yes
3	Janus Assoc.	\$196,169.00	535	127	662	yes
4	Schneider Downs	\$189,000.00	470	132	602	
5	ICS	\$111,000.00	340	225	565	
6	AT&T	\$422,000.00	480	59	539	
7	CBTS	\$191,000.00	385	131	516	
8	Presidio Networked Solutions	\$500,000.00	380	50	430	
9	SHI	\$321,700.00	305	78	383	
10	Veritable Security	\$291,000.00	275	86	361	
11	IC Synergy Int.	\$175,000.00	0	143	143	
12	Connection	\$394,000.00	0	63	63	

	Reviewers	Job Classification & Qualifications
A	Daniel Dister	Chief Information Security Officer - DoIT
B	Theresa Pare Curtis	Director of Web Services - DoIT
C	Richard Bailey	Assistant Commissioner - DOS
D	David Vigneau	IT Manager V - DoIT Dave Vigneau has been the senior member on the state's IT Security team for over 10 years.
E	Don Amendum	IT Manager V - DoIT Don Amendum is the state's senior networking expert, with responsibility for network security for over 15 years.

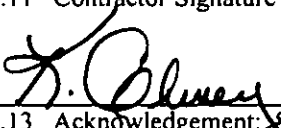
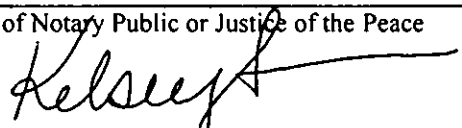

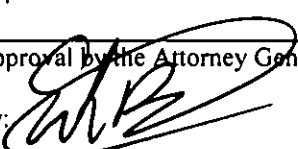
**Notice:** This agreement and all of its attachments shall become public upon submission to Governor and Executive Council for approval. Any information that is private, confidential or proprietary must be clearly identified to the agency and agreed to in writing prior to signing the contract.

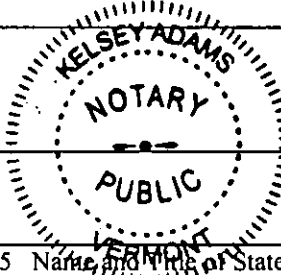
**AGREEMENT**

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

**GENERAL PROVISIONS**

**I. IDENTIFICATION.**

1.1 State Agency Name Department of Information Technology		1.2 State Agency Address 27 Hazen Drive, Concord, NH 03301	
1.3 Contractor Name NuHarbor Security, Inc.		1.4 Contractor Address 39 River Road, Suite 4 Essex Junction, VT 04542	
1.5 Contractor Phone Number 800-917-5719	1.6 Account Number 01-03-03-030030-17030000-034-500099	1.7 Completion Date June 30, 2020	1.8 Price Limitation \$499,000.00
1.9 Contracting Officer for State Agency Denis Goulet, Commissioner		1.10 State Agency Telephone Number 603-223-5703	
1.11 Contractor Signature 		1.12 Name and Title of Contractor Signatory Katherine Cheney, Director	
1.13 Acknowledgement: State of _____, County of _____ On _____, before the undersigned officer, personally appeared the person identified in block 1.12, or satisfactorily proven to be the person whose name is signed in block 1.11, and acknowledged that s/he executed this document in the capacity indicated in block 1.12.			
1.13.1 Signature of Notary Public or Justice of the Peace [Seal] 			
1.13.2 Name and Title of Notary or Justice of the Peace Kelsey Adams, Notary			
1.14 State Agency Signature 		1.15 Name and Title of State Agency Signatory KENNETH DUNN, DEPUTY COMMISSIONER	
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: 9/10/2019			
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.

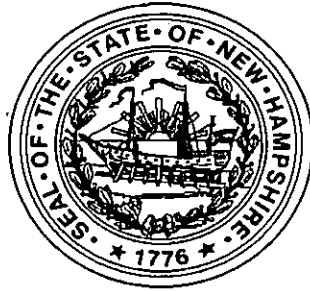
**20. THIRD PARTIES.** The parties hereto do not intend to benefit any third parties and this Agreement shall not be construed to confer any such benefit.

**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.



**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 2 - INFORMATION TECHNOLOGY PROVISIONS**



**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 2 - INFORMATION TECHNOLOGY PROVISIONS**

**TERMS AND DEFINITIONS**

The following general contracting terms and definitions apply except as specifically noted elsewhere in this document.

<b>Acceptance</b>	Notice from the State that a Deliverable has satisfied Acceptance Test or Review.
<b>Acceptance Letter</b>	An Acceptance Letter provides notice from the State that a Deliverable has satisfied Acceptance Tests or Review.
<b>Access Control</b>	Supports the management of permissions for logging onto a computer or network.
<b>Agreement</b>	A Contract duly executed and legally binding.
<b>Appendix</b>	Supplementary material that is collected and appended at the back of a document.
<b>Audit Trail Capture and Analysis</b>	Supports the identification and monitoring of activities within an application or system.
<b>Authorized Persons</b>	The Contractor's employees, contractors, subcontractors or other agents who need to access the State's personal data to enable the Contractor to perform the services required.
<b>CCP</b>	Change Control Procedures.
<b>Certification</b>	The Vendor's written declaration with full supporting and written Documentation (including without limitation test results as applicable) that the Vendor has completed development of the Deliverable.
<b>Change Order</b>	Formal documentation prepared for a proposed change in the Specifications.
<b>Completion Date</b>	End date for the Contract.
<b>Confidential Information</b>	Information required to be kept confidential from unauthorized disclosure under the Contract.

**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 2 - INFORMATION TECHNOLOGY PROVISIONS**

<b>Contract</b>	This Agreement between the State of New Hampshire and a Vendor, which creates binding obligations for each party to perform as specified in the Contract Documents.
<b>Contract Conclusion</b>	Refers to the conclusion of the Contract, for any reason, including but not limited to, the successful Contract completion, termination for convenience, or termination for default.
<b>Contract Documents</b>	Part 1, 2, and 3. The documentation consisting of both the General Provisions and the Exhibits which represents the understanding and acceptance of the reciprocal legal rights and duties of the parties with respect to the Scope of Work.
<b>Contract Managers</b>	The persons identified by the State and the Vendor who shall be responsible for all contractual authorization and administration of the Contract. These responsibilities shall include but not be limited to processing Contract Documentation, obtaining executive approvals, tracking costs and payments, and representing the parties in all Contract administrative activities.
<b>Contract Price</b>	The total, not to exceed amount to be paid by the State to the Contractor for product and services described in the Contract Agreement. This amount is listed in the General Provisions Section 1.8 (P-37).
<b>Contractor</b>	The Vendor and its employees, subcontractors, agents and affiliates who are providing the services agreed to under the contract.
<b>Contracted Vendor</b>	The Vendor whose Proposal or quote was awarded the Contract with the State and who is responsible for the Services and Deliverables of the Contract.
<b>CR</b>	Change Request

**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 2 - INFORMATION TECHNOLOGY PROVISIONS**

<b>Data</b>	State's records, files, forms, Data and other document information, in either electronic or paper format, that will be used/converted by the Vendor during the Contract term.
<b>Data Breach</b>	The unauthorized access by a non-authorized person/s that results in the use, disclosure or theft of a State's unencrypted non-public data.
<b>Deficiencies/Defects</b>	A failure, deficiency or defect in a Deliverable resulting in a Deliverable, the Software, or the System, not conforming to its Specifications.
<b>Deliverable</b>	A Deliverable is the specified work product, produced by the Vendor for the State under the terms of this Contract.
<b>Department</b>	An agency of the State.
<b>Department of Information Technology (DoIT)</b>	The Department of Information Technology established under RSA 21-R by the Legislature effective September 5, 2008.
<b>Documentation</b>	All information that describes the installation, operation, and use of the Software, either in printed or electronic format.
<b>Digital Signature</b>	Certification that guarantees the unaltered state of a file, also known as "code signing".
<b>Effective Date</b>	The Contract and all obligations of the parties hereunder shall become effective on the date the Governor and the Executive Council of the State of New Hampshire approves the Contract.
<b>Encryption</b>	Supports the transformation of data for security purposes.
<b>Governor and the Executive Council</b>	The New Hampshire Governor and the Executive Council.

**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 2 - INFORMATION TECHNOLOGY PROVISIONS**

<b>Identification and Authentication</b>	Supports obtaining information about those parties attempting to log on to a system or application for security purposes and the validation of those users.
<b>Information Technology (IT)</b>	Refers to the tools and processes used for the gathering, storing, manipulating, transmitting, sharing, and sensing of information including, but not limited to, Data processing, computing, information systems, telecommunications, and various audio and video technologies.
<b>Input Validation</b>	Ensure that the values entered by users or provided by other applications meets the size, type and format expected. Protecting the application from cross site scripting, SQL injection, buffer overflow, etc.
<b>Intrusion Detection</b>	Supports the detection of illegal entrance into a computer system.
<b>Invoking Party</b>	In a dispute, the party believing itself aggrieved.
<b>Non Exclusive Contract</b>	A contract executed by the State that does not restrict the State from seeking alternative sources for the Deliverables or Services provided under the Contract.
<b>Non-Public Information</b>	Data, other than personal data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the State because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information.
<b>Non-Software Deliverables</b>	Deliverables that are not Software Deliverables or Written Deliverables, e.g., meetings, help support, services, other.
<b>Normal Business Hours</b>	Normal Business Hours – 8:00 a.m. to 5:00 p.m. EST, Monday through Friday excluding State of New Hampshire holidays. State holidays are: New Year’s Day, Martin Luther King Day, President’s Day, Memorial Day, July 4th, Labor Day, Veterans Day, Thanksgiving Day, the day after

**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 2 - INFORMATION TECHNOLOGY PROVISIONS**

	Thanksgiving Day, and Christmas Day. Specific dates will be provided.
<b>Notice to Proceed (NTP)</b>	The State Contract Manager's written direction to the Vendor to begin work on the Contract on a given date and time.
<b>Order of Precedence</b>	The order in which Contract/documents control in the event of a conflict or ambiguity. A term or condition in a document controls over a conflicting or ambiguous term or condition in a document that is lower in the Order of Precedence.
<b>Personal Data</b>	Data that includes information relating to a person that identifies the person by name and has any of the following personally identifiable information (PII): government-issued identification numbers (e.g., Social Security, driver's license, passport); financial account information, including account number, credit or debit card numbers; or protected health information (PHI) relating to a person.
<b>Project</b>	The planned undertaking regarding the entire subject matter of an RFP and Contract and the activities of the parties related hereto.
<b>Project Team</b>	The group of State employees and Contracted Vendor's personnel responsible for managing the processes and mechanisms required such that the Services are procured in accordance with the Work Plan, budget, required Specifications and quality standards.
<b>Project Managers</b>	The persons identified who shall function as the State's and the Vendor's representative with regards to review and Acceptance of the Contract, invoice sign off, and review and approval of Change Requests (CR) utilizing the Change Control Procedures (CCP).
<b>Project Staff</b>	State personnel assigned to work with the Vendor on the Project.
<b>Proposal</b>	The submission from a Vendor in response to the request for a Proposal or statement of work.

**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 2 - INFORMATION TECHNOLOGY PROVISIONS**

<b>Protected Health Information (PHI)</b>	Individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv) and employment records held by a covered entity in its role as employer.
<b>Report</b>	All Written Deliverables under the Contract.
<b>Review</b>	The process of reviewing Deliverables for Acceptance.
<b>Review Period</b>	The period set for review of a Deliverable.
<b>RFP (Request for Proposal)</b>	A Request for Proposal which solicits proposals to satisfy State requirements by supplying Data processing service resources according to specific terms and conditions.
<b>Review Period</b>	The period set for review of a Deliverable. If none is specified then the Review Period is five (5) business days.
<b>Schedule</b>	The dates described in the Work Plan for deadlines for performance of Services and other project events and activities under the Contract.
<b>Security Incident</b>	The potentially unauthorized access by non-authorized persons to personal data or non-public data the Contractor believes could reasonably result in the use, disclosure or theft of a State's unencrypted personal data or non-public data within the possession or control of the Contractor. A security incident may or may not turn into a data breach.
<b>Services</b>	The work or labor to be performed by the Vendor on the project as described in the contract.
<b>Software</b>	All Software provided by the Vendor under the Contract.

**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 2 - INFORMATION TECHNOLOGY PROVISIONS**

<b>Specifications</b>	The written Specifications that set forth the requirements which include, without limitation, this RFP, the Proposal, the Contract, any performance standards, applicable State and federal policies, laws and regulations, state technical standards, subsequent State-approved Deliverables, and other Specifications and requirements described in the Contract Documents. The Specifications are, by this reference, made a part of the Contract as though completely set forth herein.
<b>State</b>	State is defined as: <b>State of New Hampshire Department of Information Technology 27 Hazen Drive Concord, NH 03301</b>  Reference to the term "State" shall include applicable agencies.
<b>Statement of Work (SOW)</b>	A Statement of Work clearly defines the basic requirements and objectives of a Project. The Statement of Work also defines a high level view of the architecture, performance and design requirements, the roles and responsibilities of the State and the Vendor. The Contract Agreement SOW defines the results that the Vendor remains responsible and accountable for achieving.
<b>State's Confidential Records</b>	State's information regardless of its form that is not subject to public disclosure under applicable state and federal laws and regulations, including but not limited to RSA Chapter 91-A.
<b>State Data</b>	Any information contained within State systems in electronic or paper format.
<b>State Fiscal Year (SFY)</b>	The New Hampshire State Fiscal Year extends from July 1st through June 30th of the following calendar year.
<b>State Identified Contact</b>	The person or persons designated in writing by the State to receive security incident or breach notification.

**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 2 - INFORMATION TECHNOLOGY PROVISIONS**

<b>State Project Leader</b>	State's representative with regard to project oversight.
<b>State Project Manager (PM)</b>	State's representative with regard to project management and technical matters. The Agency Project Manager is responsible for review and Acceptance of specific Contract Deliverables, invoice sign off, and review and approval of a Change Order.
<b>Subcontractor</b>	A person, partnership, or company not in the employment of, or owned by, the Vendor, which is performing Services under this Contract, under a separate Contract with or on behalf of the Vendor.
<b>System</b>	All Software, specified hardware, and interfaces and extensions, integrated and functioning together in accordance with the Specifications.
<b>TBD</b>	To Be Determined
<b>Technical Authorization</b>	Direction to a Vendor, which fills in details, clarifies, interprets, or specifies technical requirements. It must be: (1) consistent with Statement of Work within statement of Services; (2) not constitute a new assignment; and (3) not change the terms, documents of specifications of the Contract Agreement.
<b>Term</b>	Period of the Contract from the Effective Date through expected termination date.
<b>Transition Services</b>	Services and support provided when Contractor is supporting System changes.
<b>User Management</b>	Supports the administration of computer, application and network accounts within an organization.
<b>Vendor/ Contracted Vendor</b>	The Vendor whose proposal or quote was awarded the Contract with the State and who is responsible for the Services and Deliverables of the Contract.



**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 2 - INFORMATION TECHNOLOGY PROVISIONS**

<b>Verification</b>	Supports the confirmation of authority to enter a computer system, application or network.
<b>Warranty Period</b>	A period of coverage during which the Contracted Vendor is responsible for providing a guarantee for products and Services delivered as defined in the Contract.
<b>Work Plan</b>	The overall plan of activities for the project created in accordance with the Contract. The plan and delineation of tasks, activities and events to be performed and Deliverables to be produced under the project as specified in Appendix C: <i>Scope, Requirements and Deliverables</i> . The Work Plan shall include a detailed description of the Schedule, tasks/activities, Deliverables, critical events, task dependencies, and the resources that would lead and/or participate on each task.
<b>Written Deliverables</b>	Non-Software Written Deliverable documentation (letter, report, manual, book, other) provided by the Vendor either in paper or electronic format.

*Remainder of this page intentionally left blank*

**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 2 - INFORMATION TECHNOLOGY PROVISIONS**

---

**INTRODUCTION**

This Contract is by and between the State of New Hampshire, acting through New Hampshire Department of Information Technology ("State"), and NuHarbor Security, Inc., ("Contractor"), having its principal place of business at 39 River Road Suite 4, Essex Junction, VT 04542.

**RECITALS**

Whereas the State desires to have the Contractor provide a comprehensive cybersecurity risk assessment of the Executive Branch information technology enterprise. In addition to determining gaps or shortfalls in the State's cybersecurity posture, a key outcome of this assessment will be a roadmap to improve the security, readiness and effectiveness of the State of New Hampshire's cybersecurity posture.

Whereas the Contractor wishes to provide Information Security, Risk Management, and Cybersecurity managed and professional information security services.

The parties therefore agree as follows:

**1. CONTRACT DOCUMENTS**

**1.1 CONTRACT DOCUMENTS**

This Contract Agreement (2018-111) is comprised of the following documents:

Part 1 - Form P-37 General Provision

Part 2 - Information Technology Provisions

Part 3 - Exhibits

Exhibit A - Contract Deliverables

Exhibit B - Price and Payment Schedule

Exhibit C - Special Provisions

Exhibit D - Administrative Services

Exhibit E - Managed and Professional Information Security Services

Exhibit F - Testing Services (Not Applicable)

Exhibit G - Maintenance and Support Services (Not Applicable)

Exhibit H - Requirements

Exhibit I - Work Plan

Exhibit J - Software Agreement (Not Applicable)

Exhibit K - Warranty and Warranty Services

Exhibit L - Training Services (Not Applicable)

**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 2 - INFORMATION TECHNOLOGY PROVISIONS**

---

Exhibit M - Agency RFP with Addendums, by reference

Exhibit N - Vendor Proposal, by reference

Exhibit O - Certificates and Attachments

**1.2 ORDER OF PRECEDENCE**

In the event of conflict or ambiguity among any of the text of the Contract Documents, the following Order of Precedence shall govern:

1. State of New Hampshire, Department of Information Technology Contract Agreement 2018-111, including Parts 1, 2, and 3.
2. State of New Hampshire, Department of Information Technology RFP 2018-111 Comprehensive Cyber Security Risk Assessment.
3. Vendor Proposal Response to RFP 2018-111 Comprehensive Cyber Security Risk Assessment dated February 14, 2019.

**2. CONTRACT TERM**

- 2.1 The Contract and all obligations of the parties hereunder shall become effective after full execution by the parties, and the receipt of required governmental approvals, including, but not limited to, Governor and Executive Council of the State of New Hampshire approval ("Effective Date") and extend through the date indicated in Part 1, P-37 General Provisions - Block 1.7: *Completion Date*.
- 2.2 The Term may be extended for one (1) additional term of one (1) year, under the terms and conditions contained in the agreement and subject to approval by the New Hampshire Governor and Executive Council.
- 2.3 The Contractor shall commence work upon issuance of a Notice to Proceed by the State.

**3. COMPENSATION**

**3.1 CONTRACT PRICE**

The Contract Price, Part 1, P37, block 1.8 price limitation, method of payment, and terms of payment are identified and more particularly described in Section 5 of P-37 Agreement, and Part 3 Contract Exhibit B: Price and Payment Schedule.

**3.2 NON-EXCLUSIVE CONTRACT**

The State reserves the right, at its discretion, to retain other vendors to provide any of the Services or Deliverables identified under this procurement or make an award by item, part or portion of an item, group of items, or total Proposal. the Contractor shall not be responsible for any delay, act, or omission of such other vendors, except that the Contractor shall be responsible for any delay, act, or omission of the other vendors if such delay, act, or omission is caused by or due to the fault of the Contractor.

**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 2 - INFORMATION TECHNOLOGY PROVISIONS**

---

**4. CONTRACT MANAGEMENT**

The Project will require the coordinated efforts of a Project Team consisting of both the Contractor and State personnel. The Contractor shall provide all necessary resources to perform its obligations under the Contract. The Contractor shall be responsible for managing the Project to its successful completion.

**4.1 THE CONTRACTOR'S CONTRACT MANAGER**

The Contractor shall assign a Contract Manager who shall be responsible for all Contract authorization and administration.

**The Contractor's Contract Manager is:**

Luc Martin  
39 River Road, Suite 4  
Essex Junction, VT 04542  
Email: [lmartin@nuharborsecurity.com](mailto:lmartin@nuharborsecurity.com)

**4.2 THE CONTRACTOR'S PROJECT MANAGER**

**4.2.1** The Contractor shall assign a Project Manager who meets the requirements of the Contract. The Contractor's selection of the Project Manager shall be subject to the prior written approval of the State. The State's approval process may include, without limitation, at the State's discretion, review of the proposed Contractor's Project Manager's resume, qualifications, references, and background checks, and an interview. The State may require removal or reassignment of the Contractor's Project Manager who, in the sole judgment of the State, is found unacceptable or is not performing to the State's satisfaction.

**4.2.2** The Contractor's Project Manager must be qualified to perform the obligations required of the position under the Contract, shall have full authority to make binding decisions under the Contract, and shall function as the Contractor's representative for all administrative and management matters. The Contractor's Project Manager shall perform the duties required under the Contract, including, but not limited to, those set forth in Exhibit I, Section 2. The Contractor's Project Manager must be available to promptly respond during Normal Business Hours within two (2) hours to inquiries from the State, and be at the site as needed. The Contractor's Project Manager must work diligently and use his/ her best efforts on the Project.

**4.2.3** The Contractor shall not change its assignment of the Contractor's Project Manager without providing the State written justification and obtaining the prior written approval of the State. State approvals for replacement of the Contractor's Project Manager shall not be unreasonably withheld. The replacement Project Manager shall have comparable or greater skills than of the Contractor's Project Manager being replaced; meet the requirements of the Contract; and be subject to reference and background checks described above in General Provisions, Section 4.2.1: *Contract Project Manager*, and in Contract Agreement General Provisions, Section 4.6: *Reference and Background*

**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 2 - INFORMATION TECHNOLOGY PROVISIONS**

---

*Checks, below.* The Contractor shall assign a replacement of the Contractor's Project Manager within ten (10) business days of the departure of the prior Contractor's Project Manager, and the Contractor shall continue during the ten (10) business day period to provide competent Project management Services through the assignment of a qualified interim Project Manager.

- 4.2.4 Notwithstanding any other provision of the Contract, the State shall have the option, at its discretion, to terminate the Contract, declare the Contractor in default and pursue its remedies at law and in equity, if the Contractor fails to assign a the Contractor Project Manager meeting the requirements and terms of the Contract.

**The Contractor's Project Manager is:**

Kevin Moss  
39 River Road, Suite 4  
Essex Junction, VT 04542  
Email: kmoss@nuharborsecurity.com

**4.3 CONTRACTOR KEY PROJECT STAFF**

- 4.3.1 The Contractor shall assign Key Project Staff who meet the requirements of the Contract, and can provide the Services and Deliverables identified in the requirements set forth in RFP Appendix C: Requirements, Table C-3: Requirements. The State may conduct reference and background checks on the Contractor's Key Project Staff. The State reserves the right to require removal or reassignment of the Contractor's Key Project Staff who are found unacceptable to the State. Any background checks shall be performed in accordance with General Provisions Section 4.6: Background Checks.
- 4.3.2 The Contractor shall not change any of the Contractor's Key Project Staff commitments without providing the State written justification and obtaining the prior written approval of the State. State approvals for replacement of the Contractor's Key Project Staff will not be unreasonably withheld. The replacement of the Contractor's Key Project Staff shall have comparable or greater skills than of the Contractor's Key Project Staff being replaced.
- 4.3.3 Notwithstanding any other provision of the Contract to the contrary, the State shall have the option to terminate the Contract, declare the Contractor in default and to pursue its remedies at law and in equity, if the Contractor fails to assign Key Project Staff meeting the requirements and terms of the Contract or if it is dissatisfied with the Contractor's replacement Project staff.

- 4.3.3.1 The Contractor Key Project Staff shall consist of the following individuals in the roles identified below:

**Table 4.3.3.1: The Contractor's Key Project Staff**

**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 2 - INFORMATION TECHNOLOGY PROVISIONS**

---

KEY MEMBER(S)	TITLE
Paul Dusini	Director, Information Assurance
Jeffrey Bamberger	Senior Analyst
Kristof Holm	Senior Analyst
Eric Kobelski	Senior Engineer
Randy Duprey	Senior Engineer
Kevin Moss	Operations Coordinator
Ben Weber	Senior Network Engineer
Bill Giglio	Senior Network Engineer
Rick Sotomayor	Pre-Sales Engineer
Nick Calderan	Pre-Sales Engineer

**4.4 STATE CONTRACT MANAGER**

The State shall assign a Contract Manager who shall function as the State's representative with regard to Contract administration.

**The State Contract Manager is:**  
Karen Fleming  
NH Department of Information Technology  
Office: 603-223-5766  
Email: Karen.Fleming@doit.nh.gov

**4.5 STATE PROJECT MANAGER**

The State shall assign a Project Manager. The State Project Manager's duties shall include the following:

- a. Leading the Project;
- b. Engaging and managing all Contractors;
- c. Managing significant issues and risks.
- d. Reviewing and accepting Contract Deliverables;
- e. Invoice sign-offs;
- f. Review and approval of change proposals; and
- g. Managing stakeholders' concerns.

**The State Project Manager is:**  
Daniel Dister  
NH Department of Information Technology  
Office: 603-223-5734  
Mobile: 603-931-9234

**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 2 - INFORMATION TECHNOLOGY PROVISIONS**

---

Email: Daniel.Dister@doit.nh.gov

**4.6 REFERENCE AND BACKGROUND CHECKS**

- 4.6.1** The Contractor shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the contract who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Contractor shall promote and maintain an awareness of the importance of securing the State's information among the Contractor's employees and agents.
- 4.6.2** The State may, at its sole expense, conduct reference and background screening of the Contractor Staff. The State shall maintain the confidentiality of background screening results in accordance with the Contract Agreement – General Provisions- Section 11: Use of State's Information, Confidentiality.

**5. DELIVERABLES**

**5.1 CONTRACTOR RESPONSIBILITIES**

- 5.1.1** The Contractor shall be solely responsible for meeting all requirements, and terms and conditions specified in this Contract, regardless of whether or not a subcontractor is used.
- 5.1.2** The Contractor may subcontract Services subject to the provisions of the Contract, including but not limited to, the terms and conditions in the Contract Agreement. The Contractor must submit all information and documentation relating to the Subcontractor, including terms and conditions consistent with this Contract. The State will consider the Contractor to be wholly responsible for the performance of the Contract and the sole point of contact with regard to all contractual matters, including payment of any and all charges resulting from the Contract.

**5.2 DELIVERABLES AND SERVICES**

The Contractor shall provide the State with the Deliverables and Services in accordance with the time frames in the Work Plan for this Contract, and as more particularly described in Contract Exhibit A: Contract Deliverables.

**5.3 DELIVERABLES REVIEW AND ACCEPTANCE**

After receiving written Certification from the Contractor that a Deliverable is final, complete, and ready for Review, the State will Review the Deliverable to determine whether it meets the Requirements outlined in Contract Exhibit A: Contract Deliverables. The State will notify the Contractor in writing of its Acceptance or rejection of the Deliverable within five (5) business days of the State's receipt of the Contractor's written Certification. If the State rejects the Deliverable, the State shall notify the Contractor of the nature and class of the Deficiency and

**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 2 - INFORMATION TECHNOLOGY PROVISIONS**

---

the Contractor shall correct the Deficiency within the period identified in the Work Plan. If no period for the Contractor's correction of the Deliverable is identified, the Contractor shall correct the Deficiency in the Deliverable within five (5) business days. Upon receipt of the corrected Deliverable, the State shall have five (5) business days to review the Deliverable and notify the Contractor of its Acceptance or rejection thereof, with the option to extend the Review Period up to five (5) additional business days. If the Contractor fails to correct the Deficiency within the allotted period of time, the State may, at its option, continue reviewing the Deliverable and require the Contractor to continue until the Deficiency is corrected, or immediately terminate the Contract, declare the Contractor in default, and pursue its remedies at law and in equity.

**5.4 SOFTWARE REVIEW AND ACCEPTANCE (NOT APPLICABLE)**

System/Software Testing and Acceptance shall be performed as set forth in the Test Plan and more particularly described in Exhibit F: *Testing Services*.

**6. SOFTWARE (NOT APPLICABLE)**

The Contractor shall provide the State with access to the Software and Documentation set forth in the Contract, and particularly described in Exhibit J: *Software Agreement*.

**7. SERVICES**

The Contractor shall provide the Services required under the Contract Documents. All Services shall meet, and be performed, in accordance with the Specifications.

**7.1 ADMINISTRATIVE SERVICES**

The Contractor shall provide the State with the administrative Services set forth in the Contract, and particularly described in Exhibit D: *Administrative Services*.

**7.2 MANAGED AND PROFESSIONAL INFORMATION SECURITY SERVICES**

The Contractor shall provide the State with the Services set forth in the Contract, and particularly described in Exhibit E: *Managed and Professional Information Security Services Implementation Services*.

**7.3 TESTING SERVICES (NOT APPLICABLE)**

The Contractor shall perform testing Services for the State set forth in the Contract, and particularly described in Exhibit F: *Testing Services*.

**7.4 TRAINING SERVICES (NOT APPLICABLE)**

The Contractor shall provide the State with training Services set forth in the Contract, and particularly described in Exhibit L: *Training Services*.



**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 2 - INFORMATION TECHNOLOGY PROVISIONS**

---

**7.5 MAINTENANCE AND SUPPORT SERVICES (NOT APPLICABLE)**

The Contractor shall provide the State with Maintenance and Support Services set forth in the Contract, and particularly described in Exhibit G: *System Maintenance and Support*.

**7.6 WARRANTY SERVICES**

The Contractor shall provide the State with warranty Services set forth in the Contract, and particularly described in Exhibit K: *Warranty & Warranty Services*.

**8. WORK PLAN DELIVERABLE**

- 8.1** The Contractor shall provide the State with a Work Plan that shall include, without limitation, a detailed description of the Schedule, tasks, Deliverables, major milestones, task dependencies, and payment Schedule.
- 8.2** The initial Work Plan shall be a separate Deliverable and is set forth in Contract Exhibit I: Work Plan. The Contractor shall update the Work Plan as necessary, but no less than every two weeks, to accurately reflect the status of the Project, including without limitation, the Schedule, tasks, Deliverables, major milestones, task dependencies, and payment Schedule. Any such updates to the Work Plan must be approved by the State, in writing, prior to final incorporation into Contract Exhibit I: Work Plan. The updated Contract Exhibit I: Work Plan, as approved by the State, is incorporated herein by reference.
- 8.3** Unless otherwise agreed in writing by the State, changes to the Contract Exhibit I: Work Plan shall not relieve the Contractor from liability to the State for damages resulting from the Contractor's failure to perform its obligations under the Contract, including, without limitation, performance in accordance with the Schedule.
- 8.4** In the event of any delay in the Schedule, the Contractor must immediately notify the State in writing, identifying the nature of the delay, i.e., specific actions or inactions of the Contractor or the State causing the problem; its estimated duration period to reconciliation; specific actions that need to be taken to correct the problem; and the expected Schedule impact on the Project.
- 8.5** In the event additional time is required by the Contractor to correct Deficiencies, the Schedule shall not change unless previously agreed in writing by the State, except that the Schedule shall automatically extend on a day-to-day basis to the extent that the delay does not result from the Contractor's failure to fulfill its obligations under the Contract. To the extent that the State's execution of its major tasks takes longer than described in the Work Plan, the Schedule shall automatically extend on a day-to-day basis.
- 8.6** Notwithstanding anything to the contrary, the State shall have the option to terminate the Contract for default, at its discretion, if it is dissatisfied with the Vendor's Work Plan or elements within the Work Plan.

**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 2 - INFORMATION TECHNOLOGY PROVISIONS**

---

**9. CHANGE ORDERS**

- 9.1 The State may make changes or revisions to the agreed upon Statement of Work (SOW) at any time by written Change Order. The State originated changes or revisions shall be approved by the Department of Information Technology. Within five (5) business days, unless otherwise mutually agreed upon of the Contractor's receipt of a Change Order, the Contractor shall advise the State, in detail, of any impact on cost (e.g., increase or decrease), the Schedule, or the Work Plan.
- 9.2 The Contractor may request a change within the scope of the Contract by written Change Order, identifying any impact on cost, the Schedule, or the Work Plan. The State shall attempt to respond to the Contractor's requested Change Order within five (5) business days, unless otherwise mutually agreed upon. The State Agency, as well as the Department of Information Technology, must approve all Change Orders in writing. The State shall be deemed to have rejected the Change Order if the parties are unable to reach an agreement in writing.
- 9.3 All Change Order requests from the Contractor to the State, and the State acceptance of the Contractor's estimate for a State requested change, will be acknowledged and responded to, either acceptance or rejection, in writing. If accepted, the Change Order(s) shall be subject to the Contract amendment process, as determined to apply by the State.

**10. INTELLECTUAL PROPERTY**

**10.1 SOFTWARE TITLE (NOT APPLICABLE)**

- 10.1.1 In the event that the State purchases software all title, right, and interest (including all ownership and intellectual property rights) in the Software, and its associated Documentation, shall remain with the Contractor.
- 10.1.2 Upon successful completion and/or termination of the Implementation of the Project, the Contractor shall own and hold all, title, and rights in any Software modifications developed in connection with performance of obligations under the Contract, or modifications to the Contractor provided Software, and their associated Documentation including any and all performance enhancing operational plans and the Contractors' special utilities. The Contractor shall license back to the State the right to produce, publish, or otherwise use such software, source code, object code, modifications, reports, and Documentation developed under the Contract.
- 10.1.3 In no event shall the Contractor be precluded from developing for itself, or for others, materials that are competitive with, or similar to Custom Software, modifications developed in connection with performance of obligations under the Contract. In addition, the Contractor shall be free to use its general knowledge, skills, experience, and any other ideas, concepts, know-how, and techniques that are acquired or used in the course of its performance under this agreement.

**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 2 - INFORMATION TECHNOLOGY PROVISIONS**

---

**10.2 STATE'S DATA AND PROPERTY**

All rights, title and interest in State Data shall remain with the State. 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. The Contractor shall not access State user accounts or State data, except:

- a. In the course of data center operations;
- b. In response to service or technical issues;
- c. As required by the express terms of this contract; or
- d. At the State's written request.

**10.3 CONTRACTOR'S MATERIALS**

**10.3.1** Subject to the provisions of this Contract, the Contractor may develop for itself, or for others, materials that are competitive with, or similar to, the Deliverables. In accordance with the provision of this Contract, the Contractor shall not distribute any products containing or disclose any State Confidential Information. The Contractor shall be free to use its general knowledge, skills and experience, and any ideas, concepts, know-how, and techniques that are acquired or used in the course of its performance under this Contract, provided that such is not obtained as the result of the deliberate memorization of the State Confidential Information by the Contractor employees or third party consultants engaged by the Contractor.

**10.3.2** Without limiting the foregoing, the parties agree that the general knowledge referred to herein cannot include information or records not subject to public disclosure under New Hampshire RSA Chapter 91-A, which includes but is not limited to the following: records of grand juries and petit juries; records of parole and pardon boards; personal school records of pupils; records pertaining to internal personnel practices, financial information, test questions, scoring keys and other examination data use to administer a licensing examination, examination for employment, or academic examination and personnel, medical, welfare, library use, video tape sale or rental, and other files containing personally identifiable information that is private in nature.

**10.4 STATE WEBSITE COPYRIGHT**

WWW Copyright and Intellectual Property Rights. All right, title and interest in the State WWW site <NH.GOV, etc.>, including copyright to all Data and information, shall remain with the State. The State shall also retain all right, title and interest in any user interfaces and computer instructions embedded within the WWW pages. All WWW pages and any other Data or information shall, where applicable, display the State's copyright.

**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 2 - INFORMATION TECHNOLOGY PROVISIONS**

---

**10.5 CUSTOM SOFTWARE SOURCE CODE (NOT APPLICABLE)**

In the event that the State purchases software development services, which results in Custom Software, the Contractor shall provide the State with a copy of the source code for the Custom Software, which shall be subject to the License rights. The State shall receive a worldwide, perpetual, irrevocable, and non-exclusive paid –up right and license to use, copy, modify and prepare derivative works of any custom developed software. This section does not apply to the Contractor’s proprietary software code.

**10.6 SURVIVAL**

This Contract Agreement Section 10: Intellectual Property shall survive the termination of the Contract.

**11. USE OF STATE’S INFORMATION, CONFIDENTIALITY**

**11.1 USE OF STATE’S INFORMATION**

In performing its obligations under the Contract, the Contractor may gain access to information of the State, including State Confidential Information. “State Confidential Information” shall include, but not be limited to, information exempted from public disclosure under New Hampshire RSA Chapter 91-A: *Access to Public Records and Meetings* (see e.g. RSA Chapter 91-A: 5 *Exemptions*). The Contractor shall not use the State Confidential Information developed or obtained during the performance of, or acquired, or developed by reason of the Contract, except as directly connected to and necessary for the Contractor’s performance under the Contract.

**11.2 STATE CONFIDENTIAL INFORMATION**

**11.2.1** The Contractor shall maintain the confidentiality of and protect from unauthorized use, disclosure, publication, and reproduction (collectively “release”), all State Confidential Information that becomes available to the Contractor in connection with its performance under the Contract, regardless of its form.

**11.2.2** Subject to applicable federal or State laws and regulations, Confidential Information shall not include information which:

- a. Shall have otherwise become publicly available other than as a result of disclosure by the receiving party in breach hereof;
- b. Was disclosed to the receiving party on a non-confidential basis from a source other than the disclosing party, which the receiving party believes is not prohibited from disclosing such information as a result of an obligation in favor of the disclosing party;
- c. Is developed by the receiving party independently of, or was known by the receiving party prior to, any disclosure of such information made by the disclosing party; or

**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 2 - INFORMATION TECHNOLOGY PROVISIONS**

---

d. Is disclosed with the written consent of the disclosing party. A receiving party also may disclose Confidential Information to the extent required by an order of a court of competent jurisdiction.

**11.2.3** Any disclosure of the State Confidential Information shall require the prior written approval of the State. The Contractor shall immediately notify the State if any request, subpoena or other legal process is served upon the Contractor regarding the State Confidential Information, and the Contractor shall cooperate with the State in any effort the State undertakes to contest the request, subpoena or other legal process, at no additional cost to the State.

**11.2.4** In the event of the unauthorized release of State Confidential Information, the Contractor shall immediately notify the State, and the State may immediately be entitled to pursue any remedy at law and in equity, including, but not limited to, injunctive relief.

**11.3 CONTRACTOR CONFIDENTIAL INFORMATION**

Inssofar as the Contractor seeks to maintain the confidentiality of its confidential or proprietary information, the Contractor must clearly identify in writing all information it claims to be confidential or proprietary. Notwithstanding the foregoing, the State acknowledges that the Contractor considers their Documentation to be Confidential Information. The Contractor acknowledges that the State is subject to State and federal laws governing disclosure of information including, but not limited to, RSA Chapter 91-A. The State shall maintain the confidentiality of the identified Confidential Information inssofar as it is consistent with applicable State and federal laws or regulations, including but not limited to, RSA Chapter 91-A. In the event the State receives a request for the information identified by the Contractor as confidential, the State shall notify the Contractor and specify the date the State will be releasing the requested information. At the request of the State, the Contractor shall cooperate and assist the State with the collection and review of the Contractor's information, at no additional expense to the State. Any effort to prohibit or enjoin the release of the information shall be the Contractor's sole responsibility and at the Contractor's sole expense. If the Contractor fails to obtain a court order enjoining the disclosure, the State shall release the information on the date specified in the State's notice to the Contractor, without any liability to the Contractor.

**11.4 SURVIVAL**

This Contract Agreement Section 11, *Use of State's Information, Confidentiality*, shall survive termination or conclusion of the Contract.

**12. LIMITATION OF LIABILITY**

**12.1 STATE**

Subject to applicable laws and regulations, in no event shall the State be liable for any consequential, special, indirect, incidental, punitive, or exemplary damages. Subject to applicable laws and regulations, the State's liability to the Contractor shall not exceed the total Contract price set forth in Contract Agreement – General Provisions, Block 1.8.

**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 2 - INFORMATION TECHNOLOGY PROVISIONS**

---

**12.2 STATE'S IMMUNITY**

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 shall survive termination or Contract conclusion.

**12.3 SURVIVAL**

This Section 12: *Limitation of Liability* shall survive termination or Contract conclusion.

**13. TERMINATION**

**13.1 TERMINATION FOR DEFAULT**

Any one or more of the following acts or omissions of the Contractor shall constitute an event of default hereunder ("Event of Default")

- a. Failure to perform the Services satisfactorily or on schedule;
- b. Failure to submit any report required; and/or
- c. Failure to perform any other covenant, term or condition of the Contract.

**13.1.1** Upon the occurrence of any Event of Default, the State may take any one or more, or all, of the following actions:

- a. Unless otherwise provided in the Contract, the State shall provide the Contractor written notice of default and require it to be remedied within, in the absence of a greater or lesser specification of time, within thirty (30) days from the date of notice, unless otherwise indicated within by the State ("Cure Period"). If the Contractor fails to cure the default within the Cure Period, the State may terminate the Contract effective two (2) days after giving the Contractor notice of termination, at its sole discretion, treat the Contract as breached and pursue its remedies at law or in equity or both.
- b. Give the Contractor a written notice specifying the Event of Default and suspending all payments to be made under the Contract 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.
- c. 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;
- d. Treat the Contract as breached and pursue any of its remedies at law or in equity, or both.
- e. Procure Services that are the subject of the Contract from another source and the Contractor shall be liable for reimbursing the State for the replacement Services, and all administrative costs directly related to the replacement of the Contract

**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 2 - INFORMATION TECHNOLOGY PROVISIONS**

---

and procuring the Services from another source, such as costs of competitive bidding, mailing, advertising, applicable fees, charges or penalties, and staff time costs; all of which shall be subject to the limitations of liability set forth in the Contract.

**13.1.2** The Contractor shall provide the State with written notice of default, and the State shall cure the default within thirty (30) days.

**13.2 TERMINATION FOR CONVENIENCE**

**13.2.1** The State may, at its sole discretion, terminate the Contract for convenience, in whole or in part, by thirty (30) days written notice to the Contractor. In the event of a termination for convenience, the State shall pay the Contractor the agreed upon price, if separately stated in this Contract, for Deliverables for which Acceptance has been given by the State. Amounts for Services or Deliverables provided prior to the date of termination for which no separate price is stated under the Contract shall be paid, in whole or in part, generally in accordance with Contract Exhibit B, *Price and Payment Schedule*, of the Contract.

**13.2.2** During the thirty (30) day period, the Contractor shall wind down and cease Services as quickly and efficiently as reasonably possible, without performing unnecessary Services or activities and by minimizing negative effects on the State from such winding down and cessation of Services.

**13.3 TERMINATION FOR CONFLICT OF INTEREST**

**13.3.1** The State may terminate the Contract by written notice if it determines that a conflict of interest exists, including but not limited to, a violation by any of the parties hereto of applicable laws regarding ethics in public acquisitions and procurement and performance of Contracts.

**13.3.2** In such case, the State shall be entitled to a pro-rated refund of any current development, support, and maintenance costs. The State shall pay all other contracted payments that would have become due and payable if the Contractor did not know, or reasonably did not know, of the conflict of interest.

**13.3.2** In the event the Contract is terminated as provided above pursuant to a violation by the Contractor, the State shall be entitled to pursue the same remedies against the Contractor as it could pursue in the event of a default of the Contract by the Contractor.

**13.4 TERMINATION PROCEDURE**

**13.4.1** Upon termination of the Contract, the State, in addition to any other rights provided in the Contract, may require the Contractor to deliver to the State any property, including without limitation, Written Deliverables, for such part of the Contract as has been terminated.

**13.4.2** After receipt of a notice of termination, and except as otherwise directed by the State, the Contractor shall:

**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 2 - INFORMATION TECHNOLOGY PROVISIONS**

---

- a. The State shall be entitled to any post-termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of the SLA.
- b. Stop work under the Contract on the date, and to the extent specified, in the notice;
- c. Promptly, but in no event longer than thirty (30) days after termination, terminate its orders and subcontracts related to the work which has been terminated and settle all outstanding liabilities and all claims arising out of such termination of orders and subcontracts, with the approval or ratification of the State to the extent required, which approval or ratification shall be final for the purpose of this Section;
- d. Take such action as the State directs, or as necessary to preserve and protect the property related to the Contract which is in the possession of the Contractor and in which the State has an interest;
- e. During any period of service suspension, the Contractor shall not take any action to intentionally erase any State data. In the event of termination of any services or agreement in entirety, the Contractor shall not take any action to intentionally erase any State data for a period of:
  - i. 10 days after the effective date of termination, if the termination is in accordance with the contract period
  - ii. 30 days after the effective date of termination, if the termination is for convenience
  - iii. 60 days after the effective date of termination, if the termination is for cause
  - iv. After such period, the Contractor shall have no obligation to maintain or provide any State data and shall thereafter, unless legally prohibited, delete all State data in its systems or otherwise in its possession or under its control.
- f. Transfer title to the State and deliver in the manner, at the times, and to the extent directed by the State, any property which is required to be furnished to the State and which has been accepted or requested by the State; and
- g. The Contractor shall implement an orderly return of State data in a CSV or another mutually agreeable format at a time agreed to by the parties and the subsequent secure disposal of State data;
- h. The Contractor shall securely dispose of all requested data in all of its forms, such as disk, CD/ DVD, backup tape and paper, when requested by the State. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the State.
- i. Provide written Certification to the State that the Contractor has surrendered to the State all said property.



**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 2 - INFORMATION TECHNOLOGY PROVISIONS**

---

**13.5 SURVIVAL**

This Section 13: Termination shall survive termination or Contract conclusion.

**14. CHANGE OF OWNERSHIP**

In the event that the Contractor should change ownership for any reason whatsoever, the State shall have the option of continuing under the Contract with the Contractor, its successors or assigns for the full remaining term of the Contract; continuing under the Contract with the Contractor, its successors or assigns for such period of time as determined necessary by the State; or immediately terminate the Contract without liability to the Contractor, its successors or assigns.

**15. ASSIGNMENT, DELEGATION AND SUBCONTRACTS**

**15.1** The Contractor shall not assign, delegate, subcontract, or otherwise transfer any of its interest, rights, or duties under the Contract without the prior written consent of the State. Such consent shall not be unreasonably withheld. Any attempted transfer, assignment, delegation, or other transfer made without the State's prior written consent shall be null and void, and may constitute an event of default at the sole discretion of the State.

**15.2** The Contractor shall remain wholly responsible for performance of the entire Contract even if assignees, delegates, Subcontractors, or other transferees ("Assigns") are used, unless otherwise agreed to in writing by the State, and the Assigns fully assumes in writing any and all obligations and liabilities under the Contract from the Effective Date. In the absence of a written assumption of full obligations and liabilities of the Contract, any permitted assignment, delegation, subcontract, or other transfer shall neither relieve the Contractor of any of its obligations under the Contract nor affect any remedies available to the State against the Contractor that may arise from any event of default of the provisions of the contract. The State shall consider the Contractor to be the sole point of contact with regard to all contractual matters, including payment of any and all charges resulting from the Contract.

**15.3** Notwithstanding the foregoing, nothing herein shall prohibit the Contractor from assigning the Contract to the successor of all or substantially all of the assets or business of the Contractor provided that the successor fully assumes in writing all obligations and responsibilities under the Contract. In the event that the Contractor should change ownership, as permitted under Section 15: Change of Ownership, the State shall have the option to continue under the Contract with the Contractor, its successors or assigns for the full remaining term of the Contract; continue under the Contract with the Contractor, its successors or assigns for such period of time as determined necessary by the State; or immediately terminating the Contract without liability to the Contractor, its successors or assigns.

**16. DISPUTE RESOLUTION**

**16.1** 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 progressive management involvement in the dispute negotiation by written notice to the other

**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 2 - INFORMATION TECHNOLOGY PROVISIONS**

party. Such notice shall be without prejudice to the Invoking Party's right to any other remedy permitted under the Contract.

- 16.2** The parties shall use reasonable efforts to arrange personal meetings and/or telephone conferences as needed, at mutually convenient times and places, between negotiators for the parties at the following successive management levels, each of which shall have a period of allotted time as specified below in which to attempt to resolve the dispute:

<b>Table 16.1: DISPUTE RESOLUTION RESPONSIBILITY AND SCHEDULE TABLE</b>			
<b>LEVEL</b>	<b>CONTRACTOR</b>	<b>STATE</b>	<b>CUMULATIVE ALLOTTED TIME</b>
Primary	Luc Martin Project Manager (PM)	Daniel Dister State Project Manager (PM) Chief Information Security Officer	5 Business Days
First	Scott Mosher Vice President	Denis Goulet Commissioner	10 Business Days

- 16.3** The allotted time for the first level negotiations shall begin on the date the Invoking Party's notice is received by the other party. Subsequent allotted time is days from the date that the original Invoking Party's notice is received by the other party.

**17. DEPARTMENT OF INFORMATION TECHNOLOGY GENERAL TERMS AND CONDITIONS**

**17.1 COMPUTER USE**

In consideration for receiving access to and use of the computer facilities, network, licensed or developed software, systems and equipment, Documentation, information, reports, or data of any kind (hereinafter "Information"), the Contractor understands and agrees to the following rules:

- a. Every Authorized User has the responsibility to assure the protection of information from unauthorized access, misuse, theft, damage, destruction, modification, or disclosure.
- b. That information shall be used solely for conducting official State business, and all other use or access is strictly forbidden including, but not limited to, personal, or other private and non-State use and that at no time shall the Contractor access or attempt to access any information without having the express authority to do so.

**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 2 - INFORMATION TECHNOLOGY PROVISIONS**

---

- c. That at no time shall the Contractor access or attempt to access any information in a manner inconsistent with the approved policies, procedures, and /or agreements relating to system entry/access.
- d. That all software licensed, developed, or being evaluated by the State cannot be copied, shared, distributed, sub-licensed, modified, reverse engineered, rented, or sold, and that at all times the Contractor must use utmost care to protect and keep such software strictly confidential in accordance with the license or any other Agreement executed by the State. Only equipment or software owned, licensed, or being evaluated by the State, can be used by the Contractor. Personal software (including but not limited to palmtop sync software) shall not be installed on any equipment.
- e. That if the Contractor is found to be in violation of any of the above-stated rules, the User may face removal from the State Contract, and/or criminal or civil prosecution, if the act constitutes a violation of law.

**17.2 EMAIL USE**

Email and other electronic communication messaging systems are State of New Hampshire property and are to be used for business purposes only. Email is defined as "internal Email systems" or "State-funded Email systems." The Contractor understand and agree that use of email shall follow State standard policy (available upon request).

**17.3 INTERNET/INTRANET USE**

The Internet/Intranet is to be used for access to and distribution of information in direct support of the business of the State of New Hampshire according to State standard policy (available upon request).

**17.4 REGULATORY GOVERNMENT APPROVALS**

The Contractor shall obtain all necessary and applicable regulatory or other governmental approvals necessary to perform its obligations under the Contract.

**17.5 INSURANCE CERTIFICATE**

The Insurance Certificate should note the Certificate Holder in the lower left hand block including State of New Hampshire, Department Name, and name of the individual responsible for the funding of the contracts and his/her address.

**17.6 EXHIBITS**

The Exhibits referred to, in and attached to the Contract are incorporated by reference as if fully included in the text.

**17.7 VENUE AND JURISDICTION**

Any action on the Contract may only be brought in the State of New Hampshire, Merrimack County Superior Court.

**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 2 - INFORMATION TECHNOLOGY PROVISIONS**

---

**17.8 SURVIVAL**

The terms, conditions and warranties contained in the Contract that by their context are intended to survive the completion of the performance, cancellation or termination of the Contract shall so survive.

**17.9 FORCE MAJEURE**

Neither the Contractor nor the State shall be responsible for delays or failures in performance resulting from events beyond the control of such party and without fault or negligence of such party. Such events shall include, but not be limited to, acts of God, strikes, lock outs, riots, and acts of War, epidemics, acts of Government, fire, power failures, nuclear accidents, earthquakes, and unusually severe weather. Except in the event of the foregoing, Force Majeure events shall not include the Contractor's inability to hire or provide personnel needed for the Contractor's performance under the Contract.

**17.10 NOTICES**

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 following addresses.

<b>Table 17.10: Notices</b>	
TO THE CONTRACTOR	TO THE STATE OF NEW HAMPSHIRE
KATHIE CHENEY	DANIEL DISTER
NuHARBOR SECURITY	DEPARTMENT OF INFORMATION TECHNOLOGY
39 RIVER RD SUITE 4	27 HAZEN DRIVE
ESSEX JUNCTION, VT 04542	CONCORD, NH 03301
TEL: (802) 231-0308	TEL: (603) 223-5734

**17.11 DATA PROTECTION**

Protection of personal privacy and data shall be an integral part of the business activities of the Contractor to ensure there is no inappropriate or unauthorized use of State information at any time. To this end, the Contractor shall safeguard the confidentiality, integrity and availability of State information and comply with the following conditions:

- a. The Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of personal data and non-public data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Contractor applies to its own personal data and non-public data of similar kind.

**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 2 - INFORMATION TECHNOLOGY PROVISIONS**

---

- b. All data obtained by the Contractor in the performance of this contract shall become and all personal data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the Contractor is responsible for encryption of the personal data.
- c. Unless otherwise stipulated, the Contractor shall encrypt all non-public data at rest and in transit. The State shall identify data it deems as non-public data to the Contractor. The level of protection and encryption for all non-public data shall be identified and made a part of this contract.
- d. At no time shall any data or processes — that either belong to or are intended for the use of the State or its officers, agents or employees — be copied, disclosed or retained by the Contractor or any party related to the Contractor for subsequent use in any transaction that does not include the State.
- e. The Contractor shall not use any information collected in connection with the service issued from this proposal for any purpose other than fulfilling the service.

**17.12 DATA LOCATION**

The Contractor shall provide its Services to the State and its end users solely from data centers within the Continental United States. All storage, processing and transmission of State data shall be restricted to information technology systems within the Continental United States. The Contractor shall not allow its personnel or sub-contractors to store State data on portable devices, including personal computers, except as specified and allowed by the contract, and then only on devices that are used and kept at its data centers within the Continental United States. The Contractor shall permit its personnel and Contractors to access State data remotely only to provide technical support and as specified or required by the contract.

**17.13 SECURITY INCIDENT OR DATA BREACH NOTIFICATION**

The Contractor shall inform the State of any security incident or data breach in accordance with NH RSA 359-C.

- a. Incident Response: the Contractor may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the contract. Discussing security incidents with the State should be handled on an urgent as-needed basis, as part of the Contractor communication and mitigation processes as mutually agreed upon, defined by law or contained in the contract.
- b. Security Incident Reporting Requirements: the Contractor shall report a security incident to the appropriate State identified contact immediately as defined in the SLA.
- c. Breach Reporting Requirements: If the Contractor has actual knowledge of a confirmed data breach that affects the security of any State content that is subject to applicable data breach notification law, the Contractor shall (1) promptly notify the appropriate State identified contact within 24 hours or sooner, unless shorter time is required by applicable

**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 2 - INFORMATION TECHNOLOGY PROVISIONS**

---

law, and (2) take commercially reasonable measures to address the data breach in a timely manner.

**17.14 BREACH RESPONSIBILITIES**

This section only applies when a data breach occurs with respect to personal data within the possession or control of the Contractor.

- a. The Contractor, unless stipulated otherwise, shall immediately notify the appropriate State identified contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a security incident.
- b. The Contractor, unless stipulated otherwise, shall promptly notify the appropriate State identified contact within twenty four (24) hours or sooner by telephone, unless shorter time is required by applicable law, if it confirms that there is, or reasonably believes that there has been a data breach. the Contractor shall (1) cooperate with the State as reasonably requested by the State to investigate and resolve the data breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the data breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.
- c. Unless otherwise stipulated, if a data breach is a direct result of the Contractor's breach of its contract obligation to encrypt personal data or otherwise prevent its release, the Contractor shall bear the costs associated with:
  - i. The investigation and resolution of the data breach;
  - ii. Notifications to individuals, regulators or others required by State law;
  - iii. A credit monitoring service required by State (or federal) law;
  - iv. A website or a toll-free number and call center for affected individuals required by State law — all not to exceed the average per record per person cost calculated for data breaches in the United States in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute<sup>17</sup> at the time of the data breach; and
  - v. Complete all corrective actions as reasonably determined by the Contractor based on root cause; all [(i.) through (v.)] subject to this Contract's limitation of liability.

**17.15 NOTIFICATION OF LEGAL REQUESTS**

The Contractor shall contact the State upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the State's data under this contract, or which in any way might reasonably require access to the data of the State. The Contractor shall not respond to subpoenas, service of process and other legal requests related to the State without first notifying the State, unless prohibited by law from providing such notice.

**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 2 - INFORMATION TECHNOLOGY PROVISIONS**

---

**17.16 ACCESS TO SECURITY LOGS AND REPORTS**

The Contractor shall provide reports to the State in a format as agreed to by both the Contractor and the State. Reports shall include latency statistics, user access, user access IP address, user access history and security logs for all State files related to this contract.

**17.17 CONTRACT AUDIT**

The Contractor shall allow the State to audit conformance to the contract terms. The State may perform this audit or contract with a third party at its discretion and at the State's expense.

**17.18 DATA CENTER AUDIT**

The Contractor shall perform an independent audit of its data centers at least annually at its expense, and provide a redacted version of the audit report upon request. The Contractor may remove its proprietary information from the redacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.

**17.19 ADVANCE NOTICE**

The Contractor shall give advance notice (to be determined at the contract time and included in the SLA) to the State of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics. It usually includes a new version number.

**17.20 SECURITY**

The Contractor shall disclose its non-proprietary security processes and technical limitations to the State such that adequate protection and flexibility can be attained between the State and the Contractor. For example: virus checking and port sniffing — the State and the Contractor shall understand each other's roles and responsibilities.

**17.21 NON-DISCLOSURE AND SEPARATION OF DUTIES**

The Contractor shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of State data to that which is absolutely necessary to perform job duties.

**17.22 IMPORT AND EXPORT OF DATA**

The State shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the Contractor. This includes the ability for the State to import or export data to/from other service providers.

**17.23 RESPONSIBILITIES AND UPTIME GUARANTEE**

The Contractor shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the

**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 2 - INFORMATION TECHNOLOGY PROVISIONS**

---

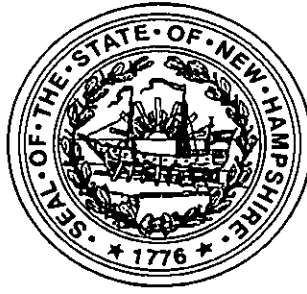
responsibilities of the Contractor. The system shall be available 24/7/365 (with agreed-upon maintenance downtime), and provide service to customers as defined in the SLA.

**17.24 RIGHT TO REMOVE INDIVIDUALS**

The State shall have the right at any time to require that the Contractor remove from interaction with State any the Contractor representative who the State believes is detrimental to its working relationship with the Contractor. The State shall provide the Contractor with notice of its determination, and the reasons it requests the removal. If the State signifies that a potential security violation exists with respect to the request, the Contractor shall immediately remove such individual. The Contractor shall not assign the person to any aspect of the contract or future work orders without the State's consent.

*Remainder of this page intentionally left blank*





**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 3 - EXHIBITS**

**STATE OF NEW HAMPSHIRE**  
**DEPARTMENT OF INFORMATION TECHNOLOGY**  
**COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT**  
**CONTRACT 2018-111**  
**PART 3 – EXHIBIT A**  
**CONTRACT DELIVERABLES**

---

**1. CONTRACT DELIVERABLES**

The State of New Hampshire, Department of Information Technology, (the “State”) requires comprehensive cybersecurity risk assessment of the Executive Branch information technology enterprise. In addition to determining gaps or shortfalls in the State’s cybersecurity posture, a key outcome of this assessment will be a roadmap to improve the security, readiness and effectiveness of the State of New Hampshire’s cybersecurity posture.

As a public entity, the State of New Hampshire is exposed to the full range of cyber threats on a continual basis: malware, botnets, ransomware, and denial of service attacks do not discriminate – any network connected to the Internet is exposed to these threats. The old boundaries of cybersecurity and cyberattacks are disappearing — from the network perimeter, to distinct types of malware, to nation-state tactics vs. that of the cybercriminal. The attacker’s advantage lies in this fluidity, exploiting endpoint vulnerabilities and inadequate security controls; reshaping attacks to evade detection; and repurposing tactics, techniques and procedures for their own use. It has been said that “You don’t know what you don’t know” and to that end, the State of New Hampshire is pursuing an independent, comprehensive cybersecurity risk assessment in order to focus cybersecurity resources on the biggest risks and gaps in our security posture.

**GOALS AND OBJECTIVES FOR THE COMPREHENSIVE CYBERSECURITY RISK ASSESSMENT:**

- i. Independently assess the cybersecurity maturity level as measured against the NIST Cybersecurity Framework and the Center for Internet Security (CIS) 20 Critical Security Controls;
- ii. Review the network architecture, including L2 and L3 routing approach, use of redundant/survivable equipment configurations, use of Firewalls, use of access control lists and remote access methodologies and evaluate its conformance with best practices for a network of this size and complexity;
- iii. Identify any security gaps, prioritize them and describe the level of effort required to mitigate them;
- iv. Discovering non-existent and/or weak information security management processes within the organization;
- v. Identifying opportunities to improve the network architecture, network consolidation, simplification and cost reduction;
- vi. Confirm cyber-protection systems and processes are properly secured from internal and external threats; and
- vii. Prepare and present a technical roadmap to improve the security, readiness and effectiveness of the State of New Hampshire’s cybersecurity posture.

**STATE OF NEW HAMPSHIRE**  
**DEPARTMENT OF INFORMATION TECHNOLOGY**  
**COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT**  
**CONTRACT 2018-111**  
**PART 3 – EXHIBIT A**  
**CONTRACT DELIVERABLES**

---

**1.1 GENERAL PROJECT ASSUMPTIONS**

- 1.1.1 The Contractor will provide project tracking tools and templates to record and manage issues, risks, Change Requests, requirements, decision sheets, and other documents used in the management and tracking of the Project. The State of New Hampshire and the Contractor's Project Managers will Review these tools and templates and determine which ones will be used for the Project. Training on these tools and templates will be conducted at the start of each phase in which they will be used.
- 1.1.2 Prior to the commencement of work on Non-Software and Written Deliverables, the Contractor shall provide to the State a template, table of contents, or agenda for Review and prior approval by the State.
- 1.1.3 The Contractor shall ensure that appropriate levels of security are implemented and maintained in order to protect the integrity and reliability of the State's Information Technology resources, information, and services. Security requirements are defined in Part 3 - Exhibit H: Requirements. The Contractor shall provide the State resources, information, and Services on an ongoing basis, with the appropriate infrastructure and security controls to ensure business continuity and to safeguard the Confidentiality and integrity of State networks, Systems and Data.
- 1.1.4 The Deliverables are set forth in the Schedule described below in Section 2.2. By unconditionally accepting a Deliverable, the State reserves the right to reject any and all Deliverables in the event the State detects any Deficiency in the System, in whole or in part, through completion of all Acceptance Testing, including but not limited to, Software/System Acceptance Testing, and any extensions thereof.
- 1.1.5 Pricing for Deliverables set forth in Part 3 - Exhibit B: Price and Payment Schedule. Pricing will be effective for the Term of this Contract, and any extensions thereof.

**2. DELIVERABLES, MILESTONES, AND ACTIVITIES SCHEDULE**

**2.1 SCOPE OF WORK**

The Contractor will conduct a comprehensive cybersecurity risk assessment of the State's Information Technology (IT) environment in order to evaluate adherence to the State's Information Security Policies, National Institute of Standards and Technology (NIST) standards, and best practices. The assessment shall include a representative sampling of devices (to be defined by the State) from across all Executive Branch agencies. The following services must be provided to meet the Contract requirements:

**2.1. (C-1.1) IT ASSET INVENTORY AND MANAGEMENT**

Provide the State with a comprehensive inventory of all IT assets within the scope of Executive Branch agencies.

**STATE OF NEW HAMPSHIRE**  
**DEPARTMENT OF INFORMATION TECHNOLOGY**  
**COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT**  
**CONTRACT 2018-111**  
**PART 3 – EXHIBIT A**  
**CONTRACT DELIVERABLES**

---

- a. Utilize active and passive discovery tools to identify all devices connected to the State's network and populate a searchable and editable hardware asset inventory.
- b. Ensure that the hardware asset inventory records the network address, hardware address, machine name, Operating System (OS), OS patch level, open ports and running services for each asset that has been detected/discovered on the network.
- c. Assess the current state and capability for a comprehensive IT hardware and software asset inventory and management system.
- d. Optional: Deliver a comprehensive IT hardware and software asset discovery and inventory management system.

**2.1. (C-1.2) NETWORK SECURITY AND ARCHITECTURE ASSESSMENT**

Provide the State with a network architecture review which evaluates the fundamental architecture approach for efficiency, maintainability, throughput, survivability/redundancy and security posture highlighting current strengths and weaknesses of implemented controls. The vendor should consider different assessment scenarios such as level of access and point of access during their assessments.

The Technical Security Assessment Report should include:

- a. Network Topology and Architecture
  - i. From a best practices perspective
  - ii. From a security perspective
- b. Network Segmentation
- c. Network Switch Configuration
- d. Network Access Control (NAC)
- e. Firewalls Configuration
- f. IDP/IDS Configuration
- g. Router Configuration
- h. Virtual Private Network (VPN) Configuration
- i. Wireless Networking Configuration
- j. Remote Sites
- k. Data Centers
- l. Voice Over IP (VoIP) Configuration

**STATE OF NEW HAMPSHIRE**  
**DEPARTMENT OF INFORMATION TECHNOLOGY**  
**COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT**  
**CONTRACT 2018-111**  
**PART 3 – EXHIBIT A**  
**CONTRACT DELIVERABLES**

---

- m. Network based security controls e.g. DLP, Antispam, etc.
- n. Configuration management methodology
  - i. Of Hardware
  - ii. Of software configurations
- o. Optional: Provide technical assistance to actively mitigate critical and high risk findings from the Network Security Assessment.

**2.1. (C-1.3) HOST/SERVER SECURITY ASSESSMENT**

Provide the State with a security focused host/server architecture review, with additional security-related information about the State's host/server operating system configurations that cannot be obtained through network scanning. The additional granularity of the host/server security assessment should enable the State to identify and assess the presence and effectiveness of technical controls and the level of compliance with State policies and other relevant industry standards and best practices. Focus should be given to:

- a. Hardening issues - Provide an in-depth review of a system's security configuration, and evaluating if available the security controls that are being used based on the roles and functions of the host.
- b. Identify known vulnerabilities and OS and 3rd party software issues.
- c. Identify host dependencies from the Service/End User standpoint and interconnection between multiple services which can compromise an end user service.
- d. Optional: Provide technical assistance to actively mitigate critical and high risk findings from the Host/Server Security Assessment.

**2.1. (C-1.4) ENDPOINT SECURITY ASSESSMENT**

The vendor will test a pre-determined sampling of workstations and peripheral endpoints in different departments/divisions from across Executive Branch agencies to perform the assessment. Provide the State with an assessment of endpoints/workstations and end user security against NIST, CIS and industry best practices, including but not limited to:

- a. Workstation Configuration
- b. Anti-Malware

**STATE OF NEW HAMPSHIRE**  
**DEPARTMENT OF INFORMATION TECHNOLOGY**  
**COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT**  
**CONTRACT 2018-111**  
**PART 3 – EXHIBIT A**  
**CONTRACT DELIVERABLES**

---

- c. Endpoint Encryption
- d. User Rights (Local/Domain)
- e. Media Access
- f. Password Practices
- g. OS and Third-Party Software Patching
- h. Peripheral Device (network printers, scanners) configuration
- i. Mobile Device Security and Management
- j. Optional: Provide technical assistance to actively mitigate critical and high risk findings from the Endpoint Security Assessment.

**2.1. (C-1.5) APPLICATION SECURITY ASSESSMENT**

- a. Conduct an Application Security Assessment that analyzes the Internet, Extranet, and Intranet applications for existence and strength of application security controls. Conduct this assessment in accordance to the OWASP top 10 reference and other baselines for application security (e.g. assessment of authentication mechanisms and authorization mechanisms, session context control mechanisms, audit logging, intrusion detection and deterrence).
- b. Conduct Application Security Assessments that target the security capabilities of critical applications. Assess if the applications have capabilities to secure information/data communications and whether the capabilities have been fully utilized. To accomplish this, the Vendor must qualitatively assess vulnerabilities that exist within targeted applications relative to both technical and non-technical security controls.
- c. For State in-house developed applications, the overall security framework used for the application development process must be reviewed.
- d. The application security review should evaluate available security features and security-relevant configuration items within the application to conclude if those controls have been configured to provide the State with the level of protection required by business, regulatory, and corporate drivers.
- e. Optional: Provide technical assistance to actively mitigate critical and high risk findings from the Application Security Assessment.

**STATE OF NEW HAMPSHIRE**  
**DEPARTMENT OF INFORMATION TECHNOLOGY**  
**COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT**  
**CONTRACT 2018-111**  
**PART 3 – EXHIBIT A**  
**CONTRACT DELIVERABLES**

---

**2.1. (C-1.6) DATA SECURITY ASSESSMENT**

Provide the State with an assessment regarding the classification, storage, transmission and use of structured and unstructured data across the Enterprise.

- a. Data classification policies and procedures
- b. Transmission and handling of Sensitive data
- c. Data Access Control
- d. Data Destruction
- e. Privacy policies, protection and compliance
- f. Provide technical assistance to actively mitigate critical and high risk findings from the Data Security Assessment
- g. Optional: Provide administrative assistance to develop and deliver new or updated documentation based on gaps or critical findings from the Data Security Assessment.

**2.1. (C-1.7) CYBERSECURITY AND RISK MANAGEMENT PROGRAM ASSESSMENT**

Provide the state with assessment, gap analysis and a strategic roadmap for improvement against NIST, CIS and best practices in the following program areas:

- a. Cybersecurity Program and Organization
- b. Governance and Compliance Management
- c. Risk Management Policies, Practices and Procedures
- d. User Security Awareness and Training
- e. Security Policies and Procedures
- f. Business Continuity and Disaster Recovery Planning
- g. Optional: Provide administrative assistance to develop and deliver new or updated program documentation based on gaps or critical findings from the Cybersecurity and Risk Management Program Assessment.

**2.2 DELIVERABLES**

Vendor shall create and provide detailed reports to DoIT as a result of analysis and assessment including but not limited to the following:

**STATE OF NEW HAMPSHIRE**  
**DEPARTMENT OF INFORMATION TECHNOLOGY**  
**COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT**  
**CONTRACT 2018-111**  
**PART 3 – EXHIBIT A**  
**CONTRACT DELIVERABLES**

---

- a. An executive summary with objectives, scope, background, summary of findings, and recommendations
- b. A report which uses the NIST Cybersecurity Framework to:
  - i. Describe the State of New Hampshire's current cybersecurity posture;
  - ii. Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process; and
  - iii. Describe the State of New Hampshire's current Framework Implementation Tiers
- c. Identification of the technical or programmatic cyber security gaps.
- d. Recommendations for eliminating, or at least reducing, security gaps and increasing the level of cybersecurity maturity
- e. Summary of areas reviewed / examined along with the methodologies / procedures used
- f. A list of security weaknesses in the form of findings, ranking of risk severity, and a list of prioritized recommendations
- g. A multi-year security improvement roadmap including additional recommendations or future considerations
- h. Recommendations on industry standard security frameworks / best practices to implement
- i. Cost projections for implementing the optional recommendations and roadmap including labor hours and licensing for software tools
- j. Listing of all software tools used to perform the Assessment
- k. Any related reference material

**2.3 DELIVERABLE METHODOLOGY**

For each deliverable that requires the vendor to complete an Assessment the following methodology shall be used:

- a. Vendor shall prepare an outline of the report which includes a scope statement and proposed table of contents for the assessment report and provide it to the State for review and comment.
- b. Vendor shall meet with the State team, no sooner than 5 business days after the outline was provided to discuss the proposed outline and approach.
- c. Upon approval of the outline and approach by the State Project Manager the vendor may commence the analysis/investigation required for the assessment.



**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 3 – EXHIBIT A  
CONTRACT DELIVERABLES**

---

- d. If at any time during the analysis the vendor discovers what they consider to be a critical security vulnerability they shall immediately notify the State Project Manager.
- e. During the assessment the vendor should provide a status update on the assessment during regular project meetings.
- f. Upon completion of the analysis/investigation the vendor shall prepare a draft report in conformance with the approved outline (Step 3) and provide it to the State for review and comment.
- g. Vendor shall, no sooner than 5 business after submitting the draft report, meet with the State team to present the findings and discuss the draft report.
- h. After consideration of the feedback from the State, the vendor shall prepare and submit a final report to the State Project Manager.
- i. After acceptance by the State Project Manager the vendor may invoice for the deliverable.

*Remainder of this page intentionally left blank*

**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 3 – EXHIBIT B  
PRICE AND PAYMENT SCHEDULE**

**1. PAYMENT SCHEDULE**

**1.1 NOT TO EXCEED**

This is a Not to Exceed (NTE) with a maximum Contract value indicated in the Contract Part 1, P-37 General Provisions - Block 1.8: Price Limitation for the period between the Effective Date through the date indicated in Part 1, P-37 General Provisions - Block 1.7: Completion Date. The Contractor shall be responsible for performing its obligations in accordance with the Contract. This Contract will allow the Contractor to invoice the State for the following activities, Deliverables, or milestones appearing in the price and payment tables below:

<b>Table 1.1: Not to Exceed total Project Cost &amp; Payment Dates</b>					
<b>Assessment Number</b>	<b>Task Name</b>	<b>Duration</b>	<b>Estimated Completion Date</b>	<b>Total Deliverable Cost</b>	<b>Invoice Date</b>
C-1.1	IT Asset Inventory and Management	2 Weeks Total (3 Days Onsite)	09/20/19	Included	N/A
C-1.3	Host/Server Security Assessment				
C-1.4	Endpoint Security Assessment				
Meeting	ForeScout CounterACT Final Report Debrief Meeting	3 Hours (Onsite, Scheduling TBD)	09/25/19	Included	N/A

**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 3 – EXHIBIT B  
PRICE AND PAYMENT SCHEDULE**

C-1.2a	Network Security and Architecture Assessment	11 Weeks	11/22/19	\$77,000	11/29/19
C-1.5	Application Security Assessment	7 Weeks	11/22/19	\$49,000	11/29/19
C-1.2b	External Network Penetration Test	3 Weeks	11/15/19	\$21,000	11/22/19
C-1.2c	Internal Network Penetration Test	6 Weeks (*not consecutive weeks, accounting for Holiday periods)	01/17/20	\$42,000	01/24/20
C-1.6	Data Security Assessment				
C-1.7	Cybersecurity and Risk Management Program Assessment	5 Weeks	02/28/20	\$70,000	03/06/20
<b>Assessment Total</b>					<b>\$259,000</b>

**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 3 – EXHIBIT B  
PRICE AND PAYMENT SCHEDULE**

C-2	Optional Services	TBD	As requested	\$240,000 (not to exceed)	TBD
<b>Project Total</b>					<b>\$499,000</b>

**2. CONTRACT PRICE**

- 2.1 Notwithstanding any provision in the Contract to the contrary, and notwithstanding unexpected circumstances, in no event shall the total of all payments made by the State exceed the amount indicated in Part 1, P-37 General Provisions - Block 1.8: Price Limitation. The payment by the State of the total Contract price shall be the only, and the complete reimbursement to the Contractor for all fees and expenses, of whatever nature, incurred by the Contractor in the performance hereof.
- 2.2 The State will not be responsible for any travel or out of pocket expenses incurred in the performance of the Services performed under this Contract. The Contractor must assume all reasonable travel and related expenses. All labor rates will be "Fully Loaded", including, but not limited to: meals, hotel/housing, airfare, car rentals, car mileage, and out of pocket expenses.

**3. INVOICING**

- 3.1 The Contractor shall submit correct invoices to the State for all amounts to be paid by the State. All invoices submitted shall be subject to the State's prior written approval, which shall not be unreasonably withheld. The Contractor shall only submit invoices for Services or Deliverables as permitted by the Contract. Invoices must be in a format as determined by the State and contain detailed information, including without limitation: itemization of each Deliverable and identification of the Deliverable for which payment is sought, and the Acceptance date triggering such payment; date of delivery and/or installation; monthly maintenance charges; any other Project costs or retention amounts if applicable.
- 3.2 Upon Acceptance of a Deliverable, and a properly documented and undisputed invoice, the State will pay the correct and undisputed invoice within thirty (30) days of invoice receipt. Invoices will not be backdated and shall be promptly dispatched.
- 3.3 ALL INVOICES SHALL BE SENT TO:  
DEPARTMENT OF INFORMATION TECHNOLOGY  
BFA  
27 HAZEN DRIVE  
CONCORD, NH 03301

**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 3 – EXHIBIT B  
PRICE AND PAYMENT SCHEDULE**

---

**4. PAYMENT ADDRESS**

4.1 ALL PAYMENTS SHALL BE SENT TO THE FOLLOWING ADDRESS:

FINANCE DEPARTMENT  
NuHARBOR SECURITY  
39 RIVER ROAD, SUITE 4  
ESSEX JUNCTION, VT 05452

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

**5. OVERPAYMENTS TO THE CONTRACTOR**

The Contractor shall promptly, but no later than fifteen (15) business days, return to the State the full amount of any overpayment or erroneous payment upon discovery or notice from the State.

**6. CREDITS**

The State may apply credits due to the State arising out of this Contract, against the Contractor's invoices with appropriate information attached.

**7. PROJECT HOLDBACK**

The State shall withhold ten percent (10%) of the last milestone payment for each assessment Deliverable as set forth in the Payment Table above, until successful conclusion of the Warranty Period.

*Remainder of this page intentionally left blank*

**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 3 – EXHIBIT C  
SPECIAL PROVISIONS**

---

Exhibit C – There are no changes to the terms outlined in the P-37 General Provisions

*Remainder of this page intentionally left blank*

**STATE OF NEW HAMPSHIRE**  
**DEPARTMENT OF INFORMATION TECHNOLOGY**  
**COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT**  
**CONTRACT 2018-111**  
**PART 3 – EXHIBIT D**  
**ADMINISTRATIVE SERVICES**

---

**1. TRAVEL EXPENSES**

The Contractor must assume all reasonable travel and related expenses. All labor rates will be “Fully Loaded”, including, but not limited to: meals, hotel/housing, airfare, car rentals, car mileage, and out of pocket expenses.

**2. SHIPPING AND DELIVERY FEE EXEMPTION**

The State will not pay for any shipping or delivery fees unless specifically itemized in the Contract.

**3. ACCESS/COOPERATION**

- 3.1 As applicable, and subject to the applicable laws and regulations, the State will provide the Contractor with access to all program files, libraries, personal computer-based Systems, Software packages, network Systems, security Systems, and hardware as required to complete the Contracted Services.
- 3.2 The State will use reasonable efforts to provide approvals, authorizations, and decisions reasonably necessary to allow the Contractor to perform its obligations under the Contract.

**4. STATE-OWNED DOCUMENTS AND COPYRIGHT PRIVILEGES**

The Contractor shall provide the State access to all State-owned documents, materials, reports, and other work in progress relating to this Contract. Upon expiration or termination of the Contract with the State, the Contractor shall turn over all State-owned documents, material, reports, and work in progress relating to this Contract to the State at no additional cost to the State. Documents must be provided in both printed and electronic format.

**5. RECORDS RETENTION AND ACCESS REQUIREMENTS**

- 5.1 The Contractor shall agree to the conditions of all applicable State and federal laws and regulations, which are incorporated herein by reference, regarding retention and access requirements, including without limitation, retention policies consistent with the Federal Acquisition Regulations (FAR) Subpart 4.7: Contractor Records Retention.
- 5.2 The Contractor and its Subcontractors shall maintain books, records, documents, and other evidence of accounting procedures and practices, which properly and sufficiently reflect all direct and indirect costs invoiced in the performance of their respective obligations under the Contract. The Contractor and its Subcontractors shall retain all such records for three (3) years following termination of the Contract, including any extensions. Records relating to any litigation matters regarding the Contract shall be kept for one (1) year following the termination of all litigation, including the termination of all appeals or the expiration of the appeal period.
- 5.3 Upon prior notice and subject to reasonable time frames, all such records shall be subject to inspection, examination, audit and copying by personnel so authorized by the State and federal

**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 3 – EXHIBIT D  
ADMINISTRATIVE SERVICES**

---

officials so authorized by law, rule, regulation or Contract, as applicable. Access to these items shall be provided within Merrimack County of the State of New Hampshire, unless otherwise agreed by the State. Delivery of and access to such records shall be at no cost to the State during the three (3) year period following termination of the Contract and one (1) year term following litigation relating to the Contract, including all appeals or the expiration of the appeal period. The Contractor shall include the record retention and Review requirements of this section in any of its subcontracts.

- 5.4** The State agrees that books, records, documents, and other evidence of accounting procedures and practices related to the Contractor's cost structure and profit factors shall be excluded from the State's Review unless the cost of any other Services or Deliverables provided under the Contract is calculated or derived from the cost structure or profit factors.

**6. ACCOUNTING REQUIREMENTS**

The Contractor shall maintain an accounting System in accordance with Generally Accepted Accounting Principles. The costs applicable to the Contract shall be ascertainable from the accounting System and the Contractor shall maintain records pertaining to the Services and all other costs and expenditures.

*Remainder of this page intentionally left blank*



**STATE OF NEW HAMPSHIRE**  
**DEPARTMENT OF INFORMATION TECHNOLOGY**  
**COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT**  
**CONTRACT 2018-111**

**PART 3 – EXHIBIT E**  
**MANAGED AND PROFESSIONAL INFORMATION SECURITY SERVICES**

---

**1. STATE MEETING AND REPORTS**

- 1.1** The State believes that effective communication and reporting are essential to Project success.
- 1.2** The Contractor Key Project Staff shall participate in meetings as requested by the State, in accordance with the requirements and terms of this Contract.
- a. Introductory Meeting:** Participants will include the Contractor's Key Project Staff and State Project leaders from both the Department of Information Technology and The Contractor. This meeting will enable leaders to become acquainted and establish any preliminary Project procedures.
  - b. Kickoff Meeting:** Participants will include the State and the Contractor's Project Team and major stakeholders. This meeting is to establish a sound foundation for activities that will follow.
  - c. Status Meetings:** Participants will include, at the minimum, the Contractor's Project Manager and the State Project Manager. These meetings will be conducted at least bi-weekly and address overall Project status and any additional topics needed to remain on Schedule and within budget. A status and error report from the Contractor shall serve as the basis for discussion.
  - d. The Work Plan:** must be Reviewed at each Status Meeting and updated, at minimum, on a bi-weekly basis, in accordance with the Contract.
  - e. Special Meetings:** Need may arise for a special meeting with State leaders or Project stakeholders to address specific issues.
  - f. Exit Meeting:** Participants will include Project leaders from the Contractor and the State. Discussion will focus on lessons learned from the Project and on follow up options that the State may wish to consider.
- 1.3** The State expects the Contractor to prepare agendas and background for and minutes of meetings. Background for each status meeting must include an updated Work Plan. Drafting of formal presentations, such as a presentation for the kickoff meeting, will also be the Contractor's responsibility.
- 1.4** The Contractor's Project Manager or the Contractor's Key Project Staff shall submit monthly status reports in accordance with the Schedule and terms of this Contract. All status reports shall be prepared in formats approved by the State. The Contractor's Project Manager shall assist the State's Project Manager, or itself produce reports related to Project Management as reasonably requested by the State, all at no additional cost to the State. The Contractor shall produce Project status reports, which shall contain, at a minimum, the following:
- a.** Project status related to the Work Plan;
  - b.** Deliverable status;
  - c.** Accomplishments during weeks being reported;
  - d.** Planned activities for the upcoming two (2) week period;

**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111**

**PART 3 – EXHIBIT E**

**MANAGED AND PROFESSIONAL INFORMATION SECURITY SERVICES**

---

- e. Future activities;
  - f. Issues and concerns requiring resolution; and
  - g. Report and remedies in case of falling behind Schedule.
- 1.5 As reasonably requested by the State, the Contractor shall provide the State with information or reports regarding the Project. The Contractor shall prepare special reports and presentations relating to Project Management, and shall assist the State in preparing reports and presentations, as reasonably requested by the State, all at no additional cost to the State.

## **2. ASSESSMENT STRATEGY**

### **2.1 KEY COMPONENTS**

The Contractor shall employ an industry-standard Implementation strategy with a timeline set forth in accordance with the Work Plan:

- a. The Contractor and the State shall adopt a change management approach to identify and plan key strategies and communication initiatives.
- b. The Contractor's team will provide training templates as defined in the Training Plan, which will be customized to address the State's specific requirements. Decisions regarding format, content, style, and presentation shall be made early on in the process, by the State, providing sufficient time for development of material as functionality is defined and configured.
- c. The Contractor shall manage Project execution and provide the tools needed to create and manage the Project's Work Plan and tasks, manage and Schedule Project staff, track and manage issues, manage changing requirements, maintain communication within the Project Team, and report status.
- d. The Contractor shall adopt an Implementation time-line aligned with the State's required time-line.

### **2.2 TIMELINE**

The timeline is set forth in the Work Plan. During the initial planning period Project task and resource plans will be established for: the preliminary training plan, the change management plan, communication approaches, Project standards and procedures finalized, and team training initiated. Timing will be structured to recognize interdependencies between applications and structure a cost effective and timely execution. Processes will be documented, training established, and the application will be ready for Implementation in accordance with the Work Plan.

### **2.3 CHANGE MANAGEMENT AND TRAINING**

The Contractor's change management and training services shall be focused on developing change management and training strategies and plans. Its approach relies on State resources for the execution of the change management and end user training.

**STATE OF NEW HAMPSHIRE**  
**DEPARTMENT OF INFORMATION TECHNOLOGY**  
**COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT**  
**CONTRACT 2018-111**  
**PART 3 – EXHIBIT E**  
**MANAGED AND PROFESSIONAL INFORMATION SECURITY SERVICES**

---

*Remainder of this page intentionally left blank*

**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 3 – EXHIBIT F  
TESTING SERVICES**

---

Exhibit F – Not Applicable to this Contract

*Remainder of this page intentionally left blank*

**STATE OF NEW HAMPSHIRE**  
**DEPARTMENT OF INFORMATION TECHNOLOGY**  
**COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT**  
**CONTRACT 2018-111**  
**PART 3 - EXHIBIT G**  
**MAINTENANCE AND SUPPORT SERVICES**

---

Exhibit G – Not Applicable to this Contract

*Remainder of this page intentionally left blank*

**STATE OF NEW HAMPSHIRE**  
**DEPARTMENT OF INFORMATION TECHNOLOGY**  
**COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT**  
**CONTRACT 2018-111**  
**PART 3 – EXHIBIT H**  
**REQUIREMENTS**

---

Exhibit H – Attachment 1: Project Requirements is hereby incorporated within.

*Remainder of this page intentionally left blank*

**STATE OF NEW HAMPSHIRE**  
**DEPARTMENT OF INFORMATION TECHNOLOGY**  
**COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT**  
**CONTRACT 2018-111**  
**PART 3 – EXHIBIT I**  
**WORK PLAN**

---

The Contractor's Project Manager and the State Project manager shall finalize the Work Plan for Implementation within thirty (30) business days of the Effective Date and further refine the tasks required to implement the Project. Continued development and management of the Work Plan is a joint effort on the part of the Contractor and State Project Managers.

The preliminary Work Plan for Project execution created by the Contractor and the State is set forth at the end of this Exhibit.

In conjunction with the Contractor's Project Management methodology, which shall be used to manage the Project's life cycle, the Contractor team and the State shall finalize the Work Plan at the onset of the Project. This plan shall identify the tasks, Deliverables, major milestones, task dependencies, and a payment Schedule required to implement the Project. It shall also address intra-task dependencies, resource allocations (both State and Contractor's team members), refine the Project's scope, and establish the Project's Schedule. The Plan is documented in accordance with the Contractor's Work Plan and shall utilize software that is agreed upon by both parties to support the ongoing management of the Project.

## **1. ASSUMPTIONS**

### **1.1 GENERAL**

- a. The State shall provide team members with decision-making authority to support the Implementation efforts, at the level outlined in the Request for Proposal Document State Staffing Matrix.
- b. All State tasks must be performed in accordance with the revised Work Plan.
- c. All key decisions will be resolved within five (5) business days. Issues not resolved within this initial period will be escalated to the State Project Manager for resolution.
- d. Any activities, decisions or issues taken on by the State that affect the mutually agreed upon Work Plan timeline, scope, resources, and costs shall be subject to the identified Change Control process.
- e. The Contractor shall maintain an accounting System in accordance with Generally Accepted Accounting Principles (GAAP).

### **1.2 PROJECT MANAGEMENT**

- a. The State shall approve the Project Management Methodology used for the Project.
- b. The State shall provide the Project Team with reasonable access to the State personnel as needed to complete Project tasks.
- c. A Project folder created within the State System shall be used for centralized storage and retrieval of Project documents, work products, and other material and information relevant to the success of the Project and required by Project Team members. This central repository is secured by determining which team members have access to the Project folder and granting either view or read/write privileges. The Contractor's

**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 3 – EXHIBIT I  
WORK PLAN**

---

Project Manager will establish and maintain this folder. The State Project Manager shall approve access for the State team. Documentation can be stored locally for the Contractor and State team on a “shared” network drive to facilitate ease and speed of access. Final versions of all Documentation shall be loaded to the State System.

- d. The Contractor assumes that an Alternate Project Manager may be appointed from time to time to handle reasonable and ordinary absences of the Project Manager.

**1.3 CONVERSIONS (NOT APPLICABLE)**

The Contractor Team’s proposal is based on the assumption that the State’s technical team is capable of implementing, with assistance from the Contractor’s technical team, a subset of the conversions. The Contractor’s Team shall lead the State with the mapping of the legacy Data to the Contractor’s applications. Additionally, the Contractor’s Team shall:

- a. Provide the State with Contractor’s application Data requirements and examples, of Data mappings, conversion scripts, and Data loaders. The Contractor’s Team shall identify the APIs the State should use in the design and development of the conversion.
- b. Provide guidance and assistance with the use of the Data loaders and conversion scripts provided.
- c. Lead the Review of functional and technical Specifications.
- d. Assist with the resolution of problems and issues associated with the development and Implementation of the conversions.

**1.4 PROJECT SCHEDULE**

The project is planned to begin within 30 days of contract approval.

**1.5 REPORTING**

The Contractor shall conduct status meetings, and provide reports that include, but are not limited to, minutes, action items, test results, and Documentation as mutually agreed upon.

**1.6 USER TRAINING (NOT APPLICABLE)**

- a. The Contractor’s Team shall lead the development of the end-user training plan.
- b. Train the trainer approach shall be used for the delivery of end-user training.
- c. The State is responsible for the delivery of end-user training.
- d. The State shall Schedule and track attendance on all end-user training classes.

**1.7 SCENARIO TESTING**

The Contractor’s Team shall provide a test workshop to identify the key scenarios to be tested, the approach and tools required, and best practices information on performance testing.



**STATE OF NEW HAMPSHIRE**  
**DEPARTMENT OF INFORMATION TECHNOLOGY**  
**COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT**  
**CONTRACT 2018-111**  
**PART 3 – EXHIBIT I**  
**WORK PLAN**

---

**2. CONTRACTOR ROLES AND RESPONSIBILITIES**

**2.1 CONTRACTOR'S TEAM PROJECT EXECUTIVE**

The Contractor Team's Project Executives (Contractor and Subcontractor Project Executives) shall be responsible for advising on and monitoring the quality of the Services throughout the Project life cycle. The Project Executive shall advise the Contractor Team Project Manager and the State's Project leadership on the best practices for implementing the Contractor Software Solution within the State. The Project Executive shall participate in the definition of the Project Plan and provide guidance to the State's Team.

**2.2 CONTRACTOR'S TEAM PROJECT MANAGER**

The Contractor Team Project Manager shall have overall responsibility for the day-to-day management of the Project and shall plan, track, and manage the activities of the Contractor's Implementation Team. The Contractor Team Project Manager will have the following responsibilities:

- a. Maintain communications with the State's Project Manager;
- b. Work with the State in planning and conducting a kick-off meeting;
- c. Create and maintain the Work Plan;
- d. Assign the Contractor Team consultants to tasks in the Implementation Project according to the scheduled staffing requirements;
- e. Define roles and responsibilities of all the Contractor Team members;
- f. Provide updated progress reports to the State Project Manager upon request;
- g. Notify the State Project Manager of requirements for State resources in order to provide sufficient lead time for resources to be made available;
- h. Review task progress for time, quality, and accuracy in order to achieve progress;
- i. Review requirements and scheduling changes and identify the impact on the Project in order to identify whether the changes may require a change of scope;
- j. Implement scope and schedule changes as authorized by the State Project Manager and with appropriate Change Control approvals as identified in the Implementation Plan;
- k. Inform the State Project Manager and staff of any urgent issues if and when they arise;
- l. Provide the State completed Project Deliverables and obtain sign-off from the State's Project Manager;
- m. Manage handoff to the Contractor operational staff;
- n. Manage Transition Services as needed.

**STATE OF NEW HAMPSHIRE**  
**DEPARTMENT OF INFORMATION TECHNOLOGY**  
**COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT**  
**CONTRACT 2018-111**  
**PART 3 – EXHIBIT I**  
**WORK PLAN**

---

**2.3 CONTRACTOR'S TEAM ANALYSIS**

The Contractor Team shall conduct analysis of requirements, validate the Contractor Team's understanding of the State business requirements by application, and perform business requirements mapping:

- a. Construct and confirm application test case scenarios;
- b. Produce application configuration definitions and configure the applications;
- c. Conduct testing of the configured application;
- d. Conduct follow-up meetings to obtain feedback, results, and concurrence/approval from the State;

**2.4 CONTRACTOR'S TEAM TASKS**

The Contractor team shall assume the following tasks:

- a. Development and Review of functional and technical Specification to determine that they are at an appropriate level of detail and quality;

**3. STATE ROLES AND RESPONSIBILITIES**

The following State resources have been identified for the Project. The time demands on the individual State team members will vary depending on the phase and specific tasks of the Implementation. The demands on the Subject Matter Experts' time will vary based on the need determined by the State Leads and the phase of the Implementation.

**3.1 STATE PROJECT MANAGER**

The State Project Manager shall work side-by-side with the Contractor's Project Manager. The role of the State Project Manager is to manage State resources (IF ANY), facilitate completion of all tasks assigned to State staff, and communicate Project status on a regular basis. The State Project Manager represents the State in all decisions on Implementation Project matters, provides all necessary support in the conduct of the Implementation Project, and provides necessary State resources, as defined by the Work Plan and as otherwise identified throughout the course of the Project. The State Project Manager has the following responsibilities:

- a. Plan and conduct a kick-off meeting with assistance from the Contractor's team;
- b. Assist the Contractor's Project Manager in the development of a detailed Work Plan;
- c. Identify and secure the State Project Team members in accordance with the Work Plan;
- d. Define roles and responsibilities of all State Project Team members assigned to the Project;

**STATE OF NEW HAMPSHIRE**  
**DEPARTMENT OF INFORMATION TECHNOLOGY**  
**COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT**  
**CONTRACT 2018-111**  
**PART 3 – EXHIBIT I**  
**WORK PLAN**

---

- e. Identify and secure access to additional State end-user staff as needed to support specific areas of knowledge if and when required to perform certain Implementation tasks;
- f. Communicate issues to State management as necessary to secure resolution of any matter that cannot be addressed at the Project level;
- g. Inform the Contractor's Project Manager of any urgent issues if and when they arise;
- h. Assist the Contractor's team staff to obtain requested information if and when required to perform certain Project tasks;
- i. Manage handoff to State operational staff; and
- j. Manage State staff during Transition Services as needed.

**3.2 STATE SUBJECT MATTER EXPERT(S) (SME)**

The role of the State SME is to assist application teams with an understanding of the State's current business practices and processes, provide agency knowledge, and participate in the Implementation. Responsibilities of the SME include the following:

- a. Be the key user and contact for their Agency or Department;
- b. Attend Project Team training and acquire in-depth functional knowledge of the relevant applications;
- c. Assist in validating and documenting user requirements, as needed;
- d. Assist in mapping business requirements;
- e. Assist in constructing test scripts and Data; AND
- f. Attend Project meetings when requested.

**3.3 STATE TECHNICAL LEAD**

The State's Technical Lead reports to the State's Project Manager and is responsible for leading and managing the State's technical tasks. Responsibilities include:

- a. Attend technical training as necessary to support the Project;
- b. Assist the State and the Contractor's Team Project Managers to establish the detailed Work Plan;
- c. Manage the day-to-day activities of the State's technical resources assigned to the Project;
- d. Work with State IT management to obtain State technical resources in accordance with the Work Plan;
- e. Work in partnership with the Contractor and lead the State technical staff's efforts in documenting the technical operational procedures and processes for the Project. This

**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 3 – EXHIBIT I  
WORK PLAN**

is a Contractor Deliverable and it will be expected that the Contractor will lead the overall effort with support and assistance from the State; and

f. Represent the technical efforts of the State at Project meetings as requested.

4. SOFTWARE APPLICATION (NOT APPLICABLE)
5. CONVERSIONS (NOT APPLICABLE)
6. INTERFACES (NOT APPLICABLE)
7. APPLICATION MODIFICATION (NOT APPLICABLE)
8. PRELIMINARY WORK PLAN

The following Table 8.1 provides the preliminary agreed upon Work Plan for the Contract.

Table 8.1: High Level Preliminary NH Project Plan				
Assessment Number	Task Name	Duration	Start	Finish
C-1.1	IT Asset Inventory and Management	2 Weeks Total (3 Days Onsite)	9-Sep-19	20-Sep-19
C-1.3	Host/Server Security Assessment			
C-1.4	Endpoint Security Assessment			
Meeting	ForeScout CounterACT Final Report Debrief Meeting	3 Hours (Onsite, Scheduling TBD)	25-Sep-19	25-Sep-19

**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 3 – EXHIBIT I  
WORK PLAN**

C-1.2	Network Security and Architecture Assessment	11 Weeks	9-Sep-19	22-Nov-19
C-1.5	Application Security Assessment	7 Weeks	7-Oct-19	22-Nov-19
C-1.5a	External Network Penetration Test	3 Weeks	28-Oct-19	15-Nov-19
C-1.5b	Internal Network Penetration Test	6 Weeks (*not consecutive weeks, accounting for Holiday periods)	18-Nov-19	17-Jan-20
C-1.6	Data Security Assessment			
C-1.7	Cybersecurity and Risk Management Program Assessment	5 Weeks	27-Jan-20	28-Feb-20

*Remainder of this page intentionally left blank*

**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 3 – EXHIBIT J  
SOFTWARE AGREEMENT**

---

Exhibit J – Not Applicable to this Contract

*Remainder of this page intentionally left blank*

**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 3 – EXHIBIT K  
WARRANTY & WARRANTY SERVICE**

---

**1. WARRANTIES**

**1.1 SYSTEM (NOT APPLICABLE)**

The Contractor warrants that the Deliverables will operate and conform to the Specifications, terms, and requirements of the Contract.

**1.2 SOFTWARE (NOT APPLICABLE)**

**1.2.1** The Contractor warrants that the Deliverable, including but not limited to the individual modules or functions furnished under the Contract, is properly functioning within the System, compliant with the requirements of the Contract, and will operate in accordance with the Specifications and Terms of the Contract.

**1.2.2** For any Breach of the above Software Warranty, the State's remedy, and the Contractor's entire liability, shall be:

- a. The correction of program errors that cause Breach of the Warranty, or if the Contractor cannot substantially correct such Breach in a commercially reasonable manner, the State may end its program license if any and recover the fees paid to the Contractor for the program license and any unused, prepaid technical support fees the State has paid for the program license; or
- b. The re-performance of the deficient Services; or
- c. If the Contractor cannot substantially correct a Breach in a commercially reasonable manner, the State may end the relevant Services and recover the fees paid to the Contractor for the deficient Services.

**1.3 NON-INFRINGEMENT**

The Contractor warrants that it has good title to, or the right to allow the State to use, all Services, equipment, and Software ("Material") provided under this Contract, and that such Services, equipment, and Software do not violate or infringe any patent, trademark, copyright, trade name or other intellectual property rights or misappropriate a trade secret of any third party.

**1.4 VIRUSES; DESTRUCTIVE PROGRAMMING**

The Contractor warrants that all Software used shall not contain any viruses, destructive programming, or mechanisms designed to disrupt the performance of the State of New Hampshire Network and Systems in accordance with the Specifications.

**1.5 COMPATIBILITY (NOT APPLICABLE)**

The Contractor warrants that all System components, including but not limited to the components provided, including any replacement or upgraded System Software components

**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 3 – EXHIBIT K  
WARRANTY & WARRANTY SERVICE**

---

provided by the Contractor to correct Deficiencies or as an Enhancement, shall operate with the rest of the System without loss of any functionality.

**1.6 SERVICES**

The Contractor warrants that all Services to be provided under the Contract will be provided expediently, in a professional manner, in accordance with industry standards and that Services will comply with performance standards, Specifications, and terms of the Contract.

**1.7 PERSONNEL**

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.

**1.8 BREACH OF DATA**

The Contractor shall be solely liable for costs associated with any Breach of State Data housed at their location(s) including but not limited to notification and any damages assessed by the courts.

**2. WARRANTY PERIOD**

The Warranty Period shall remain in effect until the conclusion or termination of this Contract and any extensions, with the exception of the Warranty for non-infringement, which shall survive the termination of this Contract.

*Remainder of this page intentionally left blank*



**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 3 – EXHIBIT L  
TRAINING SERVICES**

---

Exhibit L – Not Applicable to this Contract

*Remainder of this page intentionally left blank*

**STATE OF NEW HAMPSHIRE**  
**DEPARTMENT OF INFORMATION TECHNOLOGY**  
**COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT**  
**CONTRACT 2018-111**  
**PART 3 – EXHIBIT M**  
**AGENCY RFP WITH ADDENDUMS, BY REFERENCE**

---

State of New Hampshire, Department of Information Technology RFP 2018-111 Comprehensive Cyber Security Risk Assessment is hereby incorporated by reference as fully set forth herein.

*Remainder of this page intentionally left blank*

**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 3 – EXHIBIT N  
VENDOR PROPOSAL, BY REFERENCE**

---

Vendor Proposal Response to RFP 2018-111 Comprehensive Cyber Security Risk Assessment dated February 14, 2019 is hereby incorporated by reference as fully set forth herein.

*Remainder of this page intentionally left blank*

**STATE OF NEW HAMPSHIRE  
DEPARTMENT OF INFORMATION TECHNOLOGY  
COMPREHENSIVE CYBER SECURITY RISK ASSESSMENT  
CONTRACT 2018-111  
PART 3 – EXHIBIT O  
CERTIFICATES AND ATTACHMENTS**

---

Attached are:

- A. Exhibit H Requirements – Attachment 1
- B. Contractor's Certificate of Good Standing
- C. Contractor's Certificate of Vote/Authority
- D. Contractor's Certificate of Insurance

*Remainder of this page intentionally left blank*

# State of New Hampshire

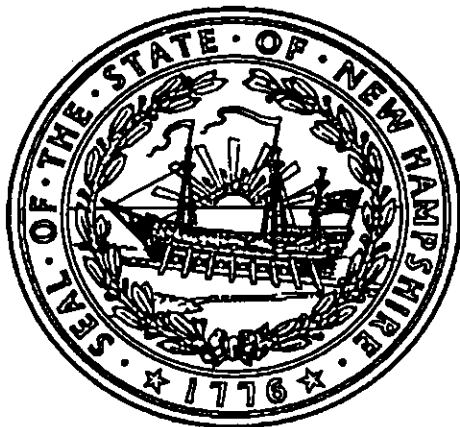
## Department of State

### CERTIFICATE

I, William M. Gardner, Secretary of State of the State of New Hampshire, do hereby certify that NUHARBOR SECURITY INC. is a Vermont Profit Corporation registered to transact business in New Hampshire on November 18, 2015. 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: 735135

Certificate Number: 0004534898



IN TESTIMONY WHEREOF,  
I hereto set my hand and cause to be affixed  
the Seal of the State of New Hampshire,  
this 1st day of July A.D. 2019.

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

William M. Gardner  
Secretary of State

CERTIFICATE OF VOTE  
(Corporation With Seal)

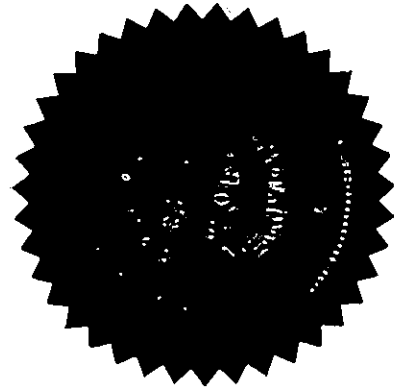
I, **Justin Fimlaid**, do hereby represent and certify that:

- (1) I am **Managing Director** of **NuHarbor Security**, an **S-corporation** (the "Corporation").
- (2) I maintain and have custody of and am familiar with the Seal and the minutes of the Corporation.
- (3) I am duly authorized to issue certificates with respect to the contents of such books.
- (4) The following statements are true and accurate based on the resolutions adopted by the Board of Directors of the Corporation at a meeting of the said Board of Directors held on **August 3<sup>rd</sup>, 2018**, which meeting was duly held in accordance with **Vermont** law and the by-laws of the Corporation.
- (5) The signature of **Katherine Cheney**, **Director** of this Corporation affixed to any contract instrument or document shall bind the corporation to the terms and conditions of the contract instrument or document.
- (6) The foregoing signature authority has not been revoked, annulled or amended in any manner whatsoever, and remains in full force and effect as of the date hereof.

IN WITNESS WHEREOF, I have hereunto set my hand as **Managing Director** of the Corporation and have affixed its corporate seal this **19<sup>th</sup> of August, 2019**.

  
Justin Fimlaid, **Managing Director**, 8/19/19

(SEAL)

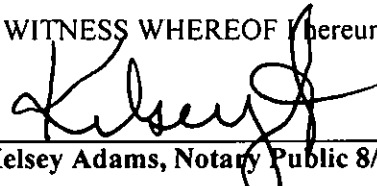


STATE OF **Vermont**

COUNTY OF **Chittenden**

On this the **19<sup>th</sup>** day of **August, 2019**, before me, **Justin Fimlaid**, personally appeared and acknowledged himself to be the **Managing Director**, of **NuHarbor Security**, a **Vermont** corporation, and that she/he, as such being authorized to do so, executed the foregoing instrument.

IN WITNESS WHEREOF I hereunto set my hand and official seal.

  
Kelsey Adams, **Notary Public** 8/19/19

My Commission Expires: **January 31, 2021**



# CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)

9/17/2019

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

**IMPORTANT:** If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

<b>PRODUCER</b> Winooski, LLC 2300 St. George Road Williston VT 05495		<b>CONTACT NAME:</b> Tracie Higgins <b>PHONE (A/C, No, Ext):</b> (802) 655-9000 <b>E-MAIL ADDRESS:</b> tracieh@winooski.com <b>FAX (A/C, No):</b> (802) 871-5609	
<b>INSURED</b> NuHarbor Security, Inc. 39 River Road #4 Essex Jct VT 05452		<b>INSURER(S) AFFORDING COVERAGE</b> <b>INSURER A:</b> Travelers Property Casualty Ins Co <b>INSURER B:</b> <b>INSURER C:</b> <b>INSURER D:</b> <b>INSURER E:</b> <b>INSURER F:</b>	
		<b>NAIC #</b> 36161	

**COVERAGES**      **CERTIFICATE NUMBER:** CL1991717121      **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR HYD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS
A	<input checked="" type="checkbox"/> COMMERCIAL GENERAL LIABILITY <input type="checkbox"/> CLAIMS-MADE <input checked="" type="checkbox"/> OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: <input type="checkbox"/> POLICY <input type="checkbox"/> PRO-JECT <input type="checkbox"/> LOC <input type="checkbox"/> OTHER:			2986752B	9/17/2019	9/17/2020	EACH OCCURRENCE \$ 2,000,000 DAMAGE TO RENTED PREMISES (Ea occurrence) \$ 100,000 MED EXP (Any one person) \$ 5,000 PERSONAL & ADV INJURY \$ Not Included GENERAL AGGREGATE \$ 4,000,000 PRODUCTS - COMP/OP AGG \$ 4,000,000 \$
A	AUTOMOBILE LIABILITY <input type="checkbox"/> ANY AUTO ALL OWNED AUTOS <input checked="" type="checkbox"/> HIRED AUTOS <input checked="" type="checkbox"/> SCHEDULED AUTOS NON-OWNED AUTOS			2986752B	9/17/2019	9/17/2020	COMBINED SINGLE LIMIT (Ea accident) \$ 2,000,000 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 <input type="checkbox"/> DED <input type="checkbox"/> RETENTION \$						EACH OCCURRENCE \$ AGGREGATE \$ \$
	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below	Y/N	N/A				<input type="checkbox"/> PER STATUTE <input type="checkbox"/> OTHER E.L. EACH ACCIDENT \$ E.L. DISEASE - EA EMPLOYEE \$ E.L. DISEASE - POLICY LIMIT \$
A	Cyber Liability Professional Liability			2986752B 2986752B	9/17/2019 9/17/2019	9/17/2020 9/17/2020	Aggregate 5,000,000 Aggregate 5,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

**CERTIFICATE HOLDER****CANCELLATION**

State of NH - Department of Information T Attn: Denis Goulet 27 Hazen Drive 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 Tracie Higgins/TRH <i>Tracie Higgins</i>
--------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

© 1988-2014 ACORD CORPORATION. All rights reserved.