



info@nuharborsecurity.com  
nuharborsecurity.com  
(800) 917-5719

November 18, 2021

Region 14 Education Service Center  
1850 TX-351  
Abilene, Texas 79601

Submitted via the NCPA Bonfire Portal: <https://ncpa.bonfirehub.com/opportunities/52831>

NuHarbor Security, Inc. is pleased to submit to the Region 14 Education Service Center our response to **RFP # 34-21 for “Cyber-Security Solutions, Malware, Ransomware Protection, Other Related Products and Services.”** This due diligence initiative to make quality cybersecurity solutions more accessible and affordable for public agencies seeking to elevate their security postures is timely and wise. At no other time have security infrastructures been as vulnerable—new threats are emerging at an unprecedented rate, and proactive risk reduction is essential for the protection of users and information assets.

NuHarbor Security is a leading national information consulting and advisory firm providing tactical and strategic cybersecurity services from our headquarters in Colchester, VT, and strategically located regional offices in New York, NY; Boston, MA; Washington, DC; Charlotte, NC; Atlanta, GA; and Miami, FL. Since 2014, NuHarbor has helped its client partners design, implement, and sustain comprehensive Information Security, Compliance, and Risk Management programs. **Our firm is led by a team of highly certified former Fortune 500 Chief Information Security Officers (CISOs) and industry Information Security Directors who offer years of hands-on experience working alongside clients to deliver actionable results.** We proudly deliver end-to-end security solutions and services to an extensive roster of both public sector and commercial clients. From small private companies and higher education institutions to local governments and large state agencies, we serve as their “Trusted Advisor” for best-in-breed information security services.

NuHarbor stands apart from other providers of professional security services because **we are 100% focused on the information security sector.** We define our methodologies and services in accordance with industry best practices and standards like NIST, ISO, CIS, PCI, HIPAA, and other major guidelines. NuHarbor has an unwavering commitment to keeping our hands on the pulse of this rapidly growing and increasingly complex industry. Our innovation and thought leadership challenge traditional methodologies and promote a new understanding of sustainable information security. Security is our core business mission.

NuHarbor works with public agencies most often and most successfully, having offered our award-winning Managed Services to governmental and educational organizations of many sizes since our inception. Our qualifications described in the following proposal demonstrate not only NuHarbor’s comprehensive security approach and technical expertise, but our deep commitment to keeping the diverse security postures of our clients safe and secure. Our client-first perspective makes us the ideal long-term security partner – we can help safeguard your assets today and will remain committed to your security as more sophisticated threats emerge.



info@nuharborsecurity.com  
nuharborsecurity.com  
(800) 917-5719

Should you have any questions or seek clarification, please contact me directly via phone, (802) 448-4394, or via email, [smosher@nuharborsecurity.com](mailto:smosher@nuharborsecurity.com).

Sincerely,

Scott Mosher  
Vice President

<b>Company Name</b>	NuHarbor Security, Inc.		
<b>Address</b>	553 Roosevelt Hwy, #102 Colchester, VT 05446	<b>Main Phone</b>	(802) 448-9058
<b>Website</b>	<a href="http://www.nuharborsecurity.com">http://www.nuharborsecurity.com</a>		
<b>Authorized Officer</b>	<b>Scott Mosher</b> Vice President   Principal Officer <a href="mailto:smosher@nuharborsecurity.com">smosher@nuharborsecurity.com</a> phone: (802) 881-4224		

NOVEMBER 18, 2021



TECHNICAL PROPOSAL | RFP # 34-21  
CYBER-SECURITY SOLUTIONS, MALWARE, RANSOMWARE  
PROTECTION, OTHER RELATED PRODUCTS AND SERVICES

**PREPARED FOR:**

National Cooperative Purchasing Alliance | Region 14 Education Service Center  
1850 TX-351  
Abilene, Texas | 79601

**PREPARED BY:**

NuHarbor Security  
553 Roosevelt Highway | Suite 102  
Colchester, VT 05446  
[www.nuharborsecurity.com](http://www.nuharborsecurity.com)

## CONTENTS

TAB 1. Master Agreement/Signature Form .....	4
TAB 2. NCPA Administration Agreement .....	6
TAB 3. Vendor Questionnaire .....	10
TAB 4. Vendor Profile.....	13
4.1 Company Name.....	13
4.2 Company History.....	13
4.3 D&B Number .....	13
4.4 Organizational Chart .....	13
4.5 Locations .....	14
Key Contacts.....	15
4.6 Payment Terms .....	15
4.7 Competition .....	16
4.8 Annual Sales.....	16
4.9 Differentiators.....	16
Technology Partners .....	18
Industry Recognition   Awards & Accolades .....	18
Strategic Partnerships.....	19
4.10 Marketing Plan.....	19
4.11 Internal Marketing Plan .....	20
4.12 Online Catalog.....	20
4.13 Business Operations.....	20
4.14 Employee Certification and Accreditation .....	20
SOC 2 Type 1 Audit.....	20
Splunk Accreditation .....	20
Managed Services Skills Matrix.....	21
4.15 Licensing and Ownership .....	22
4.16 Customer Service .....	23
4.17 Green Initiatives.....	23
4.18 Vendor Certifications .....	23
TAB 5. Products and Services/Scope.....	24
5.1 Security Audits .....	24
5.1.1 Risk Assessment Audit – Internal Exposure .....	24

---

5.1.2 Gap Assessments or Readiness Assessments against Security Framework.....	25
5.2 Professional Services.....	25
5.2.1 Installation Services (list approved/qualified partners).....	25
5.3 Managed Services .....	25
5.3.1 Managed Detect and Response Services (MDR).....	25
5.3.2 Vulnerability Management as a Service.....	26
5.3.3 Security Information and Event Management (SIEM) as a Service .....	27
5.3.4 Identity and Access Management (IAM) as a Service .....	27
TAB 6. References ( <b>HIGHLY CONFIDENTIAL</b> ) .....	28
TAB 7. Pricing .....	30
TAB 8. Value Added Products and Services .....	31
TAB 9. Required Documents .....	32
9.1 Clean Air and Water Act / Debarment Notice .....	32
9.2 Contractors Requirements.....	33
9.3 Antitrust Certification Statements.....	34
9.4 Required Clauses for Federal Funds Certifications .....	35
9.5 Required Clauses for Federal Assistance by FTA.....	35
9.6 State Notice Addendum.....	35

## TAB 1. MASTER AGREEMENT/SIGNATURE FORM

NuHarbor Security agrees to the terms in the Master Agreement.

# Tab 1 – Master Agreement General Terms and Conditions

---

- ◆ Customer Support
  - The vendor shall provide timely and accurate technical advice and sales support. The vendor shall respond to such requests within one (1) working day after receipt of the request.
  
- ◆ Disclosures
  - Respondent affirms that he/she has not given, offered to give, nor intends to give at any time hereafter any economic opportunity, future employment, gift, loan, gratuity, special discount, trip, favor or service to a public servant in connection with this contract.
  - The respondent affirms that, to the best of his/her knowledge, the offer has been arrived at independently, and is submitted without collusion with anyone to obtain information or gain any favoritism that would in any way limit competition or give an unfair advantage over other vendors in the award of this contract.
  
- ◆ Renewal of Contract
  - Unless otherwise stated, all contracts are for a period of three (3) years with an option to renew for up to two (2) additional one-year terms or any combination of time equally not more than 2 years if agreed to by Region 14 ESC and the vendor.
  
- ◆ Funding Out Clause
  - Any/all contracts exceeding one (1) year shall include a standard “funding out” clause. A contract for the acquisition, including lease, of real or personal property is a commitment of the entity’s current revenue only, provided the contract contains either or both of the following provisions:
    - Retains to the entity the continuing right to terminate the contract at the expiration of each budget period during the term of the contract and is conditioned on a best efforts attempt by the entity to obtain appropriate funds for payment of the contract.
  
- ◆ Shipments (if applicable)
  - The awarded vendor shall ship ordered products within seven (7) working days for goods available and within four (4) to six (6) weeks for specialty items after the receipt of the order unless modified. If a product cannot be shipped within that time, the awarded vendor shall notify the entity placing the order as to why the product has not shipped and shall provide an estimated shipping date. At this point the participating entity may cancel the order if estimated shipping time is not acceptable.
  
- ◆ Tax Exempt Status
  - Since this is a national contract, knowing the tax laws in each state is the sole responsibility of the vendor.

- ◆ Payments
  - The entity using the contract will make payments directly to the awarded vendor or their affiliates (distributors/business partners/resellers) as long as written request and approval by NCPA is provided to the awarded vendor.
- ◆ Adding authorized distributors/dealers
  - Awarded vendors may submit a list of distributors/partners/resellers to sell under their contract throughout the life of the contract. Vendor must receive written approval from NCPA before such distributors/partners/resellers considered authorized.
  - Purchase orders and payment can only be made to awarded vendor or distributors/business partners/resellers previously approved by NCPA.
  - Pricing provided to members by added distributors or dealers must also be less than or equal to the pricing offered by the awarded contract holder.
  - All distributors/partners/resellers are required to abide by the Terms and Conditions of the vendor's agreement with NCPA.
- ◆ Pricing
  - All pricing submitted shall include the administrative fee to be remitted to NCPA by the awarded vendor. It is the awarded vendor's responsibility to keep all pricing up to date and on file with NCPA.
  - All deliveries shall be freight prepaid, F.O.B. destination and shall be included in all pricing offered unless otherwise clearly stated in writing
- ◆ Warranty
  - Proposals should address each of the following:
    - Applicable warranty and/or guarantees of equipment and installations including any conditions and response time for repair and/or replacement of any components during the warranty period.
    - Availability of replacement parts
    - Life expectancy of equipment under normal use
    - Detailed information as to proposed return policy on all equipment
- ◆ Indemnity
  - The awarded vendor shall protect, indemnify, and hold harmless Region 14 ESC and its participants, administrators, employees and agents against all claims, damages, losses and expenses arising out of or resulting from the actions of the vendor, vendor employees or vendor subcontractors in the preparation of the solicitation and the later execution of the contract.
- ◆ Franchise Tax
  - The respondent hereby certifies that he/she is not currently delinquent in the payment of any franchise taxes.



◆ Supplemental Agreements

- The entity participating in this contract and awarded vendor may enter into a separate supplemental agreement to further define the level of service requirements over and above the minimum defined in this contract i.e. invoice requirements, ordering requirements, specialized delivery, etc. Any supplemental agreement developed as a result of this contract is exclusively between the participating entity and awarded vendor.

◆ Certificates of Insurance

- Certificates of insurance shall be delivered to the Public Agency prior to commencement of work. The insurance company shall be licensed in the applicable state in which work is being conducted. The awarded vendor shall give the participating entity a minimum of ten (10) days notice prior to any modifications or cancellation of policies. The awarded vendor shall require all subcontractors performing any work to maintain coverage as specified.

◆ Legal Obligations

- It is the Respondent's responsibility to be aware of and comply with all local, state, and federal laws governing the sale of products/services identified in this RFP and any awarded contract and shall comply with all while fulfilling the RFP. Applicable laws and regulation must be followed even if not specifically identified herein.

◆ Protest

- A protest of an award or proposed award must be filed in writing within ten (10) days from the date of the official award notification and must be received by 5:00 pm CST. Protests shall be filed with Region 14 ESC and shall include the following:
  - Name, address and telephone number of protester
  - Original signature of protester or its representative
  - Identification of the solicitation by RFP number
  - Detailed statement of legal and factual grounds including copies of relevant documents and the form of relief requested
- Any protest review and action shall be considered final with no further formalities being considered.

◆ Force Majeure

- If by reason of Force Majeure, either party hereto shall be rendered unable wholly or in part to carry out its obligations under this Agreement then such party shall give notice and full particulars of Force Majeure in writing to the other party within a reasonable time after occurrence of the event or cause relied upon, and the obligation of the party giving such notice, so far as it is affected by such Force Majeure, shall be suspended during the continuance of the inability then claimed, except as hereinafter provided, but for no longer period, and such party shall endeavor to remove or overcome such inability with all reasonable dispatch.
- The term Force Majeure as employed herein, shall mean acts of God, strikes, lockouts, or other industrial disturbances, act of public enemy, orders of any kind of government of the

United States or any civil or military authority; insurrections; riots; epidemics; landslides; lighting; earthquake; fires; hurricanes; storms; floods; washouts; droughts; arrests; restraint of government and people; civil disturbances; explosions, breakage or accidents to machinery, pipelines or canals, or other causes not reasonably within the control of the party claiming such inability. It is understood and agreed that the settlement of strikes and lockouts shall be entirely within the discretion of the party having the difficulty, and that the above requirement that any Force Majeure shall be remedied with all reasonable dispatch shall not require the settlement of strikes and lockouts by acceding to the demands of the opposing party or parties when such settlement is unfavorable in the judgment of the party having the difficulty

◆ Prevailing Wage

- It shall be the responsibility of the Vendor to comply, when applicable, with the prevailing wage legislation in effect in the jurisdiction of the purchaser. It shall further be the responsibility of the Vendor to monitor the prevailing wage rates as established by the appropriate department of labor for any increase in rates during the term of this contract and adjust wage rates accordingly.

◆ Miscellaneous

- Either party may cancel this contract in whole or in part by providing written notice. The cancellation will take effect 30 business days after the other party receives the notice of cancellation. After the 30th business day all work will cease following completion of final purchase order.

◆ Open Records Policy

- Because Region 14 ESC is a governmental entity responses submitted are subject to release as public information after contracts are executed. If a vendor believes that its response, or parts of its response, may be exempted from disclosure, the vendor must specify page-by-page and line-by-line the parts of the response, which it believes, are exempt. In addition, the respondent must specify which exception(s) are applicable and provide detailed reasons to substantiate the exception(s).
- The determination of whether information is confidential and not subject to disclosure is the duty of the Office of Attorney General (OAG). Region 14 ESC must provide the OAG sufficient information to render an opinion and therefore, vague and general claims to confidentiality by the respondent are not acceptable. Region 14 ESC must comply with the opinions of the OAG. Region 14 ESC assumes no responsibility for asserting legal arguments on behalf of any vendor. Respondent are advised to consult with their legal counsel concerning disclosure issues resulting from this procurement process and to take precautions to safeguard trade secrets and other proprietary information.

# Process

---

Region 14 ESC will evaluate proposals in accordance with, and subject to, the relevant statutes, ordinances, rules, and regulations that govern its procurement practices. NCPA will assist Region 14 ESC in evaluating proposals. Award(s) will be made to the prospective vendor whose response is determined to be the most advantageous to Region 14 ESC, NCPA, and its participating agencies. To qualify for evaluation, response must have been submitted on time, and satisfy all mandatory requirements identified in this document.

- ◆ Contract Administration
  - The contract will be administered by Region 14 ESC. The National Program will be administered by NCPA on behalf of Region 14 ESC.
- ◆ Contract Term
  - The contract term will be for three (3) year starting from the date of the award. The contract may be renewed for up to two (2) additional one-year terms or any combination of time equally not more than 2 years.
  - It should be noted that maintenance/service agreements may be issued for up to (5) years under this contract even if the contract only lasts for the initial term of the contract. NCPA will monitor any maintenance agreements for the term of the agreement provided they are signed prior to the termination or expiration of this contract.
- ◆ Contract Waiver
  - Any waiver of any provision of this contract shall be in writing and shall be signed by the duly authorized agent of Region 14 ESC. The waiver by either party of any term or condition of this contract shall not be deemed to constitute waiver thereof nor a waiver of any further or additional right that such party may hold under this contract.
- ◆ Products and Services additions
  - Products and Services may be added to the resulting contract during the term of the contract by written amendment, to the extent that those products and services are within the scope of this RFP.
- ◆ Competitive Range
  - It may be necessary for Region 14 ESC to establish a competitive range. Responses not in the competitive range are unacceptable and do not receive further award consideration.
- ◆ Deviations and Exceptions
  - Deviations or exceptions stipulated in response may result in disqualification. It is the intent of Region 14 ESC to award a vendor's complete line of products and/or services, when possible.
- ◆ Estimated Quantities
  - The estimated dollar volume of Products and Services purchased under the proposed Master Agreement is \$50 million dollars annually. This estimate is based on the anticipated volume of Region 14 ESC and current sales within the NCPA program. There is no guarantee or commitment of any kind regarding usage of any contracts resulting from this solicitation

- ◆ Evaluation
  - Region 14 ESC will review and evaluate all responses in accordance with, and subject to, the relevant statutes, ordinances, rules and regulations that govern its procurement practices. NCPA will assist the lead agency in evaluating proposals. Recommendations for contract awards will be based on multiple factors, each factor being assigned a point value based on its importance.
- ◆ Formation of Contract
  - A response to this solicitation is an offer to contract with Region 14 ESC based upon the terms, conditions, scope of work, and specifications contained in this request. A solicitation does not become a contract until it is accepted by Region 14 ESC. The prospective vendor must submit a signed Signature Form with the response thus, eliminating the need for a formal signing process.
- ◆ NCPA Administrative Agreement
  - The vendor will be required to enter and execute the National Cooperative Purchasing Alliance Administration Agreement with NCPA upon award with Region 14 ESC. The agreement establishes the requirements of the vendor with respect to a nationwide contract effort.
- ◆ Clarifications / Discussions
  - Region 14 ESC may request additional information or clarification from any of the respondents after review of the proposals received for the sole purpose of elimination minor irregularities, informalities, or apparent clerical mistakes in the proposal. Clarification does not give respondent an opportunity to revise or modify its proposal, except to the extent that correction of apparent clerical mistakes results in a revision. After the initial receipt of proposals, Region 14 ESC reserves the right to conduct discussions with those respondent's whose proposals are determined to be reasonably susceptible of being selected for award. Discussions occur when oral or written communications between Region 14 ESC and respondent's are conducted for the purpose clarifications involving information essential for determining the acceptability of a proposal or that provides respondent an opportunity to revise or modify its proposal. Region 14 ESC will not assist respondent bring its proposal up to the level of other proposals through discussions. Region 14 ESC will not indicate to respondent a cost or price that it must meet to neither obtain further consideration nor will it provide any information about other respondents' proposals or prices.
- ◆ Multiple Awards
  - Multiple Contracts may be awarded as a result of the solicitation. Multiple Awards will ensure that any ensuing contracts fulfill current and future requirements of the diverse and large number of participating public agencies.
- ◆ Past Performance
  - Past performance is relevant information regarding a vendor's actions under previously awarded contracts; including the administrative aspects of performance; the vendor's history of reasonable and cooperative behavior and commitment to customer satisfaction; and generally, the vendor's businesslike concern for the interests of the customer.

# Evaluation Criteria

---


- ◆ Pricing (40 points)
  - Electronic Price Lists
    - Products, Services, Warranties, etc. price list
    - Prices listed will be used to establish both the extent of a vendor's product lines, services, warranties, etc. available from a particular bidder and the pricing per item.
  
- ◆ Ability to Provide and Perform the Required Services for the Contract (25 points)
  - Product Delivery within participating entities specified parameters
  - Number of line items delivered complete within the normal delivery time as a percentage of line items ordered.
  - Vendor's ability to perform towards above requirements and desired specifications.
  - Past Cooperative Program Performance
  - Quantity of line items available that are commonly purchased by the entity.
  - Quality of line items available compared to normal participating entity standards.
  - Provide both On-premise solutions as well as Cloud based solutions.
  
- ◆ References (15 points)
  - A minimum of ten (10) customer references for product and/or services of similar scope dating within past 3 years
  
- ◆ Technology for Supporting the Program (10 points)
  - Electronic on-line catalog, order entry use by and suitability for the entity's needs
  - Quality of vendor's on-line resources for NCPA members.
  - Specifications and features offered by respondent's products and/or services
  
- ◆ Value Added Services Description, Products and/or Services (10 points)
  - Marketing and Training
  - Minority and Women Business Enterprise (MWBE) and (HUB) Participation
  - Customer Service

# Signature Form

---

The undersigned hereby proposes and agrees to furnish goods and/or services in strict compliance with the terms, specifications and conditions at the prices proposed within response unless noted in writing. The undersigned further certifies that he/she is an officer of the company and has authority to negotiate and bind the company named below and has not prepared this bid in collusion with any other Respondent and that the contents of this proposal as to prices, terms or conditions of said bid have not been communicated by the undersigned nor by any employee or agent to any person engaged in this type of business prior to the official opening of this proposal.

Prices are guaranteed: **120 days**

Company name	<u>NuHarbor Security</u>
Address	<u>553 Roosevelt Highway, Suite 102</u>
City/State/Zip	<u>Colchester, VT 05446</u>
Telephone No.	<u>(802) 881-4224</u>
Fax No.	<u>n/a</u>
Email address	<u>smosher@nuharborsecurity.com</u>
Printed name	<u>Scott Mosher</u>
Position with company	<u>Vice President</u>
Authorized signature	<u></u>

## TAB 2. NCPA ADMINISTRATION AGREEMENT

NuHarbor Security agrees to the terms in the NCPA Administration Agreement.

# Tab 2 – NCPA Administration Agreement

---

This Administration Agreement is made as of December 13, 2021, by and between National Cooperative Purchasing Alliance (“NCPA”) and NuHarbor Security, Inc. (“Vendor”).

## Recitals

WHEREAS, Region 14 ESC has entered into a certain Master Agreement dated December 13, 2021, referenced as Contract Number 01-133, by and between Region 14 ESC and Vendor, as may be amended from time to time in accordance with the terms thereof (the “Master Agreement”), for the purchase of Cyber-Security Solutions, Malware, Ransomware Protection, Other Related Products and Services ;

WHEREAS, said Master Agreement provides that any state, city, special district, local government, school district, private K-12 school, technical or vocational school, higher education institution, other government agency or nonprofit organization (hereinafter referred to as “public agency” or collectively, “public agencies”) may purchase products and services at the prices indicated in the Master Agreement;

WHEREAS, NCPA has the administrative and legal capacity to administer purchases under the Master Agreement to public agencies;

WHEREAS, NCPA serves as the administrative agent for Region 14 ESC in connection with other master agreements offered by NCPA

WHEREAS, Region 14 ESC desires NCPA to proceed with administration of the Master Agreement;

WHEREAS, NCPA and Vendor desire to enter into this Agreement to make available the Master Agreement to public agencies on a national basis;

NOW, THEREFORE, in consideration of the payments to be made hereunder and the mutual covenants contained in this Agreement, NCPA and Vendor hereby agree as follows:

### ◆ General Terms and Conditions

- The Master Agreement, attached hereto as Tab 1 and incorporated herein by reference as though fully set forth herein, and the terms and conditions contained therein shall apply to this Agreement except as expressly changed or modified by this Agreement.
- NCPA shall be afforded all of the rights, privileges and indemnifications afforded to Region 14 ESC under the Master Agreement, and such rights, privileges and indemnifications shall accrue and apply with equal effect to NCPA under this Agreement including, but not limited to, the Vendor’s obligation to provide appropriate insurance and certain indemnifications to Region 14 ESC.
- Vendor shall perform all duties, responsibilities and obligations required under the Master Agreement in the time and manner specified by the Master Agreement.
- NCPA shall perform all of its duties, responsibilities, and obligations as administrator of purchases under the Master Agreement as set forth herein, and Vendor acknowledges that NCPA shall act in the capacity of administrator of purchases under the Master Agreement.
- With respect to any purchases made by Region 14 ESC or any Public Agency pursuant to the Master Agreement, NCPA (a) shall not be construed as a dealer, re-marketer, representative, partner, or agent of any type of Vendor, Region 14 ESC, or such Public



Agency, (b) shall not be obligated, liable or responsible (i) for any orders made by Region 14 ESC, any Public Agency or any employee of Region 14 ESC or Public Agency under the Master Agreement, or (ii) for any payments required to be made with respect to such order, and (c) shall not be obligated, liable or responsible for any failure by the Public Agency to (i) comply with procedures or requirements of applicable law, or (ii) obtain the due authorization and approval necessary to purchase under the Master Agreement. NCPA makes no representations or guaranties with respect to any minimum purchases required to be made by Region 14 ESC, any Public Agency, or any employee of Region 14 ESC or Public Agency under this Agreement or the Master Agreement.

- The Public Agency participating in the NCPA contract and Vendor may enter into a separate supplemental agreement to further define the level of service requirements over and above the minimum defined in this contract i.e. invoice requirements, ordering requirements, specialized delivery, etc. Any supplemental agreement developed as a result of this contract is exclusively between the Public Agency and Vendor. NCPA, its agents, members and employees shall not be made party to any claim for breach of such agreement.

◆ **Term of Agreement**

- This Agreement shall be in effect so long as the Master Agreement remains in effect, provided, however, that the obligation to pay all amounts owed by Vendor to NCPA through the termination of this Agreement and all indemnifications afforded by Vendor to NCPA shall survive the term of this Agreement.

◆ **Fees and Reporting**

- The awarded vendor shall electronically provide NCPA with a detailed quarterly report showing the dollar volume of all sales under the contract for the previous quarter. Reports are due on the fifteenth (15<sup>th</sup>) day after the close of the previous quarter. It is the responsibility of the awarded vendor to collect and compile all sales under the contract from participating members and submit one (1) report. The report shall include at least the following information as listed in the example below:

Entity Name	Zip Code	State	PO or Job #	Sale Amount

**Total** \_\_\_\_\_

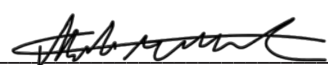

- Each quarter NCPA will invoice the vendor based on the total of sale amount(s) reported. From the invoice the vendor shall pay to NCPA an administrative fee based upon the tiered fee schedule below. Vendor’s annual sales shall be measured on a calendar year basis. Deadline for term of payment will be included in the invoice NCPA provides.

<b><u>Annual Sales Through Contract</u></b>	<b><u>Administrative Fee</u></b>
0 - \$30,000,000	2%
\$30,000,001 - \$50,000,000	1.5%
\$50,000,001+	1%

- Supplier shall maintain an accounting of all purchases made by Public Agencies under the Master Agreement. NCPA and Region 14 ESC reserve the right to audit the accounting for a period of four (4) years from the date NCPA receives the accounting. In the event of such an audit, the requested materials shall be provided at the location designated by Region 14 ESC or NCPA. In the event such audit reveals an under reporting of Contract Sales and a resulting underpayment of administrative fees, Vendor shall promptly pay NCPA the amount of such underpayment, together with interest on such amount and shall be obligated to reimburse NCPA's costs and expenses for such audit.

◆ General Provisions

- This Agreement supersedes any and all other agreements, either oral or in writing, between the parties hereto with respect to the subject matter hereof, and no other agreement, statement, or promise relating to the subject matter of this Agreement which is not contained herein shall be valid or binding.
- Awarded vendor agrees to allow NCPA to use their name and logo within website, marketing materials and advertisement. Any use of NCPA name and logo or any form of publicity regarding this contract by awarded vendor must have prior approval from NCPA.
- If any action at law or in equity is brought to enforce or interpret the provisions of this Agreement or to recover any administrative fee and accrued interest, the prevailing party shall be entitled to reasonable attorney's fees and costs in addition to any other relief to which such party may be entitled.
- Neither this Agreement nor any rights or obligations hereunder shall be assignable by Vendor without prior written consent of NCPA, provided, however, that the Vendor may, without such written consent, assign this Agreement and its rights and delegate its obligations hereunder in connection with the transfer or sale of all or substantially all of its assets or business related to this Agreement, or in the event of its merger, consolidation, change in control or similar transaction. Any permitted assignee shall assume all assigned obligations of its assignor under this Agreement.
- This Agreement and NCPA's rights and obligations hereunder may be assigned at NCPA's sole discretion, to an existing or newly established legal entity that has the authority and capacity to perform NCPA's obligations hereunder
- All written communications given hereunder shall be delivered to the addresses as set forth below.

<b>National Cooperative Purchasing Alliance:</b>	<b>Vendor:</b>	NuHarbor Security, Inc.
Name: <u>Matthew Mackel</u>	Name: <u>Scott Mosher</u>	
Title: <u>Director, Business Development</u>	Title: <u>Vice President</u>	
Address: <u>PO Box 701273</u>	Address: <u>553 Roosevelt Hwy, Ste 102</u>	
<u>Houston, TX 77270</u>	<u>Colchester, VT 05446</u>	
Signature: <u></u>	Signature: <u></u>	
Date: <u>December 13, 2021</u>	Date: <u>11/18/2021</u>	

# Tab 3 – Vendor Questionnaire

---

Please provide responses to the following questions that address your company’s operations, organization, structure, and processes for providing products and services.

◆ States Covered

- Bidder must indicate any and all states where products and services can be offered.
- Please indicate the price co-efficient for each state if it varies.

**50 States & District of Columbia** (Selecting this box is equal to checking all boxes below)

- |   |   |   |
|---|---|---|
| <input type="checkbox"/> Alabama              | <input type="checkbox"/> Maryland       | <input type="checkbox"/> South Carolina |
| <input type="checkbox"/> Alaska               | <input type="checkbox"/> Massachusetts  | <input type="checkbox"/> South Dakota   |
| <input type="checkbox"/> Arizona              | <input type="checkbox"/> Michigan       | <input type="checkbox"/> Tennessee      |
| <input type="checkbox"/> Arkansas             | <input type="checkbox"/> Minnesota      | <input type="checkbox"/> Texas          |
| <input type="checkbox"/> California           | <input type="checkbox"/> Mississippi    | <input type="checkbox"/> Utah           |
| <input type="checkbox"/> Colorado             | <input type="checkbox"/> Missouri       | <input type="checkbox"/> Vermont        |
| <input type="checkbox"/> Connecticut          | <input type="checkbox"/> Montana        | <input type="checkbox"/> Virginia       |
| <input type="checkbox"/> Delaware             | <input type="checkbox"/> Nebraska       | <input type="checkbox"/> Washington     |
| <input type="checkbox"/> District of Columbia | <input type="checkbox"/> Nevada         | <input type="checkbox"/> West Virginia  |
| <input type="checkbox"/> Florida              | <input type="checkbox"/> New Hampshire  | <input type="checkbox"/> Wisconsin      |
| <input type="checkbox"/> Georgia              | <input type="checkbox"/> New Jersey     | <input type="checkbox"/> Wyoming        |
| <input type="checkbox"/> Hawaii               | <input type="checkbox"/> New Mexico     |   |
| <input type="checkbox"/> Idaho                | <input type="checkbox"/> New York       |   |
| <input type="checkbox"/> Illinois             | <input type="checkbox"/> North Carolina |   |
| <input type="checkbox"/> Indiana              | <input type="checkbox"/> North Dakota   |   |
| <input type="checkbox"/> Iowa                 | <input type="checkbox"/> Ohio           |   |
| <input type="checkbox"/> Kansas               | <input type="checkbox"/> Oklahoma       |   |
| <input type="checkbox"/> Kentucky             | <input type="checkbox"/> Oregon         |   |
| <input type="checkbox"/> Louisiana            | <input type="checkbox"/> Pennsylvania   |   |
| <input type="checkbox"/> Maine                | <input type="checkbox"/> Rhode Island   |   |

**All US Territories and Outlying Areas** (Selecting this box is equal to checking all boxes below)

American Samoa

Northern Marina Islands

Federated States of Micronesia

Puerto Rico

Guam

U.S. Virgin Islands

Midway Islands

◆ **Minority** **and Women**

**Business Enterprise (MWBE) and (HUB) Participation**

➤ It is the policy of some entities participating in NCPA to involve minority and women business enterprises (MWBE) and historically underutilized businesses (HUB) in the purchase of goods and services. Respondents shall indicate below whether or not they are an M/WBE or HUB certified.

▪ **Minority / Women Business Enterprise**

• Respondent Certifies that this firm is a M/WBE

▪ **Historically Underutilized Business**

• Respondent Certifies that this firm is a HUB

◆ **Residency**

➤ Responding Company's principal place of business is in the city of Colchester, State of VT

◆ **Felony Conviction Notice**

➤ Please Check Applicable Box;

A publically held corporation; therefore, this reporting requirement is not applicable.

Is not owned or operated by anyone who has been convicted of a felony.

Is owned or operated by the following individual(s) who has/have been convicted of a felony

➤ If the 3<sup>rd</sup> box is checked, a detailed explanation of the names and convictions must be attached.

◆ **Distribution Channel**

➤ Which best describes your company's position in the distribution channel:

Manufacturer Direct  Certified education/government reseller

Authorized Distributor  Manufacturer marketing through reseller

Value-added reseller  Other: Managed Services Provider

◆ **Processing Information**

➤ Provide company contact information for the following:

▪ **Sales Reports / Accounts Payable**

Contact Person: Marisa Lane

Title: AR/AP/Payroll Specialist

Company: NuHarbor Security, Inc.

Address: 553 Roosevelt Hwy, Ste 102

City: Colchester State: Vermont Zip: 05446

Phone: 802-391-8878 Email: mlane@nuharborsecurity.com

- Purchase Orders

Contact Person: Scott Mosher  
 Title: Vice President  
 Company: NuHarbor Security, Inc.  
 Address: 553 Roosevelt Hwy, Ste 102  
 City: Colchester State: Vermont Zip: 05446  
 Phone: 802-881-4224 Email: smosher@nuharborsecurity.com

- Sales and Marketing

Contact Person: Scott Mosher  
 Title: Vice President  
 Company: NuHarbor Security, Inc.  
 Address: 553 Roosevelt Hwy, Ste 102  
 City: Colchester State: Vermont Zip: 05446  
 Phone: 802-881-4224 Email: smosher@nuharborsecurity.com

- ◆ Pricing Information

- In addition to the current typical unit pricing furnished herein, the Vendor agrees to offer all future product introductions at prices that are proportionate to Contract Pricing.
  - If answer is no, attach a statement detailing how pricing for NCPA participants would be calculated for future product introductions.
    - Yes  No
- Pricing submitted includes the required NCPA administrative fee. The NCPA fee is calculated based on the invoice price to the customer.
  - Yes  No
- Vendor will provide additional discounts for purchase of a guaranteed quantity.
  - Yes  No

- ◆ Cooperatives

- List any other cooperative or state contracts currently held or in the process of securing.

Cooperative/State Agency	Discount Offered	Expires	Annual Sales Volume

## TAB 4. VENDOR PROFILE

### 4.1 COMPANY NAME

NuHarbor Security, Inc.

### 4.2 COMPANY HISTORY

NuHarbor Security is a leading national information consulting and advisory firm delivering tactical and strategic cybersecurity services to clients spanning all industry verticals across both private and public sectors, with a deep commitment to supporting State and Local Government and Education entities. NuHarbor is 100% focused on the information security sector – we exist to help all businesses and institutions secure their data with progressive security solutions and ease the complexity of cybersecurity. Our security approach, comprehensive offerings, and client-first perspective make us the ideal long-term security partner.

Since 2014, NuHarbor has helped clients design, implement, and sustain comprehensive Information Security, Compliance, and Risk Management programs. Our innovation and thought leadership challenge traditional methodologies and promote a new understanding of sustainable information security. Founded by former CISOs and security leaders unsatisfied with the options available for Information Security services, NuHarbor emerged as a true end-to-end security provider. Grounded in our services-driven approach, we take pride in being a full security lifecycle provider – our services are designed to support any information security need an organization might have. We are committed to serving our clients in the creation and maintenance of robust Information Security Programs and Enterprise Architecture by integrating premier security solutions from our highly selective technology partner portfolio. Our firm is led by a team of highly certified former Fortune 500 Chief Information Security Officers (CISOs) and industry Information Security Directors who offer years of hands-on experience working alongside clients to deliver actionable results. From small private companies and higher education institutions to local governments and large state agencies, we serve as their “Trusted Advisor” for best-in-breed information security services.

### 4.3 D&B NUMBER

079956526

### 4.4 ORGANIZATIONAL CHART

NuHarbor Security does not furnish employee information in public record documents. Upon receipt of a fully executed Statement of Work (SOW), appropriate personnel will be assigned, and resumes can be supplied for client approval.

In comparison with most security service firms, NuHarbor offers its clients a truly unique organizational experience. Our services are designed and overseen by former industry leaders who have practical knowledge built around implementing and maintaining Information System Security Programs. Our team of highly credentialed and easily accessible managed services experts are all U.S.-based, full-time employees.

Project teams and plans are built via collaboration. NuHarbor believes that projects move more seamlessly and better meet clients’ requirements when we engage their input from start to finish. By

working with NuHarbor, clients enjoy full visibility into our methodology and deliverables, and are fully engaged in approving team members, defining deliverables, establishing milestones, etc.

### **Security Audits**

Our tenured, highly certified Information Assurance (IA) analyst team averages 10 years of compliance experience and maintains a strong focus on the National Institute of Standards and Technology (NIST) frameworks. The IA team offers comprehensive compliance services including security advisory and policy development, and performs gap assessments and audits for CMMC, HIPAA, ISO 27001, FISMA, NIST, PCI, and more. Assessments serve as the foundation for other services that we provide. Assessing the strengths and vulnerabilities in our clients' security landscapes provides insight into each of our recommendations and decisions.

The resources assigned to Security Audit engagements described in [Section 5.1](#) will include a project lead (IA Program Manager), team of IA Analysts, and an IA Coordinator. The Program Manager serves as the senior resource and lead point of contact for ongoing engagements and provides executive level advisory services and strategic guidance to client partners. All vendor communication and status tracking are managed by the assigned IA Coordinator; Risk Assessments and Analysis are conducted by experienced IA Analysts.

### **Managed Services and Professional Services**

As described in [Section 5.2](#) and [Section 5.3](#), NuHarbor's next generation MSSP is grounded in Splunk – a software-based solution that runs on off-the-shelf commodity hardware – our primary tool for the delivery of security services. We have offered Security Monitoring, Admin and Development, and Professional Services around Splunk Enterprise and Enterprise Security (ES) since 2014, and specialize in helping our customers install, configure, upgrade, and maintain Splunk. Our US-based team of Professional and Managed Services analysts and engineers help clients customize the Splunk platform to drive security of the enterprise, meet compliance requirements, and build security capabilities across the organization.

NuHarbor's Project Management, Security Engineering, and Security Operations teams participate in the deployment and ongoing support requirements for Managed Services engagements. NuHarbor designates a Project Manager (PM) to operate as the primary point of contact with day-to-day responsibility for, and authority to manage, client satisfaction. The PM will develop a project schedule that details the tasks, timelines, and deliverables for the solution, and apply PMI principles to ensure on-time and within-budget delivery. Each Client is assigned a named Primary Engineer and Primary Analyst. We assign our engineers and analysts by sector experience. The proposed staff will also work with other State and Local entities utilizing our Managed Service – we find this to be beneficial as the engineers and analysts have knowledge of these unique environments. 100% of NuHarbor Security Engineers and Analysts hold security certifications. Our security staff averages 7-10 years of experience performing security monitoring or security consulting. Collectively our fully accredited team holds 85+ Splunk certifications.

## **4.5 LOCATIONS**

NuHarbor Security is headquartered in Colchester, VT, and has strategically located regional offices in New York, NY; Boston, MA; Washington, DC; Charlotte, NC; Atlanta, GA; and Miami, FL. We provide

security services in all 50 U.S. States and have clients nationwide. NuHarbor utilizes both our Physical Security Operations Center (SOC) in the Vermont headquarters and a dispersed Virtual SOC of securely networked engineers and analysts. Our Virtual SOC is staffed 24/7/365.

### Key Contacts

Primary Contact for all areas:

#### Scott Mosher

Vice President

553 Roosevelt Highway, Suite 102

Colchester, VT 05446

[smosher@nuharborsecurity.com](mailto:smosher@nuharborsecurity.com)

Cell: (802) 881-4224



Scott Mosher | VP Sales

[smosher@nuharborsecurity.com](mailto:smosher@nuharborsecurity.com)

(802) 881-4224

Katy Feifs | Sales Operations + Partnerships

[kfeifs@nuharborsecurity.com](mailto:kfeifs@nuharborsecurity.com)

(802) 210-1267

	NAME	TITLE	TERRITORY	EMAIL	PHONE
NORTHEAST	Sam Martin	Regional Sales Director, Northeast	CA (State/Local)	<a href="mailto:smartin@nuharborsecurity.com">smartin@nuharborsecurity.com</a>	(802) 310-2361
	Luc Martin	Regional Sales Manager	VT, NH, ME, Upstate NY	<a href="mailto:lmartin@nuharborsecurity.com">lmartin@nuharborsecurity.com</a>	(802) 448-5807
	Nyles Lawson	Regional Sales Manager	CT, MA, RI	<a href="mailto:nlawson@nuharborsecurity.com">nlawson@nuharborsecurity.com</a>	(617) 315-2524
	Jim Judge	Regional Sales Manager	NYC Metro	<a href="mailto:jjudge@nuharborsecurity.com">jjudge@nuharborsecurity.com</a>	(917) 748-0344
	Alex Johnson	Inside Sales Manager	CA (Commercial)	<a href="mailto:ajohnson@nuharborsecurity.com">ajohnson@nuharborsecurity.com</a>	(802) 383-8371
MID-ATLANTIC	Nick Calderan	Sr. Sales Engineer	Northeast/Mid-Atlantic	<a href="mailto:ncalderan@nuharborsecurity.com">ncalderan@nuharborsecurity.com</a>	(603) 566-3470
	Travis Sanchez	Regional Sales Director, Mid-Atlantic	DC, NoVA, MD, DE	<a href="mailto:tsanchez@nuharborsecurity.com">tsanchez@nuharborsecurity.com</a>	(301) 461-2445
	Brendan McDonald	Regional Sales Manager	PA, NJ, WV, OH	<a href="mailto:bmcdonald@nuharborsecurity.com">bmcdonald@nuharborsecurity.com</a>	(434) 216-8210
	Rowman Basham	Regional Sales Manager	NC, SC, SoVA	<a href="mailto:rbasham@nuharborsecurity.com">rbasham@nuharborsecurity.com</a>	(757) 630-4712
SOUTHEAST	Wes Lyle	Sr. Security Solutions Architect	Mid-Atlantic/Southeast	<a href="mailto:wlyle@nuharborsecurity.com">wlyle@nuharborsecurity.com</a>	(404) 641-2563
	Robert Clark	Regional Sales Director, Southeast	GA, AL, MS, TX, AR, TN, KY, CA (Higher Ed)	<a href="mailto:rclark@nuharborsecurity.com">rclark@nuharborsecurity.com</a>	(404) 660-6407
	Paul Weir	Regional Sales Manager	FL, LA	<a href="mailto:pweir@nuharborsecurity.com">pweir@nuharborsecurity.com</a>	(732) 221-8129

## 4.6 PAYMENT TERMS

Net 30



## 4.7 COMPETITION

NuHarbor Security is an end-to-end provider of security solutions powered by our portfolio of best in breed technology partners. We specialize in Managed Security Services, Compliance Assessment and Advisory, Technical Testing, and Offensive Operations.

Our competitors include firms that offer cybersecurity monitoring and management services.

## 4.9 DIFFERENTIATORS

Partnership	Expertise	Pure Play
<ul style="list-style-type: none"><li>✓ Co-Managed Model</li><li>✓ Client-Focused Consultation + Collaboration</li><li>✓ Impactful Communication</li><li>✓ 100% U.S.-Based Operations</li></ul>	<ul style="list-style-type: none"><li>✓ Highly-Credentialed + Accessible Staff</li><li>✓ Proactive Threat-Hunting + Analytics</li><li>✓ Custom Threat Intelligence</li><li>✓ Tailored Tuning</li></ul>	<ul style="list-style-type: none"><li>✓ 100% Cybersecurity-Focused, Services-Driven</li><li>✓ Maximum Efficacy, Efficiency, + Cost Reduction</li><li>✓ Leading Edge Technology Portfolio</li></ul>

### **NuHarbor Security Key Differentiators**

- 1. Pure Play:** NuHarbor is a 100% Cybersecurity-focused firm, and inherently services-driven. Security is our core mission. Our solutions are grounded in our leading-edge technology portfolio.
- 2. SLED:** NuHarbor has a strong focus on State and Local Government and Education. More than 70% of our Professional Services and Managed Services work is dedicated to Higher Education, State, County, and Municipal Governments. We are fluent in the complex needs of SLED entities. Accordingly, NuHarbor wrote the Splunk APPs for CJIS compliance and IRS Form 1075 compliance for our customer base. NuHarbor's tenured Information Assurance and Technical Testing teams have provided significant value to numerous R1 Schools. This output has informed best practices when delivering managed security services.
- 3. Access:** NuHarbor's highly credentialed and easily accessible staff are 100% US-based, available by call, click, or email. We provide our clients with a dedicated Named Analyst and Named Engineer,

and our Analyst and Engineering teams support an average of only three (3) clients each.

4. **Impactful Communication:** Clients receive comprehensive, actionable escalations, weekly cadence calls, biweekly and quarterly threat briefings, and daily health checks.
5. **Expertise:** We are quick to understand your risk and threats, and tailor threat intelligence to your unique business needs. We offer threat hunting through analyst-augmented automated detection, but also perform targeted threat hunting, leveraging our Cyber Threat Analysis Cell (CTAC) to explore your attack surface with an adversarial mindset. Our subject matter experts are there to offer guidance around next steps.
6. **Flexibility + Collaboration:** There's no "one-size-fits-all" solution for security. NuHarbor offers multiple managed service options to provide clients with the ultimate flexibility required to meet their needs today and in the future.

Our signature MSSP works as a truly co-managed model (i.e., client data ownership, 100% visibility, and control), complete with goal-focused onboarding and proactive security analysis and guidance. NuHarbor provides meaningful escalations and detailed investigations with real remediation recommendations allowing for quick action and effective resolution by the Client. Because our approach is a co-managed model, our clients have immediate context and visibility to the same data and workflow process as our Analysts have during an event. Together we mitigate the threat/event quickly and with less effort.

Our fully managed model – Security Operations Center (SOC) as a Service Powered by Splunk – allows businesses to leverage the visibility and analytics-driven intelligence of Splunk without the complexity of ownership, and benefit from the on-demand administration, human security review, and threat intelligence services of NuHarbor's highly customizable Splunk MSSP.

7. **False Positive Mitigation:** In concert with Splunk Enterprise Security, NuHarbor leverages the Advanced Correlated Search functionality of Enterprise Security and through continual tuning and data source hygiene activities, we successfully decrease "False Positive" activity significantly, thus providing meaningful escalations our clients can take immediate action against.
8. **MITRE:** NuHarbor Security maps our Alert escalations to the MITRE ATT&CK Framework/MITRE Categories. This allows our clients to map and track the number of alert escalations to the various categories that provide an impactful view of where the majority of vulnerabilities exist in their environment today quickly and intelligently.

NuHarbor Security delivers end-to-end security programs and is a trusted partner to business and public organizations alike. We offer a complete portfolio of security services and best of breed security technologies to our clients. We are *not* a security value-added reseller offering hundreds of security products. We are *not* an accounting firm doing an occasional security assessment. We are *not* a provider of a single security service, rather we offer a comprehensive portfolio of solutions so we can *partner* with our clients and deliver their end-to-end security services. Our approach to security, comprehensive offerings, and client-first perspective makes NuHarbor the ideal long-term security partner.

## Technology Partners

We are committed to serving our clients in the creation and maintenance of Information Security Programs and Enterprise Architecture by integrating premier security solutions from our best-in-breed technology partner portfolio. We exist to help secure all organizations and ease the complexity of cybersecurity. To this point, we have developed a best-of-breed philosophy around security technology and have developed deep industry expertise around those technologies.



NuHarbor's highly customizable MSSP is built around Splunk— the only IT Ops + SIEM solution that we support and sell – and seamlessly integrates with CrowdStrike for MDR, and/or Tenable for vulnerability management. Our offering of an enterprise-class SIEM built with the Splunk Enterprise Security (ES) platform provides 24/7/365 monitoring of log data. Additionally, NuHarbor is a certified reseller of other industry-leading solutions including Proofpoint, Imperva, CyberArk, Okta, Palo Alto Networks, ForeScout, and Veracode. These security technology partnerships support our services, and therefore we are very purposeful about striving to provide best-in-breed services supported by best-in-breed security technologies. We chose these solution partners because they work better together and are continuously evaluating and evolving our partner portfolio to best address the needs of our clients.

## Industry Recognition | Awards & Accolades

- CRN's Managed Service Provider (MSP) 500 List in the Security 100 Category
- Best Places to Work in Vermont
- Best Entrepreneurial Companies in America by Entrepreneur Magazine
- Splunk Elite Partner
- Splunk SLED Partner of the Year
- Splunk National Partner of the Year
- Tenable GOLD Medallion Status

## Strategic Partnerships

At NuHarbor, we are all about helping our clients win. In further commitment to the public sector, we have teamed up with our exclusive strategic partners to meet the specific needs of our clients – we’re stronger together. With the shared goal of helping clients defend themselves from the growing threat of cybersecurity attacks, we provide comprehensive solutions that are scalable and right sized to meet all our partner’s needs. NuHarbor, powered by Splunk and Tenable, is the exclusively endorsed partner to providing a turnkey managed cybersecurity solution for Counties and Cities nationwide.



### **National Association of Counties**

We deliver a turnkey managed security and vulnerability solution for the National Association of Counties (NACo) and its members. This comprehensive strategy is rightsized and customizable to meet the unique and specific needs of NACo

member counties across the United States. NuHarbor Powered by Splunk + Tenable maximizes the cost and operational efficiency of cutting-edge software solutions, and as a compliment to counties’ existing information security programs, will enhance resource utilization while upholding the highest cybersecurity standards.

In partnership with NACo, the goal is to help improve the ability of member counties to defend themselves from the growing threat of ransomware and other cybersecurity attacks.

Visit: <https://www.naco.org/> to learn more about NACo.



### **National League of Cities**

With industry leaders, Splunk and Tenable we are working to secure U.S. cities and towns from today’s most pressing threats via a partnership with the National League of Cities (NLC). Through the partnership, NuHarbor delivers a turnkey managed cybersecurity solution to NLC and its members. This comprehensive offering is scalable to meet the unique and specific needs of NLC member cities, towns, and villages across the United States.

Cyberattacks against local municipalities are on the rise as bad actors continue to target critical services. As the threats surge, local governments often struggle with a lack of resources and funding to secure their expanding attack surface.

NuHarbor powered by Splunk + Tenable maximizes the cost effectiveness and operational efficiency of cutting-edge software solutions and, as a complement to existing information security programs, enhances resource utilization while upholding the highest cybersecurity standards.

Visit: <https://www.nlc.org/> to learn more about NLC.

## 4.10 MARKETING PLAN

NuHarbor intends to build marketing collateral (e.g., one pager, presentation slides, email templates, etc.) outlining the contract and its value to the marketplace. We will also include marketing information related to the NCPA contract on our website and provide introductory and continuous messaging via social platforms (e.g., via LinkedIn).

#### 4.11 INTERNAL MARKETING PLAN

NuHarbor intends to kick off internal communications with enterprise-wide email messaging to announce the NCPA contract and terms and highlight the value of the contract to the market. We will host a Q&A session for NuHarbor's account management team and sales engineering professionals to address strategic positioning of the contract nationally to support as many SLED entities as possible in their efforts to stay safe and secure.

#### 4.12 ONLINE CATALOG

NuHarbor Security does not host an online catalog or digital marketplace for its Managed Services offerings. We believe there is no "one size fits all" approach to security. After conversation-based discovery, NuHarbor experts can understand the risks and threats unique to a client environment, and with that situational awareness, begin to craft a solution tailored specifically to those client needs.

#### 4.13 BUSINESS OPERATIONS

***Is all work performed within the United States? Is work performed by employees, contractors or sub-contractors. Please indicate the percentage performed by each group.***

We hire the 'best of the best' to protect every client's most sensitive information – 100% of our Managed Services are performed by NuHarbor employees within the United States. In alignment with stringent staffing requirements, NuHarbor maintains a non-possessing top-secret site security clearance issued by the U.S. Department of Energy Cybersecurity Divisions. As a requirement of this clearance, 100% of NuHarbor staff – all U.S. citizens based on U.S. soil – are subject to a rigorous background screening.

#### 4.14 EMPLOYEE CERTIFICATION AND ACCREDITATION

***Indicate the level of certification and accreditation of you employees or contractor on the tools they use in the delivery of services.***

##### SOC 2 Type 1 Audit

This report is valuable because it assures potential customers that their sensitive data will be handled safely by a vendor.

NuHarbor Security has third-party attestation of its SOC Program and Security Operations Center in Colchester, VT. The report clearly demonstrates that the NuHarbor SOC has best practices in place. A detailed copy of this SOC 2 report can be provided after a mutual non-disclosure agreement is signed between NuHarbor and the Client.

##### Splunk Accreditation

**NuHarbor Security is an Elite Splunk Partner** and was recently globally recognized as the **2021 Splunk Public Sector SLED Partner of the Year**. Collectively our fully accredited team holds 85+ Splunk certifications. NuHarbor engineers have successfully completed over 350 small, medium, and large state and local public-sector and commercial implementations and bring a wealth of practical experience to each new client. We employ numerous Analysts and Engineers with the highest levels of Splunk certification: Consultant, Architect, and Enterprise Admin. Our consultants are leveraged by Splunk to provide professional services on their behalf to Splunk clients across the country. We are proud to offer



clients a deep bench of Splunk experts to help ensure their Splunk instance scales efficiently for years to come.

Certificate/Accreditation Type	NuHarbor Employees
Splunk Accredited IT & App Sales Rep	1
Splunk Accredited Sales Engineer I	5
Splunk Accredited Sales Engineer II	3
Splunk Accredited Sales Rep I	18
Splunk Accredited Sales Rep II	5
Splunk Accredited Security Sales Rep I	1
Splunk Accredited Security SME I (SE)	1
Splunk Core Certified Consultant	2
Splunk Core Certified Power User	17
Splunk Core Certified User	12
Splunk Enterprise Certified Admin	13
Splunk Enterprise Certified Architect	7
Splunk Enterprise Security Certified Admin	1

### Managed Services Skills Matrix

100% of NuHarbor Security Analysts and Engineers hold security certifications. Our security staff averages 7-10 years of experience performing security monitoring or security consulting. Our Managed SOC teams possess the following minimum certifications and experience:

Skill	Analyst I	Analyst II	Sr. Analyst	Analyst Lead
Bachelor's degree in Computer Science, Information Security, Cyber Security or 5+ Years Relevant Experience	REQUIRED	REQUIRED	REQUIRED	REQUIRED
Industry Certifications from GIAC, SANS, ISC2, CompTIA, Vendors	REQUIRED	REQUIRED	REQUIRED	REQUIRED
2 Years' Experience	DESIRED	REQUIRED	REQUIRED	REQUIRED
3 Years' Experience	DESIRED	REQUIRED	REQUIRED	REQUIRED
Offensive security tools, techniques + procedures	DESIRED	REQUIRED	REQUIRED	REQUIRED
Defensive mitigation techniques + strategies	DESIRED	REQUIRED	REQUIRED	REQUIRED
Threat Modeling + Business Risk	DESIRED	DESIRED	REQUIRED	REQUIRED

### Additional Staff Certifications

- CISSP (Certified Information Systems Security Professional)
- CrowdStrike Partner Sales Engineer
- Certified Information Systems Auditor (CISA)
- C|CISO (Certified Chief Information Security Officer)
- ISO27001 Lead Implementer Certified

- ISO27001 Lead Auditor Certified
- PRINCE2 Project Management Certified
- Independent Security Assessor (ISA), PCI Council
- Certified Public Accountant (CPA)
- Certified Internal Auditor (CIA)
- Certified in Risk and Information Systems Control (CRISC), ISACA
- Certified Information Security Manager (CISM)
- ForeScout Certified Partner Engineer
- CMNA (Cisco Meraki Networking Associate)
- LogRhythm Certified Pre-Sales Consultant
- LogRhythm Certified Support Engineer
- Tenable Certified Network Sales Engineer
- Tenable Certified Security Center Sales Engineer
- CCNP Security
- CCNA Security
- CCNA Security+
- Certified Meraki Network Administrator
- Palo Alto Networks Accredited Configuration Engineer
- EMC Proven Professional RecoverPoint
- CNSS 4013 Cisco ISE Field Engineer
- Sourcefire Certified Professional
- Sourcefire Certified Security Engineer
- Cisco IPS Specialist
- Cisco Firewall Security Specialist
- Cisco IOS Security Specialist
- Cisco VPN Specialist
- Cisco ASA Specialist
- Cisco Connected Physical Security Specialist
- Cisco FireJumper FirePOWER
- MCSA 2012
- MCSE Communications Lync 2013
- CSA (BSA)
- LPIC 1 and 2 (Linux)

#### 4.15 LICENSING AND OWNERSHIP

***Where services are to be supplied – what are the choices of license model. Does the customer own the software license or the vendor? Is there a choice?***

Our signature Managed Security Services offering is structured as a truly co-managed model (i.e., client data ownership, 100% visibility, and control), complete with goal-focused onboarding and proactive security analysis and guidance. With this approach, the client maintains license ownership, and enjoys immediate context and visibility to the same data and workflow process our Analysts have during an event.

We also offer a fully-hosted MSSP offering – SOC as a Service Powered by Splunk – in which NuHarbor owns licensing, but the customer still owns 100% of its data.

***Who owns the security data artifacts and where are they held? What is the process of supplying the data to the customer at termination of services?***

With our signature co-managed offering, customer data never leaves the customer system, and they always have access to said data. Therefore, there is zero disruption upon termination of NuHarbor services. If leveraging the fully hosted MSSP offering, data is hosted in Splunk Cloud (AWS). Upon termination of NuHarbor services, that system’s licensing can be easily transferred to the customer or migrated to another destination in Splunk Cloud via a Professional Services agreement with NuHarbor.

#### 4.16 CUSTOMER SERVICE

Full-service hours of operation for the NuHarbor SOC are 8:00am-5:00pm ET on normal business days. The SOC responds to critical events 24x7x365. Critical events are defined in the Managed Services Agreements (MSA) specific to each of our offerings and defined with the customer during scoping conversations. NuHarbor utilizes both our Physical SOC in the Vermont headquarters and a dispersed Virtual SOC of securely networked engineers and analysts for extensive coverage. Our Virtual SOC is staffed 24/7/365. The SOC is staffed with deeply vetted and highly credentialed security engineers and analysts – all U.S. citizens based on U.S. soil – that are direct employees of NuHarbor.

#### 4.17 GREEN INITIATIVES

NuHarbor has a Zero Waste Policy and practices recycling of paper, plastic, glass bottles and food scraps. We follow the recommendations of the State of Vermont Environmental Protection Agency.

We use at least 50% remanufactured toner cartridges in printers. We use Green Cleaning products (certified by UL Ecologo, GreenSeal or SaferChoice) in all cleaning or janitorial services, including recycled paper towels. All printers, microwaves, refrigerators are Energy Star or EPEAT certified models.

#### 4.18 VENDOR CERTIFICATIONS

Copies of Vendor Certifications related to our technology partners for our Managed Services will be provided UPON ACCEPTANCE TO THE NCPA CONTRACT.



## TAB 5. PRODUCTS AND SERVICES/SCOPE

### 5.1 SECURITY AUDITS

#### Information Assurance (IA) Services

Our tenured team of easily accessible and highly certified IA analysts averages 10 years of compliance experience in the field and maintains a strong focus on the National Institute of Standards and Technology (NIST) frameworks. Through the lens of cybersecurity, our team is committed to protecting and defending our clients' information and information systems by ensuring their availability, integrity, authenticity, confidentiality, and non-repudiation. We offer comprehensive compliance services including security advisory and policy development, and perform gap assessments and audits for NIST 800-171, NIST 800-053, NIST CSF, FISMA, HIPAA, PCI, ISO 27001, the Cybersecurity Maturity Model Certification (CMMC), and more.

##### 5.1.1 Risk Assessment Audit – Internal Exposure

NuHarbor partners with clients to build effective Risk Management programs that include the performance of ongoing Risk Assessments. Based on NIST-800-30 guidance, below are example steps in the NuHarbor process:

*To support the enhancement of the client's overall security posture, NuHarbor Security recommends the development of a risk management program and completion of an initial risk assessment of the client's current security program. This assessment will identify, analyze, document, and categorize information security risks, including the analysis of threats and vulnerabilities that are meaningful and applicable to the organization. This activity will provide the Client with a foundation to build a new, or improve an existing, security program and make better risk-informed decisions around security strategy and controls.*

*This project will consist of two major phases:*

*Phase 1 has the following primary objectives:*

- *Develop and document the components of the client's risk management program, including a risk management plan.*
- *Perform an analysis of three systems to identify a relative risk rating/priority and determine which system merits a more rigorous risk assessment in Phase 2.*

*Phase 2 has the following primary objectives:*

- *Identify information security risks for the system identified in Phase 1.*
- *Identify current information security controls in place to address identified risks.*
- *Develop control recommendations for identified risks.*
- *Develop client awareness and understanding of ongoing risk management activities to maintain risk management efforts and general best practices.*
- *Develop and provide to the client a risk assessment report and a risk register (to facilitate tracking of, and accountability for, identified relevant risks).*

### 5.1.2 Gap Assessments or Readiness Assessments against Security Framework

NuHarbor’s IA team specializes in gap assessments and audits for a wide variety of security and compliance frameworks. These include the NIST Risk Management Framework (RMF) as well as other NIST security and controls publications (SP 800-171, 800-53, 800-30, etc.), CMMC, HIPAA Security Rule, ISO 27001, MARS-E, and PCI DSS. In addition, our IA team has significant experience providing security consulting and support to help meet a variety of other compliance needs.

A Compliance Gap Assessment assesses a company’s security posture against a certain framework or standard to identify:

1. If implemented controls are designed and operating effectively.
2. If there are missing/inadequate controls – then we assign a corresponding risk level.
3. Recommendations for implementing a missing control or mitigating certain risks.
4. Realistic and tactical recommendations for remediating gaps.

Other related Services:

- Security Policy Development
- Facilitation of Incident Response tabletop exercises

## 5.2 PROFESSIONAL SERVICES

### 5.2.1 Installation Services (list approved/qualified partners)

#### **Splunk**

NuHarbor Security holds an Elite Status (highest level) Certificate of Partnership with Splunk in the Splunk Partner+ Managed Service Provider Program. As such, we are also a “Professional Services Qualified Partner” having completed 350+ Splunk implementations to date.

NuHarbor employ numerous Analysts and Engineers with the highest levels of Splunk certification: Consultant, Architect, and Enterprise Admin. Our consultants are leveraged by Splunk to provide professional services on their behalf to Splunk clients across the country. We are proud to offer clients a deep bench of Splunk experts to help ensure their Splunk instance scales efficiently for years to come.

NuHarbor’s Splunk-certified Engineers and skilled Project Managers work with our customers to determine their unique needs, then design and implement the precise configuration for their environment. We have expertise in Splunk Enterprise, Splunk Cloud, Splunk Enterprise Security, Splunk App for CMMC, and many of the other Splunk APPs and technology add-ons (TAs). The customer may choose their installation preference – we can install Splunk on-premises, in the Cloud platform of choice, or in Splunk Cloud.

## 5.3 MANAGED SERVICES

### 5.3.1 Managed Detect and Response Services (MDR)

Our Managed Detection & Response (MDR) service operates on CrowdStrike Falcon Enterprise, which integrates seamlessly with Splunk Enterprise Security when available. NuHarbor chooses to provide only the best-in-class information security solutions to our clients. We believe CrowdStrike offers the sharpest Endpoint Detection Response (EDR) solutions on the market today. Leveraging CrowdStrike

Falcon, the NuHarbor MDR service run by our expert SOC analysts provides excellent protection and visibility, and exceptional 24x7 protection from potential breaches and infections.

With CrowdStrike Falcon EDR/MDR service, clients take environment-wide visibility to the next level (e.g., an employee working from home or at Starbucks with their laptop). The Falcon agent also offers us additional response options (e.g., quarantine machine or take offline) and can be automated where appropriate or validated by a NuHarbor security analyst before action is taken.

NOTE: Pricing for MDR is based on # of endpoints included in a CrowdStrike license.

### 5.3.2 Vulnerability Management as a Service

NuHarbor utilizes the Tenable framework and its addons for Vulnerability Assessment and Management.

NuHarbor implements the following methodology for implementing the Tenable Concierge service:

- Collect organizational context.
- Define organizational reporting metrics and scan success criteria.
- Configure Tenable to support organization structure (i.e., multi-tenancy, etc.).
- Perform discovery scans.
- Coordinate agent deployment where necessary.
- Configure authenticated scans.
- Test scan policies against QA systems and remediate configuration problems.
- Perform production scans.

Once the client environment gains visibility into assets and vulnerabilities, NuHarbor begins providing curated analysis of scan results. This process follows these general steps:

- Use Common Vulnerability Scoring System metrics to prioritize vulnerabilities.
- Cross reference prioritized vulnerabilities against asset priority and asset attack surface.
- Review lower priority vulnerabilities to determine if any should be addressed immediately.
- Review curated list of vulnerabilities with client stakeholders.
- Review list of outstanding vulnerabilities and provide recommendations for appropriate compensating controls.

Assets are initially prioritized using the following methodology:

- CVSS Score which includes Attack Vector, Attack Complexity, Required Privileges, User Interaction, Confidentiality, Integrity, and Availability.
- Asset priority to business mission.
- Asset attack surface based on location in the network.
- Relation to kill chain phase and MITRE ATT&CK framework categories.
- Difference between first seen and last seen.

The NuHarbor Security Operations Center (24x7 SOC) will configure scheduled and ad-hoc scans and manage them for the customer. We deliver prioritized reports to the customer's patching team in a format appropriate to support patching. After a patch cycle has completed, NuHarbor can run follow up reports to validate that previously identified vulnerabilities have been adequately addressed.

### 5.3.3 Security Information and Event Management (SIEM) as a Service

NuHarbor is proud to offer a fully-hosted MSSP (SIEM/SOC/SOAR as a Service) offering – SOC as a Service Powered by Splunk – in which NuHarbor owns licensing, but the customer still owns 100% of its data. NuHarbor will stand up, host, and fully manage the Splunk instance on behalf of our customer.

Our signature Managed Security Services offering is structured as a truly co-managed model. With this approach, the client maintains license and data ownership, and enjoys 100% visibility and control. With this model, our Admin & Dev Engineers and SOC Security Analysts will work with client resources to protect the organization. The customer will have full access to the system and can use as frequently as desired. NuHarbor’s SOC and Cyber Threat (CTAC) Analysts work to protect the client 24x7x365. NuHarbor’s Admin & Dev team take responsibility for maintaining the health of the environment, loading new data sources, and creating new dashboards, searches, reports, or alerts upon customer request. NuHarbor will perform all upgrades, patches, fixes, and other support tasks on the Splunk instance. We are available via phone, text, email, or service ticket.

Escalation options with NuHarbor are very flexible and will be defined with the customer at onboarding through the creation of a “Call Tree” and “Rules of Engagement” document. Communication options include phone, text (SMS), email, or ticket system. Escalation rules can vary depending on hours and business days and be customized by customer preference. Any escalation can be followed up by phone with the Analyst who escalated the incident to gain deeper insight and begin work on a resolution. The escalation will contain suggestions for where to begin.

An optional Integration into other enterprise support and/or service desk applications (e.g., Altiris, Remedy, SNOW, etc.) is available. This allows both teams to work within the system they are most accustomed to.

### 5.3.4 Identity and Access Management (IAM) as a Service

The NuHarbor Identity and Access Management (IAM) as a Service solution is one part access administration and one part security monitoring and optimization. The administration service provides continuous IAM hygiene managing rules and policies around the user life cycle and support of a flexible identity store and token services for a progressive identity architecture. The security service provides MSSP-like capabilities on top of the existing identity store to proactively identify and alert on suspicious access and authentication events. The service also generates high-fidelity security telemetry that can be integrated to other security products for a robust security alerting system.

## TAB 8. VALUE ADDED PRODUCTS AND SERVICES

### Offensive Security Operations | Technical Testing and Readiness

At NuHarbor Security we take pride in being a full security lifecycle provider. All our services are designed to support any information security need an organization might have. Since inception, NuHarbor has partnered with clients to plan offensive services that flex to their unique needs.

Our REDSEC team provides remote and on-site services including:

- Web Application Penetration Testing
- Internal/External Penetration Testing
- Wireless Penetration Testing
- Infrastructure Penetration Testing
- Source Code Reviews
- Phishing Attack Assessments
- Vulnerability Scanning
- Dynamic Application Scanning



Clients are drawn to our focus on the offensive penetration testing space, supplemented with years of testing experience and a comprehensive reporting structure. There is no such thing as a standard penetration test or vulnerability scan – automated testing cannot find common errors that stem from misconfiguration and human oversight. NuHarbor’s veteran engineers can uncover the vulnerabilities before someone else does.

In addition, our team provides assessment and advisory services including incidence response planning, security program reviews, and security risk assessments.

***NOTE: All pricing is based on the scope of work.***

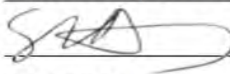
## TAB 9. REQUIRED DOCUMENTS

## 9.1 CLEAN AIR AND WATER ACT / DEBARMENT NOTICE

**Clean Air and Water Act & Debarment Notice**

I, the Vendor, am in compliance with all applicable standards, orders or regulations issued pursuant to the Clean Air Act of 1970, as Amended (42 U.S. C. 1857 (h), Section 508 of the Clean Water Act, as amended (33 U.S.C. 1368), Executive Order 117389 and Environmental Protection Agency Regulation, 40 CFR Part 15 as required under OMB Circular A-102, Attachment O, Paragraph 14 (1) regarding reporting violations to the grantor agency and to the United States Environment Protection Agency Assistant Administrator for the Enforcement.

I hereby further certify that my company has not been debarred, suspended or otherwise ineligible for participation in Federal Assistance programs under Executive Order 12549, "Debarment and Suspension", as described in the Federal Register and Rules and Regulations

Potential Vendor	NuHarbor Security, Inc.
Print Name	Scott Mosher
Address	553 Roosevelt Hwy, Ste 102
City, State, Zip	Colchester, VT 05446
Authorized signature	
Date	11/18/2021



## 9.2 CONTRACTORS REQUIREMENTS

### **Contractor Requirements**

#### **Contractor Certification Contractor's Employment Eligibility**

By entering the contract, Contractor warrants compliance with the Federal Immigration and Nationality Act (FINA), and all other federal and state immigration laws and regulations. The Contractor further warrants that it is in compliance with the various state statues of the states it is will operate this contract in.

Participating Government Entities including School Districts may request verification of compliance from any Contractor or subcontractor performing work under this Contract. These Entities reserve the right to confirm compliance in accordance with applicable laws.

Should the Participating Entities suspect or find that the Contractor or any of its subcontractors are not in compliance, they may pursue any and all remedies allowed by law, including, but not limited to: suspension of work, termination of the Contract for default, and suspension and/or debarment of the Contractor. All costs necessary to verify compliance are the responsibility of the Contractor.

The offeror complies and maintains compliance with the appropriate statutes which requires compliance with federal immigration laws by State employers, State contractors and State subcontractors in accordance with the E-Verify Employee Eligibility Verification Program.

Contractor shall comply with governing board policy of the NCPA Participating entities in which work is being performed

#### **Fingerprint & Background Checks**

If required to provide services on school district property at least five (5) times during a month, contractor shall submit a full set of fingerprints to the school district if requested of each person or employee who may provide such service. Alternately, the school district may fingerprint those persons or employees. An exception to this requirement may be made as authorized in Governing Board policy. The district shall conduct a fingerprint check in accordance with the appropriate state and federal laws of all contractors, subcontractors or vendors and their employees for which fingerprints are submitted to the district. Contractor, subcontractors, vendors and their employees shall not provide services on school district properties until authorized by the District.

The offeror shall comply with fingerprinting requirements in accordance with appropriate statutes in the state in which the work is being performed unless otherwise exempted.

Contractor shall comply with governing board policy in the school district or Participating Entity in which work is being performed

#### **Business Operations in Sudan, Iran**

In accordance with A.R.S. 35-391 and A.R.S. 35-393, the Contractor hereby certifies that the contractor does not have scrutinized business operations in Sudan and/or Iran.

Authorized signature



Scott Mosher, Vice President

Date

11/18/2021

---

### 9.3 ANTITRUST CERTIFICATION STATEMENTS

#### **Antitrust Certification Statements (Tex. Government Code § 2155.005)**

I affirm under penalty of perjury of the laws of the State of Texas that:

(1) I am duly authorized to execute this contract on my own behalf or on behalf of the company, corporation, firm, partnership or individual (Company) listed below;

(2) In connection with this bid, neither I nor any representative of the Company has violated any provision of the Texas Free Enterprise and Antitrust Act, Tex. Bus. & Comm. Code Chapter 15;

(3) In connection with this bid, neither I nor any representative of the Company has violated any federal antitrust law; and

(4) Neither I nor any representative of the Company has directly or indirectly communicated any of the contents of this bid to a competitor of the Company or any other company, corporation, firm, partnership or individual engaged in the same line of business as the Company.

Company name	NuHarbor Security, Inc.
Address	553 Roosevelt Hwy, Ste 102
City/State/Zip	Colchester, VT 05446
Telephone No.	802-881-4224
Fax No.	n/a
Email address	smosher@nuharborsecurity.com
Printed name	Scott Mosher
Position with company	Vice President
Authorized signature	



#### 9.4 REQUIRED CLAUSES FOR FEDERAL FUNDS CERTIFICATIONS

NuHarbor Security acknowledges the terms included.

#### 9.5 REQUIRED CLAUSES FOR FEDERAL ASSISTANCE BY FTA

NuHarbor Security acknowledges the terms included.

#### 9.6 STATE NOTICE ADDENDUM

NuHarbor Security acknowledges the terms included.