



Lexington-Fayette Urban County Government

Request for Proposal

The Lexington-Fayette Urban County Government hereby requests proposals for **RFP #5-2021 Information Technology Consulting and Technical Services** to be provided in accordance with terms, conditions and specifications established herein.

Online proposals will be received at <https://lexingtonky.ionwave.net/> until **2:00 PM**, prevailing local time, on **March 30, 2021**.

Proposals received after the date and time set for opening proposals will not be considered for award of a contract and will be returned unopened to the Proposer. It is the sole responsibility of the Proposer to assure that his/her proposal is received (uploaded to <https://lexingtonky.ionwave.net/>) by the Division of Central Purchasing before the date and time set for opening proposals.

Additional copies of this Request For Proposals are available from the Division of Central Purchasing, Room 338 Government Center, 200 East Main Street, Lexington, KY 40507, (859)-258-3320, at no charge.

Proposals, once submitted, may not be withdrawn for a period of sixty (60) calendar days.

The Proposer must upload one (1) electronic version in PDF format to <https://lexingtonky.ionwave.net/>.

The Lexington-Fayette Urban County Government reserves the right to reject any or all proposals, and to waive technicalities and informalities when such waiver is determined by the Lexington-Fayette Urban County Government to be in its best interest.

Signature of this proposal by the Proposer constitutes acceptance by the Proposer of terms, conditions and requirements set forth herein.

Minor exceptions may not eliminate the proposal. Any exceptions to the specifications established herein shall be listed in detail on a separate sheet and attached hereto. The Lexington-Fayette Urban County Government shall determine whether any exception is minor.

The Lexington-Fayette Urban County Government encourages the participation of minority- and women-owned businesses in Lexington-Fayette Urban County Government contracts. This proposal is subject to Affirmative Action requirements attached hereto.

Please do not contact any LFUCG staff member or any other person involved in the selection process other than the designated contact person(s) regarding the project contemplated under this RFP while this RFP is open and a selection has not been finalized. Any attempt to do so may result in disqualification of the firm's submittal for consideration.

Laws and Regulations

All applicable state laws, ordinances and resolutions (including but not limited to Section 2-33 (Discrimination due to sexual orientation or gender identity) and Chapter 13 (Licenses and Regulations) of the Lexington-Fayette Urban County Government Code of Ordinances, and Resolution No. 484-17 (Minority, Women, and Veteran-Owned Businesses)) and the regulations of all authorities having jurisdiction over the project shall apply to the contract, and shall be deemed to be incorporated herein by reference.

Equal Employment Opportunity

The Entity (regardless of whether construction contractor, non-construction contractor or supplier) agrees to provide equal opportunity in employment for all qualified persons, to prohibit discrimination in employment because of race, color, religion, sex (including pregnancy, sexual orientation or gender identity), national origin, disability, age, genetic information, political affiliation, or veteran status, and to promote equal employment through a positive, continuing program from itself and each of its sub-contracting agents. This program of equal employment opportunity shall apply to every aspect of its employment policies and practices.

Kentucky Equal Employment Opportunity Act

The Kentucky Equal Employment Opportunity Act of 1978 (KRS 45.560-45.640) requires that any "county, city, town, school district, water district, hospital district, or other political subdivision of the state shall include in directly or indirectly publicly funded contracts for supplies, materials, services, or equipment hereinafter entered into the following provisions:

"During the performance of this contract, the contractor agrees as follows:

- (1) The contractor will not discriminate against any employee or applicant for employment because of race, color, religion, sex, age, or national origin;
- (2) The contractor will state in all solicitations or advertisements for employees placed by or on behalf of the contractors that all qualified applicants will receive consideration for employment without regard to race, color, religion, sex, age, or national origin;
- (3) The contractor will post notices in conspicuous places, available to employees and applicants for employment, setting forth the provision of the nondiscrimination clauses required by this section; and
- (4) The contractor will send a notice to each labor union or representative of workers with which he has a collective bargaining agreement or other contract or understanding advising the labor union or workers' representative of the contractor's commitments under the nondiscrimination clauses."

The Act further provides:

"KRS 45.610. Hiring minorities -- Information required

- (1) For the length of the contract, each contractor shall hire minorities from other sources within the drawing area, should the union with which he has collective bargaining agreements be unwilling to supply sufficient minorities to satisfy the agreed upon goals and timetables.
- (2) Each contractor shall, for the length of the contract, furnish such information as required by KRS 45.560 to KRS 45.640 and by such rules, regulations and orders issued pursuant thereto and will permit access to all books and records pertaining to his employment practices and work sites by the contracting agency and the department for purposes of investigation to ascertain compliance with KRS 45.560 to 45.640 and such rules, regulations and orders issued pursuant thereto.

KRS 45.620. Action against contractor -- Hiring of minority contractor or subcontractor

- (1) If any contractor is found by the department to have engaged in an unlawful practice under this chapter during the course of performing under a contract or subcontract covered under KRS 45.560 to 45.640, the department shall so certify to the contracting

agency and such certification shall be binding upon the contracting agency unless it is reversed in the course of judicial review.

(2) If the contractor is found to have committed an unlawful practice under KRS 45.560 to 45.640, the contracting agency may cancel or terminate the contract, conditioned upon a program for future compliance approved by the contracting agency and the department. The contracting agency may declare such a contractor ineligible to bid on further contracts with that agency until such time as the contractor complies in full with the requirements of KRS 45.560 to 45.640.

(3) The equal employment provisions of KRS 45.560 to 45.640 may be met in part by a contractor by subcontracting to a minority contractor or subcontractor. For the provisions of KRS 45.560 to 45.640, a minority contractor or subcontractor shall mean a business that is owned and controlled by one or more persons disadvantaged by racial or ethnic circumstances.

KRS 45.630 Termination of existing employee not required, when

Any provision of KRS 45.560 to 45.640 notwithstanding, no contractor shall be required to terminate an existing employee upon proof that employee was employed prior to the date of the contract.

KRS 45.640 Minimum skills

Nothing in KRS 45.560 to 45.640 shall require a contractor to hire anyone who fails to demonstrate the minimum skills required to perform a particular job."

It is recommended that all of the provisions above quoted be included as special conditions in each contract. In the case of a contract exceeding \$250,000, the contractor is required to furnish evidence that his workforce in Kentucky is representative of the available workforce in the area from which he draws employees, or to supply an Affirmative Action plan which will achieve such representation during the life of the contract.

LFUCG Non-Appropriation Clause

Contractor acknowledges that the LFUCG is a governmental entity, and the contract validity is based upon the availability of public funding under the authority of its statutory mandate.

In the event that public funds are unavailable and not appropriated for the performance of the LFUCG's obligations under this contract, then this contract shall automatically expire without penalty to the LFUCG thirty (30) days after written notice to Contractor of the unavailability and non-appropriation of public funds. It is expressly agreed that the LFUCG shall not activate this non-appropriation provision for its convenience or to circumvent the requirements of this contract, but only as an emergency fiscal measure during a substantial fiscal crisis, which affects generally its governmental operations.

In the event of a change in the LFUCG's statutory authority, mandate and mandated functions, by state and federal legislative or regulatory action, which adversely affects the LFUCG's authority to continue its obligations under this contract, then this contract shall automatically terminate without penalty to the LFUCG upon written notice to Contractor of such limitation or change in the LFUCG's legal authority.

Contention Process

Vendors who respond to this invitation have the right to file a notice of contention associated with the RFP process or to file a notice of appeal of the recommendation made by the Director of Central Purchasing resulting from this invitation.

Notice of contention with the RFP process must be filed within 3 business days of the bid/proposal opening by (1) sending a written notice, including sufficient documentation to support contention, to the Director of the Division of Central Purchasing or (2) submitting a written request for a meeting with the Director of Central Purchasing to explain his/her contention with the RFP process. After consulting with the Commissioner of Finance the Chief Administrative Officer and reviewing the documentation and/or hearing the vendor, the Director of Central Purchasing shall promptly respond in writing findings as to the compliance with RFP processes. If, based on this review, a RFP process irregularity is deemed to have occurred the Director of Central Purchasing will consult with the Commissioner of Finance, the Chief Administrative Officer and the Department of Law as to the appropriate remedy.

Notice of appeal of a RFP recommendation must be filed within 3 business days of the RFP recommendation by (1) sending a written notice, including sufficient documentation to support appeal, to the Director, Division of Central Purchasing or (2) submitting a written request for a meeting with the Director of Central Purchasing to explain his appeal. After reviewing the documentation and/or hearing the vendor and consulting with the Commissioner of Finance and the Chief Administrative Officer, the Director of Central Purchasing shall in writing, affirm or withdraw the recommendation.

SELECTION CRITERIA:

1. Specialized experienced and technical competence of the person or firm with the type of service required. **20 Points Max.**
2. Capacity of the person or firm to perform the work, including any specialized services, within the time limitations. **20 Points Max.**
3. Past record and performance on contracts with the LFUCG or other governmental agencies and private industry with respect to such factors as control of cost, quality of work and ability to meet scheduling.
4. Familiarity with the details of the project. **20 Points Max.**
5. Degree of local employment to be provided by the person or firm. **10 Points Max.**
6. Estimated cost of services. **10 Points Max.**

Proposals shall contain the appropriate information necessary to evaluate based on these criteria. A committee composed of government employees as well as representatives of relevant user groups will evaluate the proposals.

Questions shall be addressed to:

Todd Slatin, Director
Division of Central Purchasing
tslatin@lexingtonky.gov

Affirmative Action Plan

All vendors must submit as a part of the proposal package the following items to the Urban County Government:

1. Affirmative Action Plan for his/her firm;
2. Current Work Force Analysis Form;

Failure to submit these items as required may result in disqualification of the submitter from award of the contract. All submissions should be directed to:

Director, Division of Central Purchasing
Lexington-Fayette Urban County Government
200 East Main Street, 3rd Floor
Lexington, Kentucky 40507

All questions regarding this proposal must be directed to the Division of Central Purchasing, (859)-258-3320.

AFFIDAVIT

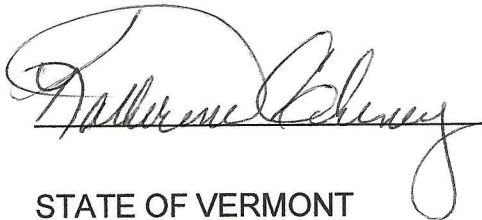
Comes the Affiant, Katherine Cheney, and after being first duly sworn, states under penalty of perjury as follows:

1. His/her name is Katherine Cheney and he/she is the individual submitting the proposal or is the authorized representative of NuHarbor Security, the entity submitting the proposal (hereinafter referred to as "Proposer").
2. Proposer will pay all taxes and fees, which are owed to the Lexington-Fayette Urban County Government at the time the proposal is submitted, prior to award of the contract and will maintain a "current" status in regard to those taxes and fees during the life of the contract.
3. Proposer will obtain a Lexington-Fayette Urban County Government business license, if applicable, prior to award of the contract.
4. Proposer has authorized the Division of Central Purchasing to verify the above-mentioned information with the Division of Revenue and to disclose to the Urban County Council that taxes and/or fees are delinquent or that a business license has not been obtained.
5. Proposer has not knowingly violated any provision of the campaign finance laws of the Commonwealth of Kentucky within the past five (5) years and the award of a contract to the Proposer will not violate any provision of the campaign finance laws of the Commonwealth.
6. Proposer has not knowingly violated any provision of Chapter 25 of the Lexington-Fayette Urban County Government Code of Ordinances, known as "Ethics Act."

Continued on next page

7. Proposer acknowledges that "knowingly" for purposes of this Affidavit means, with respect to conduct or to circumstances described by a statute or ordinance defining an offense, that a person is aware or should have been aware that his conduct is of that nature or that the circumstance exists.

Further, Affiant sayeth naught.




STATE OF VERMONT

COUNTY OF CHITTENDEN

The foregoing instrument was subscribed, sworn to and acknowledged before me by Katherine Cheney on this the 15 day of March, 2021.

My Commission expires: 01/31/2023



NOTARY PUBLIC, STATE AT LARGE



EQUAL OPPORTUNITY AGREEMENT

The Law

- Title VII of the Civil Rights Act of 1964 (amended 1972) states that it is unlawful for an employer to discriminate in employment because of race, color, religion, sex, age (40-70 years) or national origin.
- Executive Order No. 11246 on Nondiscrimination under Federal contract prohibits employment discrimination by contractor and sub-contractor doing business with the Federal Government or recipients of Federal funds. This order was later amended by Executive Order No. 11375 to prohibit discrimination on the basis of sex.
- Section 503 of the Rehabilitation Act of 1973 states:

The Contractor will not discriminate against any employee or applicant for employment because of physical or mental disability.

- Section 2012 of the Vietnam Era Veterans Readjustment Act of 1973 requires Affirmative Action on behalf of disabled veterans and veterans of the Vietnam Era by contractors having Federal contracts.
- Section 206(A) of Executive Order 12086, Consolidation of Contract Compliance Functions for Equal Employment Opportunity, states:

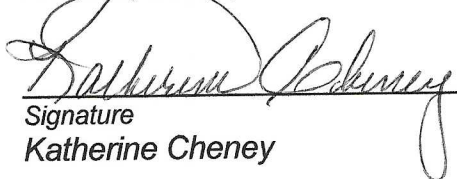
The Secretary of Labor may investigate the employment practices of any Government contractor or sub-contractor to determine whether or not the contractual provisions specified in Section 202 of this order have been violated.

The Lexington-Fayette Urban County Government practices Equal Opportunity in recruiting, hiring and promoting. It is the Government's intent to affirmatively provide employment opportunities for those individuals who have previously not been allowed to enter into the mainstream of society. Because of its importance to the local Government, this policy carries the full endorsement of the Mayor, Commissioners, Directors and all supervisory personnel. In following this commitment to Equal Employment Opportunity and because the Government is the benefactor of the Federal funds, it is both against the Urban County Government policy and illegal for the Government to let contracts to companies which knowingly or unknowingly practice discrimination in their employment practices. Violation of the above mentioned ordinances may cause a contract to be canceled and the contractors may be declared ineligible for future consideration.

Please sign this statement in the appropriate space acknowledging that you have read and understand the provisions contained herein. Return this document as part of your application packet.

Bidders

I/We agree to comply with the Civil Rights Laws listed above that govern employment rights of minorities, women, Vietnam veterans, handicapped and aged persons.

 _____ NuHarbor Security _____
 Signature Name of Business
 Katherine Cheney

WORKFORCE ANALYSIS FORM

Name of Organization: NuHarbor Security

Categories	Total	White (Not Hispanic or Latino)		Hispanic or Latino		Black or African-American (Not Hispanic or Latino)		Native Hawaiian and Other Pacific Islander (Not Hispanic or Latino)		Asian (Not Hispanic or Latino)		American Indian or Alaskan Native (not Hispanic or Latino)		Two or more races (Not Hispanic or Latino)		Total	
		M	F	M	F	M	F	M	F	M	F	M	F	M	F	M	F
Administrators	8	7	1													7	1
Professionals	45	27	9	1		3	1	1	1		1		1			32	13
Superintendents																	
Supervisors																	
Foremen																	
Technicians																	
Protective Service																	
Para-Professionals																	
Office/Clerical	20	9	7		1	2	1									11	9
Skilled Craft																	
Service/Maintenance																	
Total:	73	43	17	1	1	5	2	1	1	0	1	0	1	0	0	50	23

Prepared by: Katherine Cheney
Director, Human Resources
(Name and Title)

Date: 03/15/2021
Revised 2015-Dec-15

**DIRECTOR, DIVISION OF CENTRAL PURCHASING
LEXINGTON-FAYETTE URBAN COUNTY GOVERNMENT
200 EAST MAIN STREET
LEXINGTON, KENTUCKY 40507**

**NOTICE OF REQUIREMENT FOR AFFIRMATIVE ACTION TO ENSURE EQUAL
EMPLOYMENT OPPORTUNITIES AND DBE CONTRACT PARTICIPATION**

Notice of requirement for Affirmative Action to ensure Equal Employment Opportunities and Disadvantaged Business Enterprises (DBE) Contract participation. Disadvantaged Business Enterprises (DBE) consists of Minority-Owned Business Enterprises (MBE) and Woman-Owned Business Enterprises (WBE).

The Lexington-Fayette Urban County Government has set a goal that not less than ten percent (10%) of the total value of this Contract be subcontracted to Disadvantaged Business Enterprises, which is made up of MBEs and WBEs. The goal for the utilization of Disadvantaged Business Enterprises as subcontractors is a recommended goal. Contractor(s) who fail to meet such goal will be expected to provide written explanations to the Director of the Division of Purchasing of efforts they have made to accomplish the recommended goal, and the extent to which they are successful in accomplishing the recommended goal will be a consideration in the procurement process. Depending on the funding source, other DBE goals may apply.

For assistance in locating Disadvantaged Business Enterprises Subcontractors contact:

Sherita Miller, Division of Central Purchasing
Lexington-Fayette Urban County Government
200 East Main Street, 3rd Floor, Room 338
Lexington, Kentucky 40507
smiller@lexingtonky.gov

Lexington-Fayette Urban County Government MWDBE PARTICIPATION GOALS

A. GENERAL

- 1) The LFUCG request all potential contractors to make a concerted effort to include Minority-Owned (MBE), Woman-Owned (WBE), Disadvantaged (DBE) Business Enterprises and Veteran-Owned Businesses as subcontractors or suppliers in their bids.
- 2) Toward that end, the LFUCG has established 10% of total procurement costs as a Goal for participation of Minority-Owned, Woman-Owned and Disadvantaged Businesses on this contract.
- 3) **It is therefore a request of each Bidder to include in its bid, the same goal (10%) for MWDBE participation and other requirements as outlined in this section.**
- 4) The LFUCG has also established a 3% of total procurement costs as a Goal for participation for of Veteran-Owned Businesses.
- 5) **It is therefore a request of each Bidder to include in its bid, the same goal (3%) for Veteran-Owned participation and other requirements as outlined in this section.**

B. PROCEDURES

- 1) The successful bidder will be required to report to the LFUCG, the dollar amounts of all payments submitted to Minority-Owned or Woman-Owned subcontractors and suppliers for work done or materials purchased for this contract. (See Subcontractor Monthly Payment Report)
- 2) Replacement of a Minority-Owned or Woman-Owned subcontractor or supplier listed in the original submittal must be requested in writing and must be accompanied by documentation of Good Faith Efforts to replace the subcontractor / supplier with another MWDBE Firm; this is subject to approval by the LFUCG. (See LFUCG MWDBE Substitution Form)
- 3) For assistance in identifying qualified, certified businesses to solicit for potential contracting opportunities, bidders may contact:
 - a) The Lexington-Fayette Urban County Government, Division of Central Purchasing (859-258-3320)

- 4) The LFUCG will make every effort to notify interested MWDBE and Veteran-Owned subcontractors and suppliers of each Bid Package, including information on the scope of work, the pre-bid meeting time and location, the bid date, and all other pertinent information regarding the project.

C. DEFINITIONS

- 1) A Minority-Owned Business Enterprise (MBE) is defined as a business which is certified as being at least 51% owned and operated by persons of African American, Hispanic, Asian, Pacific Islander, American Indian or Alaskan Native Heritage.
- 2) A Woman-Owned Business Enterprise (WBE) is defined as a business which is certified as being at least 51% owned and operated by one or more Non-Minority Females.
- 3) A Disadvantaged Business (DBE) is defined as a business which is certified as being at least 51% owned and operated by a person(s) that are economically and socially disadvantaged.
- 4) A Veteran-Owned Business is defined as a business which is certified as being at least 51% owned and operated by a veteran and/or a service disabled veteran.
- 5) Good Faith Efforts are efforts that, given all relevant circumstances, a bidder or proposer actively and aggressively seeking to meet the goals, can reasonably be expected to make. In evaluating good faith efforts made toward achieving the goals, whether the bidder or proposer has performed the efforts outlined in the Obligations of Bidder for Good Faith Efforts outlined in this document will be considered, along with any other relevant factors.

D. OBLIGATION OF BIDDER FOR GOOD FAITH EFFORTS

- 1) **The bidder shall make a Good Faith Effort to achieve the Participation Goal for MWDBE subcontractors/suppliers. The failure to meet the goal shall not necessarily be cause for disqualification of the bidder; however, bidders not meeting the goal are required to furnish with their bids written documentation of their Good Faith Efforts to do so.**
- 2) Award of Contract shall be conditioned upon satisfaction of the requirements set forth herein.

- 3) The Form of Proposal includes a section entitled “MWDBE Participation Form”. The applicable information must be completed and submitted as outlined below.
- 4) **Failure to submit this information as requested may be cause for rejection of bid.**

E. DOCUMENTATION REQUIRED FOR GOOD FAITH EFFORTS

- 1) Bidders reaching the Goal are required to submit only the MWDBE Participation Form.” The form must be fully completed including names and telephone number of participating MWDBE firm(s); type of work to be performed; estimated value of the contract and value expressed as a percentage of the total Lump Sum Bid Price. The form must be signed and dated, and is to be submitted with the bid.
- 2) Bidders not reaching the Goal must submit the “MWDBE Participation Form”, the “Quote Summary Form” and a written statement documenting their Good Faith Effort to do so. If bid includes no MWDBE participation, bidder shall enter “None” on the subcontractor / supplier form). In addition, the bidder must submit written proof of their Good Faith Efforts to meet the Participation Goal:
 - a. Advertised opportunities to participate in the contract in at least two (2) publications of general circulation media; trade and professional association publications; small and minority business or trade publications; and publications or trades targeting minority, women and disadvantaged businesses not less than fifteen (15) days prior to the deadline for submission of bids to allow MWDBE firms to participate.
 - b. Included documentation of advertising in the above publications with the bidders good faith efforts package
 - c. Attended LFUCG Central Purchasing Economic Inclusion Outreach event
 - d. Attended pre-bid meetings that were scheduled by LFUCG to inform MWDBEs of subcontracting opportunities
 - e. Sponsored Economic Inclusion event to provide networking opportunities for prime contractors and MWDBE firms
 - f. Requested a list of MWDBE subcontractors or suppliers from LFUCG Economic Engine and showed evidence of contacting the companies on the list(s).
 - g. Contacted organizations that work with MWDBE companies for assistance in finding certified MWBDE firms to work on this project. Those

contacted and their responses should be a part of the bidder's good faith efforts documentation.

h. Sent written notices, by certified mail, email or facsimile, to qualified, certified MWDBEs soliciting their participation in the contract not less than seven (7) days prior to the deadline for submission of bids to allow them to participate effectively.

i. Followed up initial solicitations by contacting MWDBEs to determine their level of interest.

j. Provided the interested MWDBE firm with adequate and timely information about the plans, specifications, and requirements of the contract.

k. Selected portions of the work to be performed by MWDBE firms in order to increase the likelihood of meeting the contract goals. This includes, where appropriate, breaking out contract work items into economically feasible units to facilitate MWDBE participation, even when the prime contractor may otherwise perform these work items with its own workforce

l. Negotiated in good faith with interested MWDBE firms not rejecting them as unqualified without sound reasons based on a thorough investigation of their capabilities. Any rejection should be so noted in writing with a description as to why an agreement could not be reached.

m. Included documentation of quotations received from interested MWDBE firms which were not used due to uncompetitive pricing or were rejected as unacceptable and/or copies of responses from firms indicating that they would not be submitting a bid.

n. Bidder has to submit sound reasons why the quotations were considered unacceptable. The fact that the bidder has the ability and/or desire to perform the contract work with its own forces will not be considered a sound reason for rejecting a MWDBE quote. Nothing in this provision shall be construed to require the bidder to accept unreasonable quotes in order to satisfy MWDBE goals.

o. Made an effort to offer assistance to or refer interested MWDBE firms to obtain the necessary equipment, supplies, materials, insurance and/or bonding to satisfy the work requirements of the bid proposal

p. Made efforts to expand the search for MWBE firms beyond the usual geographic boundaries.

q. Other--any other evidence that the bidder submits which may show that the bidder has made reasonable good faith efforts to include MWDBE participation.

Failure to submit any of the documentation requested in this section may be cause for rejection of bid. Bidders may include any other documentation deemed relevant to this requirement. Documentation of Good Faith Efforts are to be submitted with the Bid, if the participation Goal is not met.



MINORITY BUSINESS ENTERPRISE PROGRAM

Sherita Miller, MPA
Minority Business Enterprise Liaison
Division of Central Purchasing
Lexington-Fayette Urban County Government
200 East Main Street
Lexington, KY 40507
smiller@lexingtonky.gov
859-258-3323

OUR MISSION: The mission of the Minority Business Enterprise Program is to facilitate the full participation of minority and women owned businesses in the procurement process and to promote economic inclusion as a business imperative essential to the long term economic viability of Lexington-Fayette Urban County Government.

To that end the city council adopted and implemented resolution 167-91—Disadvantaged Business Enterprise (DBE) 10% Goal Plan in July of 1991. The resolution states in part (a full copy is available in Central Purchasing):

“A Resolution supporting adoption of the administrative plan for a ten percent (10%) Minimum goal for disadvantaged business enterprise participation in Lexington-Fayette Urban County Government construction and professional services contracts; Providing that as part of their bids on LFUCG construction contracts, general Contractors shall make a good faith effort to award at least ten percent (10%) of All subcontracts to disadvantaged business enterprises; providing that divisions of LFUCG shall make a good faith effort to award at least ten percent of their Professional services and other contracts to disadvantaged business enterprises...”

A Disadvantaged Business Enterprise is defined as a business that has been certified as being at least 51% owned, operated and managed by a U.S. Citizen of the following groups:

- African-American
- Hispanic-American
- Asian/Pacific Islander
- Native American/Native Alaskan
- Non-Minority Female
- Economically and Socially Disadvantaged

In addition, to that end the city council also adopted and implemented resolution 167-91—Veteran-owned Businesses, 3% Goal Plan in July of 2015. The resolution states in part (a full copy is available in Central Purchasing):

“A resolution adopting a three percent (3%) minimum goal for certified veteran-owned small businesses and service disabled veteran-owned businesses for certain of those Lexington-Fayette Urban County contracts related to construction for professional services, and authorizing the Division of Purchasing to adopt and implement guidelines and/or policies consistent with the provisions and intent of this resolution by no later than July 1, 2015.”

We have compiled the list below to help you locate certified MBE, WBE and DBE certified businesses. Below is a listing of contacts for LFUCG Certified MWDBEs in Economic Engine (<https://lexingtonky.ionwave.net>)

Business	Contact	Email Address	Phone
LFUCG	Sherita Miller	smiller@lexingtonky.gov	859-258-3323
Commerce Lexington – Minority Business Development	Tyrone Tyra	ttyra@commercelexington.com	859-226-1625
Tri-State Minority Supplier Diversity Council	Sonya Brown	sbrown@tsmsdc.com	502-625-0137
Small Business Development Council	Dee Dee Harbut UK SBDC	ddharbut@uky.edu	859-257-7668
	Shirie Mack	smack3@email.uky.edu	859-257-7666
Community Ventures Corporation	James Coles	jcoles@cycky.org	859-231-0054
KY Department of Transportation	Melvin Bynes	Melvin.bynes2@ky.gov	502-564-3601
	Shella Eagle	Shella.Eagle@ky.gov	502-564-3601
Ohio River Valley Women’s Business Council (WBENC)	Rea Waldon	rwaldon@gcul.org	513-487-6534
Kentucky MWBE Certification Program	Yvette Smith, Kentucky Finance Cabinet	Yvette.Smith@ky.gov	502-564-8099
National Women Business Owner’s Council (NWBOC)	Janet Harris-Lange	janet@nwbo.org	800-675-5066
Small Business Administration	Robert Coffey	robertcoffey@sba.gov	502-582-5971
LaVoz de Kentucky	Andres Cruz	lavozydeky@yahoo.com	859-621-2106
The Key News Journal	Patrice Muhammad	paatricem@keynewsjournal.com	859-373-9428



LFUCG MWDBE PARTICIPATION FORM
Bid/RFP/Quote Reference #____ RFP #5-2021

The MWDBE subcontractors listed have agreed to participate on this Bid/RFP/Quote. If any substitution is made or the total value of the work is changed prior to or after the job is in progress, it is understood that those substitutions must be submitted to Central Purchasing for approval immediately.

MWDBE Company, Name, Address, Phone, Email	Work to be Performed	Total Dollar Value of the Work	% Value of Total Contract
1. None yet identified – will try again if we bid on a specific project.	We had hoped to find a local Splunk Certified Engineer to do configuration work.		Could be 50% of a Splunk project.
2.			
3.			
4.			

The undersigned company representative submits the above list of MWDBE firms to be used in accomplishing the work contained in this Bid/RFP/Quote. Any misrepresentation may result in the termination of the contract and/or be subject to applicable Federal and State laws concerning false statements and false claims.

NuHarbor Security

Company
 3/29/2021

Date

Scott Mosher

Company Representative
 Vice President

Title



LFUCG MWDBE SUBSTITUTION FORM

Bid/RFP/Quote Reference # _____ RFP #5-2021 _

The substituted MWDBE subcontractors listed below have agreed to participate on this Bid/RFP/Quote. These substitutions were made prior to or after the job was in progress. These substitutions were made for reasons stated below and are now being submitted to Central Purchasing for approval. By the authorized signature of a representative of our company, we understand that this information will be entered into our file for this project.

SUBSTITUTED MWDBE Company Name, Address, Phone, Email	MWDBE Formally Contracted/ Name, Address, Phone, Email	Work to Be Performed	Reason for the Substitution	Total Dollar Value of the Work	% Value of Total Contract
1. N/A – we will try again if we get a project					
2.					
3.					
4.					

The undersigned acknowledges that any misrepresentation may result in termination of the contract and/or be subject to applicable Federal and State laws concerning false statements and false claims.

NuHarbor Security

Company
 3/29/2021

Date

Scott Mosher

Company Representative
 Vice President

Title



MWDBE QUOTE SUMMARY FORM

Bid/RFP/Quote Reference # _____ RFP #5-2021 ____

The undersigned acknowledges that the minority subcontractors listed on this form did submit a quote to participate on this project.

Company Name	Contact Person
Address/Phone/Email	Bid Package / Bid Date

MWDBE Company Address	Contact Person	Contact Information (work phone, Email, cell)	Date Contacted	Services to be performed	Method of Communication (email, phone meeting, ad, event etc)	Total dollars \$\$ Do Not Leave Blank (Attach Documentation)	MBE * AA HA AS NA Female	Veteran
None identified at this time								

(MBE designation / AA=African American / HA= Hispanic American/AS = Asian American/Pacific Islander/ NA= Native American)

The undersigned acknowledges that all information is accurate. Any misrepresentation may result in termination of the contract and/or be subject to applicable Federal and State laws concerning false statements and claims.

NuHarbor Security

Company

3/29/2021

Date

Scott Mosher

Company Representative

Vice President

Title



LFUCG SUBCONTRACTOR MONTHLY PAYMENT REPORT

The LFUCG has a 10% goal plan adopted by city council to increase the participation of minority and women owned businesses in the procurement process. In order to measure that goal LFUCG will track spending with MWDBE vendors on a monthly basis. By the signature below of an authorized company representative, you certify that the information is correct, and that each of the representations set forth below is true. Any misrepresentation may result in termination of the contract and/or prosecution under applicable Federal and State laws concerning false statements and false claims. Please submit this form monthly to the Division of Central Purchasing/ 200 East Main Street / Room 338 / Lexington, KY 40507.

Bid/RFP/Quote #_RFP #5-2021 _____

Total Contract Amount Awarded to Prime Contractor for this Project _____

Project Name/ Contract #	Work Period/ From: _____ To: _____
Company Name:	Address:
Federal Tax ID:	Contact Person:

Subcontractor Vendor ID (name, address, phone, email)	Description of Work	Total Subcontract Amount	% of Total Contract Awarded to Prime for this Project	Total Amount Paid for this Period	Purchase Order number for subcontractor work (please attach PO)	Scheduled Project Start Date	Scheduled Project End Date
N/A							

By the signature below of an authorized company representative, you certify that the information is correct, and that each of the representations set forth below is true. Any misrepresentations may result in the termination of the contract and/or prosecution under applicable Federal and State laws concerning false statements and false claims.

NuHarbor Security

Company
 3/29/2021

Date

Scott Mosher

Company Representative
 Vice President

Title

in the contract not less than seven (7) days prior to the deadline for submission of bids to allow them to participate effectively.

YES Followed up initial solicitations by contacting MWDBEs to determine their level of interest.

YES Provided the interested MWDBE firm with adequate and timely information about the plans, specifications, and requirements of the contract.

YES Selected portions of the work to be performed by MWDBE firms in order to increase the likelihood of meeting the contract goals. This includes, where appropriate, breaking out contract work items into economically feasible units to facilitate MWDBE participation, even when the prime contractor may otherwise perform these work items with its own workforce

none identified with required certifications Negotiated in good faith with interested MWDBE firms not rejecting them as unqualified without sound reasons based on a thorough investigation of their capabilities. Any rejection should be so noted in writing with a description as to why an agreement could not be reached.

N/A Included documentation of quotations received from interested MWDBE firms which were not used due to uncompetitive pricing or were rejected as unacceptable and/or copies of responses from firms indicating that they would not be submitting a bid.

none identified with required certifications Bidder has to submit sound reasons why the quotations were considered unacceptable. The fact that the bidder has the ability and/or desire to perform the contract work with its own forces will not be considered a sound reason for rejecting a MWDBE quote. Nothing in this provision shall be construed to require the bidder to accept unreasonable quotes in order to satisfy MWDBE goals.

NO Made an effort to offer assistance to or refer interested MWDBE firms to obtain the necessary equipment, supplies, materials, insurance and/or bonding to satisfy the work requirements of the bid proposal

we searched across four (4) counties Made efforts to expand the search for MWDBE firms beyond the usual geographic boundaries.

YES Other - any other evidence that the bidder submits which may show that the bidder has made reasonable good faith efforts to include MWDBE participation.

Failure to submit any of the documentation requested in this section may be cause for rejection of bid. Bidders may include any other documentation deemed relevant to this requirement. Documentation of Good Faith Efforts are to be submitted with the Bid, if the participation Goal is not met.

The undersigned acknowledges that all information is accurate. Any misrepresentations may result in termination of the contract and/or be subject to applicable Federal and State laws concerning false statements and claims.

NuHarbor Security	Scott Mosher
<hr/>	<hr/>
Company	Company Representative
3/29/2021	Vice President
<hr/>	<hr/>
Date	Title

Good Faith Effort

NuHarbor Security was introduced too late to this RFP to post local advertisements. We have been unable to find any reference to any pre-bid meetings, but we may have been too late. We were unable to find any local Economic Inclusion events to attend.

NuHarbor did reach and exchange a few emails with Ms. Sherita Miller on March 15th, 2021. Ms. Miller supplied a list of ~463 LFUCG-certified vendors for review. NuHarbor filtered and searched the vendors on this list seeking those working in the Cybersecurity field in which NuHarbor works exclusively. We identified a total of 28 vendors that matched our search criteria. Six (6) of these were local within a few counties of Lexington. We emailed these six (6) on 3/16/21 with an introductory letter inviting them to participate in a discussion around the opportunity in this RFP. You may find copies of those emails below. Two firms quickly responded that they were not appropriate for the opportunity. Those responses are included below. We received a failed email attempt notice for a third, and no response from the remaining three (3). A closer search of their respective websites indicted one may be out of business and the other two (2) were not in the correct field.

At this point we investigated the websites of the 28 vendors identified in our search above (expanding our criteria). We did not identify additional firms with cybersecurity resources that were also within a 250-mile radius. We placed a phone call to one vendor that may have had access to the correct skillset, but said call was not returned.

NuHarbor has been unsuccessful at locating a local minority vendor that can supply correctly credentialed cybersecurity personnel to potentially perform services listed in this RFP that are in NuHarbor's area of expertise.

If we are accepted into the pool of approved vendors and presented with a specific RFP, that defines the precise skills required for that project, we will again perform a local search, and include local advertising as time allows.

This is the list of 28 we researched or attempted to contact:

360Water Inc.
Advanced Digital Solutions International Inc.
All-N-One Services, LLC
Americas Engineers, Inc.
ASK IT Consulting Inc.
CentraComm
Diverse Staffing Services, Inc. DBA DSS Consulting
ERP Analysts Inc.
Edwards Management Consultants, Inc.
Etech Consulting, LLC
GNO Consulting, Inc.
HyperGen Inc.
Information Systems Consultants, Inc.
iNovate Solution
ISI PROFESSIONAL SERVICES, LLC
John O'Bryan, LLC
LABUSA
McCoy Computer Services, LLC
Nextgen Consulting, Inc. - dba NGCI
N-ovation Technology Group LLC
Rang Technologies, LLC
RedSalsa Technologies, Inc.

Safety Research Corporation of America
Samiti Technology, Inc.
Starboard Consulting
Strategic Communications LLC
Sustainment Solutions, Inc.
Team Fishel
https://matrixintegration.com/

These are the six (6) we emailed:

John O'Bryan, LLC
LABUSA
McCoy Computer Services, LLC
Strategic Communications LLC
Sustainment Solutions, Inc.
Team Fishel

It turned out that none are appropriate for the job: employing cybersecurity professionals with specialization and certifications in Splunk and IT security audit specialties. The email we sent details the specifics of what we were looking for.

RFP-5-2021



Wes Lyle
To john@obryan.us

Reply Reply All Forward ...

Tue 3/16/2021 2:41 PM

Greetings Mr. O'Brian,

NuHarbor Security is responding to RFP-5-2021 for Lexington-Fayette Urban County Government. This RFP is for Information Technology Consulting and Technical Services. There is not a specific project or proposal associated with this RFP. The goal is rather to qualify into an approved pool for future work in various categories.

NuHarbor is looking to identify local Minority, Woman, and Disadvantaged Business Enterprises (MWDBEs) and Veteran-Owned Businesses that might partner with NuHarbor to satisfy some of these requirements. Again, there is no immediate project to bid on. We are strictly seeking to identify talent for future projects.

NuHarbor is a Cybersecurity company based in Vermont, with local presence along the East Coast. The pools we would like to qualify for are specific to our technology partners and portfolio of offerings. Below is a list of these categories and the type of skills required to perform the task envisioned.

Technology/Software	Skills Required/Relevant Certifications
Palo Alto Networks – Firewalls	Palo Alto Networks Certified Network Security Engineer (PCNSE)
Splunk	Splunk Enterprise Security Certified Admin
	Splunk Enterprise Certified Architect
	Splunk Core Certified Consultant
Information Security Services	Required Certifications
	Policy Development and Review – CISSP, CISA, CISM
	Planning and Analysis – CISM
	Penetration Testing – OSCP, OSWE, CISSP, GPEN
	Vulnerability Testing – OSCP, OSWE, CISSP, GPEN
	Risk Management Assessment – CISSP, CISA, CISM, CRISC
	Info Security Audit and Compliance – CISA
	Info Security Remediation – CISSP


If your business has employees with any of the above skill sets and certifications and you would like to discuss opportunities to partner with NuHarbor on these future projects, please respond indicating your interest and availability to discuss options.

Thank you,
Wes Lyle

Wes Lyle, CISSP

SR. CYBERSECURITY SOLUTIONS ARCHITECT
Splunk SE1, CSPSE, TCSA, FCPE, MCSE, MCSA, LCSE, CMNA, LPIC
(404) 641-2563
wlyle@nuharborsecurity.com
nuharborsecurity.com

RFP-5-2021

 **Wes Lyle**
To prioritysales@labusa.com

[Reply](#) [Reply All](#) [Forward](#) [...](#)

Tue 3/16/2021 2:45 PM

Greetings Mr. Laster,

NuHarbor Security is responding to RFP-5-2021 for Lexington-Fayette Urban County Government. This RFP is for Information Technology Consulting and Technical Services. There is not a specific project or proposal associated with this RFP. The goal is rather to qualify into an approved pool for future work in various categories.

NuHarbor is looking to identify local Minority, Woman, and Disadvantaged Business Enterprises (MWDDBEs) and Veteran-Owned Businesses that might partner with NuHarbor to satisfy some of these requirements. Again, there is no immediate project to bid on. We are strictly seeking to identify talent for future projects.

NuHarbor is a Cybersecurity company based in Vermont, with local presence along the East Coast. The pools we would like to qualify for are specific to our technology partners and portfolio of offerings. Below is a list of these categories and the type of skills required to perform the task envisioned.

Technology/Software	Skills Required/Relevant Certifications
Palo Alto Networks – Firewalls	Palo Alto Networks Certified Network Security Engineer (PCNSE)
Splunk	Splunk Enterprise Security Certified Admin
	Splunk Enterprise Certified Architect
	Splunk Core Certified Consultant
	Required Certifications
Information Security Services	Policy Development and Review – CISSP, CISA, CISM
	Planning and Analysis – CISM
	Penetration Testing – OSCP, OSWE, CISSP, GPEN
	Vulnerability Testing – OSCP, OSWE, CISSP, GPEN
	Risk Management Assessment – CISSP, CISA, CISM, CRISC
	Info Security Audit and Compliance – CISA
	Info Security Remediation – CISSP

If your business has employees with any of the above skill sets and certifications and you would like to discuss opportunities to partner with NuHarbor on these future projects, please respond indicating your interest and availability to discuss options.

Thank you,

Wes Lyle

RFP-5-2021 for Lexington-Fayette Urban County Government



Wes Lyle
 To dedrea.mccoy@mccoyscomputerservices.com

↩ Reply
↩ Reply All
→ Forward
⋮

Tue 3/16/2021 2:47 PM

Greetings Ms. McCoy,

NuHarbor Security is responding to RFP-5-2021 for Lexington-Fayette Urban County Government. This RFP is for Information Technology Consulting and Technical Services. There is not a specific project or proposal associated with this RFP. The goal is rather to qualify into an approved pool for future work in various categories.

NuHarbor is looking to identify local Minority, Woman, and Disadvantaged Business Enterprises (MWDBEs) and Veteran-Owned Businesses that might partner with NuHarbor to satisfy some of these requirements. Again, there is no immediate project to bid on. We are strictly seeking to identify talent for future projects.

NuHarbor is a Cybersecurity company based in Vermont, with local presence along the East Coast. The pools we would like to qualify for are specific to our technology partners and portfolio of offerings. Below is a list of these categories and the type of skills required to perform the task envisioned.

Technology/Software	Skills Required/Relevant Certifications
Palo Alto Networks – Firewalls	Palo Alto Networks Certified Network Security Engineer (PCNSE)
Splunk	Splunk Enterprise Security Certified Admin
	Splunk Enterprise Certified Architect
	Splunk Core Certified Consultant
Information Security Services	Required Certifications
	Policy Development and Review – CISSP, CISA, CISM
	Planning and Analysis – CISM
	Penetration Testing – OSCP, OSWE, CISSP, GPEN
	Vulnerability Testing – OSCP, OSWE, CISSP, GPEN
	Risk Management Assessment – CISSP, CISA, CISM, CRISC
	Info Security Audit and Compliance – CISA
	Info Security Remediation – CISSP

If your business has employees with any of the above skill sets and certifications and you would like to discuss opportunities to partner with NuHarbor on these future projects, please respond indicating your interest and availability to discuss options.

Thank you,

Wes Lyle

RFP-5-2021 for Lexington-Fayette Urban County Government



Wes Lyle
To cpayne@yourstrategic.com

↩ Reply
↩ Reply All
→ Forward
⋮

Tue 3/16/2021 2:49 PM

Greetings Mr Payne,

NuHarbor Security is responding to RFP #5-2021 for Lexington-Fayette Urban County Government. This RFP is for Information Technology Consulting and Technical Services. There is not a specific project or proposal associated with this RFP. The goal is rather to qualify into an approved pool for future work in various categories.

NuHarbor is looking to identify local Minority, Woman, and Disadvantaged Business Enterprises (MWDBEs) and Veteran-Owned Businesses that might partner with NuHarbor to satisfy some of these requirements. Again, there is no immediate project to bid on. We are strictly seeking to identify talent for future projects.

NuHarbor is a Cybersecurity company based in Vermont, with local presence along the East Coast. The pools we would like to qualify for are specific to our technology partners and portfolio of offerings. Below is a list of these categories and the type of skills required to perform the task envisioned.

Technology/Software	Skills Required/Relevant Certifications
Palo Alto Networks – Firewalls	Palo Alto Networks Certified Network Security Engineer (PCNSE)
Splunk	Splunk Enterprise Security Certified Admin
	Splunk Enterprise Certified Architect
	Splunk Core Certified Consultant
Information Security Services	Required Certifications
	Policy Development and Review – CISSP, CISA, CISM
	Planning and Analysis – CISM
	Penetration Testing – OSCP, OSWE, CISSP, GPEN
	Vulnerability Testing – OSCP, OSWE, CISSP, GPEN
	Risk Management Assessment – CISSP, CISA, CISM, CRISC
	Info Security Audit and Compliance – CISA
Info Security Remediation – CISSP	

If your business has employees with any of the above skill sets and certifications and you would like to discuss opportunities to partner with NuHarbor on these future projects, please respond indicating your interest and availability to discuss options.

Thank you,

Wes Lyle

RFP-5-2021 for Lexington-Fayette Urban County Government



Wes Lyle
To: aburikhanov@ssi-worldwide.com

Tue 3/16/2021 2:51 PM

Greetings Mr. Burikhanov,

NuHarbor Security is responding to RFP-5-2021 for Lexington-Fayette Urban County Government. This RFP is for Information Technology Consulting and Technical Services. There is not a specific project or proposal associated with this RFP. The goal is rather to qualify into an approved pool for future work in various categories.

NuHarbor is looking to identify local Minority, Woman, and Disadvantaged Business Enterprises (MWDBEs) and Veteran-Owned Businesses that might partner with NuHarbor to satisfy some of these requirements. Again, there is no immediate project to bid on. We are strictly seeking to identify talent for future projects.

NuHarbor is a Cybersecurity company based in Vermont, with local presence along the East Coast. The pools we would like to qualify for are specific to our technology partners and portfolio of offerings. Below is a list of these categories and the type of skills required to perform the task envisioned.


Technology/Software	Skills Required/Relevant Certifications
Palo Alto Networks – Firewalls	Palo Alto Networks Certified Network Security Engineer (PCNSE)
Splunk	Splunk Enterprise Security Certified Admin
	Splunk Enterprise Certified Architect
	Splunk Core Certified Consultant
Information Security Services	Required Certifications
	Policy Development and Review – CISSP, CISA, CISM
	Planning and Analysis – CISM
	Penetration Testing – OSCP, OSWE, CISSP, GPEN
	Vulnerability Testing – OSCP, OSWE, CISSP, GPEN
	Risk Management Assessment – CISSP, CISA, CISM, CRISC
	Info Security Audit and Compliance – CISA
	Info Security Remediation – CISSP

If your business has employees with any of the above skill sets and certifications and you would like to discuss opportunities to partner with NuHarbor on these future projects, please respond indicating your interest and availability to discuss options.

Thank you,

Wes Lyle

RFP-5-2021 for Lexington-Fayette Urban County Government


Wes Lyle
 To avdattilo@teamfishel.com

Tue 3/16/2021 2:52 PM

Greetings Mr. Dattilo,

NuHarbor Security is responding to RFP #5-2021 for Lexington-Fayette Urban County Government. This RFP is for Information Technology Consulting and Technical Services. There is not a specific project or proposal associated with this RFP. The goal is rather to qualify into an approved pool for future work in various categories.

NuHarbor is looking to identify local Minority, Woman, and Disadvantaged Business Enterprises (MWDDBEs) and Veteran-Owned Businesses that might partner with NuHarbor to satisfy some of these requirements. Again, there is no immediate project to bid on. We are strictly seeking to identify talent for future projects.

NuHarbor is a Cybersecurity company based in Vermont, with local presence along the East Coast. The pools we would like to qualify for are specific to our technology partners and portfolio of offerings. Below is a list of these categories and the type of skills required to perform the task envisioned.

Technology/Software	Skills Required/Relevant Certifications
Palo Alto Networks – Firewalls	Palo Alto Networks Certified Network Security Engineer (PCNSE)
Splunk	Splunk Enterprise Security Certified Admin
	Splunk Enterprise Certified Architect
	Splunk Core Certified Consultant
	Required Certifications
Information Security Services	Policy Development and Review – CISSP, CISA, CISM
	Planning and Analysis – CISM
	Penetration Testing – OSCP, OSWE, CISSP, GPEN
	Vulnerability Testing – OSCP, OSWE, CISSP, GPEN
	Risk Management Assessment – CISSP, CISA, CISM, CRISC
	Info Security Audit and Compliance – CISA
	Info Security Remediation – CISSP

If your business has employees with any of the above skill sets and certifications and you would like to discuss opportunities to partner with NuHarbor on these future projects, please respond indicating your interest and availability to discuss options.

Thank you,

Wes Lyle

Below are the two responses we did receive.

RE: RFP-5-2021 for Lexington-Fayette Urban County Government



Dedrea McCoy <Dedrea.McCoy@mccoycomputerservices.com>
To Wes Lyle

Reply Reply All Forward ...

Tue 3/16/2021 2:52 PM

CAUTION: External Email Sender. Do not click on links or open attachments unless it's a trusted and expected source.

Hello!

Thank you for reaching out, however, at this time, our business is not able to accommodate. If you should ever need someone for Cloudbase Office, VoIP or Technical Support, please feel free to contact me. Unfortunately, we are in the process of downsizing at this time.

From: Wes Lyle <wyle@nuharborsecurity.com>
Sent: Tuesday, March 16, 2021 2:47 PM
To: Dedrea McCoy <Dedrea.McCoy@mccoycomputerservices.com>
Subject: RFP-5-2021 for Lexington-Fayette Urban County Government

Greetings Ms. McCoy,

NuHarbor Security is responding to RFP-5-2021 for Lexington-Fayette Urban County Government. This RFP is for Information Technology Consulting and Technical Services. There is not a specific project or proposal associated with this RFP. The goal is rather to qualify into an approved pool for future work in various categories.

NuHarbor is looking to identify local Minority, Woman, and Disadvantaged Business Enterprises (MWDBEs) and Veteran-Owned Businesses that might partner with NuHarbor to satisfy some of these requirements. Again, there is no immediate project to bid on. We are strictly seeking to identify talent for future projects.

NuHarbor is a Cybersecurity company based in Vermont, with local presence along the East Coast. The pools we would like to qualify for are specific to our technology partners and portfolio of offerings. Below is a list of these categories and the type of skills required to perform the task envisioned.

Technology/Software	Skills Required/Relevant Certifications
Palo Alto Networks – Firewalls	Palo Alto Networks Certified Network Security Engineer (PCNSE)
Splunk	Splunk Enterprise Security Certified Admin
	Splunk Enterprise Certified Architect
	Splunk Core Certified Consultant
Information Security Services	Required Certifications
	Policy Development and Review – CISSP, CISA, CISM
	Planning and Analysis – CISM
	Penetration Testing – OSCP, OSWE, CISSP, GPEN
	Vulnerability Testing – OSCP, OSWE, CISSP, GPEN
	Risk Management Assessment – CISSP, CISA, CISM, CRISC
	Info Security Audit and Compliance – CISA
Info Security Remediation – CISSP	

If your business has employees with any of the above skill sets and certifications and you would like to discuss opportunities to partner with NuHarbor on these future projects, please respond indicating your interest and availability to discuss options.

Re: RFP-5-2021 for Lexington-Fayette Urban County Government



Gus Dattilo <avdattilo@teamfishel.com>
To: Wes Lyle

Reply Reply All Forward ...

Tue 3/16/2021 3:06 PM

You replied to this message on 3/16/2021 3:10 PM.
If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

CAUTION: External Email Sender. Do not click on links or open attachments unless it's a trusted and expected source.

Hi Wes and thanks. Unfortunately, Team Fishel is a physical security company, not cyber. If you need any help with the copper, fiber, or wireless infrastructure, we can help with that. AS well as door access or surveillance solutions.

I appreciate the consideration.

Regards,

Gus

Gus Dattilo - Security Sales Consultant

m: 812-207-1256

www.teamfishel.com



This message is intended solely for the designated recipient, may contain privileged or confidential information and may be subject to confidentiality agreement(s). Access to this email by anyone else is unauthorized. If you are not the intended recipient, any disclosure, copying, distribution or any action taken or omitted to be taken in reliance on it, is prohibited and may be unlawful. If you have received this message in error, please notify the sender immediately by reply e-mail and destroy the original communication.

The Fishel Company d/b/a Team Fishel

On Tue, Mar 16, 2021 at 2:52 PM Wes Lyle <wlyle@nuharborsecurity.com> wrote:

Greetings Mr. Dattilo,

NuHarbor Security is responding to RFP #5-2021 for Lexington-Fayette Urban County Government. This RFP is for Information Technology Consulting and Technical Services. There is not a specific project or proposal associated with this RFP. The goal is rather to qualify into an approved pool for future work in various categories.

NuHarbor is looking to identify local Minority, Woman, and Disadvantaged Business Enterprises (MWDBEs) and Veteran-Owned Businesses that might partner with NuHarbor to satisfy some of these requirements. Again, there is no immediate project to bid on. We are strictly seeking to identify talent for future projects.

NuHarbor is a Cybersecurity company based in Vermont, with local presence along the East Coast. The pools we would like to qualify for are specific to our technology partners and portfolio of offerings. Below is a list of these categories and the type of skills required to perform the task envisioned.

Below is the one failed delivery:

File **Report**

Delete | Send Again | Forward | Quick Steps | Move | Rules | Mark Unread | ...

From Mail Delivery Subsystem <MAILER-DAEMON@mx0a-002eb601.pphosted.com> Sent Sun 3/21/2021 2:51 P
To Wes Lyle
Subject Undeliverable: RFP-5-2021 for Lexington-Fayette Urban County Government

Delivery has failed to these recipients or groups:

aburikhanov@ssi-worldwide.com
Your message wasn't delivered because, despite repeated attempts to contact it, the recipient's email system didn't respond.

Contact the recipient by some other means (by phone, for example) and ask them to tell their email admin that their email system isn't accepting connection requests from your email system. It's likely that the recipient's email admin is the only one who can fix this problem.

For more information, see [Status code 4.4.7](#).

The following organization rejected your message: ssi-worldwide.com.

Diagnostic information for administrators:

Generating server: mx0a-002eb601.pphosted.com

aburikhanov@ssi-worldwide.com
ssi-worldwide.com
Remote Server returned '554 4 4 7 <ssi-worldwide.com #4 4 7>'

GENERAL PROVISIONS

1. Each Respondent shall comply with all Federal, State & Local regulations concerning this type of service or good.

The Respondent agrees to comply with all statutes, rules, and regulations governing safe and healthful working conditions, including the Occupational Health and Safety Act of 1970, 29 U.S.C. 650 *et. seq.*, as amended, and KRS Chapter 338. The Respondent also agrees to notify the LFUCG in writing immediately upon detection of any unsafe and/or unhealthful working conditions at the job site. The Respondent agrees to indemnify, defend and hold the LFUCG harmless from all penalties, fines or other expenses arising out of the alleged violation of said laws.

2. Failure to submit ALL forms and information required in this RFP may be grounds for disqualification.
3. Addenda: All addenda, if any, shall be considered in making the proposal, and such addenda shall be made a part of this RFP. Before submitting a proposal, it is incumbent upon each proposer to be informed as to whether any addenda have been issued, and the failure to cover in the bid any such addenda may result in disqualification of that proposal.
4. Proposal Reservations: LFUCG reserves the right to reject any or all proposals, to award in whole or part, and to waive minor immaterial defects in proposals. LFUCG may consider any alternative proposal that meets its basic needs.
5. Liability: LFUCG is not responsible for any cost incurred by a Respondent in the preparation of proposals.
6. Changes/Alterations: Respondent may change or withdraw a proposal at any time prior to the opening; however, no oral modifications will be allowed. Only letters, or other formal written requests for modifications or corrections of a previously submitted proposal which is addressed in the same manner as the proposal, and received by LFUCG prior to the scheduled closing time for receipt of proposals, will be accepted. The proposal, when opened, will then be corrected in accordance with such written request(s), provided that the written request is contained in a sealed envelope which is plainly marked "modifications of proposal".
7. Clarification of Submittal: LFUCG reserves the right to obtain clarification of any point in a bid or to obtain additional information from a Respondent.
8. Bribery Clause: By his/her signature on the bid, Respondent certifies that no employee of his/hers, any affiliate or Subcontractor, has bribed or attempted

to bribe an officer or employee of the LFUCG.

9. Additional Information: While not necessary, the Respondent may include any product brochures, software documentation, sample reports, or other documentation that may assist LFUCG in better understanding and evaluating the Respondent's response. Additional documentation shall not serve as a substitute for other documentation which is required by this RFP to be submitted with the proposal,
10. Ambiguity, Conflict or other Errors in RFP: If a Respondent discovers any ambiguity, conflict, discrepancy, omission or other error in the RFP, it shall immediately notify LFUCG of such error in writing and request modification or clarification of the document if allowable by the LFUCG.
11. Agreement to Bid Terms: In submitting this proposal, the Respondent agrees that it has carefully examined the specifications and all provisions relating to the work to be done attached hereto and made part of this proposal. By acceptance of a Contract under this RFP, proposer states that it understands the meaning, intent and requirements of the RFP and agrees to the same. The successful Respondent shall warrant that it is familiar with and understands all provisions herein and shall warrant that it can comply with them. No additional compensation to Respondent shall be authorized for services or expenses reasonably covered under these provisions that the proposer omits from its Proposal.
12. Cancellation: If the services to be performed hereunder by the Respondent are not performed in an acceptable manner to the LFUCG, the LFUCG may cancel this contract for cause by providing written notice to the proposer, giving at least thirty (30) days notice of the proposed cancellation and the reasons for same. During that time period, the proposer may seek to bring the performance of services hereunder to a level that is acceptable to the LFUCG, and the LFUCG may rescind the cancellation if such action is in its best interest.

A. Termination for Cause

- (1) LFUCG may terminate a contract because of the contractor's failure to perform its contractual duties
- (2) If a contractor is determined to be in default, LFUCG shall notify the contractor of the determination in writing, and may include a specified date by which the contractor shall cure the identified deficiencies. LFUCG may proceed with termination if the contractor fails to cure the deficiencies within the specified time.

- (3) A default in performance by a contractor for which a contract may be terminated shall include, but shall not necessarily be limited to:
 - (a) Failure to perform the contract according to its terms, conditions and specifications;
 - (b) Failure to make delivery within the time specified or according to a delivery schedule fixed by the contract;
 - (c) Late payment or nonpayment of bills for labor, materials, supplies, or equipment furnished in connection with a contract for construction services as evidenced by mechanics' liens filed pursuant to the provisions of KRS Chapter 376, or letters of indebtedness received from creditors by the purchasing agency;
 - (d) Failure to diligently advance the work under a contract for construction services;
 - (e) The filing of a bankruptcy petition by or against the contractor; or
 - (f) Actions that endanger the health, safety or welfare of the LFUCG or its citizens.

B. At Will Termination

Notwithstanding the above provisions, the LFUCG may terminate this contract at will in accordance with the law upon providing thirty (30) days written notice of that intent, Payment for services or goods received prior to termination shall be made by the LFUCG provided these goods or services were provided in a manner acceptable to the LFUCG. Payment for those goods and services shall not be unreasonably withheld.

13. **Assignment of Contract:** The contractor shall not assign or subcontract any portion of the Contract without the express written consent of LFUCG. Any purported assignment or subcontract in violation hereof shall be void. It is expressly acknowledged that LFUCG shall never be required or obligated to consent to any request for assignment or subcontract; and further that such refusal to consent can be for any or no reason, fully within the sole discretion of LFUCG.
14. **No Waiver:** No failure or delay by LFUCG in exercising any right, remedy, power or privilege hereunder, nor any single or partial exercise thereof, nor the exercise of any other right, remedy, power or privilege shall operate as a waiver hereof or thereof. No failure or delay by LFUCG in exercising any right, remedy, power or privilege under or in respect of this Contract shall affect the rights, remedies, powers or privileges of LFUCG hereunder or shall operate as a waiver thereof.
15. **Authority to do Business:** The Respondent must be a duly organized and

authorized to do business under the laws of Kentucky. Respondent must be in good standing and have full legal capacity to provide the services specified under this Contract. The Respondent must have all necessary right and lawful authority to enter into this Contract for the full term hereof and that proper corporate or other action has been duly taken authorizing the Respondent to enter into this Contract. The Respondent will provide LFUCG with a copy of a corporate resolution authorizing this action and a letter from an attorney confirming that the proposer is authorized to do business in the State of Kentucky if requested. All proposals must be signed by a duly authorized officer, agent or employee of the Respondent.

16. **Governing Law:** This Contract shall be governed by and construed in accordance with the laws of the Commonwealth of Kentucky. In the event of any proceedings regarding this Contract, the Parties agree that the venue shall be the Fayette County Circuit Court or the U.S. District Court for the Eastern District of Kentucky, Lexington Division. All parties expressly consent to personal jurisdiction and venue in such Court for the limited and sole purpose of proceedings relating to this Contract or any rights or obligations arising thereunder. Service of process may be accomplished by following the procedures prescribed by law.
17. **Ability to Meet Obligations:** Respondent affirmatively states that there are no actions, suits or proceedings of any kind pending against Respondent or, to the knowledge of the Respondent, threatened against the Respondent before or by any court, governmental body or agency or other tribunal or authority which would, if adversely determined, have a materially adverse effect on the authority or ability of Respondent to perform its obligations under this Contract, or which question the legality, validity or enforceability hereof or thereof.
18. Contractor understands and agrees that its employees, agents, or subcontractors are not employees of LFUCG for any purpose whatsoever. Contractor is an independent contractor at all times during the performance of the services specified.
19. Contractor [or Vendor or Vendor's Employees] will not appropriate or make use of the Lexington-Fayette Urban County Government (LFUCG) name or any of its trade or service marks or property (including but not limited to any logo or seal), in any promotion, endorsement, advertisement, testimonial or similar use without the prior written consent of the government. If such consent is granted LFUCG reserves the unilateral right, in its sole discretion, to immediately terminate and revoke such use for any reason whatsoever. Contractor agrees that it shall cease and desist from any unauthorized use immediately upon being notified by LFUCG.

20. If any term or provision of this Contract shall be found to be illegal or unenforceable, the remainder of the contract shall remain in full force and such term or provision shall be deemed stricken.

Signature  Date 3/29/2021

Firm Submitting Proposal: NuHarbor Security

Complete Address: 553 Roosevelt Hwy, #102 Colchester, VT 05446
Street City Zip

Contact Name: Scott Mosher Title: Vice President

Telephone Number: 802.881.4224 Fax Number: n/a

Email address: smosher@nuharborsecurity.com

**RISK MANAGEMENT PROVISIONS
INSURANCE AND INDEMNIFICATION**

INDEMNIFICATION AND HOLD HARMLESS PROVISION

- (1) It is understood and agreed by the parties that Consultant hereby assumes the entire responsibility and liability for any and all damages to persons or property caused by or resulting from or arising out of any act or omission on the part of Consultant or its employees, agents, servants, owners, principals, licensees, assigns or subcontractors of any tier (hereinafter "Consultant") under or in connection with this agreement and/or the provision of goods or services and the performance or failure to perform any work required thereby.
- (2) Consultant shall indemnify, save, hold harmless and defend the Lexington-Fayette Urban County Government and its elected and appointed officials, employees, agents, volunteers, and successors in interest (hereinafter "LFUCG") from and against all liability, damages, and losses, including but not limited to, demands, claims, obligations, causes of action, judgments, penalties, fines, liens, costs, expenses, interest, defense costs and reasonable attorney's fees that are in any way incidental to or connected with, or that arise or are alleged to have arisen, directly or indirectly, from or by Consultant's performance or breach of the agreement and/or the provision of goods or services provided that: (a) it is attributable to personal injury, bodily injury, sickness, or death, or to injury to or destruction of property (including the loss of use resulting therefrom), or to or from the negligent acts, errors or omissions or willful misconduct of the Consultant; and (b) not caused solely by the active negligence or willful misconduct of LFUCG.
- (3) Notwithstanding, the foregoing, with respect to any professional services performed by Consultant hereunder (and to the fullest extent permitted by law), Consultant shall indemnify, save, hold harmless and defend LFUCG from and against any and all liability, damages and losses, including but not limited to, demands, claims, obligations, causes of action, judgments, penalties, fines, liens, costs, expenses, interest, defense costs and reasonable attorney's fees, for any damage due to death or injury to any person or injury to any property (including the loss of use resulting therefrom) to the extent arising out of, pertaining to or relating to the negligence, recklessness or willful misconduct of Consultant in the performance of this agreement.
- (4) In the event LFUCG is alleged to be liable based upon the above, Consultant shall defend such allegations and shall bear all costs, fees and expenses of such defense, including but not limited to, all reasonable attorneys' fees and expenses, court costs, and expert witness fees and expenses, using attorneys approved in writing by LFUCG, which approval shall not be unreasonably withheld.

- (5) These provisions shall in no way be limited by any financial responsibility or insurance requirements, and shall survive the termination of this agreement.
- (6) LFUCG is a political subdivision of the Commonwealth of Kentucky. CONSULTANT acknowledges and agrees that LFUCG is unable to provide indemnity or otherwise save, hold harmless, or defend the CONSULTANT in any manner.

FINANCIAL RESPONSIBILITY

CONSULTANT understands and agrees that it shall, prior to final acceptance of its proposal and the commencement of any work or services, demonstrate the ability to assure compliance with the above Indemnity provisions and these other risk management provisions.

INSURANCE REQUIREMENTS

YOUR ATTENTION IS DIRECTED TO THE INSURANCE REQUIREMENTS BELOW, AND YOU MAY NEED TO CONFER WITH YOUR INSURANCE AGENTS, BROKERS, OR CARRIERS TO DETERMINE IN ADVANCE OF SUBMISSION OF A RESPONSE THE AVAILABILITY OF THE INSURANCE COVERAGES AND ENDORSEMENTS REQUIRED HEREIN. IF YOU FAIL TO COMPLY WITH THE INSURANCE REQUIREMENTS BELOW, YOU MAY BE DISQUALIFIED FROM AWARD OF THE CONTRACT.

Required Insurance Coverage

CONSULTANT shall procure and maintain for the duration of this contract the following or equivalent insurance policies at no less than the limits shown below and cause its subcontractors to maintain similar insurance with limits acceptable to LFUCG in order to protect LFUCG against claims for injuries to persons or damages to property which may arise from or in connection with the performance of the work or services hereunder by CONSULTANT. The cost of such insurance shall be included in any bid:

<u>Coverage</u>	<u>Limits</u>
General Liability million aggregate (Insurance Services Office Form CG 00 01) limit	\$1 million per occurrence, \$2 or \$2 million combined single limit
Professional Liability	\$1 million per occurrence
Worker's Compensation	Statutory
Employer's Liability	\$100,000

The policies above shall contain the following conditions:

- a. All Certificates of Insurance forms used by the insurance carrier shall be properly filed and approved by the Department of Insurance for the Commonwealth of Kentucky. LFUCG shall be named as an additional insured in the General Liability Policy and Commercial Automobile Liability Policy using the Kentucky DOI approved forms.
- b. The General Liability Policy shall be primary to any insurance or self-insurance retained by LFUCG.
- c. The General Liability Policy shall include a Products and Completed Operations endorsement or Premises and Operations Liability endorsement and a Products Liability endorsement unless they are deemed not to apply by LFUCG.
- d. The General Liability Policy shall have a Professional Liability endorsement (including Errors and Omissions) for any services performed pursuant to the contract, and/or a separate Professional Liability Policy shall be obtained unless it is deemed not to apply by LFUCG.
- e. The Professional Liability policy shall be maintained for a minimum of three years beyond the completion date of the project, to the extent commercially available. If not commercially available, CONSULTANT shall notify LFUCG and obtain similar insurance that is commercially available and acceptable to LFUCG.
- f. LFUCG shall be provided at least 30 days advance written notice via certified mail, return receipt requested, in the event any of the required policies are canceled or non-renewed.
- g. Said coverage shall be written by insurers acceptable to LFUCG and shall be in a form acceptable to LFUCG. Insurance placed with insurers with a rating classification of no less than Excellent (A or A-) and a financial size category of no less than VIII, as defined by the most current Best's Key Rating Guide shall be deemed automatically acceptable.

Renewals

After insurance has been approved by LFUCG, evidence of renewal of an expiring policy must be submitted to LFUCG, and may be submitted on a manually signed renewal endorsement form. If the policy or carrier has changed, however, new evidence of coverage must be submitted in accordance with these Insurance Requirements.

Deductibles and Self-Insured Programs

IF YOU INTEND TO SUBMIT A SELF-INSURANCE PLAN IT MUST BE FORWARDED TO LEXINGTON-FAYETTE URBAN COUNTY GOVERNMENT, DIVISION OF RISK MANAGEMENT, 200 EAST MAIN STREET, LEXINGTON, KENTUCKY 40507 NO LATER THAN A MINIMUM OF FIVE (5) WORKING DAYS PRIOR TO THE RESPONSE DATE. Self-insurance programs, deductibles, and self-

insured retentions in insurance policies are subject to separate approval by Lexington-Fayette Urban County Government's Division of Risk Management, upon review of evidence of CONSULTANT's financial capacity to respond to claims. Any such programs or retentions must provide LFUCG with at least the same protection from liability and defense of suits as would be afforded by first-dollar insurance coverage. If CONSULTANT satisfies any portion of the insurance requirements through deductibles, self-insurance programs, or self-insured retentions, CONSULTANT agrees to provide Lexington-Fayette Urban County Government, Division of Risk Management, the following data prior to the final acceptance of bid and the commencement of any work:

- a. Latest audited financial statement, including auditor's notes.
- b. Any records of any self-insured trust fund plan or policy and related accounting statements.
- c. Actuarial funding reports or retained losses.
- d. Risk Management Manual or a description of the self-insurance and risk management program.
- e. A claim loss run summary for the previous five (5) years.
- f. Self-Insured Associations will be considered.

Safety and Loss Control

CONSULTANT shall comply with all applicable federal, state, and local safety standards related to the performance of its works or services under this Agreement and take necessary action to protect the life, health and safety and property of all of its personnel on the job site, the public, and LFUCG.

Verification of Coverage

CONSULTANT agrees to furnish LFUCG with all applicable Certificates of Insurance signed by a person authorized by the insurer to bind coverage on its behalf prior to final award, and if requested, shall provide LFUCG copies of all insurance policies, including all endorsements.

Right to Review, Audit and Inspect

CONSULTANT understands and agrees that LFUCG may review, audit and inspect any and all of its records and operations to insure compliance with these Insurance Requirements.

DEFAULT

CONSULTANT understands and agrees that the failure to comply with any of these insurance, safety, or loss control provisions shall constitute default and that LFUCG

may elect at its option any single remedy or penalty or any combination of remedies and penalties, as available, including but not limited to purchasing insurance and charging CONSULTANT for any such insurance premiums purchased, or suspending or terminating the work.

00471865

Information Technology Consulting and/or Technical Services

Introduction

The Lexington-Fayette Urban County Government (LFUCG) is soliciting proposals from qualified professional vendors for information technology (IT) services. The qualified vendor(s) will enable LFUCG to significantly improve information technology effectiveness, enhance its quality of services, minimize down time and support costs, ensure security of data, and maximize investment in IT. These services may be categorized into two general areas, IT Technical Services and IT Consulting Services.

Technical Services include, but are not limited to, software development, system configuration, system implementation, database design/maintenance, infrastructure maintenance, network support, and IT technical training.

Consulting Services include, but are not limited to, IT strategic planning, IT process design, IT governance, disaster recovery planning, business continuity, IT project management, requirements gathering, and IT administrative training.

Purpose

LFUCG supports a wide range of technologies that are both process and mission critical. Due to the volume of IT projects and required availability of existing IT services, LFUCG may leverage external expertise if internal resources are unavailable. The objective of this RFP is to identify vendors possessing formidable knowledge or skills that can be applied to support existing IT services or assist with new IT initiatives. Once the RFP process is complete and a list of vendors is established, these services may be engaged on short notice with a scope of work document.

Background Information

Server Hardware Infrastructure – LFUCG primarily uses Dell and IBM hardware to support stand-alone servers, SAN's, and a mission critical virtual environment powered by Dell VxRail solution. Dell, IBM's and VMWare SAN/vSAN technologies are used in the majority of LFUCG's server environment.

Server Application Infrastructure – Microsoft's Server suite and MicroSoft 365 (Office 365 tenant) is the foundation of LFUCG's mail, domain, web, database, intranet, and server environments. A strong skill set and proven experience will be necessary to work with these environments.

Software Infrastructure –Microsoft Power Shell, Microsoft .NET, and Microsoft Office suite are all involved with major projects that may require support from a qualified vendor. Applications may be custom tailored to a division's specific needs and processes.

ERP – PeopleSoft FSCM and HCM modules facilitate LFUCG's financial and human capital processes.

Vendor Requirements

Submittals shall include completed attachments and responses to questions. Responses are required only for the specific services offered by your company. LFUCG recognizes that is unlikely for any vendor to be experienced or skilled in all of the areas listed.

Technology Assessment – Due to the variety of technologies used by LFUCG, all proposals must contain a completed copy of Attachment A to facilitate the vendor selection process. Vendors should include technologies which are not listed that LFUCG may benefit from or should be considered during the vendor selection process.

Support Services – The following questions must be answered. Proposals may include additional comments to help LFUCG gain a better understanding of how support would be provided.

1. Is help desk support available? NuHarbor does not offer a helpdesk, but if you are engaged with NuHarbor on a project you will have direct access to your assigned team or consultant.
2. When is support available throughout the week? Standard (fully staffed) support is 8:00am-5:00pm ET, 5 days a week. NuHarbor does have 24x7 support for our managed service offerings.
3. Do you provide a process for escalating support issues? Yes, we have a Jira ticket system and portal where tickets can be opened and tracked, and a call tree for escalations.
4. How are charges for support structured, documented, and tracked? We can define a particular need if required. Most of our Managed Service offering all come with 24x7 support at no additional cost.

Software Development – LFUCG may have needs for software development from a qualified vendor. In addition to the technology assessment, proposals should include their application programming methodology, development life cycle, documentation standards, and other components of software development.

Consulting – Services may be required to provide technical leadership and guidance for information technology issues. Consulting services may include: requirements gathering, strategic planning, process documentation, needs assessment, solution selection, disaster recovery, IT governance, IT project management, IT security or other IT services. If your company proposes to offer consulting services, provide an overview of each area, outlining your company's experience, approach, and applied methodologies.

Please clearly define the approach and process your company employs to facilitate these services.

Cost of Services – The proposal must contain the information to address the items below:

1. A fee schedule that includes hourly rates for proposed services. Hourly rates for our services are \$225/hr. with a minimum commitment of one (1) week.

2. Describe how your services are priced and any specific pricing. We can produce a quote based on a scope of work once we have mutually defined that scope. We can also sell “Blocks” of service hours more loosely defined for general purpose – these must be committed in one-week minimums though.
3. Define any additional charges. (e.g. travel expenses) We have not been traveling for the past 12 months, but may resume limited travel again this summer as conditions change. If we do travel it will be billed at actuals.
4. Provide a completed copy of Attachment B. Included below.

Company Information – Please provide the following information:

1. Company name and address.
NuHarbor Security
553 Roosevelt Hwy, Suite 102
Colchester, VT 05446
2. Identify all business partners you have with technology and consulting firms.
Splunk
CrowdStrike
Tenable
CyberArk
Okta
Palo Alto Networks
Imperva
Forescout
Proofpoint
Veracode
SafeGuard Cyber
ThreatConnect
3. Provide resumes for all individuals being submitted for work under this RFP, along with the following information:
 - a. location of staff
Our Headquarters and SOC are located in Colchester, VT – just north of Burlington. 50% of our employees live in that area; the other half are distributed nationwide, mostly along the East Coast. We have field offices in the following metro areas: Boston, MA; New York, NY; Washington, D.C., Raleigh-Durham, NC; Atlanta, GA; and Miami, FL.
 - b. hourly rate of pay
List is \$250/hr. but we discount government work at \$225/hr. We do require one-week minimums to book our Engineers, Analysts, and Consultants.
 - c. travel and living expenses per week
We pass actuals to the customer when we travel, though nearly all work is performed remotely.
 - d. indicate if the staff is sub-contracted or an employee
NuHarbor will utilize only full-time, US-based employees for these services.

Below are sample resumes of NuHarbor personnel that perform duties

relevant to this RFP. We will later confirm personnel based on experience and availability once a project is scoped and can resubmit resumes if appropriate at that time.

INFORMATION ASSURANCE MANAGER

NuHarbor Security, Burlington, VT

Information Assurance Manager

August 2015 – Present

- *Assigned to State of Vermont VHC project since July 2015. Serve as primary lead on State of Vermont VHC project since July 2017.*
- *Provide policy and procedure guidance.*
- *Develop and lead risk management process.*
- *Organize and lead MARS-E, Pub 1075 controls assessments and risk assessments and provide reports for both CMS and IRS.*
- *Provide oversight for the maintenance and reporting of CMS POAM and IRS CAP, VHC security architecture and third-party risk assessments.*
- *Organize and lead MARS-E and Pub 1075 controls assessments.*
- *Coordinate managed security information event management (SIEM) using Splunk, Tenable support and penetration testing including remediation of findings*
- *Consult weekly with VHC and AHS Security teams.*
- *Represent VHC in weekly meetings with Optum and other subcontractors.*

Keurig Green Mountain Inc., Waterbury, VT

IT Risk Manager

July 2013 – August 2015

- *Identify and manage all risk associated with technology projects and systems.*
- *Oversee ISO 27001 gap assessment.*
- *Perform security risk assessments of third-party vendors*
- *Select and implement privileged account management solution.*
- *Implement advanced persistent threat solution.*
- *Review and test IT disaster recovery plans.*
- *Work to address PCI and SOX compliance requirements.*

Keurig Green Mountain Inc., Waterbury, VT

Systems Implementation Manager

September 2011 – August 2013

- *Manage implementation of information systems supporting sales and marketing.*
- *Project manager for S&OP and trade promotion implementation for multiple business units.*
- *Project manager for implementation of CRM application.*
- *Manage budget, vendor resources and project plans.*

Champlain College

CIO/AVP Information Systems and Security

January 2005 – September 2011

- *Responsible for all business and academic technology and information security.*
- *Recruit, hire and develop all technology staff.*
- *Member of institutional leadership team.*
- *Actively involved with departmental and institutional strategic planning.*
- *Responsible for overall technology budget.*
- *Oversee infrastructure, application and support teams supporting more than 3000 users globally.*

Education

- *University of Vermont – MBA*
- *University of Vermont – BA*
- *Champlain College - AS*

Certifications

- *Certified Information Systems Auditor (CISA)*
- *Certified in Information Security Management (CISM)*
- *Certified in Information Systems Risk Management (CRISC)*

SENIOR INFORMATION SECURITY ANALYST

NuHarbor Security, Essex, VT

Senior Information Security Analyst

Feb 2018 – Present

- *Performed NIST Cybersecurity Framework reviews.*
- *Wrote policies and procedures for information security, acceptable use, backup and recovery, change management, and SDLC.*

State Street Corporation, Quincy, MA

Assistant Vice President, Governance, Risk, and Compliance

September 2015 – June 2017

- *Led Material Risk Identification (MRI) and Risk and Control Self-Assessment (RCSA) exercises*
- *Led First Line of Defense controls writing workshops, collaborating with stakeholders across all IT business units to identify, document, and self-test Cyber Security, Access, Change management, Information and data Security controls.*
- *Developed metrics and baselines for regulatory mandated risk programs, leveraged legacy KPIs as well as data from operational support teams to drive a shift from qualitative to quantitative risk measurement.*
- *Developed a comprehensive risk self-assessment questionnaire and facilitated completion by enterprise IT.*
- *Wrote business requirements, developed reports, built UAT scripts, led user testing, built and delivered training materials, a FAQ SharePoint site, for the implementation of a new GRC solution.*

Cabot Corporation, Boston, MA

Senior Internal Auditor

September 2013 – September 2015

- *Led audit team with scope covering 44 plants and 30 sales/administrative offices in 21 countries.*
- *Led development and implementation of internal SOX IT audit program.*
- *Developed SharePoint site and best practice testing procedures for multiple IT and Financial control cycles including standardizing work-programs.*
- *Presented audit results to top executives including CIO, segment vice presidents, and regional finance directors and provided recommendations for identified IT, financial, and business risks.*

Liberty Mutual Insurance, Boston, MA

IT Auditor

Jan 2013 – September 2013

- *Performed a wide range of technical audits including OS, DB, RACF, midrange and mainframe, change management, application logical security, processing controls, and System development lifecycle (SDLC) projects.*
- *Utilized computer aided auditing tools (CAATs) to parse security configuration outputs and analyze large data sets for population analysis.*

PricewaterhouseCoopers, Boston, MA

Risk Assurance Associate

July 2010 – December 2012

- *Facilitated implementation of periodic user access reviews on over 250 applications for a fortune 100 pharmacy client. Developed process and procedure documentation to merge tables of users and assigned security groups.*
- *Performed Information Technology General Controls (ITGC) testing for SOX and non-SOX audits.*

Education

University of Massachusetts, Amherst, MA

Dual-Degree, Bachelor of Business Administration, Accounting and Information Systems, B.S.

Economics

2006-2010

Certifications

- *Certified Public Accountant (CPA)*
- *Certified Information Systems Auditor (CISA)*
- *Certified Internal Auditor (CIA)*

SECURITY ENGINEER

NuHarbor Security, Essex Junction, VT Security Engineer

- *Perform infrastructure, and wireless penetration testing security assessments*
- *Perform vulnerability assessments*
- *Apply offensive cybersecurity testing techniques, coordinate testing projects with internal and external system owners*
- *Report the nature of identified cyber security risks and recommend risk mitigation measures to improve the cyber security posture of the enterprise*
- *Identify security flaws in computing platforms and infrastructure and devise strategies and techniques to mitigate identified cybersecurity risks*

MyWebGrocer, Winooski, VT Senior Network Security Engineer

Responsible for maintaining the design and integrity of MyWebGrocer's internal network, including customer-facing hosted and cloud environments. Provided expert technical assistance to team members with high-level system and networking request. Also responsible for designing, implementing and testing complex infrastructure in support of our customer needs.

Key Achievements:

- *Instrumental in migration of customers to cloud based SaaS.*
- *Designed and implemented Information Security Awareness training program*
- *Created policies and procedures governing business security, email and internet usage, access control, and incident response.*
- *Spearheaded compliance and BCP programs*

Vermont National Guard, Colchester, VT Cyber Operations Team Lead

Perform cyber defense; cyber operational preparation of the environment; and cyber intelligence, surveillance, and reconnaissance actions on specified systems and networks. React to cyberspace events, employ cyberspace defense infrastructure capabilities and collect digital forensics data. Analyze computer systems and network architectures, as well as determine exploitation methods. Lead soldiers in performing activities in support of defensive cyber operations. Validate critical infrastructure configurations, network alerts, and network security posture assessments. Evaluate cyber defense requirements and participate in the joint targeting process.

Key Achievements:

- *Built Industrial Controls System (ICS SCADA) range to train team members.*
- *Red Team NCOIC National Level Cyber Exercise Program*
- *Participated in Regional Critical Infrastructure Exercise*

Vermont National Guard, Colchester, VT Information Technology Security Specialist

Serve as a Regiment level Information Assurance Security Officer. Duties include assessing the cybersecurity posture of networked computer systems. Implement, monitor, and enforce DoD information system IA policies and procedures as defined by DIACAP security and accreditation policies. Daily duties include administration, monitoring and troubleshooting for all network equipment, Microsoft, ESXi and SAN systems on a DoD network. Additional duties include the design and implementation of security processes and procedures, conduct penetration tests / vulnerability assessments and perform cost benefit analysis on all recommended strategies; accountable for over \$1 million worth of equipment.

Key Achievements:

- *Instrumental in developing and implementing business continuity and disaster recovery (BCP & DRP) plans for multiple geographically separated sites.*
- *Spearheaded project to convert from physical server farm and traditional desktop environment to virtualized server infrastructure and thin clients.*
- *Hand selected to conduct cyber assessments on NATO ally countries.*
- *Created policies and procedures governing enterprise security, email and internet usage, access control, and incident response.*
- *Designed cyber range for national level government cyber exercise.*
- *Built and instructed numerous cyber security courses.*

**Vermont National Guard, Colchester, VT
Senior Network Administrator / Instructor**

Senior Network Administrator and Instructor for multiple Army cyber security courses. Responsible for maintaining and configuring Microsoft, Sun Solaris, Linux and UNIX operating systems. Responsible for preparation of classroom computer equipment based on various processor platforms to include configuration of Cisco firewalls, routers and switches. Provide upper level support to subordinate network technicians and system administrators.

Key Achievements:

- *Certified as Computer Incident Response Handler*
- *Developed Red Team training program*

Certifications

- *CISSP – Certified Information Systems Security Professional*
- *CASP – CompTIA Advanced Security Practitioner*
- *GSEC – Security Essentials*
- *GCIH – Certified Incident Handler*
- *GPEN – Certified Penetration Tester*
- *GICSP – Global Industrial Cyber Security Professional*
- *CEH – Certified Ethical Hacker*
- *Security+*
- *Network+*
- *A+*

4. Number of years your company has been providing technology/consulting services.

Seven (7) years.

5. Provide two references for IT services work your company has performed over the last year.

Out of respect for our clients' time and privacy, please work through NuHarbor to coordinate discussions.

San Antonio Water System (SAWS)

Victor M. Gonzalez

Enterprise Security Architect

(210) 233-3778

MCPHS University

Allen Basey

Senior Security Analyst

Allen.Baey@mcphs.edu

Additional Information

The consultant(s) will be selected from those proposals submitted in response to this RFP. A committee composed of government employees as well as representatives of relevant user groups will evaluate proposals.

It is the intent of the LFUCG to award this contract to multiple vendors to establish a list of firms to provide services as needed. However, the LFUCG reserves the right to award this contract in its best interest. Additionally, the contract term will be for three years with the option to renew for two additional one year terms.

If your firm requires execution of a standard contract, include a draft of the contract with the response.

All materials developed, data collected, or reports prepared under the terms of the project agreement become the property of the LFUCG. LFUCG reserves the non-exclusive rights to copy such material and publish, disseminate, and otherwise use the materials developed under the terms of the agreement in print or electronically.

Attachment A

Attachment A contains a list of the technologies used by the Lexington-Fayette Urban County Government. Please enter the average experience (years) of qualified employees who may provide IT services in the Experience column. You may enter the number of employees the average applies to, e.g. "5 years, 3 employees". The Comments column should be used to provide LFUCG with information that should be considered during the vendor selection process.

Technology	Experience	Comments
Microsoft Windows Server (2012, 2016) and the latest generally available release (currently Windows Server Version 2019)		
Microsoft Windows 8, 10 Desktop		
Microsoft 365, Architecture and Design		
Microsoft PowerShell		
Microsoft Active Directory		
Microsoft Exchange 2016, 2019		
AIX versions 5.x, 6.x, 7.x, 8.x, 9.x		
Linux – Various Distributions		
IBM i Operating System		
IBM i5/OS2 Operating System		
Internet Information Server (IIS)		
F5 BigIP		
VMware VirtualCenter		
VMware ESXi		
Microsoft Access		
Microsoft SQL Server (2012 – 2019)		
IBM DB/2 Database		
SharePoint Services (on premise and		
Microsoft .NET Framework 3+		
ESRI ArcGIS Enterprise (10.8.1 +)		
ESRI ArcGIS Desktop – ArcMap (10.8.1		
ESRI ArcGIS Desktop – ArcGis Pro (2.6 +)		
ESRI ArcGIS Online		
ESRI ArcGIS API for Javascript		
ESRI ArcGIS API for Python		
Visual Studio		
VBA		
Python		
JavaScript		
HTML5		
C#		
C++		
Ruby		
Technology	Experience	Comments

Ruby on Rails		
Visual Basic 6.0		
ASP.NET		
VB.NET		
jQuery		
Web Services		
PHP Development		
Apache HTTP Web Server		
RPG Freeform		
BCD Presto		
ADO		
Moodle		
AJAX		
Node.js		
Chef, Puppet, Troposphere		
Amazon Web Services (AWS) Architecture		
Amazon Web Services (AWS) DevOps		
Microsoft Azure Architecture		
Microsoft Azure DevOps		
Palo Alto Firewalls		
Splunk	7 yr. avg for 36 emp	NuHarbor is an Elite Splunk Partner
Extreme Networks – wired and wireless		
Switching & Routing (SPBm)		
Vulnerability Scanning (Nessus)		
Patch Management		
IBM BigFix/HCL		
PeopleSoft HCM 9.2, PUM 36 and higher		
PeopleSoft FSCM 9.2, PUM 37 and higher		
PeopleTools 8.57.11		

Attachment B

Attachment B contains a list of services the Lexington-Fayette Urban County Government may need provided. Please use the notes column to identify any information that should be considered during the vendor selection process. Exceptions to billing should be included in the notes, e.g. weekend rate adjustments.

Service		Rate	Notes
Software Development	ASP.NET C# JavaScript Ruby Ruby on Rails C++ HTML5 VB.NET Python Visual Basic 6.0 ESRI ArcGIS ADO 2.X + Web Services		
Database Design	SQL Server SQL Server Express MySQL ESRI Enterprise Geodatabase Oracle		
Consulting	Disaster Recovery/Bus Continuity Technical Requirements Gathering IT Strategic Planning IT Governance IT Project Management Certified Project Management (PMP) Network Technologies Software Development PeopleSoft HCM (9.2) PeopleSoft FSCM (9.2) ESRI ArcGIS Enterprise Portal Requirements and Design		
Service		Rate	Notes

Server Application Implementation	Microsoft SharePoint Microsoft Project Server Microsoft SQL Server Microsoft Exchange Microsoft Windows VMware Virtual Center VMware ESX ESRI ArcGIS Enterprise Apache HTTP Web Server		
Training	Microsoft SharePoint Microsoft Project Server Microsoft SQL Server Visual Studio Team Suite Visual Studio 2008 VMware ESRI ArcGIS (Online, Portal & Pro)		
Network Support	F5 BigIP Microsoft Active Directory Microsoft Windows VMware		
Information Security	Policy Development and Review Planning and Analysis Penetration Testing Vulnerability Testing Risk Management Assessment Info Security Audit and Compliance Info Security Remediation Info Security End-User Training	\$225/hr.	Minimum engagement is 1 week
Enterprise DevOps & "Cloud"	Cloud Architecture and Design Code Deployment and Maintenance Enterprise System Administration Version Control Infrastructure as Code (IaC) Platform as a Service (Paas) Software as a Service (SaaS) Infrastructure as a Service (IaaS)		

Services Description

Splunk

NuHarbor Security is an Elite Splunk partner (the highest level) with 50+ employees holding Splunk certifications – many at the very highest levels, like Enterprise Architect and Consultant. We have executed 350+ Splunk implementations and are certified to offer Professional Services directly for Splunk. All NuHarbor’s Splunk work is driven by best practices and deep expertise. NuHarbor can meet any Splunk need from HealthCheck through Managed Phantom SOAR as a service.

In addition to our Splunk PS expertise, we offer 3 Managed Service bundles around Splunk.

Service	Offerings		
	Base	Standard	Complete
Splunk Health Monitoring	24x7	24x7	24x7
Splunk Data onboarding			
Splunk Development			
Security Monitoring		24x7	24x7
Threat Intelligence			
NuHarbor Service Desk			
Client Service Desk		OPTION	
Advanced Threat Intelligence			
Advanced Threat Hunting			
SOAR			
Discounts on IA & RedSec			
Splunk Component	Splunk Enterprise (core)	Splunk Enterprise Security	Splunk Phantom

These Managed Service offerings are in addition to our Professional Services for customers that want help running their Splunk instance or want the benefits of a 24x7 SOC without the staffing requirements.

Information Security:

Policy Development and Review

NuHarbor will develop a current state Information Security Policy that is enforceable and accurately reflects the current Information Security Program for Client.

NuHarbor also recommends that policies developed align with required policies per the NIST Cyber Security Framework. Other frameworks are available if preferred. The below outline is based on NIST.

Client Information Security Policies and Procedures, to address the following areas as applicable:

- Acceptable Use Policy
- BYOD Policy
- Clean Desk Policy
- Confidentiality Agreement
- Data Classification and Usage Policy
- Gramm-Leach-Bliley
- Incident Response Plan
- IoT Policy
- Password Policy
- Red Flag Identity Theft Prevention Program
- Written Information Security Plan

Approach and Methodology

NuHarbor personnel and Client will collaborate on this engagement as follows. The party with “Primary” responsibility shall have the obligation of completing that task with input and support from the “Assist” party. “Review” indicates that the responsible party will need to provide feedback on the task.

Task	Description	NuHarbor Responsibility	Client Responsibility
Development and enhancement of policies to align with Client requirements	Work with Client to develop current state policies referenced above to align to Client requirements.	Primary	Assist

Planning and Analysis

NuHarbor can customize a service to meet exactly what is desired by the customer for Planning and Analysis. This is a broad category. Here are a few items that may fall into this space:

- **Security Posture Assessment**

NuHarbor Security has significant experience partnering with clients to deliver security controls assessments, security risk assessments, and other compliance-based reviews. NuHarbor specializes in industry-specific standards such as HIPAA, FISMA, IRS-Pub 1075, MARS-E 2.0, and FFIEC. Our deep understanding of NIST 800-53, NIST 800-30, NIST 800-171, and NIST Cyber Security Frameworks provides a path for clients to improve their security posture. Our deep level of partnership allows for ongoing interaction to ensure sustainable success for our clients.

Penetration Testing

External Penetration Testing Services typically include a series of assessments aimed at identifying vulnerabilities that could be present on the analyzed assets. These assessments may or may not include the following tasks:

- **Information gathering tests:** Attempt to identify live hosts, network topology, operating system services provided, access control mechanisms, access servers, and the interactions between systems.
- **Generic vulnerability tests:** Attempt to determine the presence of known vulnerabilities and to exploit them. This includes vulnerabilities related to legitimately provided services such as HTTP, FTP, SMTP mail exchangers and gateways, DNS, IMAP/POP, file- and print-sharing services, etc.
- **Network characteristics and topology tests:** Attempt to determine the presence and exploit vulnerabilities related to network topology, network components configuration and design principles, and protocol specific characteristics. These include tests that consider spoofing techniques, protocol specific tests such as usage of IP options, fragmentation, exploit of trust relationships, protocol encapsulation, routing tricks, design, and implementation flaws in several network protocols and related services, etc.
- **Misconfiguration tests:** Attempt to identify and exploit typical misconfiguration problems.
- **Backdoor tests:** Attempt to identify the presence of known backdoors in the company's infrastructure and exploit them.
- **Authentication and access control schemes tests:** Attempt to subvert authentication and access control mechanisms based on common attacks that exploit the lack of a strict security policy or the enforcement of such. This includes dictionary and brute force attacks on reusable passwords, exploit of weak authentication schemes, social engineering, exploit of contingency plan procedures, etc.

The tests include common hacking techniques and may include the use of automated Penetration Testing tools, both homegrown and commercially available.

The Penetration Testing effort is focused on but not limited to:

- Assessing the external security posture with regards to the network ranges to be analyzed, which includes:
 - Performing information gathering tests to identify live hosts and the services they provide.
 - Determining potential vulnerabilities which might affect the hosts, services, and applications discovered.
 - Exploiting the potential vulnerabilities in a controlled fashion to weed out false positives and appraise the degree of exposure caused by the vulnerability.
 - Identify solutions to address the security issues found.

- Investigating the consequences of a targeted attack by specialized individuals, as well as evaluating the skill set required by an attacker to carry out a successful attack.
- Analyzing the potential outcome of a successful compromise.
- Providing recommendations to remediate or mitigate the issues found as well as prevent similar issues from recurring issues.
- Documenting the results of the tests performed to construct a foundation for future testing as well as a quarterly snapshot of the security stance. This allows the client to compare future penetration testing efforts as a means of evaluating the efficiency and effectiveness of client's efforts to secure its external posture.

Internal Penetration Testing Services follow the same assessment methodology as External Penetration Testing Services but are conducted from within the client's network. Additionally, Internal Penetration Testing seeks to validate proper network segmentation.

Vulnerability Testing

NuHarbor Security will conduct a remote vulnerability scan, aimed at identifying vulnerabilities on systems included in MCPHS's internal and external network. The vulnerability scan will focus on high-risk issues with immediate exploitability but will also review medium/low-risk vulnerabilities that may be more difficult to exploit or have a lower impact on confidentiality, integrity, or availability.

Our methodology includes connecting through remote jump box or VPN. The scanning scope is then clearly defined, documented, and agreed to between NuHarbor Security and MCPHS. Vulnerability Scans are then conducted against all identified active devices and systems to identify potential vulnerabilities.

NuHarbor utilizes the Common Vulnerability Scoring System (CVSS) to determine vulnerability criticality as well as human logic for organizational risks. The NuHarbor Technical Testing team is also well-versed with NIST 800-115 for the purposes of assisting organizations in planning and conducting technical information security tests and examinations, analyzing findings, and developing mitigation strategies. Using NIST 800-115 as a baseline provides practical recommendations for designing, implementing, and maintaining technical information security test and examination processes and procedures.

Similar to how we assign organizational risks with CVSS backed by NIST 800-115 methodology, NuHarbor includes technical security testing and functional security testing (business logic exploitation) to assign risk to individual hosts within the client network.

A contact will need to be assigned for the project. NuHarbor Security will report to that contact all high-risk vulnerabilities discovered on Lexington's network and targeted applications, as well as the corrective action information (the implementation steps for the corrective actions will be the sole responsibility of the client).

To reduce false positives, NuHarbor's preference is to perform authenticated scans, and work with Lexington to find a proper risk tolerance for unauthenticated vs. authenticated scans.

All deliverables for this engagement will utilize NuHarbor templates, formats, and structure. The level of effort for this project is contingent upon this assumption.

- **Vulnerability Scanning**

NuHarbor Security will conduct remote vulnerability scans, aimed at identifying vulnerabilities on systems included in the scanning scope. The vulnerability scan will focus on high-risk issues with immediate exploitability but will also review medium/low-risk vulnerabilities that may be more difficult to exploit or have a lower impact on confidentiality, integrity, or availability.

Deliverables: Vulnerability Scan Report and Action Plan

All our reports follow the format of:

1. Technical Report – A comprehensive explanation of the vulnerability scan and findings.
2. All supporting evidence is property of the client and is attached as an Appendix to the report.

Roles and Responsibilities

NOTE: The party with “Primary” responsibility shall have the obligation of completing that task or Deliverable with input and support from the “Assist” party. “Review” indicates the party will need to provide feedback on the deliverable.

Service Phase	Description	NuHarbor Security	Client	Location
#1	The testing scope is clearly defined, documented, and agreed to between NuHarbor Security and Client.	Primary	Assist: Support defining test scope.	Remote
#2	Discovery scans are conducted to identify active devices and systems within the defined scope.	Primary	N/A	Remote
#3	Vulnerability Scans are conducted against all identified active devices and systems to identify potential vulnerabilities.	Primary	N/A	Remote
#4	A combination of automated and manual testing techniques are used in attempt to exploit all identified vulnerabilities.	Primary	N/A	Remote
#5	Where exploitation is successful and the exploit does not directly result in "root" or "admin" level access, further manual and automated testing will be leveraged in attempt to escalate privileges to "root" or "admin."	Primary	N/A	Remote
#6	An attempt is made to deploy a temporary agent onto all exploited systems which then serves as a proxy for the test to "pivot" and conduct a new discovery scan to identify which internal systems are visible to the exploited host. Where no exploitation is successful, a temporary agent can be deployed intentionally onto a system to test pivot exposure under a hypothetical exploitation scenario.	Primary	N/A	Remote
#7	Depending on the scoping of the engagement at this phase the test either concludes or phases #3-#6 are repeated until reaching a pre defined destination within the network or no further systems are found to be exploitable.	Primary	N/A	Remote

Risk Management Assessment

Security Risk Management is a three-step process applying knowledge of security policy, procedures, and structure to design, develop, and implement computing and system architectures. Beginning with evaluation of the current state of organizational controls, NuHarbor works with key personnel to understand risk tolerance and overall objectives. A risk rating is provided and applied to each control in non-compliance. Phase two is an overall gap analysis and development of a remediation plan to provide the organization with insights.

NuHarbor would then provide input on the Agency's cybersecurity process activities and related documentation and help design security architectures for use within the network environment. NuHarbor would also support Program Managers responsible for the acquisition of agency information systems to ensure cybersecurity initiatives are properly addressed.

Info Security Audit and Compliance

NIST Cybersecurity Framework Assessment Engagement Overview (others available)

NuHarbor will conduct an assessment of the Client's security posture against the Administrative, Technical, and Physical security controls included in NIST Cybersecurity Framework baseline. This engagement will consist of documentation review, personnel interviews, and observation of process and procedure. This test is limited to the scope defined in the scoping section below.

Service Phases

The following service phases will be conducted under this engagement.

NOTE: The party with "Primary" responsibility shall have the obligation of completing that phase or deliverable with input and support from the "Assist" party. "Review" indicates the party will need to provide feedback on the deliverable. "Shared" indicates that both parties are responsible for completing the task.

Phase	Description	NuHarbor Security	Client	Location
#1	NuHarbor provides Document Request List to client, and due date for requested documents.	Shared	Shared	Remote
#2	NuHarbor provides list of interview and assessment topics to client to schedule interviews. Client begins scheduling requested interviews.	Shared	Shared	Remote
#3	NuHarbor reviews all customer provided documentation (policies, procedures, standards, and other supporting documentation). Additional or supporting documentation may be requested at this time.	Primary	Assist (provide additional documentation, explanations, etc.)	Remote
#4	Client confirms interview schedules	Assist	Primary	Remote
#5	NuHarbor conducts interviews with client staff to review security controls.	Primary	Assist	Combined Onsite and Remote
#6	Additional documentation reviewed as needed.	Primary	Assist	Combined Onsite and Remote
#7	NuHarbor reviews security controls requiring additional evidence (screenshots, device configurations, etc.)	Primary	Assist	Combined Onsite and Remote
#8	Client gathers responses and evidence for specific controls as requested by NuHarbor as follow-up. NuHarbor will provide follow-up requests during steps 5, 6, and 7 above.	Assist	Primary	Onsite

Deliverables: NIST Cybersecurity Framework Assessment Report

All our reports follow the format of:

1. Executive Summary: 1–2-page document that gives a high-level summary of the project, high-level results of the assessment, top risks identified, and summary

recommendations. It also details prevailing themes and proposed strategic objectives (if applicable) to reduce any risk quickly while enabling client strategic objectives.

2. Detailed Assessment Report: A comprehensive explanation of observations for each security control assessed during the engagement. Each control will be assigned an implementation status and risk rating based on NuHarbor's understanding of the client business goals and other factors. This risk rating does not meet any control requirement for a formal risk assessment and is only meant to be used as input for remedial effort prioritization. This may be attached as an appendix to the Executive Summary in Excel format at NuHarbor's discretion.

Assessment Scope

This proposed service includes a security assessment of the client's Information Security based on the NIST Cybersecurity Framework. If additional Information Security or Compliance services are desired, NuHarbor will furnish an estimate for specific services.

Info Security Remediation

NuHarbor does not do direct "boots on the ground" remediation services, but we can provide an Incident Response Readiness Assessment and we can provide recommendations.

Incident Response Readiness Assessment

NuHarbor has prepared numerous General Security Incident Response Plans that align with industry standard best practices and include adaptations to meet specific requirements and needs of the client. The Incident Response Plan does not address how to respond to specific incident types but will instead provide a foundational baseline and organizational plan for responding to general security incidents. As an extension of this project, the plan could be further adapted and modified to develop "playbooks" to respond to specific types of security incidents.

The Incident Response Readiness Assessment is broken down into the following phases:

Phase	Description	NuHarbor Security	Client
#1	NuHarbor conducts interviews and gathers necessary organizational information regarding incident response plan <u>components</u>	Shared	Shared
#2	NuHarbor develops and provides draft IR Plan to client	Primary	Assist
#3	Client reviews plan with appropriate client staff members. Client contacts gather feedback and works with NuHarbor staff to implement necessary changes within scope of the engagement	Assist	Primary
#4	NuHarbor revises drafted IR plan as needed, delivers final IR Plan to client	Primary	Assist
Phase	Description	NuHarbor Security	Client
#5	NuHarbor reviews delivered plan with appropriate client contacts. Upon acceptance, engagement is complete	Shared	Shared

General Security Incident Response Plan

NuHarbor will deliver a documented Incident Response Plan and graphical flowchart to follow in the event of a general security incident. The plan will include:

1. Roles and responsibilities for plan phases and tasks
2. Communication requirements and contact information
3. Incident categories
4. Incident reporting requirements as applicable
5. Definition of applicable incident response teams
6. Documentation of the following major response phases:
 - a. Preparation
 - b. Incident Identification
 - c. Incident Response
 - d. Incident Recovery
 - e. Incident Follow-Up

Each major phase will include detailed steps for required actions and will indicate the purpose, roles, task details, any work aids used or referenced, measurable outcomes, and consequences for skipped steps. Additionally, any metrics or time-based exceptions will be defined as needed.

7. A graphical flow chart of a General Security Incident Process to accompany the General Security Incident Playbook.

8. Identification of intersecting points with IT, Legal, Public Relations, and Law Enforcement.

Info Security End-User Training

Security Awareness Program and Training Recommendations

Security training and awareness will include a single day (maximum 8 hours) of on-site training. NuHarbor will meet with client staff to plan content and structure of the one-day training/awareness session. Content and structure of training will be agreed upon prior to the engagement commencing.

Deliverables: Recommendation Documentation

All our reports follow the format of:

1. A one-page, executive recommendation around potential opportunities for improvement of the security awareness program will be provided.