BOARD OF COOPERATIVE EDUCATIONAL SERVICES OF NASSAU COUNTY

REQUEST FOR PROPOSALS

RISK ASSESSMENT AND PENETRATION TESTING FOR NASSAU BOCES PARTICIPATING SCHOOL DISTRICTS

RFP # 2416

ISSUED May 19, 2017

VENDOR QUESTIONS DUE BY May 31, 2017 AT 2:00 PM

PROPOSALS DUE JUNE 19, 2017 AT 2:00 PM

BOARD OF COOPERATIVE EDUCATIONAL SERVICES OF NASSAU COUNTY
DEPARTMENT OF BUSINESS SERVICES
George Farber Administrative Center
71 Clinton Road
P. O. Box 9195
Garden City, New York 11530-9195

RFP # 2416

RISK ASSESSMENT AND PENETRATION TESTING FOR NASSAU BOCES PARTICIPATING SCHOOL DISTRICTS

ISSUED MAY 19, 2017

QUESTIONS FROM VENDORS DUE MAY 31, 2017 AT 2 PM

PROPOSALS DUE JUNE 19, 2017 AT 2 PM

CONTACT INFORMATION

Questions regarding the Technical information regarding this proposal shall be directed to:

Mr. Matthew Hejna
mhejna@nasboces.org
(516) 608-6648
Nassau BOCES
1 Merrick Avenue
Westbury, NY 11590

Questions regarding RFP procedure and submission of proposals may be directed to:

Mr. Michael Perina
mperina@nasboces.org
(516) 396-2240
Nassau BOCES
71 Clinton Road
Garden City, NY 11530
Fax 516-997-1053

Note: Please do not contact school districts directly regarding this RFP. Any and all necessary contacts with Nassau school districts must be coordinated through Nassau BOCES.

REQUEST FOR PROPOSAL #2416
RISK ASSESSMENT AND PENETRATION TESTING FOR NASSAU BOCES PARTICIPATING SCHOOL DISTRICTS

I. PURPOSE/OBJECTIVE:

Nassau BOCES is requesting formal, sealed request for proposals for Risk Assessment and Penetration Testing for Nassau BOCES participating school districts. Within this Request for Proposal (RFP) is the concept that many of our 56 school districts will participate in this RFP to contract for these services with qualified personnel. All services will be contracted directly through the participating school districts. Proper Board Resolutions and contracts must be filed and board approved prior to use. This RFP is for those Nassau BOCES districts that subscribe to the Nassau BOCES Data Privacy and Security Services (DPSS) and for other New York State school districts through their Regional Information Center (RIC).

II. THE AGENCY

Compressed into 287 square miles within Nassau County, The Board of Cooperative Educational Services of Nassau County, New York ("The Nassau BOCES") is a public educational shared-services agency that serves fifty-six component community school districts comprising over 330 schools and over 180,000 students.

In addition to services being rendered directly to students, The Nassau BOCES provides many application and data support services directly to local public school administrators, teachers and staff members. Among these services, we provide State Reporting, Student Management Systems and Special Education Application expertize to the schools within the county and throughout New York State.

The Nassau BOCES is a centralized support organization with responsibilities for diverse missions, threaded with the goal of providing excellent service. This includes for state reporting: assisting central office administrators and building level administrators in their efforts to plan, manage and evaluate the policies and procedures related to data collection and state reporting. For Student Management Systems it includes training staff, trouble shooting and managing the Student Management System. For Special Education, it includes providing a depth of understanding regarding Special Education Applications to include understanding the relationships with state reporting and Student Management Systems. The agency's mission is to provide a high level of expertise in regards to data decisions related to State Reporting, Student Management Systems and Special Education Applications within the Nassau BOCES and to component school districts.

The Nassau BOCES mission is to provide cost-effective, timely, convenient, reliable, and secure services aligned to FERPA, HIPPA and Education Law 2D to the schools and school districts of Nassau County.

III. PROPOSAL PROCEDURES:

A. SCHEDULE OF PROPOSAL

RFP Issuance Date	May 19, 2017
Questions from Vendors Due	May 31, 2017** at 2:00 PM
RFP Proposals Due	June 19, 2017 at 2:00 PM
Approximate Date Services to Start	July 1, 2017

** Written questions will be accepted from any and all organizations. Inquiries pertaining to the RFP must give the RFP number, title and acceptance date. All material questions will be answered in writing and will be distributed to all organizations who receive the RFP. However, all questions are to be received no later than May 31, 2017 at 2:00 PM.

Nassau BOCES Purchasing Department will issue all addenda. Addenda will be faxed, emailed or mailed to all who are known to have received an RFP.

B. PREPARATION OF PROPOSAL

Each proposal shall be prepared simply and economically, avoiding the use of elaborate promotional materials beyond those sufficient to provide a complete, accurate and reliable presentation.

Each proposal prepared in response to this RFP will be proposed solely at the cost and expense of the proposer with the express understanding that there will be no claim whatsoever for reimbursement from Nassau BOCES.

C. NUMBER OF PROPOSAL COPIES

Six (6) copies of the proposal consisting of 2 separate envelopes in the format marked RFP 2416: Technical Proposal for Risk Assessment and Penetration Testing for Nassau BOCES Participating School Districts and RFP 2416: Cost Proposal for Risk Assessment and Penetration Testing for Nassau BOCES Participating School Districts should be submitted to the Purchasing Agent of Nassau BOCES. The address is as follows:

Mr. Michael R. Perina
Purchasing Agent
Nassau BOCES
71 Clinton Road
Garden City, New York 11530-9195

The cost proposals must contain firm pricing for years 1 & 2 and pricing for (3) three additional 1 year extensions, years 3 & 4 & 5, by mutual consent.

D. SUBMISSION OF PROPOSALS

All submissions must be in sealed envelopes and clearly indicate vendor's name and return address, clearly noting the RFP # and response due date and time, as indicated on the cover of this document. Submission of a proposal indicates acceptance by the firm of the conditions contained in this Request for Proposal submitted.

E. TIME AND LOCATION OF PROPOSER'S PRESENTATION

During the evaluation process, BOCES reserves the right, where it may serve BOCES' best interest, to request additional information and clarifications from proposers, or to allow corrections of errors or omissions. Any such information given, either orally or in writing, is not given in confidence and may be used, or disclosed to others, for any purpose at any time without obligation or compensation and without liability of any kind whatsoever.

Selected vendors may be requested to provide oral and/or technical presentations; proposers will be notified to arrange for a mutually agreeable date and time, and the location of presentations shall be at the Nassau BOCES George Farber Administrative Center.

Out of pocket expenses for the firm personnel (e.g., travel, lodging and subsistence) will be the responsibility of the firm. **A statement must be included in the dollar cost proposal stating the firm will not seek reimbursement for travel, lodging, subsistence, or other out-of-pocket costs incurred in connection with this engagement.**

F. EFFECTIVE PERIOD OF PROPOSALS

All proposals must state the period for which the proposal prices, terms and conditions shall remain in effect after the date of submission. Such period shall be not less than one hundred and eighty (180) days from proposal due date.

G. METHOD OF AWARD

The Nassau BOCES Evaluation Committee shall begin the review of all received proposal packages as early as practicable. Nassau BOCES reserves the right to hold all proposals for a period of up to one hundred and eighty (180) days beyond the final date for submission of proposals before making any determination.

Selection Criteria: In order to facilitate choosing the best proposal for Nassau BOCES, each proposal shall be evaluated with emphasis on the following factors:

- Proposal conciseness, completeness and clarity of presentation.
- Prior experience in performing services of the type contemplated by this RFP, particularly within K-12 School Districts.
- Cost/Pricing structure and the amounts.
- Readiness to work within the parameters outlined in this RFP.
- References and Reputation.
- Level of skill/expertise.
- Any other information that would assist the RFP evaluation committee in the selection process.

H. EVALUATION CRITERIA

Proposals will be evaluated using three sets of criteria: mandatory, service and cost. Mandatory criteria refers to adhering to the instructions in this RFP on preparing and submitting the Proposal as well as having no conflict of interest with regard to any other work performed by the firm for Nassau BOCES participating school districts. Certain criteria will be evaluated by the Nassau BOCES interview committee and will service to pre-qualify firms. (See Appendix C.) Service criteria refers to the firm's past experience with Nassau BOCES, school districts, staff qualifications, quality of references, past experience and performance with other organizations. Cost criteria is the third criteria but will not be the sole factor in the selection of the firm or firms. Firms meeting mandatory criteria will have their proposals scored for both technical qualifications and the fee structure submitted. A rating sheet for this purpose will be used and is attached to this Request for Proposal for your examination (Appendix C & D).

As this is a proposal, price will not be the sole determination in making an award. Proposals will be evaluated on the following criteria:

a. Firm's experience performing Risk Assessment and/or Penetration Testing for school districts (15 points)
b. Firm's experience performing Risk Assessment and/or Penetration Testing for other organizations (15 points)
c. Quality and experience of firm's proposed staff (20 points)
d. Pricing Schedule (10 points)
e. Quality of references (15 points)
f. Location of firm and consultants (10 points)
g. Samples of deliverables provided to districts i.e. reports, presentations, etc. (15 points)

See Appendix C & D for a sample form of the Rating Sheets.

I. RIGHT OF REJECTION

Notwithstanding any other provisions of this RFP, Nassau BOCES reserves the right to recommend an award of contract to the vendor(s) that best meet the requirements of the RFP, and not necessarily to the lowest proposer. Further, Nassau BOCES reserves the right, for any or no reason and in its sole and absolute discretion, to (1) Amend, in whole or in part, withdraw, or cancel this RFP, and (2) Accept or reject any or all proposals prior to execution of the services contract for any or no reason and with no penalty to The Board of Cooperative Educational Services of Nassau County.

J. AWARD OF CONTRACT

Nassau BOCES may select a vendor by means of a Notice of Award issued by the RFP evaluation committee. Neither the selection of a vendor nor the issuance of a Notice of Award shall constitute Nassau BOCES' acceptance of the proposal or a binding commitment on behalf of Nassau BOCES to enter into a services contract with the vendor, as any binding arrangement must be set forth in definitive documentation signed by both parties and shall be subject to all requisite approvals. Each of the Nassau BOCES participating school districts or the other New York State districts who utilize this RFP through their Regional Information Center after proper resolutions are filed, must execute their own board approved contract(s) with the vendor(s).

It is the intent of Nassau BOCES to pre-qualify more than one (1) vendor for this RFP for Nassau BOCES participating school districts. See Section VI-Final Selection.

K. CONTRACT NEGOTIATIONS

Nassau BOCES participating school districts and other RIC school districts reserve the right to negotiate the terms and conditions of the Contract(s) with the selected proposer(s), if any. These negotiations may include all aspects of services and fees. Neither the selection of a vendor nor the negotiation of the Contract with such vendor(s) shall constitute the participating school districts' acceptance of the proposal or a binding commitment on behalf of the participating school districts to enter into a Contract with such vendor(s), as any binding arrangement must be set forth in the Contract signed by both parties and is subject to all requisite approvals.

L. FREEDOM OF INFORMATION

During the evaluation process, BOCES reserves the right, where it may serve BOCES' best interest, to request additional information and clarifications from proposers, or to allow corrections of errors or omissions. Any such information given, either orally or in writing, is not given in confidence and may be used, or disclosed to others, for any purpose at any time without obligation or compensation and without liability of any kind whatsoever.

All proposals submitted to Nassau BOCES in response to this RFP may be disclosed in accordance with the standards specified in the Freedom of Information Law, Article 6 of the Public Officers law of the State of New York ("FOIL"). A business submitting a proposal may provide in writing, at the time of its submission, a detailed description of the specific information contained in its submission which it has determined is a trade secret and which, if disclosed, would substantially harm such firm's competitive position. This characterization shall not be determinative, but will be considered when evaluating the applicability of any exemptions in response to a FOIL request.

M. CONTRACT PERIOD

The anticipated term of the contract will be defined in the Contract Agreement, but is expected to begin July 1, 2017 and run for two (2) years through June 30, 2019 with an option to renew for three (3) additional one-year periods (July 1, 2019 through June 30, 2020, and July 1, 2020 through June 30, 2021, and July 1, 2021 through June 30, 2022 respectively) by mutual agreement at the conclusion of the contract term. The participating school districts reserve the right to schedule work assignments as deemed appropriate and do not guarantee work as a result of the award of a contract.

The cost proposals must contain firm pricing for years 1 & 2 and pricing for (3) three additional 1 year extensions, years 3 & 4 & 5, by mutual consent.

N. **CONFIDENTIALITY AND DATA SECURITY AND PRIVACY STANDARDS**:

a. Vendor, its employees, and/or agents agree that all information obtained in connection with the services provided is deemed confidential information. Vendor, its employees, and/or agents shall not use, publish, discuss, disclose or communicate the contents of such information, directly or indirectly with third parties, except as provided for the Contract. Vendor further agrees that any information received by Vendor, its employees, and/or agents during the course of the services provided which concerns the personal, financial, or other affairs of Nassau BOCES, its employees, agents, clients, and/or students will be treated by Vendor, its employees, and/or agents in full confidence and will not be revealed to any other persons, firms, or organizations.

b. Further, Vendor and Nassau BOCES understand that Vendor may receive and/or come into contact with *protected health information* as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and/or protected information under the Family Educational Rights and Privacy Act ("FERPA"). Vendor and Nassau BOCES hereby acknowledge their respective responsibilities pursuant to HIPAA and FERPA and, if necessary, shall execute any necessary agreements, including, but not limited to, a Business Associate Agreement in connection with such responsibilities.

c. Vendor acknowledges that it may receive and/or come into contact with personally identifiable information, as defined by New York Education Law Section 2-d, from records maintained by Nassau BOCES that directly relate to a student(s) (hereinafter referred to as "education record"). Vendor understands and acknowledges that in the event it receives personally identifiable information from education records (hereinafter referred to as "student data") it shall have in place sufficient protections and internal controls to ensure that information is safeguarded in accordance with applicable laws and regulations, and understands and agrees that it is responsible for complying with state data security and privacy standards relating to the protection of student data, and it shall:

    i. limit internal access to education records to those individuals that are determined to have legitimate educational interests;

    ii. not use the education records for any other purposes that those explicitly authorized in this Agreement;

    iii. maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of education records in its custody; and

iv. use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the secretary of the United States department of health and human services in guidance issued under Section 13402(H)(2) of Public Law 111-5.

d. Vendor further understands and agrees that in the event it receives student data it will be responsible for submitting a data security and privacy plan to the Nassau BOCES prior to the start of the term of this Agreement. Such plan must outline how all state, federal and local data security and privacy contract requirements will be implemented over the life of the contract consistent with Nassau BOCES's policy on data security and privacy, as adopted. Further, such plan must include a signed copy of Nassau BOCES's Parents' Bill of Rights and the training requirement established by Vendor for all employees who will receive student data.

e. Vendor understands that as part of Nassau BOCES's obligations under New York Education Law Section 2-d, if Vendor will receive student data, VENDOR must provide Nassau BOCES with supplemental information to be included in Nassau BOCES's Parents' Bill of Rights. Such supplemental information must include:
   i. the exclusive purposes for which the student data will be used;
   ii. how Vendor will ensure that subcontractors, persons or entities that Vendor will share the student data with, if any, will abide by data protection and security requirements;
   iii. that student data will be returned or destroyed upon expiration of the Agreement;
   iv. if and how a parent, student, or eligible student may challenge the accuracy of the student data that is collected; and
   v. where the student data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

f. In the event of a breach of the within confidentiality and data security and privacy standards provision and unauthorized release of student data, Vendor shall immediately notify Nassau BOCES and advise it as to the nature of the breach and steps Vendor has taken to minimize said breach. In the case of required notification to a parent or eligible student, Vendor shall promptly reimburse Nassau BOCES for the full cost of such notification. Vendor shall indemnify and hold Nassau BOCES harmless from any claims arising from its breach of the within confidentiality and data security and privacy standards provision.

g. Upon termination of the Contract, Vendor shall return or destroy all confidential information obtained in connection with the services provided herein and/or student data. Destruction of the confidential information and/or student data shall be accomplished utilizing an approved method of confidential destruction, including, shredding, burning or certified/witnessed destruction of physical materials and verified erasure of magnetic media using approved methods of electronic file destruction. The parties further agree that the terms and conditions set forth herein shall survive the expiration and/or termination of the agreement.

IV. PROPOSAL REQUIREMENTS

1. General Requirements

a. The purpose of the Technical Proposal is to demonstrate the qualifications, competence and capacity of the firms seeking to provide services for Nassau BOCES participating school districts in conformity with the requirements of this Request for Proposals. As such, the substance of the proposals will carry more weight than their form or manner of presentation. The Technical Proposal should demonstrate the qualifications of the firm and of the particular staff to be assigned to this contract.

b. The Proposing Firm shall submit six (6) copies of the Technical Proposal in a separate envelope marked RFP 2416: Risk Assessment and Penetration Testing for Nassau BOCES Participating School Districts, as outlined in Section III-C.
(No Dollars should be included in the Technical Proposal.)

The Technical Proposal should address all the points outlined in the Request for Proposals. The Proposal should be prepared simply and economically, providing a straightforward, concise description of the proposing firm's capabilities to satisfy the requirements of the Request for Proposals. While additional data may be presented, the following subject, items numbered 2 through 8, must be included. These represent criteria against which the proposal will be evaluated.

1. Title Page – Indicate that the document is RFP 2416: Risk Assessment and Penetration Testing for Nassau BOCES Participating School and include the following:

Date;
Vendor name;
Title;
Main Address;
Local address;
Telephone number;
Fax number;
Email; and
Contact person
Non-Collusion Statement (Appendix A); and
Iran Divestment Certification (Appendix B).

2. Table of Contents

3. Transmittal Letter – Provide a signed letter of transmittal briefly stating the interested firm's understanding of the scope of work, the commitment to perform the work, a statement describing why the firm believes itself to be the best qualified to perform the scope of work, and a statement that the proposal of the firm is a firm and irrevocable offer for services to be rendered.

4. The firm should provide an affirmative statement that it is independent of Nassau BOCES and/or participating school districts. The firm should also list and describe the firm's professional relationships involving Nassau BOCES and/or participating school districts for the past five (5) years, together with a statement explaining why such relationships do not constitute a conflict of interest relative to performing the proposed engagement. In addition, the firm shall give Nassau BOCES and/or participating school districts written notice of any professional relationships entered into during the period of this engagement.

5. Firm Qualifications and Experience – The purpose of the Qualifications portion of the Proposal is to demonstrate the qualifications, competence and capacity of the firms seeking to provide these consultant services.

a. The proposing firm should state the size of the firm, the size of the firm's staff assigned to any of these contracts, the location of the office from which the work on this contract is to be performed and the number and nature of the professional staff available to be employed in this contract both on a full-time and part-time basis. Provide a listing of all in-house services provided.

b. If the proposing firm is a joint venture or consortium, the qualifications of each firm comprising the joint venture or consortium should be separately identified and the firm that is to serve as the principal provider of consulting services should be noted, if applicable.

6. Partner and Staff Qualifications Experience

a. Identify the principal staff, including partners, managers, supervisors and specialists, who would be assigned to the contract. Provide information on the public school district consulting and/or other experience of each person, including information on relevant continuing education professional education for the past three (3) years and membership in professional organizations relevant to the performance of this contract.

b. Provide as much information as possible regarding the number, titles, responsibilities, qualifications, experience, years with firm, and training, including relevant continuing professional education, of the specific staff to be assigned to this contract. Indicate how the quality of staff over the term of the contract will be assured.

c. Principals, partners, managers, supervisors and specialists may be changed if those personnel leave the firm. These personnel may also be changed for other reasons only with the express prior written permission of the participating school districts. However, in either case, the participating school districts retain the right to approve or reject replacements.

7. Partner/Consultant/Subconsultant Firms, and Contractors – Firms must have all relevant disciplines either in house, or must list their Partner/Consultant/Subconsultant Firms, and Contractors in the Technical Proposal. All Partner/Consultant/Subconsultant Firms, and Contractors listed in response to this Request for Proposals can only be changed with the express prior written permission of the participating school districts, which retain the right to approve or reject replacements.

8. Prior Work with Nassau BOCES, Public School Districts/References – List separately all work within the last five (5) years, ranked on the basis of total staff hours. Indicate the scope of the work, date, partners, the location of the firm's office from which the work was performed, and the name, title and telephone number of the principal client contact.

9. Similar Projects with Other Organizations/References

a. For the firm's office that will be assigned responsibility for this contract, list the work performed in the last five (5) years that are similar to the type(s) of work described in this Request for Proposals.

b. The work should be ranked on the basis of total staff hours. Indicate the scope of the work, date, partners, and the name, title and telephone number of the principal client contact.

10. Provide any other information that you believe will assist Nassau BOCES and the participating school districts in making its selection. Such information may be in this last section of the proposal or may be represented in one or more appendixes.

11. Required Insurance Certificate – The Firm hereby agrees to effectuate the naming of Nassau BOCES/participating district as an unrestricted additional insured on the firm's insurance policies, with the exception of workers' compensation and errors and omissions insurance. If the policy is written on a claims-made basis, the retroactive date must precede the date of the contract.

The policy naming Nassau BOCES/participating district as an additional insured shall:

a. Be an insurance policy from an A.M. Best rated "secured" New York State licensed insurer.

b. State that the organization's coverage shall be primary coverage for Nassau BOCES, participating districts, its Board, employees and volunteers. Nassau BOCES and/or the participating district shall be listed as an additional insured by using endorsement CG 2010 11 85 or equivalent. The certificate must state that this endorsement is being used. If another endorsement is used, a copy shall be included with the certificate of insurance.

c. Required Policy Limits:

- **Commercial General Liability Insurance:**
  $1,000,000 per occurrence/ $2,000,000 aggregate.
- **Workers' Compensation and N.Y.S. Disability:**
  Statutory Workers' Compensation, Employers' Liability and N.Y.S. Disability Benefits Insurance for all employees.
- **Errors and Omissions Insurance:**
  $5,000,000 per occurrence/ $5,000,000 aggregate for the professional acts of the firm performed under the contract for Nassau BOCES/participating district. If written on a "claims-made" basis, the retroactive date must pre-date the inception of the contract or agreement.

d. The firm acknowledges that failure to obtain such insurance on behalf of Nassau BOCES/participating BOCES/participating districts constitutes a material breach of contract. The firm is to provide Nassau BOCES and/or the participating district with a certificate of insurance evidencing the above requirements have been met, prior to the commencement of work. The failure of Nassau BOCES/participating district to object to the contents of the certificate or the absence of same shall not be deemed a waiver of any and all rights held by Nassau BOCES/participating districts.

V. SCOPE OF SERVICES

A. RFP OVERVIEW

This Request for Proposal (RFP) is issued to select one or more vendors to provide and/or perform Risk Assessment and Penetration Testing services for Nassau BOCES participating school districts. Within this Request for Proposal (RFP) is the concept that many of our 56 school districts will participate in this RFP to contract for these services with qualified personnel. All services will be contracted directly through the participating school districts. Proper Board Resolutions and contracts must be filed and board approved prior to use. This RFP is for those Nassau BOCES districts that subscribe to the Nassau BOCES Data Privacy and Security Services (DPSS) and for other New York State school districts through their Regional Information Center (RIC).

It is not a competitive bid and terms for individual contracts will be negotiated at the rates provided by vendors in this RFP. Contracts may be for specific number of hours or days per week, or weeks/months per year, depending on the needs of the participating school districts. All participating vendors should be willing to negotiate such terms as appropriate.

Vendors will be required to agree to the Basic Requirements outlined in the RFP or supply significant reasons, supported by appropriate documentation if applicable, for their inability to do so.

The types of services being addressed in this request include: Application Security Testing for Web & Mobile apps, Network Penetration Testing, Infrastructure Assessment, Vulnerability Scanning for Networks and Applications, and Phishing Expeditions. Vendors are NOT required to provide all service types; they are welcome to submit proposals only on their specific areas of competency.

Vendors should provide pricing for each of the services that they list as being qualified to perform.

B. BASIC REQUIREMENTS

All proposers will agree to the following conditions of employment. BOCES reserves the right to reject any submitted proposal that does not meet any or all conditions regardless of the reason. Should any of these conditions conflict with existing corporate, personal and/or Union contract terms or policies, the proposer may submit evidence of same and request an exception for that specific condition(s).

The following personnel information must be submitted and approved before the designated individual(s) will be assigned:

- The proposer will supply the names of all individuals who will be working in any school District premises. The list would include those permanently assigned and their usual backups. Any employee that will replace the regularly assigned individual or their backup must have been vetted, as described below, and their information available.
- **Security background checks must be provided and paid for by the proposer prior to being assigned, and be available for review by Nassau BOCES Human Resources Department. Security checks must include, but not be limited to, crimes committed against property or persons, particularly children.**
- **All staff must be fingerprinted and/or cleared by the Nassau BOCES Human Resources Department prior to being assigned to a school district.**
    - **If previously fingerprinted for New York State Dept. of Education, please complete the OSPRA 102 form and return to Nassau BOCES Human Resources Department.**
    - **If not previously fingerprinted, fingerprinting is required.**
- Employees are required to abide by the Confidentiality and Data Security and Privacy Standards as set forth in this RFP.
- Proposer is responsible for insurance on the employee and their actions. Proof of said insurance must be provided upon request by BOCES or the District.
- A current photo ID must be available and worn at all times.
- The proposer will be responsible for maintaining workmen's compensation and income tax withholding for themselves and their employees.
- The proposer will be deemed independent contractors and not employees of Nassau BOCES.
- Nassau BOCES reserves the right to remove or replace a vendor at any time at their discretion or that of the School District.

It is important to understand that this is NOT A COMPETITIVE BID! Its purpose is to establish the vendor's firm on a pre-qualified list from which authorized users may choose from depending on their needs. Participating School Districts will have the ability to select the vendor(s) that they identify as most appropriate for any or all of the Service Types described below. The scope of services will be determined by need and budgetary consideration.

Payment Methodology

The vendor(s) will provide participating School Districts with a detailed invoice which will be paid via a Purchase Order (PO) that will be created for the full contracted amount. The PO will be amended beyond the contracted amount only for work that was pre-approved by the District.

C. TYPES OF SERVICES

1. **Application Security Testing for Web & Mobile apps**
   Vendor will perform testing that is intended to validate the implementation and effectiveness of the applications security controls and configurations. Vendor methodology should follow nationally recognized standards.
    a. Information Gathering
    b. Configuration and Deployment Management Testing
    c. Identity Management Testing
    d. Authentication Testing
    e. Authorization Testing

f. Session Management Testing
g. Input Validation Testing
h. Error Handling
i. Cryptography
j. Business Logic Testing
k. Client Side Testing

2. **Network Penetration Testing**
Vendor will provide network penetration testing in one or more of the following areas. Vendor will perform penetration testing using standardized methodologies. In general,
   a. External networks
      i. Vendor will focus on attacking and assessing the external internet facing network systems and services.
   b. Internal networks
      ii. Vendor will perform an assessment and analysis of district's internal network. Assessment could include attempts to gain access to high value internal systems and servers. This can be performed with either on-site, or remotely via a method agreed upon by the vendor and district.
   c. Wireless networks
      iii. Vendor will perform an assessment of district's wireless network. Testing may include attempts to break wireless encryption, insert traffic into the wireless system, capture wireless communications, and spoofing a wireless access point (AP), or otherwise attempt to gain access to the wireless network.

3. **Infrastructure Security Assessment**
Vendor will perform a detailed review of existing technology including network devices, computers and servers, LAN/WAN communications, operating metrics (e.g. Uptime), Log Management, and identify any risks associated with existing infrastructure.

4. **Vulnerability Scanning for Networks and Applications**
Vendor will conduct regular vulnerability scans on external and internal networks using industry standard tools such as Tenable Nessus or Qualys, or equivalent. Results will be reviewed and reported on. In addition, devices with a high number of administrative accounts will be identified so the network administrator can then determine if those rights are needed, or if they are extraneous. Vendors may provide recommendations for the remediation of discovered vulnerabilities.

5. **Phishing Expeditions**
Vendor will perform phishing expeditions based on an agreed upon set of goals with the district. The expeditions may include spearfishing, social engineering, broad scope e-mails to all users in district, and other similar methodologies. The vendor will provide reporting to the districts on the outcome of the phishing expeditions.

For all above services, vendor must provide reports on the findings of services rendered. These can include remediation plans, risk assessments, audit reporting, and/or other similar documentation.

D. PRICING MATRIX:

The proposing firm shall submit six (6) copies of a Dollar Cost Proposal in a separate envelope marked: RFP 2416: Risk Assessment and Penetration Testing for Nassau BOCES Participating School Districts.

The cost proposals must contain firm pricing for years 1 & 2 and pricing for (3) three additional 1 year extensions, years 3 & 4 & 5, by mutual consent.

Vendor must provide pricing for each of the services that they list as being qualified to perform. It is understood that the total cost of a given project will be based on the estimated hours of effort and skill level of personnel required to complete the scope of work. Provide detailed information specifying how estimates are calculated including hourly, daily, and/or monthly labor rates, and the process for determining scope of work such as the number of locations, devices, IP addresses, work stations, laptops, servers, LAN networking devices, etc. Include a value proposition specifying any factors that distinguish your company from others in the marketplace.

Pricing matrix responses should be clearly stated as they will be made available to school districts to assist in their decision-making process in selecting vendors to contract for services.

VI. FINAL SELECTION

In order for a school district to participate in this RFP, the district must notify Matthew Hejna, Supervisor at Nassau BOCES, in writing prior to beginning the mini-RFP process and selecting a firm. More than one firm may be selected, depending on the type or types of projects anticipated.

Following the mini-RFP process (Appendix D, rating, interviews, etc.) the interview committees of Nassau BOCES participating school districts shall make a determination whether they wish to proceed with a recommendation of one or more firms to their Board of Education. The approval of a firm by each Board of Education is required in order for a district to proceed in the RFP process.

Nassau BOCES participating school district's Boards of Education will select a firm or firms based on their own interviews and the recommendation of their Superintendent. Nassau BOCES participating school district's Boards of Education may elect to conduct a second round of interviews prior to making a final selection. A contract with their selected firm or firms shall be prepared by Nassau BOCES participating school districts incorporating the terms of this RFP. The contract(s) shall be approved by each Board of Education in accordance with their Board policy for all selected firms.

APPENDIX A -STATEMENT OF NON-COLLUSION
RFP 2416 – RISK ASSESSMENT AND PENETRATION TESTING FOR NASSAU BOCES PARTICIPATING SCHOOL DISTRICTS

Your bid is subject to the following Non-Collusion Statement of Section 103-D of the General Municipal Law which reads as follows:

"103-D. Statement of non-collusion in bids and proposals to political subdivision of the state. Every bid or proposal hereafter made to a political subdivision of the state or any public department, agency or official thereof where competitive bidding is required by statute, rule, regulation or local law, for work or services performed, to be performed, or goods sold or to be sold, shall contain the following statement subscribed by the bidder and affirmed by such bidder as true under the penalties of perjury: Non-collusive bidding certification.

(A) By submission of this bid, each bidder and each person signing on behalf of any bidder certifies, and in the case of a joint bid each party thereto certifies as to its own organization, under penalty of perjury, that to the best of knowledge and belief:

(1) The prices in this bid have been arrived at independently without collusion, consultation, communication, or agreement, for the purpose of restricting competition, as to any matter relating to such prices with any other bidder or with any competitor;

(2) Unless otherwise required by law, the prices which have been quoted in this bid have not been knowingly disclosed by the bidder and will not knowingly be disclosed by the bidder prior to opening, directly or indirectly, to any other bidder or to any competitor; and

(3) No attempt has been made or will be made by the bidder to induce any other person, partnership or corporation to submit or not to submit a bid for the purpose of restricting competition.

(B) A bid shall not be considered for award nor shall any award be made where (A) (1), (2) and (3) above have not been complied with; provided, however, that if in any case the bidder cannot make the foregoing certification, the bidder shall so state and shall furnish with the bid a signed statement which sets forth in detail the reasons therefore. Where (A) (1), (2) and (3) above have not been complied with, the bid shall not be considered for award nor shall any award be made unless the head of the purchasing unit of the political subdivision, or his designee, determines that such disclosure was not made for the purpose of restricting competition.

The fact that the bidder (a) has published price lists, rates, or tariffs covering items being procured, (b) has informed prospective customers of proposed or pending publication of new or revised price lists for such items, or (c) has sold the same items to other customers at the same prices being bid, does not constitute, without more, a disclosure within the meaning of subparagraph one (A).

Any bid hereafter made to any subdivision of the state or any public department, agency or official thereof by a corporate bidder for work or services performed or goods sold or to be sold, where competitive bidding is required by statute, rule, regulation, or local law, and where such bid contains the certification referred to in subdivision one of the section, shall be deemed to have been authorized by the board of directors of the bidder, and such authorization shall be deemed to include the signing and submission of the bid and the inclusion therein of the certificate as to non-collusion as the act and deed of the corporation.

COMPANY_____ SIGNED_____

ADDRESS_____ TITLE_____

APPENDIX B
CERTIFICATION OF COMPLIANCE WITH THE IRAN DIVESTMENT ACT
RFP 2416- RISK ASSESSMENT AND PENETRATION TESTING FOR NASSAU BOCES PARTICIPATING SCHOOL DISTRICTS

As a result of the Iran Divestment Act of 2012 (the "Act"), Chapter 1 of the 2012 Laws of New York, a new provision has been added to State Finance Law (SFL) § 165-a and New York General Municipal Law § 103-g, both effective April 12, 2012. Under the Act, the Commissioner of the Office of General Services (OGS) has developed a list of "persons" who are engaged in "investment activities in Iran" (both are defined terms in the law) (the "Prohibited Entities List"). Pursuant to SFL § 165-a (3) (b), this list will be posted on the New York Office of General Services website.

By submitting a bid in response to this solicitation or by assuming the responsibility of a Contract awarded hereunder, each Bidder/Contractor, any person signing on behalf of any Bidder/Contractor and any assignee or subcontractor and, in the case of a joint bid, each party thereto, certifies, under penalty of perjury, that it is not on the "Entities Determined To Be Non-Responsive Bidders/Offerers Pursuant to The New York State Iran Divestment Act of 2012" list ("Prohibited Entities List") posted on the OGS website at http://www.ogs.ny.gov/about/regs/docs/ListofEntities.pdf and further certifies that it will not utilize on such Contract any subcontractor that is identified on the Prohibited Entities List. Additionally Bidder/Contractor is advised that should it seek to renew or extend a Contract awarded in response to the solicitation, it must provide the same certification at the time the Contract is renewed or extended.

During the term of the Contract, should Nassau BOCES receive information that a person (as defined in State Finance Law Section 165-a) is in violation of the above-referenced certifications, Nassau BOCES will review such information and offer the person an opportunity to respond. If the person fails to demonstrate that it has ceased its engagement in the investment activity which is in violation of the Act within 90 days after the determination of such violation, then Nassau BOCES shall take such action as may be appropriate and provided for by law, rule, or contract, including, but not limited to, seeking compliance, recovering damages, or declaring the Contractor in default.

Nassau BOCES reserves the right to reject any bid, request for assignment, renewal or extension for an entity that appears on the Prohibited Entities List prior to the award, assignment, renewal or extension of a contract, and to pursue a responsibility review with respect to any entity that is awarded a contract and appears on the Prohibited Entities list after contract award.

COMPANY
NAME_____

COMPANY REPRESENTATIVE (IN PRINT)
_____

TITLE OF COMPANY
REPRESENTATIVE_____

COMPANY REPRESENTATIVE
SIGNATURE_____

COMPANY
ADDRESS_____

APPENDIX C

REQUEST FOR PROPOSALS 2416

RISK ASSESSMENT AND PENETRATION TESTING FOR NASSAU BOCES PARTICIPATING SCHOOL DISTRICTS
FIRM PRE-QUALFICIATION SHEET
TOTAL SCORE, ALL COMMITTEE MEMBERS

NAME OF FIRM	Firm Meets Licensing /Insurance Requirements (Yes/No)	Firm Meets Non-Conflict of Interest Requirements (Yes/No)	Firm Adheres to RFP Instructions and Requirements (Yes/No)	Firm Demonstrates Minimum Qualifications and Experience (Yes/No)	Quality of references Acceptable (Yes/No)	Vendor Provides Acceptable Samples of Deliverables Provided to Districts (Yes/No)	FIRM PRE-QUALIFIED (Yes/No)

APPENDIX D

REQUEST FOR PROPOSALS 2416

RISK ASSESSMENT AND PENETRATION TESTING FOR NASSAU BOCES PARTICIPATING SCHOOL DISTRICTS

FIRM RATING SHEET

TOTAL SCORE, ALL COMMITTEE MEMBERS

NAME OF FIRM	Firm's experience performing Risk Assessment and/or Penetration Testing for school districts	Firm's experience performing Risk Assessment and/or Penetration Testing for other organizations	Quality and experience of firm's proposed staff	Pricing Schedule	Quality of references	Location of firm and consultants	Samples of deliverables provided to districts i.e. reports, presentations, etc.	TOTAL SCORE
(Points)	(15)	(15)	(20)	(10)	(15)	(10)	(15)	(100)

Rating Scale: Using a rating scale of 1-5 (5 being the best) multiply by the assigned weighted value of each criterion.