RFP # 2416 FAQ

Risk Assessment and Penetration Testing for Nassau BOCES Participating School Districts

WHO MAY PARTICIPATE IN THIS RFP?
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). 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.

WILL CONTRACTED SERVICES BE PURCHASED THROUGH BOCES?
No. 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.

In order for a school district to participate in this RFP, the district must notify Matthew Hejna (mhejna@nasboces.org), 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.

WHAT IS THE PROCUREMENT PROCESS?
Following the mini-RFP process, the interview committees of 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.

Participating school district's Boards of Education will select a firm or firms based on their own interviews and the recommendation of their Superintendent. 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 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.

ARE COSTS FOR CONTRACTED SERVICES AIDABLE?
Nassau RIC component districts will not receive State aid for expenses. Other districts should check with their local RIC to determine if costs are aidable.

WHAT WAS THE CRITERIA FOR SELECTING PRE-QUALIFIED VENDORS?

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

WHAT ARE THE SCOPE OF SERVICES INCLUDED IN THIS RFP?
The types of services being addressed in this request include:

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.

Vendors are not required to provide all service types so be sure to review RFP to confirm availability.

PRE-QUALIFIED VENDORS

COMPANY	CONTACT	EMAIL	PHONE
Atlanticcare IT	Justin Schwartz	jschwartz@tomorrowsoffice.com	914.674.4500 x5476
The Bonadio Group	Brett Coburn	bcoburn@bonadio.com	315.214.7843
CDWG	Ralph Sharkis	ralph.sharkis@cdwg.com	866.643.9333
Core BTS, Inc.	Matt Pomara	matt.pomara@corebts.com	631.982.4798
CSDNET	Fred Zappolo	fred.zappolo@csdnet.net	631.924.7474
Dyntek	Alan Gottesman	alan.gottesman@dyntek.com	646-213-4702
Edu Tek	Matthew Orifici	matthew.orifici@edutekltd.com	914.686.7777
ePlus Technology	Alan Stein	astein@eplus.com	631.478.6531