GUILFORD COUNTY SCHOOLS

Request for Qualifications Guilford County Schools Security Information and Event Management and Security Operations Center

Addendum 1

Purchasing Department
501 W. Washington Street
Greensboro, NC 27401

Direct all inquiries to:	**Invitation for Bids: 6550**
Shayla C. Parker	**Bid due date: February 13, 2023**
TechRFPQ@gcsnc.com	**Commodity: SIEM Setup/Configuration and SOC 24/7 Monitoring**

NOTICE TO BIDDERS:

Please be advised that this is Addendum I for RFP 6550 - Request for Qualifications Guilford County Schools Security Information and Event Management and Security Operations Center 24/7 Security Operation Center Monitoring and SIEM. The questions and responses from vendors are listed below:

Q1. - RFQ Section; II. Firm Information - Page 5
"This section must include name of firm, address, telephone number, fax number, email address, home page URL, type of firm (i.e., corporation), and **North Carolina business license number.** Provide a brief history of the firm including the year the firm was established as presently organized. Include total number of staff by job category, and registration. Include a company profile that lists the primary services (disciplines) offered. Identify the location of the office that will be responsible for the implementation of services provided to GCS."
Question - Do we need to obtain a North Carolina business license number; our company is based out of IL however we provide our services globally.
A1. A North Carolina Business license number is not required but a Business license from the State of operation would be expected.

Q2. #2 - RFQ Section; V. Project Experience - Page 5-6
"Provide a comprehensive list of SIEM projects your firm has worked on in the past 5 years, indicating services provided. To be used as references, list a minimum of two jobs of this size (roughly 80,000 users)."

Question - When referring to the term "roughly" in terms of users, what would be an acceptable number below the 80k threshold?
A2. A minimum of 60k to make sure a project at large scale can be accommodated.

Q3. Please explain the desire to consider other SEIM solutions.
A3. Currently we are using a Provider but due to unpredictable costs and the projection of the potentially for higher cost in the future, we would be willing to consider other alternatives.

Q4. Is the desire to stay with Crowdstrike?
A4. The main desire to stay with Crowdstrike is that NCDPI currently pays for licenses and MCNC helps monitor the solution. This monitoring helps with workload for the district. If there are other alternatives to Crowdstrike, we would be interested to know but we must be able to fund it through NCDPI as a funding source.

Q5. Is there a desire to leverage existing Microsoft licensing?
A5. Whenever possible we would like to use Microsoft licensing.

Q6. Is there an option to take over the existing SIEM platform for the management or expect to replace existing SIEM environment?
A6. Depending on ultimate price and solution fit of the current SIEM solution it could be considered.

Q7. Is cloud monitoring in scope? if yes, please specify. Azure, AWS, IBM Cloud, Google, etc.
A7. Cloud monitoring is in scope. Currently, using Azure.

Q8. Any data residency requirements?
A8. Data needs to reside in the United States

Q9. Any onsite requirements to perform work or can work be performed remotely?
A9. Work can be performed remotely.

Q10. How many on-premises data centers are in scope?
A10. Two data centers are in scope.

Q11. Are there any requirements for US based resources, NC residency, etc.? If so, please provide requirements
A11.NC residency is not required but US based resource is required.

Q12. What is the contract length the school board is anticipating? 36 months, 60 months etc.?
A12. 36 months is most likely the contract length with the option to extend. This is subject to change.

Q13. Is it required that the vendors who intend to provide a response complete the Execution section on page 2 of the RFQ **prior to** submitting our response on 2/13/23 or can this be submitted along with our response by 2/13/23? If it is required prior to 2/13 submittal, in what

format should we be returning the execution page to Guilford County Schools (email, Docusign, etc.)?
A13. You can submit along with the response

Q14. Is Guilford County Schools expecting the selected vendor for the SIEM monitoring to take action on the Crowdstrike logs that are ingested?
A14. If it is a Crowdstrike alert, then no because another vendor will be handling the response. If the alert links up with a bigger scale attack that Crowdstrike did not detect then an alert to GCS is expected. Response to the alert can be built in but is not required.

Q15. Are there plans to leverage other components of the Microsoft A5 license such as any of the Defenders?
A15.We are open to use any components of our license that we can to make our environment more secure.

Q16. Is it important for Guilford County Schools to maintain data custody or are you entertaining solutions which require you to send your data to a SIEM provider as an option?
A16.We are entertaining sending data to a SIEM provider if the solution allows for the amount of throughput that we need.

Q17. What kind of device management solution does Guilford County Schools currently use?
A17. Intune/SCCM for Windows and JAMF for Apple devices.

Q18. What kinds of devices do Guilford County Schools use? (Chromebooks, MACs, Windows, etc.?)
A18.Windows or Mac for faculty or staff for the most part and iPad and Chromebook for students depending on grade. K-3 currently get iPad and 4-12 get Chromebooks.

Q19. Do Guilford County schools expect students as well as faculty to be supported in the SIEM solution?
A19. More information on what is meant by supported is needed.

Q20. Are you open to considering an all-encompassing SIEM/SOC as a service solution such as MDR (Managed Detection and Response)?
A20. We are open to MDR solutions depending on capabilities and pricing.