Questions & Answers for EDR Meeting 4/12/2023 at 2:30 p.m.

1. Do you want the same protection/features for both students and staff? If not, please specify the differences. *Yes*

2. Should the quotes be for 15,116 seats? (12,916 students + 2,200 staff) If not, please specify the quantity (or quantities if students and staff will have different protection/features) on which to base the quotes. Please break out quantities by OS (Windows/MacOS/ChromeOS/etc.)
Please provide a quote for 250 seats initially. Potential growth to ~15000

3. Do you plan to manage the day-to-day operations with your own SOC team, or are you looking for a fully managed solution?
Combination managed and own team for day-to-day. Managed remediation

4. Regarding item A1 (The system must integrate well and be compatible with Google for Education / Google Portal Products): what functions from EDR would integrate with these Google products?
Noting that we are a Google for Education environment

5. Regarding item A3 (The system shall provide a mobile platform usable by all constituents including administrators, teachers, and students): what functions are expected of this mobile platform?
A dashboard that is compatible with mobile devices is preferred

6. Regarding item A4 (The system shall provide data integrity and security): what data do you want the system to secure? (Internal EDR data, full disk encryption of endpoints, removable drives, other?) What sort of protection are you looking for? (e.g.: encryption, removable device control?)
Ransomware, malware, virus protection

7. Regarding item A5 (The system shall allow for integration with 3rd Party Applications (e.g. Custom Intuitive Data Imports/Exports)): what kind of data are you planning to import into the EDR system?
If possible, data from the old system regarding endpoints.

8. Regarding item A7 (The system shall provide modules that are fully integrated, eliminating the need for redundant data entry): what kind of data will be entered using "data entry"?*Hopefully not a lot but we would want the product to pass data between modules if applicable.*

9. Do you use cloud Microsoft 365, or on-premises Microsoft Office products? *On-premises Microsoft.*

10. For "disaster recovery capabilities" are you asking about the EDR product's ability to recover or DR for the entire network environment? *We are asking about recovery from Ransomware, for example*

11. For "Data Conversion Process Steps and Activities", what data are you converting? *Importing or converting policies/settings from existing EDR system(s)*

12. Is there an idea of the number of endpoints to be quoted for the scope of this EDR RFP? I can provide multiple options but couldn't seem to locate anything within the RFP that calls out quantity. *Approximately 250*

13. Can you provide quantities of the following devices that you are looking to protect with EDR?
    a. Mobile
        i. iphones
        ii. iPads
        iii. Android Tablets
        iv. Android phones
        v. Chromebooks
        vi. What is the count of Windows/Mac?
    b. Workstations (laptops/computers)
    c. Servers *250 - only servers at this time*

14. Can you share a breakdown of operating systems within scope? Ie both Windows and Linux servers, ChromeOS, etc? *Windows*

15. Does North Penn have a breakdown of endpoints by device type and operating system? *Looking at Windows Server and Windows 11 Workstations at this time*

16. Do you have a Current Endpoint that is supported? If so which solution are you using? What AV or EDR solution does the district use today? *Trend Micro Apex One*

17. Are you only looking for an EDR Solution? Or are you looking for Endpoint & EDR Solution? *Endpoint and EDR*

18. Are you looking for a managed solution? *Yes*

19. Are you looking for an endpoint with all the capabilities or are you looking for just an endpoint? *Endpoint, additional capabilities optional*

20. Please define what you consider a guest network. *A network that is separate from the production that students and parents can connect to from personal devices*

21. Are you looking for the capability to block mobile devices from accessing phishing sites? *Not at this time.*

22. Is the ability to detect malicious WiFi networks and alerting users to disconnect from the network of value? *Yes, it is of value.*

23. Is the ability to assess all mobile apps for undesired violations of privacy or unsecure development practices of importance to the district? *Yes, however, that requirement is not in the scope of this RFP.*

24. How do you remediate devices that have already been compromised today? *We currently use a manual process with our network staff.*

25. What email platform is used for students and staff today? *Gmail*

26. How are you controlling application downloading on student/admin devices today? *The staff has download ability, but students do not.*

27. Are risk scores associated with Chrome extensions of interest? *Not at this time.*

28. What are your preferred deployment methods for the mobile devices of the school district? (ex MSFT Intune. GWA) **SCCM, JAMF, Google Admin**

29. Does NPSD have a cyber insurance or compliance requirement to store a certain amount of days worth of data for each endpoint? 30 days, 90 days, 365 days for example *Not at this time*

30. In the Corporate Overview Section 2.2, does the VAR or Vendor provide answers to the questions? **Vendor**

31. How many NPSD IT members will be managing the EDR platform? *3-5*

32. What SIEM does NPSD utilize today if any? *None at this time*

33. Does North Penn have a 24/7 IT shift team? *No*

34. For the 1 Geographical Reference, how close in proximity must they be? *Like-size district is more important than geography*

    How many total references are needed? *3*

35. In the cost proposal section, what is the definition of "data conversion costs" *If we are bringing data from another system, is there a cost for that?*

36. Is NPSD open to utilizing a separate solution for web filtering/content filtering/classroom monitoring from the EDR solution? *Yes*

37. Is the district interested in a managed (MDR) option as well as EDR? *Yes*

38. Is North Penn looking to manage the solution internally, or are you looking for help with managed services/professional services for 24x7x365 monitoring, alerting, and response support? *Combination of internal and managed services*

39. What are the security tools currently deployed at North Penn? *We will not be disclosing this information on this FAQ to protect the Cybersecurity posture of the district. Questions can be addressed in finalist interviews as applicable.*

40. Do you have a network diagram/topology that can be shared? *We will not be disclosing this information on this FAQ to protect the Cybersecurity posture of the district. Questions can be addressed in finalist interviews as applicable.*

41. Is there an incumbent solution provider in place currently? **Yes**

42. What, if any, are the other agents installed on the endpoints? *Trend Micro*

43. Is there an allocated and approved budget for this project? *There is a proposed budget that needs to be approved by the school board as part of the overall district budget in June.*

44. Is there a current solution in place that is being considered for replacement? **Yes**

   Are there any critical systems that this solution will need to integrate with? i.e., a SIEM solution, a PowerBI analytics platform, etc. *Not at this time*

45. Will you implement this solution with internal resources, or will you require assistance deploying it? *Combination of internal and external resources*

46. Do you need a rollback capability? *In the event of Ransomware, yes*

47. Would you require full access to the dashboard to make changes to policies or do you require this to be managed? *Combination of internal and managed services*

48. What is your timeline for making a decision on a provider? *May 2023*

49. What is your timeline for the completion of the project? *Sept 2023*

50. Did any specific event create the need for this project? *No*

51. Describe the structure/expertise/experience of your current security team. *We will not be disclosing this information on this FAQ to protect the Cybersecurity posture of the district. Questions can be addressed in finalist interviews as applicable.*

52. What features/functions are a top priority as part of an endpoint security solution? *Prompt isolation and remediation*

53. What is your current solution for 3rd party access control? *We will not be disclosing this information on this FAQ to protect the Cybersecurity posture of the district. Questions can be addressed in finalist interviews as applicable.*

54. What is your current visibility into east-west traffic? *We will not be disclosing this information on this FAQ to protect the Cybersecurity posture of the district. Questions can be addressed in finalist interviews as applicable.*

55. "Which legacy platforms are you still supporting? What critical applications are running on your legacy platforms?" *We will not be disclosing this information on this FAQ to protect the Cybersecurity posture of the district. Questions can be addressed in finalist interviews as applicable.*

56. Do you have a data retention requirement for event data and logs? *Not at this time.*

57. Do you follow a specific security framework currently? *We are partnered with FR Secure.*

58. Describe your network segmentation. *We will not be disclosing this information on this FAQ to protect the Cybersecurity posture of the district. Questions can be addressed in finalist interviews as applicable.*

59. Will your team require training for the proposed solution? *Yes*

60. Will you require a proof of concept/proof of value? *If that is helpful to us in choosing you as a vendor. It is not a specific requirement.*

61. As part of the solution, what native forensic/response tools are required/in scope for the solution? *No requirement, but would like to see options from vendors*

62. What are the most important expectations you have for a security partner? *Industry footprint and proven track record*

63. What are your top requirements for the solution provider you choose which will set them apart from other bidders? *Industry footprint and proven track record*

64. Can offshore personnel (Outside of the United States) work on this project? *Yes*

65. Do you want 24/7 threat remediation of the alerts found on EDR? *We would like to see that as an option with the cost provided.*

66. Can you share what the existing av/edr solution is today that you use on servers/workstations? If not all good - *Trend Micro Apex One*

   Just to confirm. The RFP makes mention of 12,916 students and 2,200 staff. While the students have Chromebooks and staff have mostly workstations, the RFP does not cover these. You are just after EDR for 200 Servers and 50 workstations that are primarily Windows. Nothing else is required apart from EDR protection for these 250 devices. *At this time, that is correct.*

67. Are there any requirements/considerations to include patch management on these Endpoints? *There is no requirement for patch management*

68. You mentioned you use Google for email, would that be within the scope or strictly focused on the clients/endpoints? *Google for email is not currently in the scope.*

69. Are there any data retention requirements? *Not at this time.*

70. What is your firewall for integration?
   Currently using Palo Alto firewall

71. Is it necessary to send in a hard copy of the RFP?
   Yes, we want to have one copy on hand with all original signatures.

72. Would the purchase need to be on PEPPM or Costars? Or is no contract vehicle needed since it's an RFP? There is a possibility of using Federal Funds.
   Please include the contact information for your company if you are part of either of these.

73. Can you please confirm if there are any contract requirements?
   Contracts will need to be provided after approval/award of the RFP.

74. The website for RFP updates is listed as https://www.npenn.org/page/695 in the RFP, but that page doesn't exist.
   https://www.npenn.org/central_office/business_office/bid_specifications