Questions & Answers - 1

Solicitation	22-680-009 - Security Audit
Buying Organization	Poudre School District

No	Question/Answer	Question Date
Q1	**Question: Project Timeline** We would like to know what would be the project timeline. please advise. **Answer:** Poudre School District would like to have the security audit complete within two months of the award.	03/23/2022
Q2	**Question: Project Amount** We would like to know the project amount. **Answer:** A budget for this project has not been determined.	03/23/2022
Q3	**Question: Scope of Service: CIS Level** Can the District please confirm it is interested in CIS Version 8, Level 2, controls for this audit? **Answer:** Yes, the District is interested in Level 2 controls for this audit	03/24/2022
Q4	**Question: Scope of Service: Physical Security** The CIS Level 8 does not include physical or environmental security, is the District interested in adding in additional controls to address physical and environmental security? **Answer:** The District is NOT interested in adding anything related to physical security or environmental security.	03/24/2022
Q5	**Question: Location of Performance** Does the District have a preference for performing the effort remote via video conference, on-site in person, or a combination? **Answer:** The District would prefer to have the audit performed on-site but would be willing to entertain a combination if all requirements could be met.	03/24/2022
Q6	**Question: Prior Assessments** Have you done a CIS assessment, or other best practice framework assessment in the past? If so, what framework and when was it done? **Answer:** The District has not done a CIS assessment or other best practice framework in the past.	03/25/2022
Q7	**Question: Org Chart and departments** Can you provide a high-level org chart of the administrative functions, please? In particular, we would like to know the number and names of administrative departments. Obviously, individual names are not necessary. Just the overall structure. **Answer:** See attached org chart.	03/25/2022

No	Question/Answer	Question Date
Q8	**Question: Security Team** Please provide a high-level overview of your security team, such as size and function. **Answer:** The District currently does not have any dedicated security people or team. The security functions are handled by various positions such as Network Engineers, System Administrators, and Enterprise Architects.	03/25/2022
Q9	**Question: Project Management Resources** How will project management work on your side? Will you have project manager(s) assigned to this who will assist with coordinating assessment activities? **Answer:** The District will have a project manager and District employees available to assist with coordinating assessment activities.	03/25/2022
Q10	**Question: 22-680-009 - Security Audit** 1.While we have not performed 3 contracts for similar school districts, we have several other type contracts where we provided similar services. Is it a mandatory requirement for our references to be from similar type school districts? 2.Is there currently an incumbent company or previous incumbent, who completed similar contract performing these services? If so - are they eligible to bid on this project and can you please provide incumbent contract number, dollar value and period of performance? 3.Specify the VLAN details how many is included in the Scope? 4.Can you please provide current number of infrastructure details (Physical Server, Virtual Server, Network Devices etc. 5.Approximately how many computer endpoints do you have (desktop PCs, laptops, servers)? 6.Can you tell the total number of endpoints you want protected? 7.What’s your headcount of users (employees + contractors + interns)? What number/percentage of your workforce resides within organizational facilities? What number/percentage works remotely? 8.How much (%) of the infrastructure is in cloud? 9.What is the size of the IT environment? 10.How many physical locations? 11.What is the aggregate Internet Capacity per location (<300mbps, <1gbps, <4gbps, up to 10gbps)? 12.Do you manage your own data Center, or do you utilize any 3rd-party/colocation facilities? 13.What is the approximate budget? **Answer:** 1. Educational references are acceptable. 2. There is no incumbent provider. 3. Approximately 25 4. 60 Physical, 200 Virtual, 2 firewalls, 2 routers, numerous switches 5. 32,000 6. Approximately 30,000 endpoints and 300 servers 7. Approximately 27,000 student end-users and 4,500 employees 8. Approximately 50% cloud / on premise 9. 53 employees 10. Two (2) data centers and 50 school sites 11. The District has two 10gbps connections to the internet from its data center. It has 35 sites on a fiber ring connecting back to its data center. It has 15 point-to-point connections from sites to its data center. 12. Manage own data center 13. A budget for this project has not been determined.	03/26/2022

No	Question/Answer	Question Date
Q11	**Question: How many public** How many public-facing IP’s are owned (for Penetration Testing)? **Answer:** The District owns a full Class B subnet of public IP addresses.	03/28/2022
Q12	**Question: How many SSID's** How many SSID’s are in use (for Penetration Testing)? **Answer:** The District currently has 4 SSIDs for its wireless network	03/28/2022
Q13	**Question: Off-prem computing** What is/are your off-prem computing/storage hosting environment(s) (Vendor, Product)? **Answer:** The District uses Microsoft Azure as its cloud provider.	03/28/2022
Q14	**Question: Off-prem compute** How is/are your off-prem compute/storage environment(s) connected? **Answer:** The District's backup data center is connected via a 10gbps fiber ring. There is no direct connection to its cloud provider.	03/28/2022
Q15	**Question: What VM platform** What VM platform are you using (VMware, Hyper-V, Citrix, KVM, etc.)? **Answer:** VMware platform	03/28/2022
Q16	**Question: What is the composition** What is the composition of your VM Guests (# Windows, # Linux, #Other)? **Answer:** 95% of VM’s are Microsoft Windows, 5% are Linux	03/28/2022
Q17	**Question: Are you using** Are you using a management platform for Apple devices (JAMF, InTune, etc.)? **Answer:** The District uses JAMF Pro	03/28/2022
Q18	**Question: How many security** How many security devices are online and in-scope (Firewalls, IDS/IPS/etc.)? **Answer:** The District uses two (2) load balanced Firewalls at its edge that also offer functionality such as IDS/IPS/Malware protection, etc.	03/28/2022
Q19	**Question: Microsoft Enterprise** Does “Microsoft Enterprise” indicate/include Microsoft Azure? a.If yes, what is the composition of services consumed in Azure (Virtual servers, services, integrations)? **Answer:** Yes, the District does use Microsoft answer for web hosting, some virtual servers, backup storage, Azure AD.	03/28/2022
Q20	**Question: Start and complete** What are the expected start and completion dates for this work? **Answer:** The District's preference is to start this work within 30 days of the RFP closing and have it complete within 2 months of the award.	03/28/2022

No	Question/Answer	Question Date
Q21	**Question: Cost Proposal** Should the Cost Proposal be submitted separately from the Technical Proposal? **Answer:** The Cost Proposal can be submitted with the Technical Proposal.	03/29/2022
Q22	**Question: Organization Centralization:** Is the IT organization centralized or decentralized? **Answer:** It is centralized.	03/29/2022
Q23	**Question: District's Budget** What is District's budget for this project? **Answer:** A budget for this project has not been determined.	03/29/2022
Q24	**Question: Security Framework** Has the CIS framework already been adopted? If yes, has an audit been completed in the past? **Answer:** No - the CIS framework has not already been adopted.	03/29/2022
Q25	**Question: Policies and Procedures** Are there documented IT policies, procedures, standards, and guidelines in place? If so, how many? **Answer:** There are no documented IT policies, procedures, standards, and guidelines in place.	03/29/2022
Q26	**Question: Applications** How many enterprise applications are included in the scope for the security audit? **Answer:** Approximately 40 internal applications and approximately 50 external third party applications	03/29/2022
Q27	**Question: Data Centers** How many data centers are in scope for testing? **Answer:** Two (2) data centers	03/29/2022
Q28	**Question: IT Staff and IT Security STaff** How many fulltime IT staff are there? How many are dedicated to security? **Answer:** Fulltime IT staff = 52. None are dedicated to security.	03/29/2022
Q29	**Question: Security Audit RFP Question** Is this assessment required for the entire footprint or for any specific subset of the environment? **Answer:** The assessment is required for the entire footprint.	03/30/2022
Q30	**Question: Security Audit RFP Question** Have you ever conducted any sort of framework assessment before? **Answer:** A framework assessment has not been conducted.	03/30/2022
Q31	**Question: Security Audit RFP Question** How many virtualized machines and servers do you have? **Answer:** Approximately 300 servers	03/30/2022

No	Question/Answer	Question Date
Q32	**Question: Security Audit RFP Question** Is your primary Backup system same as your DR? **Answer:** The District's primary backup solution is separate from its DR solution.	03/30/2022
Q33	**Question: Security Audit RFP Question** How many Network Devices are there that are not wireless? Is there central management of network or is it distributed? **Answer:** The District has 50 sites that are networked with multiple layer 3 switches per site. Central management of networking.	03/30/2022
Q34	**Question: Security Audit RFP Question** Will we be permitted to go onsite to assess their physical controls at the datacenter and schools? **Answer:** Yes - onsite assessment of physical controls at the datacenter and schools will be permitted.	03/30/2022
Q35	**Question: Security Audit RFP Question** Section 3.1 – Determining the criticality of systems, and assessing their risks is normally conducted via a Business Impact Assessment (BIA) as opposed to assessing the IT and policy controls that are assessed via the CIS v8 critical security controls. Would the district be interested in having a BIA assessment be included as an optional service? **Answer:** Yes the District would be interested as that being added as an “optional” service.	03/30/2022
Q36	**Question: Start Date** Can District provide an anticipated start date for the project? **Answer:** Within 30 days of the award	03/30/2022
Q37	**Question: Previous CIS or cybersecurity audit** Has the District performed a CIS or similar cybersecurity audits/assessments in prior years? Would the results of that assessment(s) be made available? **Answer:** The District has not had an assessment since 2012 and would not make the assessment results available.	03/30/2022
Q38	**Question: Risk Register** Does the District maintain a risk register or otherwise track remediation efforts related to gaps in CIS requirements? **Answer:** The District does not maintain a risk register.	03/30/2022
Q39	**Question: IT Administrative Functions** Are IT administrative functions centralized at one location, e.g. logical access provisioning, change management, network security, etc.? If some functions are distributed, would the local administrators be participating in the audit? **Answer:** The administrative functions are centrally located.	03/30/2022
Q40	**Question: Primary Contact** Does the District have a designated Information Security Officer or similar who will be available to act as the primary point of contact during the audit? **Answer:** The District does NOT have an information security officer	03/30/2022

No	Question/Answer	Question Date
Q41	**Question: Project Dates** Does the District have a preference for fieldwork start dates? Final report date? **Answer:** Within 30 days of the award	03/30/2022
Q42	**Question: Fieldwork location** Does the District prefer fieldwork to be performed fully remotely, fully on site, or some combination that is agreeable to the audit key participants? **Answer:** The District prefers a combination of onsite and offsite.	03/30/2022
Q43	**Question: Travel Time & Expenses** Should travel time and expenses be rolled into the fee estimate or should those be billed separately at actual and reasonable costs? **Answer:** Please include travel time and expenses into the fee estimate as a separate line item.	03/30/2022
Q44	**Question: Operating Effectiveness Testing** Does the District prefer the audit be a review of the DESIGN of safeguards (“test of one”) or does it expect the service auditor to perform OPERATING EFFECTIVENESS testing on all of the 153 CIS safeguards? If operating effectiveness testing is required, can the District provide sampling guidance in the near-term so that it can be used to develop an accurate fee estimate? **Answer:** The service auditor will perform operating effectiveness testing on all of the 153 CIS safeguards.	03/30/2022
Q45	**Question: Asset Discovery Tool** Does the District have an asset (hardware/software) discovery tool or does the service auditor need to provide one? **Answer:** The District prefers the service auditor provide an asset (hardware/software) discovery tool.	03/30/2022
Q46	**Question: Policies, Procedures, & Guidelines** Does the District have an up-to-date comprehensive set of policies, procedures, and guidelines that are built around the CIS Safeguards? **Answer:** No - the District does not have an up-to-date comprehensive set of policies, procedures, and guidelines that are built around the CIS Safeguards	03/30/2022
Q47	**Question: Network and Data Flow Diagrams** Does the District maintain network diagrams and data flow diagrams at Level 0? Level 1? **Answer:** The District has networking diagrams but not to any specific standard.	03/30/2022
Q48	**Question: Out-of-Scope** Are there any portions of the infrastructure that will be out-of-scope? **Answer:** No portions of the infrastructure will be out-of-scope.	03/30/2022
Q49	**Question: Data Center Locations** What are the locations of the primary and any secondary data centers? **Answer:** Information Technology Center - 2413 Laporte Avenue, Fort Collins 80521; Fort Collins High School - 3400 Lambkin Way, Fort Collins 80525	03/30/2022

No	Question/Answer	Question Date
Q50	**Question: Third-Party Service Providers** Does the District rely on any third-party service providers to execute or support any of the CIS safeguards? If so, which safeguards? Do the service providers issue an annual Service and Organization Controls Report (or similar) that are reviewed by management? Does the District map any Client User Entity Control Considerations to its internal controls? **Answer:** No - the District does not rely on any third-party service providers to execute or support any of the CIS safeguards.	03/30/2022