

Request For Proposals Addendum

Addendum Number 1: Vendor Q & A

Date: Tuesday, June 24, 2025

**RFP #2-ERCSP-0825 Ohio E-Rate Cyber Security Pilot Program – Form 470#
CBR420250453**

To: All Prospective Vendors

The following questions were sent in response to the referenced Solicitation for further clarification. Questions and Answers are listed below.

Question 1: Network & Identity Protection – DDoS Protection with Load Balancer & WAF:
What DDoS protection solution is currently deployed, and how effective has it been in mitigating attacks?

Answer: We do not have any DDoS protection currently in place.

Question 2: Network & Identity Protection – DDoS Protection with Load Balancer & WAF:
Are you looking to retain your existing solution, or are you considering replacing it with a different provider?

Answer: Looking for a new solution as we don't currently have a solution in place.

Question 3: Network & Identity Protection – DDoS Protection with Load Balancer & WAF:
Should the WAF integrate with existing security policies or allow for custom rule sets?

Answer: Yes, it should allow for custom rule sets for each application and should be able to integrate with current security policies.

Question 4: Network & Identity Protection – DDoS Protection with Load Balancer & WAF:

Is cloud-native deployment preferred over hybrid models?

Answer: Cloud-native deployment.

Question 5: Network & Identity Protection – Secure DNS Filtering: What DNS filtering service is currently in use, and does it meet your security and visibility requirements?

Answer: We currently use Spectrums in house DNS. The current product doesn't meet security and visibility requirements.

Question 6: Network & Identity Protection – Secure DNS Filtering: Would you like vendors to enhance the current service, or are you exploring an entirely new solution?

Answer: We are looking to replace our current solution

Question 7: Network & Identity Protection – Secure DNS Filtering: Should the solution include on-prem DNS filtering alongside cloud-based services?

Answer: Fully cloud-based solution and service.

Question 8: Network & Identity Protection – Secure DNS Filtering: What reporting and analytics capabilities are needed to support IT operations?

Answer: The solution should provide visibility into the number of hits by URL or domain, detect any attacks targeting specific URLs or domains, and offer insights into network utilization and potential indicators of attack.

Question 9: Network & Identity Protection – Identity Governance (Shield ID or Equivalent): How well does the current identity governance platform (Rapid Identity) integrate with your security framework?

Answer: The current platform meets all requirements for our current framework standards and controls.

Question 10: Network & Identity Protection – Identity Governance (Shield ID or Equivalent): Are you satisfied with its capabilities, or are you looking for a more advanced solution?

Answer: We are only looking to add to our current solution.

Question 11: Network & Identity Protection – Identity Governance (Shield ID or Equivalent): What level of automation is expected for access provisioning and de-provisioning?

Answer: This is a security feature add-on to our current identity management solution. We are not looking to replace our current solution.

Question 12: Network & Identity Protection – Identity Governance (Shield ID or Equivalent): Should the solution integrate with existing IAM platforms (Azure AD, Rapid Identity)?

Answer: It must integrate with Rapid Identity and tie in with Azure AD as well.

Question 13: Network & Identity Protection – SASE with Browser Isolation: What web security or isolation solutions are currently being used to prevent web-based threats?

Answer: IBoss content filter and ZTNA.

Question 14: Network & Identity Protection – SASE with Browser Isolation: Are you seeking to expand on current capabilities, or do you need a more robust security architecture?

Answer: We want to expand/add-on to our current platform iBoss.

Question 15: Network & Identity Protection – Data Loss Prevention (DLP): What DLP tools are currently deployed, and have they been effective in securing sensitive data?

Answer: We currently are using Microsoft’s Sensitivity Labeling and DLP. The solution has had many bugs and the behavior is inconsistent.

Question 16: Network & Identity Protection – Data Loss Prevention (DLP): Would you prefer enhancements to the existing solution, or are you open to replacing it?

Answer: We are open to both options, either enhancing the current solution or replacing the solution with something more robust.

Question 17: Network & Identity Protection – Data Loss Prevention (DLP): What sensitivity classification standards should be used (Microsoft DLP Labels, FERPA, HIPAA)?

Answer: Microsoft Sensitivity Labels (Confidential, Restricted, Public). These labels should follow FERPA, HIPAA, and additional if needed.

Question 18: Network & Identity Protection – Data Loss Prevention (DLP): Should the DLP solution scan cloud applications (e.g., Office 365, Google Workspace)?

Answer: Yes, it needs to be able to support in-house applications and cloud applications as well as network shares.

Question 19: Network & Identity Protection – Data Loss Prevention (DLP): How should the system respond to detected violations (blocking, quarantining, alerting)?

Answer: The system should be able to alert, block, quarantine or bypass based on security policies.

Question 20: Network & Identity Protection – Web Application Vulnerability Scanning: What vulnerability scanning tools are currently in place for web applications?

Answer: We use Rapid 7 AppSec through Arctic Wolf.

Question 21: Network & Identity Protection – Web Application Vulnerability Scanning: Are you looking for additional automation and integrations, or an entirely new platform?

Answer: We are looking to have an additional platform for web scanning.

Question 22: Network & Identity Protection – Web Application Vulnerability Scanning: Is integration required with CI/CD pipelines for DevSecOps practices?

Answer: Yes, the integration should have CI/CD pipelines for DevSecOps.

Question 23: Network & Identity Protection – Web Application Vulnerability Scanning: Are specific compliance reports (OWASP Top 10, PCI-DSS) required?

Answer: Yes Compliance reports must be provided.

Question 24: Network & Identity Protection – Internal & External Penetration Testing (Ad-Hoc): How frequently do you conduct penetration testing, and which vendors or methodologies do you currently use?

Answer: We currently perform 1 annual pentest. Vendor name(s) will be provided at the time of award.

Question 25: Network & Identity Protection – Internal & External Penetration Testing (Ad-Hoc): What is the scope of penetration testing (external networks, web apps, cloud environments)?

Answer: Blackbox testing (external networks, internal networks).

Question 26: Network & Identity Protection – Internal & External Penetration Testing (Ad-Hoc): Should testing simulate real-world attack scenarios (MITRE ATT&CK framework)?

Answer: Yes, but tests cannot make changes to the production environment and/or bring services down. Severe vulnerabilities should be prompt notifications to administrators.

Question 27: Network & Identity Protection – Internal & External Penetration Testing (Ad-Hoc): Is post-testing remediation support expected from vendors?

Answer: Yes, include detailed reporting, prioritization of discovered vulnerabilities which should be clearly defined in a Statement of Work.

Question 28: Network & Identity Protection – Internal & External Penetration Testing (Ad-Hoc): Are you satisfied with your existing testing approach, or are you looking for a more tailored engagement?

Answer: We are satisfied with the current testing approach but are open to a tailored engagement.

Question 29: Network & Identity Protection – SOC Integration & Threat Intelligence: What level of integration currently exists between Arctic Wolf's SOC and your cybersecurity solutions?

Answer: We have a combination of API integrations and Syslog forwarding between our network appliances and applications.

Question 30: Network & Identity Protection – SOC Integration & Threat Intelligence:

Would you like vendors to provide additional SOC integration capabilities, or is your current setup sufficient?

Answer: We are satisfied with our current setup.

Question 31: Network & Identity Protection – Incident Response & Alerting: How well

does your current incident response workflow function in terms of automated alerts and forensic analysis?

Answer: Its fully integrated and we are not looking to change it.

Question 32: Network & Identity Protection – Incident Response & Alerting: Are you

seeking to enhance existing incident response protocols, or would you prefer a new strategy?

Answer: We are not looking for a new solution or strategy.

Question 33: Network & Identity Protection – Implementation & Support: What has been

your experience with past installation and configuration efforts—have vendors provided adequate post-deployment support?

Answer: Vendors have provided turnkey solutions, with documentation, training, and sign-off meetings detailing project completion and all SOW met.

Question 34: Network & Identity Protection – Implementation & Support: Are you looking

for a fully managed service, or do you only need vendor assistance during onboarding?

Answer: We are only looking for initial setup support, onboarding, and training. There is no need for a fully managed service.

Question 35: What about the Dark Web?

Answer: IDEA does have some products that already support us with dark web scanning, but if the product does have that capability, it is a plus.

Question 36: Since we received the RFP 2 days before deadline for NDA's our reseller partner was not able to get them returned in before the Pre-Proposal Meeting. Our company does have our NDA's, can we still use that reseller if they can get their NDA's in before submission deadline?

Answer: If the reseller is the entity submitting the proposal and did **not** submit the required NDAs by the specified deadline, they were ineligible to attend the Pre-Proposal Meeting. As outlined on page 4 of the RFP, attendance at the Pre-Proposal Meeting is mandatory for all proposers to submit a proposal in response to this RFP. However, if your company submitted the NDAs on time, attended the Pre-Proposal Meeting, and will be the entity submitting the proposal, then you may include the reseller as a partner. In this case, the reseller would operate under your company's NDA. The entity submitting the proposal must be the same entity that met the NDA submission deadline and attended the mandatory meeting.

Question 37: Regarding the 3 states for the pilot, do we need to be certified in all states to bid on the 3 states?

Answer: Yes, vendors must be certified to operate in each state they bid on.

Question 38: Can we obtain a copy of the meeting recording?

Answer: Since this meeting required an NDA for admittance, IDEA's Procurement Team will provide the PPT slides via email to the individuals who attended the meeting. IDEA is unable to share internal files, such as recordings, with external users.

Question 39: Have you done cost realism exercises for these budgets?

Answer: No.

Question 40: Is there a capability requirement matrix specifically for the DLP section or are we just going off the summary that was provided in the RFP.

Answer: Please utilize the information provided within the RFP.

Question 41: Since you're going to be 3 separate states, are they all going to be managed independently or centrally?

Answer: Preferably 1 centralized portal for all licenses.

Question 42: What type of certifications does IDEA require for this type of project?

Answer: Vendors must be qualified to do business in Texas, Florida, and Ohio if bidding in all three states. If formed outside these states (e.g., Delaware), they must register with the Secretary of State and obtain any required tax IDs to legally operate in each applicable state.

Question 43: Why is the budget different for the 3 states?

Answer: The budgets are different because the counts for each state are vastly different. IDEA operates as two entities: IDEA Public Schools (Texas) and IPS (Florida & Ohio). These entities operate independently.

Question 44: "Identity governance & Technologies" quantity for each of the 3 states says "entire region". How do we bid on 3 different bids with 3 different budgets? Have you already considered this in the evaluation process?

Answer: Each individual region requires a quantity based on enrolled users dependent on the region. Yes, we have already considered this. Below are the estimated counts for Ohio:
Ohio 1,500

Question 45: You mention the product shield; can you disclose who makes it?

Answer: Rapid Identity.

Question 46: You mention that you use iboss, is that correct? Are you happy with that product?

Answer: Yes, correct.

Question 47: Who is going to be managing/controlling DNS?

Answer: IDEA prefers this to be a provided solution where IDEA simply goes in to manage and maintain our own external DNS entries. All DNS securities should be maintained by the provider.

Question 48: We are currently certified in Florida. Do we need to be certified in Ohio and Texas to bid on the solutions for those states, or will being certified in Florida suffice?

Answer: You should be certified to operate in all states that you intend to bid on.

Question 49: Could we register now for the states we are not currently certified in?

Answer: The time constraint would be dependent on the respondent, but as far as IDEA goes, we do require certification to operate per state. IDEA does not have any control over the time it takes to obtain certification. If a vendor is not certified to operate in a state they bid on, IDEA will not be able to utilize that vendor.

Question 50: For DNS requirements, are you looking for basically protective DNS or DNS service?

Answer: We are looking for a hosted third-party solution to host our external DNS entries as SaaS. It is the vendor's responsibility to secure the platform; we are only adding custom DNS records.

Question 51: If we don't have a vendor profile in public purchase, I'm assuming we just go through the registration for free process and then we're able to it'll give us login and then we can submit our answers through the public purchase portal.

Answer: If you wish to submit electronically via Public Purchase or Tyler Munis Vendor Self-Service, you must register as a vendor before you are able to submit a response. You may also submit via mail to the address listed under *"Proposal Submission"* of the RFP.

Question 52: If our proposal is over budget, are we disqualified if we don't fit all six requests within your budget?

Answer: We would like proposals to be within IDEA's budget; however, if you have options outside of our request, please provide that. Pricing for the items we are asking for must be provided utilizing IDEA's pricing attachments, but if you'd like to provide additional options, you may submit separate documents for that.

Question 53: Are we required to bid on all six requests?

Answer: No, you may bid on the requests your company is capable of handling. The request(s) for which you bid must be specified within your proposal.

Question 54: Are you looking for self-managed or 24/7 monitoring and management from the provider?

Answer: We are only looking for initial setup support, onboarding, and training. There is no need for a fully managed service.

Question 55: Are you looking for a provider that will be providing monetary and management, or you're just looking for licensing solutions?

Answer: IDEA is looking for a cloud-based solution that I can point all of my applications to and redirect via load balancing feature to their final destination. The solution should provide DDoS protection against URLs and web application firewall features and protection for those domains/URLs.

Question 56: Will IDEA be managing the URLs?

Answer: Yes.

Question 57: On your SaaS, is everything on Office 365 or do you have Google G Suite?

Answer: Everything is on Office 365. IDEA does not use G Suite for business operating, but we do for Chromebook management only.

Question 58: Do you have multiple points of origin? For DNS, are we expecting it to come from one place or many places?

Answer: IDEA has two egress points at this time.

Question 59: Is there a current solution at the moment to allow SSL decryption as a part of in flight network DLP or not?

Answer: No

Question 60: Since you're going to be in 3 separate states, are they all going to be managed independently or centrally?

Answer: Preferably 1 centralized portal for all licenses.

Question 61: If the proposed DLP solution requires SSL decryption for visibility, is that something that IDEA's willing to meet?

Answer: Yes, we have a PKI infrastructure on premises already built. If that's needed, then IDEA can accommodate that.

Question 62: According to the schedule on all 3 RFP's the timeline shows the following:

Anticipated Board Meeting & Approval: August 2025

Initial Proposed Contract Term: Renewal option #1: July 1, 2026

Does this mean that if an award is made after the Anticipated Board Meeting & Approval August 2025, the initial purchase order would be issued within 30-60 days?

Answer: The agreement is contingent on the approval of the Cybersecurity Pilot E-Rate 471 application being approved. The expectation is to begin services on July 1, 2026.

Question 63: Specific to Request Five and DLP: If the proposed DLP solution requires SSL decryption for traffic visibility, is the customer willing to meet this prerequisite?

Answer: Yes.

Question 64: Specific to Request Five and DLP: Regarding the statement, "connectivity to on-prem file shares and data repositories, including SMB/CIFS shares and database (if applicable)"; could IDEA Public Schools specify whether the intent is on scanning data at rest within these repositories, monitoring data in transit to and from them, or both?

Answer: Both.

Question 65: Regarding the statement, "connectivity to on-prem file shares and data repositories, including SMB/CIFS shares and database (if applicable)"; could IDEA Public Schools specify whether the intent is on scanning data at rest within these repositories, monitoring data in transit to and from them, or both?

Answer: Both.

Question 66: For Web App testing: How many functions/dynamic pages does the app have?

Answer: Web app solution should have the capacity to web crawl the entire application.

Question 67: For Web App testing: How many user roles exist for the application?

Answer: It should have up to 10 user roles. Roles are unique to team and/or application.

Question 68: For Web App testing: Is it just one app, or how many?

Answer: Up to 50 applications/URLs.

Question 69: For Internal PEN Test: Number of live hosts/IP's that are running and will be in scope.

Answer: Up to 400 servers and 200 network devices. This is for all 3 regions simultaneously. Below are the numbers for Ohio:
10 devices in Ohio

Question 70: For Internal PEN Test: How many domain accounts are in the internal environment?

Answer: 100,000, this is for all 3 regions simultaneously. Below are the numbers for Ohio:1,076 Ohio

Question 71: For Internal PEN Test: Can we VPN into their environment?

Answer: No, because if this is an internal test you should already be in the internal network or should have gained access to the internal network.

Question 72: Can you confirm the number of unique domains and subdomains for WAF/load balancer coverage?

Answer: Up to 50.

Question 73: How many origin endpoints will need to be load balanced?

Answer: Up to 50.

Question 74: Do you require L3/L4 DDoS protection, or only application-layer (L7) DDoS protection?

Answer: L3-7.

Question 75: Do you have estimated or peak bandwidth usage for the protected applications?

Answer: 500MB

Question 76: Should we include Bot Management in the WAF scope? If you experience a high level of Bot Traffic it is recommended.

Answer: Yes.

Question 77: Can you please confirm the number of active user and services accounts in your environment/active directory?

Answer: 100,000 accounts, the remaining accounts are service account and accounts that will be filled once enrollment and hiring is complete after summer. Below are the numbers for Ohio:

1,076 Ohio

Question 78: We are able to find the Texas bid documents on the main IDEA site and the link you provided; however, we cannot locate the bid documents on Public Purchase for the Florida or Ohio RFPs. Can you provide alternate link for bid documents and response?

Answer: The Ohio RFP and all relevant attachments can be found on Public Purchase at <https://www.publicpurchase.com/gems/login/login>. You must register as a new vendor if you have not done so in order to access this platform. The Ohio RFP and all relevant attachments may also be found on IDEA Greater Cincinnati Inc.'s website under "Open Solicitations" at <https://ideapublicschools.org/regions/greater-cincinnati/>.

Question 79: The DNS Filtering user count is 92,500—Is this staff + students only? Can you please break off staff vs student count?

Answer: 81,350 student, 12,319 staff; numbers are subject to change because enrollment/hiring is in progress.

Question 80: Is agentless DNS filtering acceptable, or do you require endpoint-based filtering for roaming users?

Answer: Agentless only.

Question 81: For DLP, how many of the 9,251 users need full coverage (e.g., web + email + data at rest)?

Answer: 120 Ohio.

Question 82: Will DLP need to integrate with Microsoft 365 sensitivity labels and cloud apps?

Answer: Yes.

Question 83: Is DLP focused on data-in-transit, or also data-at-rest classification?

Answer: DLP is focused with both data-in-transit, data-at-rest and data-in-use.

Question 84: What security tools are currently in use?

Answer: Reference the RFP

Question 85: Is Rapid Identity the only SSO provider, or are there others in place?

Answer: Azure SSO and DUO SSO.

Question 86: What authentication protocols does Rapid Identity support (e.g., SAML, OIDC, LDAP)?

Answer: SAML, OIDC, LDAP.

Question 87: What is the current Zero Trust architecture or platform used (e.g., iboss)?

Are there specific policies to be maintained?

Answer: Iboss ZTNA is the current Zero Trust platform we are using. Policies are maintained by security admins.

Question 88: What systems or services are currently integrated into Arctic Wolf SOC?

Answer: Azure, Firewalls, network cores, iboss, servers and user endpoints.

Question 89: What kind of alerting and logging does the Arctic Wolf integration require (e.g., via Syslog, API)?

Answer: They use multiple methods of integration Syslog, API, and additional if needed..

Question 90: Are there existing RBAC models documented and aligned with job roles?

Answer: Yes.

Question 91: What real-time data or metrics are critical for you?

Answer: There is not enough information in this question to provide accurate information.

Question 92: Are there any preferred tools or platforms for analytics and dashboards?

Answer: We would prefer the analytics and dashboards to integrate with our SOC and also have its own section in the security platform.

Question 93: What log retention period is required for compliance purposes?

Answer: minimum 30 and optimal 60+.

Question 94: Are there specific compliance frameworks to adhere to (HIPAA, FERPA, CJIS)?

Answer: ISO, HIPAA, DERPA, CJIS, PCI-DSS and additional if needed.

Question 95: Will the reporting solution need to support custom audit reports or only predefined templates?

Answer: Ideally reporting should allow for both custom and predefined templates.

Question 96: What is the total count of EndPoints?

Answer: 45,000 windows and 98,000 chromebooks total. Below please find the numbers for Ohio:

Windows

Ohio: 200

Chromebook

Ohio: 950

Question 97: How many physical locations are in scope?

Answer: There is not enough information to answer your question.

Question 98: What is the total number of users?

Answer: Numbers are subject to change because enrollment/hiring is in progress.

81,353 Student total - 956 Ohio

12,319 Staff total - 120 Ohio

Question 99: What are the total Internet and WAN connections?

Answer: 2 egress points totaling 20GB at each datacenter location.

Question 100: What is currently implemented?

Answer: There is not enough information to answer your question.

Question 101: Is there any vendor or choice of Product already selected?

Answer: No. Selection will be made after evaluations have been completed.

Question 102: Must the offeror be registered to do business in the State for the bid or is getting registered before the execution of the contract sufficient?

Answer: The offeror must be registered to do business in the State for bid upon proposal submission.

Question 103: Is it permissible for Certificates of Insurance to be provided post award – prior to doing any work, and not as part of the RFP response.

Answer: As stated in the RFP, Certificate of Insurance with the specified coverages must be provided upon proposal submission.

Question 104: Under Contract Terms: It states “ The agreement(s) resulting from this RFP will begin on or about July 1, 2026, with services expected to be effective as of that date.” Please clarify. Is this contract to begin on that date or are you looking for the contract to begin sometime post award but with licensing and all services being provided to be up and running by July 1, 2026?

Answer: The agreement is contingent on the approval of the Cybersecurity Pilot E-Rate 471 application being approved. The expectation is to begin services on July 1, 2026.

Question 105: The RFP mentions the vendor is responsible to “ensure compliance with IDEA’s security policies and network standards.” Can you provide those policies and standards?

Answer: You can use the ISO 27001 for OH as a baseline.

Question 106: What is meant by 50 units of Load Balancer/WAF/DDos?

Answer: 1 unit would equal 1 url added in the load balancer or waf. So, for example, if you want to protect www.google.com that would utilize 1 unit of the 50 available units.

Question 107: Please provide Internet connectivity information by location and bandwidth?

Answer: 2 egress points totaling 20GB at each datacenter location.

Question 108: How are Chromebooks managed?

Answer: Google Admin Console.

Question 109: How do Chromebooks get their DNS today?

Answer: Using internal DNS servers.

Question 110: How many domains do you want to host?

Answer: 50.

Question 111: Are you able to do WAN forwarding on your firewall?

Answer: Yes, we can, but we have appliances that sit in front of the firewall on the edge.

Question 112: Do you need help in managing the DNS protection service?

Answer: No.

Question 113: Do you want DNS protection for Chromebooks off campus?

Answer: We are already doing that with iBoss

Question 114: Are you willing to tunnel Chromebook traffic back to campus?

Answer: We are already doing that with iBoss.

Question 115: How many employees are part of the IT team?

Answer: We have about 16 people.

Question 116: How many Windows, Mac, and Chromebook devices?

Answer: Windows 45,000, Chromebooks 98,000 total. Below please find the numbers for

Ohio:

Windows

Ohio: 200

Chromebook

Ohio: 950

Question 117: How many IPs do you want external penetration tested?

Answer: 512. This will be performed across all sites together.

Question 118: How many IPs do you want internal penetration tested?

Answer: 400 servers, 50 network devices, 200 endpoints. This will be performed across all sites.

Question 119: Which of the requirement services does IDEA plan on managing after deployment?

Answer: We plan to manage all deployed services.

Question 120: For Browser Isolation, how many concurrent browser isolation sessions does IDEA expect?

Answer: 500.

Question 121: Is IDEA seeking private IP visibility? If yes, a local gateway appliance can be utilized. How many locations do you desire this visibility for?

Answer: No, we are not looking for private IP visibility solution.

Question 122: Is IDEA looking for exact data matching as well?

Answer: There is not enough information to answer this question.

Question 123: Please provide a firm number of users, licenses, and number of url/domain sites to be managed.

Answer:

50 Sub Domains

Numbers are subject to change based on enrollment/hiring

81,353 Student total - 956 Ohio

12,319 Staff total - 120 Ohio

Question 124: IDEA specifies certain technologies such as Shield ID, Varonis, and Rapid Identity. Could IDEA provide additional criteria or expectations for what constitutes 'equivalent' products or services in these categories?

Answer: This is already defined in the RFP posting.

Question 125: Will documentation demonstrating equivalency be evaluated by technical staff during the review, and can vendors request pre-validation of alternative technologies before full proposal submission?

Answer: Pre-validation of alternative technologies before full proposal submission will not be allowed. All proposals will be evaluated by IDEA's designated evaluation committee during the designated evaluation period.

Question 126: Can you provide specific technical documentation or architecture diagrams for current integrations (e.g., with iboss, Rapid Identity, Sentinel One, Azure SSO) to better align our proposed integration approach?

Answer: These are all cloud-based solutions, the only integrations will be API and SSO integrations. These are common integrations that can be found in vendor documentation for each of the solutions.

Question 127: Are there any legacy systems or constraints within IDEA's environment that we should be aware of which could limit API-based integrations or SaaS deployment?

Answer: No, all security solutions in place have API integrations available.

Question 128: For the hybrid DLP solution, does IDEA have preferences or constraints on endpoint agents vs agentless monitoring across student/staff devices?

Answer: Prefer agentless.

Question 129: In the case of enterprise browser isolation, should the solution support student devices running unmanaged operating systems (e.g., BYOD with Chrome OS or iOS)?

Answer: Yes, it should support all OS types.

Question 130: Should pricing be structured on a per-year basis across the 3-year term, or is IDEA seeking blended multi-year discounts?

Answer: IDEA is looking for a 3-year term with annual payments.

Question 131: In Attachment K, for Identity Governance & Technologies, the quantity refers to an entire region. Will you provide additional insight into the count of users or personas that should be utilized here to consistently price the work?

Answer:

81,353 Student total - 956 Ohio

12,319 Staff total - 120 Ohio

Question 132: In Attachment K, for Identity Governance & Technologies, the quantity refers to an entire region. Should bidders assume the quantity of identities to be equal to the 92,500 Users in the Secure DNS type of service?

Answer: Yes, it is for all 92,500 users.

Question 133: Would IDEA be open to cost-splitting models that separate eligible FCC pilot program items from non-eligible features, for transparency in Attachment K?

Answer: Any non-eligible feature is out of scope and will not be evaluated. The price sheet automatically calculates eligible and ineligible costs toward the bottom of the sheet.

Question 134: Would IDEA provide more clarity on how they expect bidders to separate eligible FCC pilot program items from non-eligible features, in Attachment K?

Answer: Anything that is outside of the FCC pilot program list like a non-eligible feature is considered out of scope and will not be evaluated. The price sheet automatically calculates eligible and ineligible costs toward the bottom of the sheet.

Question 135: Are optional professional services such as optimization workshops or advanced analytics training considered ineligible and should be listed separately?

Answer: If you have options outside of our request, please provide that. Pricing for the items we are asking for must be provided utilizing IDEA's pricing attachments, but if you'd like to provide additional options, you may submit separate documents for that.

Question 136: IDEA emphasizes FERPA, HIPAA, CIPA, and ISO 27001 compliance. Would the district value enhanced reporting and audit trail capabilities that go beyond baseline compliance (e.g., real-time compliance dashboards, AI-aided risk scoring)?

Answer: Yes.

Question 137: How will value-added features not explicitly listed in the RFP (e.g., AI-based threat detection or data enrichment) be considered in the scoring rubric under "Technical & Functional Suitability"?

Answer: Please refer to the section titled "*Explanation of Evaluation Criteria*" within the RFP for a more detailed description of the evaluation criteria.

Question 138: How recent must engagements be to be considered 'relevant'?

Answer: Please refer to the instructions/description within the references attachment of the RFP for additional information.

Question 139: Are there blackout windows for implementation due to academic calendars or standardized testing periods?

Answer: Yes.

Question 140: Can you clarify expected milestones between award (August 2025) and the go-live target (July 1, 2026)?

Answer: Timelines and milestones are subject to installation of product and solution.

Question 141: For solutions requiring training (e.g., DLP, SASE, Identity Governance), what is the preferred method (on-site vs. virtual), and is a train-the-trainer model acceptable?

Answer: Virtual and train-the-trainer model.

Question 142: Should ongoing support costs be bundled with the license or broken out separately in Attachment K?

Answer: Should be bundled with the licensing.

Question 143: The RFP specifies disqualification for generic/encyclopedic proposals. Would inclusion of product datasheets or case studies in appendices be permitted?

Answer: Datasheets and case studies are permitted.

Question 144: How many live IP addresses are in scope? Please estimate to the nearest hundred. If unable to estimate to the nearest hundred, please estimate to the nearest thousand.

Answer: 512.

Question 145: List IP ranges that are in scope (e.g. 1.2.3.4/24) and any domains that are in scope. If any of the in-scope IPs are dynamically assigned, please do not include the IPs, and instead provide the fully qualified domain names (FQDNs) to ensure that testing is only performed on customer-owned systems.

Answer: Specific IP and Subdomains will be provided upon award.

Question 146: Which cloud platforms (AWS, Azure, GCP, Digital Ocean, etc.) does the organization have known assets in?

Answer: We have cloud platforms in AWS, Azure, GCP, Digital Ocean.

Question 147: Do you want retesting of findings to be included in the scope of this engagement?

Answer: Yes.

Question 148: Do you have any hard deadlines on the project completion or report delivery date?

Answer: July 1 2026.

Question 149: What are the primary attacker objective goals you would like the manufacturer to pursue for this exercise?

- Determine whether a threat actor can access sensitive data
- Determine whether a threat actor can access other environment such as other Active Directory domains or cloud environments
- Determine whether a threat actor could deploy ransomware
- Determine whether a threat actor can access artificial intelligence related systems, data, or environments
- Other (will require follow up scoping call)

Answer: All the bullet points listed above are what we are looking for in the exercise.

Question 150: What is your preferred initial access method?

- VDI Access (recommended)

- VPN Access to company virtual machine or workstation (recommended)
- Witting click
- Physical laptop shipped to Red Team
- Other (will require scooping call)

Answer: VPN Access.

Question 151: Would you like the manufacturer to start from more than one initial access user or system so they have multiple perspectives on the network? If yes, provide details.

Answer: 1 standard user.

Question 152: Would you like vendors to identify exploitable attack paths in more than one environment? If yes, please provide details.

Answer: Yes. For further explanation, please refer to the Scope of Work within the RFP.

Question 153: Does your environment use Active Directory for SSO? If not, what SSO Is used in your environment?

Answer: Azure and Rapid Identity.

Question 154: If you use Active Directory, how many AD domains and forests are in-scope?

Answer: 1 forest 1 domain.

Question 155: Are most endpoints and servers domain-joined Window systems? If not, please provide a rough breakdown of operating system in use.

Answer: Mixed environment, hybrid and azure only.

400 Servers Domain Joined/Windows

13,000 Domain Joined Windows

30,000 Azure only Windows

Question 156: Approximately how many endpoints and servers are in scope for this exercise?

Answer: 400 servers 50 network devices 200 endpoints.

Question 157: Do you want retesting of findings to be included in the scope of this engagement?

Answer: Yes.

Question 158: Will this engagement be performed under privilege, i.e. on behalf of outside legal counsel?

Answer: Legal consent will be provided prior to engagement.

Question 159: How many websites need protected via WAF?

Answer: Up to 50.

Question 160: How many uplinks from district to internet?

Answer: 2 10GB per location. 2 locations.

Question 161: How many resources are on prem vs cloud?

Answer: 60/40 on prem vs in cloud.

Question 162: For implementation service for all, to what extent are deployment services needed? Is a pilot or small subset allowed?

Answer: Pilot is allowed. Extent of services will be turnkey solution, deployment, design, implementation, and training.

End of Addendum