ROWLAND UNIFIED SCHOOL DISTRICT
1830 S. NOGALES STREET
ROWLAND HEIGHTS, CA 91748

ADDENDUM 4

CYBERSECURITY PILOT PROGRAM – Muti Layered Threat Protection

RATE FUNDING YR (3 Years)

RFQ/RFP # 2025/26: (E1)

JUNE 23, 2025

TO ALL PROSPECTIVE BIDDERS:

Note: *The following Addendum shall become part of the contract documents, and the bidder shall provide for all work as required by this Addendum. Acknowledge receipt of the Addendum on the Bid Proposal Form.*

Specifications/Clarifications:

RFI 1
Reference: Exhibit A, Page 11
Is the district seeking a unified platform with integrated management for DNS, endpoint, and email security, or is separate tooling with interoperability via APIs acceptable/preferred?
ANSWER: The District does not require a unified platform. Interoperable solutions with API integration are acceptable.

RFI 2
Reference: Exhibit A, Page 11
Does the solution need to support site-based policy segmentation (e.g., different threat policies per school or user group), or will policies be standardized district-wide?
ANSWER: Yes, the solution should support site-based and user/group-based policy enforcement.

RFI 3
Reference: Exhibit A, Page 12
What is the expected concurrency level of active endpoints for threat detection and telemetry logging (e.g., all 2,000 endpoints active daily vs. only staff vs. all devices enrolled)?
ANSWER: Vendors should assume all 2,000 endpoints will be concurrently active and monitored daily.

RFI 4
Reference: Exhibit A, Page 12
Does the district require protection for unmanaged endpoints (e.g., BYOD), guest devices, or only district-owned assets? If so, how many beyond the 2,000 prescribed endpoints?
ANSWER: The District intends to protect only district-owned assets.

RFI 5

Reference: Exhibit A, Page 12
Please confirm whether endpoint protection is required for ChromeOS devices or if DNS-layer and email protection alone are sufficient for those endpoints.
ANSWER: ChromeOS devices are expected to be covered by DNS-layer and email protection only. Endpoint protection is not required for these. It is preferred but not required.

RFI 6
Reference: Exhibit A, Page 12
Are administrative interfaces expected to support SSO integration (e.g., with Google Workspace, Azure AD), and should support for RBAC (Role-Based Access Control) extend to integration with existing identity systems?
ANSWER: Yes, SSO integration and RBAC are expected and should align with current identity systems such as Google Workspace Active Directory, or Azure AD.

RFI 7
Reference: Exhibit A, Page 12
Will email protection need to support outbound email filtering, DLP, and encryption? Or is inbound threat protection only in scope?
ANSWER: Inbound threat protection is in scope. Outbound email filtering, DLP, and encryption are not requested on the RFP, specified on RFP Page 13.

RFI 8
Reference: Exhibit A, Page 12
Should vendors include licensing and/or configuration support for DMARC monitoring/reporting and sender identity protection?
ANSWER: YES

RFI 9
Reference: Exhibit A, Page 12
Does the DNS-layer solution need to enforce custom content filtering policies (e.g., CIPA-compliant categories) in addition to threat blocking?
ANSWER: Yes, DNS-layer solutions must also enforce CIPA-compliant content filtering.

RFI 10
Reference: Exhibit A, Page 13
Should vendors itemize individual SKUs for DNS/email/endpoint subcomponents (e.g., sandboxing, threat emulation), or can features be quoted in a single bundled SKU?
ANSWER: Yes, all items should have individual SKUs for each DNS, Email, and Endpoint.

RFI 11
Reference: Exhibit A, Page 13
If proposing physical or virtual appliances, does the district require high availability (HA) for on-premises components, and if so, what redundancy standard (active/passive or active/active)?
ANSWER: No appliances are required. Cloud-delivered services are preferred. HA for on-prem solutions is not in scope.

RFI 12
Reference: Exhibit A, Page 13 Does the district require support for mobile device protection (iOS/Android) under endpoint security or DNS clients?

ANSWER: iOS/Android endpoint security protection and DNS client applications are not required.

RFI 13
Reference: Section 2.9.1, Page 5 &amp; Exhibit A, Page 12
Will vendors be responsible for developing DNS/email/endpoint security policies in collaboration with the district, or should vendors deploy pre-defined best practices only?
ANSWER: Vendors are expected to collaborate with District staff on policy development, not rely solely on pre-defined templates.

RFI 14
Reference: Section 2.9.1, Page 5
Should endpoint agent deployment and validation on both Intune and Mosyle platforms be performed by the vendor, or is it sufficient to provide documentation and guidance? Is global deployment of agents required by the vendor, or will district IT push agents via MDM tools?
ANSWER: Vendors must support deployment through Intune and Mosyle. District IT will handle agent distribution vendors may provide configuration and documentation.

RFI 15
Reference: Section 2.9.1, Page 5
Should the scope of work include DNS-over-HTTPS (DoH) or DNS-over-TLS (DoT) configurations and validation for client devices?
ANSWER: DoH/DoT is not specifically mentioned. Vendors may propose these configurations as added value.

RFI 16
Reference: Exhibit A, Page 12
Does the professional services scope include configuring integrations between proposed solutions and the district's existing SIEM or analytics platform? If so, please provide log ingestion methods supported by the district (Syslog, REST API, etc.).
ANSWER: Vendors are expected to collaborate with District staff on integration with SIEM/XDR tools. Support for API- based and log ingestion methods should be provided.

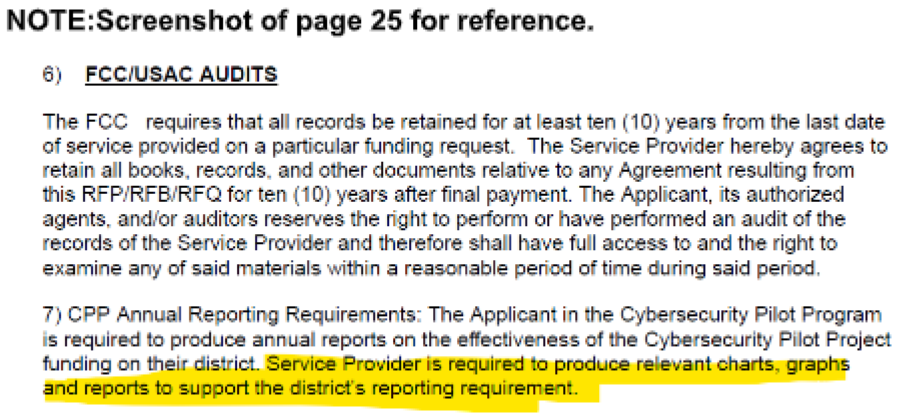
RFI 17
Reference: Section 2.9.1, Page 5
Please confirm if the scope includes creating correlation rules or detection signatures for cross-vector threat analysis (e.g., endpoint detection tied to DNS or email threat metadata).
ANSWER: Correlation across email, DNS, and endpoint threats is preferred but not mandatory

RFI 18
Reference: Section 2.8, Page 5
Will vendor staff be responsible for any changes to MX records, SPF, DKIM, or DMARC records in Google Workspace DNS zones, or will district IT perform those changes if advised?
ANSWER: DNS changes (e.g., MX, SPF, DKIM, DMARC) will be made by District IT with vendor guidance.

RFI 19
Reference: Section 2.8, Page 5
Does the district expect hands-on administrator training (remote or onsite) for console operations and alert handling for each product area (DNS, email, endpoint)?

ANSWER:Yes, training is expected for administrative users.

RFI 20
Reference: Exhibit F, Page 25
Is the vendor responsible for exporting and submitting raw or summarized analytics for the FCC's annual Cybersecurity Pilot Program reporting, or will this be handled by the district?
ANSWER: Vendors must support the District in meeting FCC annual reporting needs by supplying analytics and reporting artifacts. NOTE:Screenshot of page 25 for reference.



NOTE:Screenshot of page 25 for reference.

6) **FCC/USAC AUDITS**

The FCC requires that all records be retained for at least ten (10) years from the last date of service provided on a particular funding request. The Service Provider hereby agrees to retain all books, records, and other documents relative to any Agreement resulting from this RFP/RFB/RFQ for ten (10) years after final payment. The Applicant, its authorized agents, and/or auditors reserves the right to perform or have performed an audit of the records of the Service Provider and therefore shall have full access to and the right to examine any of said materials within a reasonable period of time during said period.

7) CPP Annual Reporting Requirements: The Applicant in the Cybersecurity Pilot Program is required to produce annual reports on the effectiveness of the Cybersecurity Pilot Project funding on their district. Service Provider is required to produce relevant charts, graphs and reports to support the district's reporting requirement.

RFI 21
Reference: Exhibit A, Page 12
Please confirm whether the vendor is expected to configure integration with mobile device management (MDM) solutions beyond deployment scripting e.g., policy enforcement via Intune or Mosyle APIs.
ANSWER: Vendors are not expected to directly configure or enforce MDM policies via Intune or Mosyle APIs. However, they must provide guidance and technical support to assist District IT Staff with policy configuration and ensure that deployment packaging is compatible with both platforms.

RFI 22
Reference: Section 2.6.5, Page 5
Does the district require a formal knowledge transfer session, if so what is the expectation for knowledge transfer?
ANSWER Yes, knowledge transfer is implied under support requirements. Expectations include walkthroughs and documentation.

RFI 23
Reference: Exhibit B, Page 14
Should user-based licensing be assumed for all security components, or is device-based licensing expected for endpoint and DNS services?
ANSWER: User-based licensing is assumed for all components unless otherwise specified.

RFI 24
Reference: Exhibit B, Page 14
Are roaming clients for DNS protection required for all users or only for a subset (e.g., staff laptops)? Please provide expected counts per use case.

ANSWER: NOTE: Yes, this is part of the requirements of the DNS protection as outlined in the RFP page 14. This should be part of the 2,000 user count.

RFI 25
Reference: Exhibit B, Page 14
For endpoint protection, should vendors assume protection for both staff and student devices, or only for faculty/staff?
ANSWER: The requested 2,000 endpoint licenses are to cover staff and faculty accounts.

RFI 26
Reference: Exhibit B, Page 14
For cloud email protection, is the 2,000 user count inclusive of all district staff, or should vendors account for system accounts or shared mailboxes separately?
ANSWER: The requested 2,000 endpoint licenses are to cover staff and faculty accounts.

RFI 27

Reference: Exhibit A, Page 13
Should vendors include any physical hardware or only cloud-delivered services and endpoint agents?
ANSWER: Only cloud-delivered services and agents should be quoted. No hardware is required.

RFI 28
Reference: Exhibit F, Page 25
If proposing three-year subscriptions, should all services be coterminous or will staggered start dates be accepted per product group?
ANSWER: Services must be coterminous across the three-year contract.

RFI 29
Reference: Exhibit A, Page 11
Are the district's Active Directory and Google Workspace identity systems federated, or are they siloed for authentication?
ANSWER: Identity systems are not federated. They operate separately.

RFI 30
Reference: Exhibit A, Page 12
Please confirm whether vendors must provide and configure high-availability pairs for DNS-forwarding connectors or endpoint update proxies.
ANSWER: The District currently uses Cisco Umbrella with Virtual Appliances (VAs) for internal DNS resolution. The existing environment includes high availability (HA) configurations for DNS-forwarding components. While the RFP does not specifically require vendors to provide or configure new HA pairs, proposed solutions must be compatible with HA configurations and support integration into the existing setup.

Responses to RFI's will be provided via addenda posted on the district's website at www.rowlandschools.org

The vendor must check the district's website for any addenda before submitting their proposal.

Rosana McLeod

Interim Assistant Superintendent