



## **RESPONSES TO QUESTIONS — RFP #05-2025**

### **Email Security Gateway for Google Workspace Integration**

The following page(s) are Pueblo City-County Library (PCCLD) responses to questions submitted by the April 18, 2025 deadline.

## **Email Security Gateway for Google Workspace Integration**

**QUESTION:** *Re: Threat Detection Capabilities* – Is there a preferred or minimum required benchmark for phishing, BEC, and malware detection accuracy (e.g., third-party test standards)?

**PCCLD RESPONSE:** Greater than or equal to 95% detection rate with a false-positive ratio less than 0.1-0.3%

---

**QUESTION:** *Re: Integration Timelines* – What is the expected or required deployment and testing timeline following the contract award?

**PCCLD RESPONSE:** 60 days after the PO is issued

---

**QUESTION:** *Re: Legacy Systems* – Are there any existing email security tools or configurations that need to be migrated or decommissioned as part of this deployment?

**PCCLD RESPONSE:** No

---

**QUESTION:** *Re: Pricing by Site* – Since the scope includes multiple branch locations, do you require individual licensing models or will it be a single Google tenant-wide?

**PCCLD RESPONSE:** Single Google tenant

---

**QUESTION:** *Re: Multi-Year Pricing* – Should proposals include optional multi-year pricing (e.g., 3-year, 5-year) for budgeting and E-rate forecasting?

**PCCLD RESPONSE:** It would be beneficial to provide optional longer terms

---

**QUESTION:** *Re: DLP & Encryption Requirements* – Abnormal Security's platform specializes in advanced threat protection, phishing/BEC detection, and behavioral AI-based email security. As our solution does not include native Data Loss Prevention (DLP) or encryption services, would you be open to a joint solution approach in which a supplemental vendor or existing platform (Google) is used to fulfill DLP/encryption requirements, while Abnormal covers the advanced threat detection and response components?

**PCCLD RESPONSE:** Vendors can provide joint-vendor solutions as long as the billing, support and service contracts remain with one entity (i.e. the vendor awarded). ESG/Email Encryption service are required as part of the email solution.

---

**QUESTION:** *Re: Google Licensing* – Can you please confirm the specific Google Workspace licensing tier(s) currently in use across the district? Knowing whether the district uses Google Workspace Business, Enterprise Standard, or Enterprise Plus will help us assess what native capabilities (e.g., DLP, encryption, secure transport) that may already be available to support the overall solution.

**PCCLD RESPONSE:** We currently use Google workspace for non-profits

---

**QUESTION:** How many total mailboxes are you looking to cover?

**PCCLD RESPONSE:** 467

---

**QUESTION:** What is the District currently using for email security?

**PCCLD RESPONSE:** Google’s native email security

---

**QUESTION:** Item F of Section 9, “Proposal Requirements” states: “For each location bids/proposals are required to have separate costs by line item and must list the manufacturer’s make and model/SKU number, quantity, unit cost and extended cost.” Does this mean that the District plans to manage each branch location as a separate entity? If so, can the District provide a breakdown of user and mailbox counts at each branch location?

**PCCLD RESPONSE:** The district plans to administer all email accounts by one single tenant. E-rate requires hardware costs to be broken down individually per location. Licensing cost per user is sufficient.