RFP FY25-CS01: NDR Cybersecurity Solution

July 1, 2025

Request for Clarification – Questions and Answers

The following responses address all vendor questions submitted on or before **12:00 PM** (Pacific Time) on **June 27, 2025**, in accordance with the RFP timeline and guidelines.

##	Vendor Clarification Question	GDPS Answers
01	We're seeking some clarification regarding the proposal submission requirements on page 11 of the RFP and Attachment E on page 21. The list of required submission elements appears to be missing a section for directly responding to the scope of work on pages 3 through 5 and Attachment F on pages 22 and 23. May we add a section to the proposal that directly responds to these requirements?	Attachment F, "Breakdown of NDR Solution Capability Expectations" is not listed on Attachment, E the Checklist of Required Elements. Attachment F is provided as a glossary of terms supporting the scope of work outlined on pages 3 through 5 and is not a required submission element. Vendors are encouraged to include a dedicated section in their proposal that directly responds to the **Scope of Work** outlined on **pages 3–5** and the technical capability expectations emphasized in Attachment F (pages 22–23). This content should be included in addition to the required elements listed in **Attachment E** and should provide clear evidence of how your proposed solution meets or exceeds the stated requirements.
02	Does Green Dot prefer a cloud-managed NDR solution or a hybrid deployment (cloud + on-prem sensors)?	Green Dot Public Schools is seeking a **hybrid cloud deployment model** that includes, at minimum: • An **on-premise Data Analyzer appliance**, and • An **on-premise Network Packet Collector appliance**, These components should be **centrally managed via a vendor-hosted cloud platform** (often referred to as a SaaS-based or hybrid-cloud NDR architecture).

		The cloud-based management layer must support centralized visibility, policy enforcement, alerting, and integration with third-party systems, while the on-premise components must provide localized traffic inspection and data collection.
03	Which of the following tools are currently deployed: CrowdStrike Falcon, Cisco switches/routers, Palo Alto firewalls, Stellar Cyber, Cortex XSOAR, Microsoft 365, or Azure AD/Entra ID?	This information is already provided in the RFP under the **Scope of Work** sections on **pages 2 and 3**. Vendors are encouraged to review those sections for details regarding the currently adopted tools and platforms.
04	How many data centers does Green Dot Public Schools operate?	**Number of Data Centers:** Green Dot Public Schools operates a single, centralized data center.
05	Are these data centers also in scope of including Network Detection and Response (NDR) capabilities?	Yes. The selected Network Detection and Response (NDR) solution will be deployed within this central data center via a connection at the core switch. Please refer to the Answers about (NDR) Scope.
06	Are these data centers directly managed by Green Dot Public Schools or outsourced?	**Data center Management:** This data center is fully owned and directly managed by Green Dot Public Schools; there is no third-party outsourcing of core infrastructure or operations.
07	Is the network architecture centralized or distributed (e.g., centralized data center vs decentralized campus segments)?	**Centralized Network Architecture:** • Green Dot's network architecture is **centralized**, with all 18 campuses/sites connecting back to the core data center in a hub-and-spoke architecture via 2-Gbps Uplinks for network services, traffic aggregation and 10Gbps+ connection to the internet.

08	How many sites/locations does Green Dot Public Schools have? How big is the internet connection at each of these locations? (in Gigabits per second)	Green Dot Public Schools operates **18 campus locations** including a District Office/Home Office, all connected to a centralized data center using a **hub-and-spoke network architecture** with dedicated WAN links of at least 2 Gbps per site. • All internet-bound traffic is routed from the WAN uplinks through a **core switch at the centralized data center**, which maintains a 10 Gbps sustained fiber uplink through a regional ISP.
09	How many locations total?	Green Dot Public Schools operates **a total of 19 locations**, including 18 campus sites and one centralized data center.
10	Of those locations, how many would Green Dot Public Schools like to have Network Detection and Response (NDR) capabilities?	**NDR Scope:** • Yes. The selected NDR solution will be deployed within this central data center via a connection at the core switch, providing network-wide visibility into traffic between the data center and our 18 school locations. The data center and all 18 campus locations are thus fully within scope for Network Detection and Response coverage. • All **18 Campus locations** are within scope for NDR visibility. While full-scale deployment at each site is not required, NDR visibility should extend across the entire distributed network environment via centralized deployment with mirrored/SPAN traffic from campus uplinks or regional taps as needed.
11	What is the size of the core networks at each respective location?	Due to security considerations, Green Dot Public Schools cannot publicly disclose a high-level network topology, bandwidth capacities, or the specific size and configuration of core networks at each site in this RFP.

	How many ingress/egress points are there between Green Dot Public Schools and the Internet itself? How many ingress/egress points are there between sites and the district office/home office? Is there a mock or high level network topology with the associated bandwidth capacities available to share to help visualize where Green Dot Public Schools envisions the positioning of the Network Detection and response solution?	However, regarding our centralized network architecture and NDR deployment expectations, please refer to the responses provided for **Questions 07**, **08**, **09**, and **10** above.
12	Could one share the preferred networking connectivity into the appliance? 10Gig Ethernet? SFP? Fiber?	Green Dot Public Schools prefers **10 Gigabit Ethernet connectivity** via **SFP+ interfaces** using LC-LC 10Gb 50/125 OM3 Duplex Multimode Fiber Optic Cabling (PVC jacketed). Please ensure proposed NDR appliances support **10Gb SFP+ optical modules** and are compatible with our existing OM3 multimode fiber infrastructure.
13	What is the current student enrollment across all Green Dot campuses?	As stated on **page 1 of the RFP**, Green Dot Public Schools serves approximately **10,000 students** across 18 public middle and high schools.
14	Do these devices include IoT/OT/non-user devices, or are they limited to student/staff endpoints and servers?	For a breakdown of the 18,000 in-scope devices, including approximate counts by type and management scope. Please refer to the responses to **Questions 15**, **16**, **17,** and **18**.

		Those responses include estimated counts and categories such as Chromebooks, staff workstations, servers, network infrastructure, and IoT/OT systems.
15	**Endpoint Device Count and Distribution** Reference: Page 3, "Support for 18,000+ devices and 12,000+ users" Please provide a breakdown of the 18,000 devices by type (e.g., Windows, macOS, IoT, BYOD), location, and whether they are centrally managed. Are all users assigned a 1:1 device?	All managed **Windows and macOS devices** are assigned to Green Dot staff and are **centrally managed** through **Microsoft 365, Azure Entra ID, and Intune**. All **Chromebooks** are assigned to students, and both Chromebook devices and student user accounts are managed centrally through **Google Workspace for Education**. Green Dot Public Schools does **not operate a full 1:1 model** across all user groups, though the majority of students are issued individual Chromebooks for educational use. For a breakdown of the 18,000 in-scope devices, including approximate counts by type and management scope, please refer to the **Responses** for **Questions #16** and **#17** below.
16	Of the 18,000 network devices, could you please identify the different device types that will require monitoring with a breakdown by device type, including approximate numbers for servers, workstations (Windows, macOS, Linux), Chromebooks, IoT devices, network infrastructure (routers, switches, firewalls), and any other significant device categories. Understanding this distribution will enable us to better estimate traffic analysis and tailor our solution accordingly.	All devices listed below are within scope for network traffic monitoring and behavioral visibility via the NDR platform. Device Breakdown (Approx. 18,000 total) each with a unique IP Address: • **Student Devices (Chromebooks):** 10,000 – Wi-Fi connected • **Staff Devices (Windows/macOS):** 1,800 – Mixed wired and wireless • **Servers (Windows/Linux):** 200 – Hosted in the central data center • **Network Infrastructure & IoT/OT** (~6,000 total): ○ Wireless Access Points (WAPs)

		○ LAN/WAN Switches and Routers, and UPS's ○ Enterprise Firewalls ○ IP Security Cameras ○ Building Access Control Systems ○ Environmental/Climate Control Systems
17	What is your total concurrent IP count? (how many active IPs/ devices? we typically see this as 3x the employee count)	The scope for the Network Detection and Response (NDR) solution includes coverage for approximately 18,000 managed devices. However, due to the presence of non-managed and personal mobile devices connecting to our Wi-Fi networks (e.g., BYOD, guest devices), the total number of devices and IP addresses observed on the network at any given time can reach up to 30,000. Vendors should ensure their solution can scale accordingly to provide effective visibility, behavioral analytics, and threat detection across both managed and unmanaged endpoints.
18	The RFP references 18,000 devices. Could you confirm how many unique IP addresses are associated with those devices?	Of the 18,000 in-scope network devices, there are approximately 18,000 unique IP addresses in use across the Green Dot Public Schools network. **Note:** Mobile devices (e.g., smartphones, tablets) are considered unmanaged and transient and are therefore **not in scope** for Network Detection and Response monitoring.

19	Are the 18,000 devices spread across multiple VLANs, campuses, or network segments	Each of the 18 campus locations utilizes multiple VLANs and 2 Gbps site-to-core interconnectivity, with segmentation between student, staff, infrastructure, and server networks.
20	Do you use Entra ID? If using O365, what is your license count for O365? (we typically see this match the employee count).	**Microsoft 365 License Count and Entra ID Usage** Yes, Green Dot Public Schools utilizes Microsoft 365 (formerly Office 365) and Azure Entra ID (formerly Azure Active Directory) for staff identity and productivity services. • Microsoft 365 is used exclusively by Green Dot staff (not students). • The current license count is 1,200, with approximately 1,130 active users.
21	Do you only use M365/Entra ID, or do you also have VM or serverless workloads in Azure? Do you use Azure for cloud and need coverage there? If yes, what is your current Azure footprint.	**Azure Virtual Server Workloads and Azure Cloud Coverage** Green Dot Public Schools primarily hosts our virtual server workloads on-premise at our centralized data center. However, we do currently maintain a limited Azure footprint, which includes: • A small number of Windows Server 2022 instances hosted on Microsoft Azure • **Azure Entra ID** (formerly Azure Active Directory) for identity and access management of Staff accounts only • **Microsoft 365** cloud services (Exchange Online, OneDrive, SharePoint, Teams) Given this footprint, coverage for Azure-based workloads is relevant, though limited in scope compared to our on-premise infrastructure. Vendors should outline their ability to provide visibility and protection for both environments, with appropriate scaling.

22	Do you have AWS and need coverage there?	Green Dot Public Schools does not utilize AWS at this time and therefore does not require coverage for Amazon Web Services environments.
23	Could you clarify whether you are looking to mitigate vulnerabilities primarily through endpoint protection, network switch/router, or firewall integration?	The primary goal of the NDR solution is to provide comprehensive **visibility into vulnerabilities and abnormal behavior across the network** that would otherwise go undetected without an NDR platform. While we are not relying on the NDR to directly perform mitigation, the insight it provides will inform the Green Dot Technology Team's remediation and risk treatment strategies. These actions may involve changes at the endpoint, network infrastructure (e.g., switches/routers), or firewall level, depending on the nature of the identified risk.
24	**Data Ingest Patterns and Rate and Packet Capture Expectations** *Reference: Page 4 & 6, "Lossless packet capture at 10Gbps."* • What is the assumed average daily ingest rate (Gbps) for storage planning? • Will SPAN/mirror ports be provisioned for this purpose?	Vendors should assume a sustained ingest rate of approximately **8 Gbps** during normal operations. During our recent evaluation with on-premise NDR appliances located at Green Dot's centralized data center and connected to our core switch and capturing mirrored/SPAN traffic from campus uplinks. We observed an average sustained ingest rate of approximately 8 Gbps during regular school hours (Monday through Friday) across Green Dot's network. As a public K–12 school system, network traffic patterns vary significantly based on the academic calendar. Ingest rates are significantly lower during evenings, weekends, holidays, and scheduled breaks, typical of public schools in Southern California. Vendors should account for these patterns when proposing storage, retention strategies, and throughput capacity for both packet and metadata collection.

		Proposals should be designed to support peak weekday activity, while optimizing lower traffic periods to ensure scalability and cost efficiency.
25	**Packet Retention Requirements** For the 90-day retention, when you refer to 'searchable events, logs, and network metadata,' are you envisioning all of this data residing in a single, unified platform for direct querying, or are you comfortable with a primary NDR platform holding the comprehensive network metadata, while other platforms (e.g., SIEM, EDR) handle their respective logs, all of which are integrated for correlated investigations?	Vendors should assume a sustained ingest rate of approximately **8 Gbps** during normal operations. Green Dot Public Schools expects the primary NDR platform to retain comprehensive, searchable network metadata for at least 90 days, including enriched flow data, detections, and protocol-level insights. We do not require full packet capture to be stored for 90 days, due to storage and scalability constraints associated with high-throughput networks. Instead, we prioritize solutions that offer: • **High-fidelity network metadata retention** • **Indexed, searchable detections and events within the NDR platform** • **The ability to integrate and correlate with SIEM, EDR, and other log management platforms** • **Support for investigative workflows and cross-platform threat context enrichment** Vendors are encouraged to describe how their solution achieves efficient data retention, cross-tool integration, and rapid searchability without relying on long-term full packet storage.
26	To clarify the retention requirements, could you please specify the desired retention period for each of the categories listed per the Network	Green Dot Public Schools expects the following retention periods, balancing investigative needs with practical storage considerations on a high-throughput network:

	Packet Collector component, as they may have different storage implications: **Full Packet Data** (PCAP): The raw, complete network traffic. **Records/Flow Data**: Summarized network conversation details. **Metadata**: Detailed information about the packets and flows, but not the full packet content.	• **Full Packet Data (PCAP):** Retained for a **maximum of 7 to 14 days** to support deep-dive forensic analysis in the event of a security incident. Longer retention of full packets is not feasible due to storage and cost constraints. • **Records/Flow Data:** Retained for a **minimum of 90 days** to enable historical network traffic analysis, trend identification, and baseline behavior modeling. • **Metadata:** Retained for **at least 90 days** within the primary NDR platform. This includes detailed contextual information that supports rapid threat hunting, detection validation, and correlation with other security data sources. Vendors should detail their data retention architecture and capabilities, including compression, tiered storage options, and integration with external log management or SIEM platforms to optimize scalability.
27	**Packet Retention Requirements** *Reference: Page 5, "Technical Requirements"* • Please confirm whether 90 days of retention refers to full PCAP or just metadata/logs. • What is the assumed average daily ingest rate (Gbps) for storage planning?	As previously stated in the responses to Questions **25** and **26** and for full context, please also refer to the answers previously provided under Question **24** regarding ingest patterns and rates based on K–12 traffic behavior. Green Dot Public Schools does not require full packet capture (PCAP) to be retained for 90 days due to the storage and scalability constraints of a high-throughput network (~8 Gbps sustained during peak school hours). **Data Retention expectations are as follows:** • **Full Packet Data (PCAP):** Retained for a maximum of **7 to 14 days** to support forensic investigation during incidents. • **Flow/Records Data:** Retained for a minimum of **90 days** to enable trend and traffic pattern analysis.

		• **Metadata:** Retained for **at least 90 days** within the primary NDR platform, including enriched detections, session data, and protocol insights. Vendors should assume an average sustained ingest rate of approximately 8 Gbps and are encouraged to detail how their proposed solution achieves the following: a) Efficient data retention, b) Indexed, rapid searchability, c) Seamless integration with SIEM, EDR, and log management platforms.
28	**Packet Collector Storage Format** *Reference: Page 6, "Packet Collector must support 90 days of searchable events and logs…"* • Is there a preferred data retention architecture (e.g., internal disk vs. external NAS)? Are existing storage policies in place for FERPA compliance?	Green Dot Public Schools does not prescribe a specific storage architecture (e.g., internal disk vs. external NAS) for the retention of searchable events, logs, and metadata. Vendors are expected to propose a storage solution that is scalable, cost-effective, and capable of meeting the 90-day searchable retention requirement described in the RFP. As a California public school system, Green Dot is subject to FERPA and other U.S. student data privacy laws. Any telemetry or metadata collected by the NDR solution must be encrypted in transit and at rest.
29	**MITRE ATT&CK Alignment and Mapping** *Reference: Page 22, "MITRE ATT&CK Mapping…"* • Does GDPS require visual dashboards with tactic/technique mapping, or is detection tagging/matching to MITRE sufficient? Should	Green Dot Public Schools strongly prefers visual dashboards with MITRE ATT&CK tactic and technique mapping that support exportable reports for compliance and performance tracking. As a participant in the FCC Schools and Libraries Cybersecurity Pilot Program, the District requires vendors to submit monthly metrics and an annual report to Green

	mapping be exportable for compliance reports?	Dot, so that Green Dot can adhere to the Cybersecurity Pilot Program reporting requirement to USAC. These reports must demonstrate that the adopted cybersecurity solution is being actively used and effectively integrated into security operations. While detection tagging/matching to MITRE is useful, vendors are encouraged to provide proposals that include: • Visual MITRE ATT&CK mapping dashboards • Exportable reports showing threat coverage, tactic/technique detection, and investigation workflows • Evidence that the NDR platform supports metrics generation aligned to program reporting requirements Solutions that reduce manual reporting overhead and provide actionable evidence of threat detection and mitigation will be viewed more favorably in the evaluation process.
30	Can you confirm if by 'incident' you are referring to confirmed security event(s) that requires a response, or if you are referring to all security detections, including potential threats or anomalies flagged by the system?	At Green Dot Public Schools, the term **"incident"** specifically refers to a validated security event that has been reviewed and confirmed by our IT Security Team as an **Information Security or Cybersecurity Incident**. These incidents trigger our formal incident response process, which may include playbook execution, containment actions, escalation procedures, and post-incident review. By contrast, routine security detections, alerts, anomalies, or potential threats, especially those automatically blocked or quarantined by endpoint or network security tools, are not considered **incidents** unless further investigation confirms risk or compromise.

31	Regarding the **Technical Certifications requirement**, are these certifications expected to be held by the vendor's personnel assigned to the project, and/or does Green Dot want the ability to be certified through training offered by the vendor?	Yes, **technical certifications** are expected to be held by the vendor's personnel assigned to the project. These individuals should possess current certifications and demonstrated proficiency with the proposed NDR solution, as well as relevant networking and security technologies such as Cisco, Microsoft, Palo Alto Networks, and other industry-standard platforms. **Note:** In accordance with the **FCC Cybersecurity Pilot Program guidelines**, Green Dot Public Schools cannot require vendors to provide certification training as part of the contract or evaluation criteria. However, vendors are encouraged to outline any optional training opportunities or certification programs that may be available for Green Dot staff outside the scope of this RFP.
32	**Stellar Cyber SIEM/SOAR Integration** Please confirm if native integration with Stellar Cyber is mandatory, or if integration via syslog/API with alternative SIEM platforms is acceptable.	Please refer to the **Scope of Work** on page 3 of the RFP. As stated, the proposed NDR solution must support integration with **Stellar Cyber SIEM/SOAR**, along with other platforms via API or webhook for automated response. It is the responsibility of each vendor to demonstrate how their proposed solution meets or exceeds these integration requirements. Solutions that natively integrate with Stellar Cyber may be advantageous; however, platforms offering equivalent or superior integration capabilities—via API, syslog, or other industry-standard methods—will also be considered, provided they fully support the use cases and interoperability described in the RFP.
33	**CrowdStrike Integration Expectations** *Reference: Page 4, "Automated Response"*	Green Dot Public Schools has fully adopted CrowdStrike Enterprise, including Endpoint Detection & Response (EDR) and Identity Protection integrated with Azure Entra ID (formerly Azure AD).

	Should the integration support bidirectional enforcement (e.g., containment), or is ingestion and telemetry correlation sufficient?	Vendors are expected to describe the capabilities of their proposed NDR solution in terms of integration with CrowdStrike, including: • Telemetry ingestion and correlation (e.g., detections, threat context enrichment) • Automated response capabilities such as containment, isolation, or policy enforcement • APIs, connectors, or native integration methods supported Green Dot encourages vendors to highlight bidirectional integration features where available, but will evaluate based on the overall effectiveness, flexibility, and interoperability of the proposed solution within our existing cybersecurity ecosystem.
34	**Professional Services Scope and Roles** *Reference: Page 5-6 & 17, "Installation, configuration, training..."* • Please clarify if the implementation scope includes only the NDR system deployment, or if additional services such as policy tuning, SOP creation, or incident runbook development are expected?	As clearly stated on **Page 1** of the RFP, the proposer is expected to supply, implement, and support a comprehensive NDR solution, including software, hardware, professional services, and training. Green Dot Public Schools requires vendors to provide a detailed **statement of work (SOW)** for professional services that ensures: • Successful installation and configuration of the proposed solution • Validation of full functionality as described in the vendor's proposal • Initial policy tuning, alert configuration, and dashboard/report customization aligned with Green Dot's environment • Basic training for administrative users to support operational readiness

		Vendors may not exclude the necessary services required to operationalize the platform. Any assumption that Green Dot will perform advanced configuration or tuning without vendor-led onboarding must be clearly stated in the proposal. Creation of SOPs or incident response playbooks is not required; however, proposals may include such value-added offerings if they enhance onboarding or long-term operational success.
35	**Integration Resource Requirements** *Reference: Page 4-5, "Professional services to complete integration"* • Can GDPS clarify which parties are responsible for providing API documentation, endpoint access, and credentials for integrations with systems such as CrowdStrike, Stellar Cyber, and Palo Alto?	Green Dot Public Schools will provide necessary access and credentials to enable integrations between the proposed NDR Solution and platforms such as CrowdStrike Falcon, Stellar Cyber SIEM/SOAR, Palo Alto NGFW, and other adopted security tools only to the selected vendor during the implementation phase. Green Dot's technology team includes experienced network and security engineers who are highly proficient in integrating these platforms and managing secure access. Integration of the NDR solution into our environment will be a collaborative effort between the vendor's professional services team and Green Dot's internal subject matter experts. **Vendors are expected to demonstrate** that their professional services team has prior experience and technical expertise in integrating NDR platforms with widely adopted cybersecurity and infrastructure solutions. Proposals should include personnel qualifications and real-world examples that demonstrate these capabilities.
36	Regarding SMS/text alerts, do you have a preferred or existing SMS gateway or service provider (e.g., Twilio, an internal system, or a specific mobile carrier's email-to-SMS gateway)	Please refer to the response provided about **Alerting and Notification Configuration** for **Question #37** below.

	that you would like the NDR solution to integrate with for sending these notifications?	
37	**Alerting and Notification Configuration** Reference: Page 4, "Alerts via email and SMS/text" • Can the District confirm whether they have an existing SMS gateway or prefer vendors to use a 3rd-party SMS API? Are there designated security operations staff to receive alerts?	Green Dot Public Schools does not currently utilize a specific SMS gateway or messaging service for cybersecurity notifications. However, if your proposed solution includes the ability to send SMS alerts or real-time messages, please specify which native or third-party services or messaging platforms (e.g., AWS SNS, Twilio, Slack, Microsoft Teams, or others) are supported or integrated. Please also indicate any additional setup or configuration required to enable notifications to mobile devices or messaging channels used by IT Security staff. Additionally, clarify whether your solution supports mobile device registration or configuration to ensure reliable delivery of real-time SMS alerts.
38	**Invoicing Procedures** *Reference: Page 15, "SPI invoicing via FCC Form 474…"* • Are vendors required to submit SPI invoicing directly, or may the vendor invoice GDPS in full and let the district file BEAR (Form 472)?	As outlined on page 15 of the RFP, **Service Provider Invoice (SPI) billing via FCC Form 474 is required** for this project. Vendors **must invoice USAC directly** for the CPP-eligible portion of the cost using **Form 474** and bill **only the applicant share and any ineligible portion** to Green Dot Public Schools (GDPS). GDPS **will not utilize BEAR (Form 472)** reimbursement for this procurement.
39	Is the funding mechanism funded directly from FCC/USAC (where vendor bills FCC/USAC for the entire transaction?)	**Funding Structure & Invoicing Procedures – FCC Cybersecurity Pilot Program** Green Dot Public Schools (GDPS) is participating in the FCC Cybersecurity Pilot Program (CPP), and requires the use of the Service Provider Invoice (SPI) billing method.

	Or do we bill Green Dot Public School for the full amount? Or is it a hybrid funding model?	Green Dot intends to only use the allocated Cybersecurity funding rather than additional district funding and may alter final quantities or items to conform with the established budget authorization and prefers that the vendor submit the applicant share portion to Green Dot, and the CPP portion of the invoice to USAC via SPI. **Vendors must:** • Bill USAC directly for all eligible goods and services using FCC Form 474 (SPI) GDPS will not use the Billed Entity Applicant Reimbursement (BEAR) method (Form 472). All vendor proposals must reflect this funding structure and comply with the invoicing requirements outlined in the RFP and the FCC's CPP rules.
40	**Who is your ERATE Consultant?**	All communication and questions should continue to be directed through the formal RFP process as outlined. CSM Consulting is our E-rate and Cybersecurity Consultant. Contacting anyone outside of the established contact persons on the RFP to discuss anything relating to the Cybersecurity Pilot Program competitive bidding process is grounds for disqualification.
41	**Cost Allocation Expectations** *Reference: Page 13, "Clearly designate CPP-eligible vs. ineligible items"* • Please confirm how GDPS prefers vendors to allocate shared licensing (e.g., bundle that includes SOAR + training + integrations) across eligible vs. ineligible line items in the pricing form (Attachment B).	**Cost Allocation Expectations – Shared Licensing** Vendors are required to review the Cybersecurity Pilot Eligible Services List (https://www.fcc.gov/cybersecurity-pilot/cybersecurity-pilot-eligible-services-list) prior to submitting bids. Green Dot is required to evaluate the bids based on the eligible components of the bid, meaning that that all ineligible components or costs must be separated out. (For Example: Advanced firewall features are eligible under the Cybersecurity Pilot Program, but are ineligible under E-rate.

		Basic firewall features are eligible under E-rate but ineligible under CPP. A bid response for CPP including firewall components should cost allocate out the basic firewall features and only include the advanced firewall features.) Green Dot Public Schools (GDPS) requires that vendors clearly designate CPP-eligible versus ineligible costs in Attachment B, even for bundled or shared licensing models. For bundles that include both eligible (e.g., SOAR functionality) and ineligible components (e.g., professional training, third-party integrations not covered by the FCC), vendors should reasonably allocate costs across line items based on: • **Documented internal pricing models**, • **Industry-standard valuation**, or • **A consistent methodology used across other public sector procurements.** Where exact allocation is not possible, an estimated breakdown with a brief justification is acceptable. This transparency supports FCC and USAC review processes and ensures compliance with the Cybersecurity Pilot Program's cost allocation requirements.
42	**On-Prem Appliance Installation Timeline** *Reference: Page 5, "Implementation"* • Is the 90-day deployment timeline calculated from contract award, project kickoff, or hardware delivery?	**On-Prem Appliance Installation Timeline** The 90-day deployment timeline referenced on page 5 begins at project kickoff, which is contingent upon the successful delivery and racking of all required on-prem hardware. To support timely implementation, vendors must ensure equipment is delivered and deployment resources are ready in advance of the project kickoff.

		Any anticipated delays in hardware shipment or resource availability that may impact the project timeline must be communicated proactively to the GDPS project team to allow for coordination and mitigation planning.
43	**Managed Detection and Response (MDR/SOC)** *Reference: Page 23, "Optional MDR/SOC services available..."* • Should the vendor include optional pricing or references for Managed SOC services, or will GDPS manage incident response entirely in-house?	Vendors are welcome to include optional pricing and references for Managed Detection and Response (MDR) or SOC services, provided these offerings fall within the total **RFP budget of $420,000**. Green Dot Public Schools currently co-manages incident detection and response through its internal IT security team and a third-party 24x7 SOC. However, proposals offering value-added MDR/SOC capabilities, such as extended threat monitoring, escalation support, or full 24/7 coverage, may be considered, provided they complement the proposed NDR solution and align with the FCC Cybersecurity Pilot Program budgetary and operational guidelines. All optional services must be clearly labeled as optional, with transparent pricing and defined scope, to ensure an effective and consistent evaluation process.
44	**Deployment Resource Clarification** *Reference: Page 5, "Installation of two on-premises appliances"* • Please confirm whether GDPS expects the vendor to provide onsite resources for physical appliance racking and cabling, or whether district IT staff will handle physical installation with vendor support limited to remote configuration.	Green Dot IT staff will handle the physical installation, including racking, cabling, and power connections for the on-premises appliances. The vendor is expected to provide remote support for configuration and deployment validation, but onsite services are not required for this RFP.

45	Are there any data residency, privacy, or encryption requirements that would affect cloud telemetry or metadata retention?	**Yes**. Please refer to the response provided about **Data Residency, Sovereignty Requirements** for Question **46** below.
46	**Data Residency, Sovereignty Requirements** *Reference: Page 4-5, "Hosted in secure environment."* *Does GDPS require that all telemetry, logs, and detections be stored within the United States?* *Are there restrictions on using global CDNs or non-U.S.-based backup/replication services?*	**Yes**. As a California public school system, Green Dot Public Schools is subject to federal and state regulations governing student and staff data privacy, including SOPIPA, FERPA, and the California Education Code. Accordingly, any telemetry or metadata collected, processed, or stored by the NDR solution must be encrypted in transit and at rest, and must not be used for profiling, targeted advertising, or any non-operational analytics. Green Dot prefers U.S. based data residency for any telemetry retained in the cloud. Vendors must ensure compliance with all applicable laws regarding the handling of student data and must be prepared to provide written assurances or enter into a Data Protection Agreements (DPAs) upon request. *Please also refer to the California State Administrative Manual (SAM §§ 5310 and 5320) for additional encryption and security requirements*.
47	For this evaluation criteria, are you referring to direct experience with Green Dot as the manufacturer/vendor, or does experience through a VAR/reseller also apply?	Experience working with Green Dot Public Schools may include direct engagement by the manufacturer/vendor or through an authorized value-added reseller (VAR). Both types of experience will be considered during the evaluation process, provided the relationship and scope of work are clearly described in the proposal.
48	Aside from K-12, will California references from Counties, Cities, State Agencies be accepted? In the RFP it mentions two different requirements. It says 5 references in proposal	For clarification, **a minimum of three (3) references** are required as outlined in **Attachment E**; however, vendors are encouraged to submit **up to five (5)**

	requirements and attachment E, it references - 3 minimum.	**references** as stated in the main proposal requirements to strengthen their proposal. While preference is given to references from **K–12 school districts** (in California or other states). Green Dot Public Schools will also accept references from other public sector entities, such as counties, cities, or state agencies, provided the work performed is comparable in scope and complexity to the services requested in this RFP.
49	**Required Visibility into Encrypted Traffic** *Reference: Page 4, "Including encrypted traffic with or without decryption..."* • Does GDPS expect full packet decryption via TLS inspection (e.g., MITM), or is metadata-based detection (e.g., JA3 fingerprinting, flow behavior analysis) sufficient?	Green Dot Public Schools does not require full decryption of encrypted traffic via TLS interception or MITM techniques. However, vendors must clearly describe what visibility their proposed NDR solution provides into encrypted traffic, including: • Metadata-level inspection capabilities (e.g., JA3/JA3S fingerprinting, flow behavior analytics, certificate inspection) • Whether selective payload decryption is supported for approved use cases • How encrypted traffic is handled during threat detection, investigation, and incident response—particularly when traffic originates from trusted cloud providers (e.g., AWS, Google Cloud, Azure) Solutions that provide enhanced visibility or context into encrypted sessions, with or without decryption are strongly preferred, especially when they contribute to threat validation, root cause analysis, or post-incident review. Vendors must disclose what their solution **can and cannot do** when analyzing encrypted traffic and describe how these capabilities contribute to actionable threat detection.

50	**Optional Integration with Email Security Solutions** *Reference: Page 22, "Optional integration with Mimecast..."* • Does GDPS currently use Mimecast, or was this included as an example? Are vendors required to demonstrate email-NDR correlation?	Yes, Green Dot Public Schools (GDPS) currently uses Mimecast as our Email Security Gateway. The reference to Mimecast on page 22 is not an example but reflects our current production environment. While integration with Mimecast is not a mandatory requirement, vendors are strongly encouraged to highlight any email-NDR correlation capabilities, including API/webhook integrations with Mimecast. Solutions that provide enhanced visibility into email-borne threats and lateral movement detection through correlated telemetry will be viewed favorably during evaluation.
51	**Proof of NDR Deployments with Cisco & Other Tools** What constitutes sufficient "proof" of Network Detection & Response (NDR) deployments and integration with networks and cybersecurity applications such as Cisco, CrowdStrike, Microsoft 365/Azure Entra ID Enterprise Directories, Palo Alto Firewalls, etc.? • Is a white paper or deployment guide sufficient? • Do they require named customer references demonstrating integrations? • NDR Provider has provided integration documentation in the past and wants to confirm expectations.	Vendors should provide **supporting documentation** demonstrating the proposed NDR solution's integration and interoperability with network switching architecture and cybersecurity applications such as Cisco, CrowdStrike, Microsoft 365, Azure Entra ID Enterprise Directories, and Palo Alto Network Firewalls, as applicable. **Acceptable forms of proof include:** • Vendor-issued certifications of compatibility or validated integrations • Solution briefs or technical documentation • References to published API integrations or connector frameworks • Customer case studies or deployment examples • Third-party validations or listings in trusted marketplaces (e.g., Cisco Networking App Marketplace, CrowdStrike Store, Palo Alto Networks NextWave Partner Program, Microsoft Security Partner catalog, etc.)

		The documentation should clearly show how the NDR solution supports data ingestion, alert enrichment, contextual visibility, or automated response workflows with the listed technologies.
52	**Reference Requirements** Do the customer references need to come solely from the NDR Provider/Manufacturer, or can they be joint references with Bidder?	References from K–12 school districts that have deployed the proposed NDR solution may be provided by either the NDR provider/manufacturer, the bidder/reseller, or jointly by both parties.
53	**Insurance Requirements** Please confirm that the $5,000,000 for Auto Liability is required. Are you willing to accept $1,000,000 for Automobile Liability? Can we propose a lower amount of liability insurance than what is stated in the RFP?	Please refer to the insurance requirements outlined in the published RFP. All vendors are expected to meet the stated minimum insurance coverage levels. The established insurance requirements apply only if the vendor will be responsible for on-site deployment.
54	**Attachment A: Cybersecurity Supplemental Terms and Conditions** • Section 2e – products and services must be delivered before billing." Please provided clarification on what is considered "delivered." Does the activation	Under Section 2e, "delivered" refers to the successful provisioning and activation of the product or service in a functional state, such that the recipient (Green Dot Public Schools) is able to access, deploy, and begin using the solution as intended. For software-based products or SaaS platforms, activation and access credentials enabling full use of the licensed features would constitute delivery. For hardware or on-premises solutions, physical delivery combined with successful installation and/or configuration for operational readiness would be required.

	of software constitute "delivery" for billing purposes?	Billing must **not occur prior to delivery**, as defined above, and must comply with the FCC's Cybersecurity Pilot Program rules regarding pre-disbursement verification.
55	**Attachment A Cybersecurity Supplemental Terms and Conditions** • Section 5 FCC/USAC Audits The FCC Requires all records be retained for 10 years and gives the Client or its agents the right to audit. Would you agree to a 5 year retention period rather than 10 years?	All records related to this procurement must be retained for a minimum of 10 years from the last date of service to remain in compliance with federal audit and reporting requirements. Therefore, Green Dot Public Schools cannot accept a reduced retention period of 5 years. Vendors awarded contracts under this program must agree to the full 10-year record retention and audit access requirements as outlined by the FCC and USAC.
56	**Attachment A Cybersecurity Supplemental Terms and Conditions** Are you open to contract negotiations?	No. As a public education system participating in **the FCC Cybersecurity Pilot Program**, all proposals must be final and complete as submitted. Green Dot Public Schools will not engage in post-submission contract negotiations. Vendors are expected to submit their best and most responsive offer in accordance with the terms outlined in the RFP.
57	**PoC Validation & Timeline** *Reference: Page 9, "30-day PoC for detection metrics validation"* • Is the Proof of Concept expected to be run in production, pre-staging, or simulated lab	Due to the tight timeline imposed by the FCC Cybersecurity Pilot Program and procurement milestones, GDPS will not conduct PoCs during the current proposal evaluation period. Green Dot will move forward from the vendor contract to production. Accordingly, vendors are not expected to perform a new PoC for this RFP. However, proposers should clearly document prior PoC results (if applicable), including

	conditions? What is the evaluation timeline and criteria for success?	detection rates, response latency, and false positive rates in comparable environments. Success criteria for proposed NDR Solution should include: • % value for threat detection • % value for false positive rate • Number of seconds or minutes for automated response • Seamless integrations with GDPS platforms (e.g., CrowdStrike, Palo Alto, Stellar Cyber SIEM/SOAR)
58	**Current Logging and SIEM Infrastructure** *Reference: Page 4, "Integration with SIEM/XDR… via API or webhook"* • Please confirm whether GDPS currently uses Stellar Cyber SOAR or SIEM, and whether logs are ingested via syslog, API, or agent. What is the expected log ingestion volume (EPS/log size) for integration testing?	As stated in the Scope of Work on pages 3 and 4 of the RFP, Green Dot Public Schools currently utilizes Stellar Cyber for both SIEM and SOAR capabilities. The expected events per second (EPS) or log size is not relevant to the evaluation or selection criteria for this RFP, as vendors are not being asked to size, configure, or host a log ingestion platform. Vendors should instead focus on describing how their proposed NDR solution integrates with Stellar Cyber, including supported integration methods (e.g., API, syslog, webhook) and any value-added capabilities such as alert forwarding, correlation enrichment, or automated response triggers.
59	In a perfect world with the perfect implementation where cost is not a factor, would Green Dot Public Schools prefer a single appliance to help monitor east/west and north/south traffic? Or multiple appliances	While we appreciate the question, Green Dot Public Schools must operate within the defined scope, requirements, and budgetary constraints of the FCC Cybersecurity Pilot Program and this RFP. The required architecture includes:

	distributed throughout the network at multiple levels?	• **Two on-premises appliances**, deployed at our centralized data center: 1. A **Data Packet Collector** 2. A **Data Analyzer** (NDR Brain or Processing Engine) For additional clarification, please refer to the response provided for Question #**61** below.
60	Are you interested in a virtual brain to reduce cost? If so, do you have VMware at one of your locations? Is your current traffic under 10Gbps? Are you interested in a virtual sensor to reduce cost as well? If so, do all the locations where you'd put a sensor have either VMware, KVM, or HyperV? Do all locations have under 5Gbps?	**Virtual sensors, virtualized appliances, and distributed deployments** are **not supported or considered** under this RFP. Proposals must align with the centralized appliance model described in the Scope of Work and Technical Requirements (pages 3–6). To clarify, Green Dot Public Schools operates a centralized hub-and-spoke network architecture and does not maintain VMware, KVM, or HyperV infrastructure at individual school sites. The current network design does not require nor support the placement of sensors or virtual appliances at remote locations. For additional clarification, please refer to the responses provided for Question #**61** below.
61	**Definition of "On-Premises" Appliance** *Reference: Page 5, "Installation of two on-premises appliances..."* • Can the District clarify if both appliances (analytics engine and packet collector) must be deployed at a central data center, or if	As stated in the Scope of Work and Technical Requirements (pages 3 through 6), Green Dot requires the deployment of two on-premises appliances: 1. A **Data Packet Collector**, and 2. A **Data Analyzer (NDR "Brain" or processing engine)** These appliances must be installed **at Green Dot's centralized data center**, which provides core network interconnectivity to all 18 campuses via 2 Gbps

	distributed deployment (e.g., at school sites) is required?	connections. **Distributed deployments across school sites are not required or supported in this RFP.** Vendors are expected to propose an NDR solution that supports centralized packet collection and analytics, while being capable of analyzing east-west and north-south traffic across the entire network fabric from the data center. Solutions that rely solely on lightweight edge sensors or cannot deliver integrated packet analysis and enriched detection from a centralized architecture will not meet the stated requirements. Vendors should focus proposals on solutions that meet the centralized packet analysis and detection capabilities outlined on pages 3–6 of the RFP.
62	**NDR Platform Interoperability Requirements** *Reference: Page 3-4, "The NDR solution must integrate with..."* • Can the District confirm whether integration is required or preferred for each listed vendor platform (e.g., Broadcom, Cisco Meraki, CrowdStrike Falcon, Palo Alto NGFW, etc.)? Is telemetry ingestion and correlation needed, or is alert/event forwarding sufficient?	As stated in the Scope of Work on pages 3 and 4, the NDR solution must demonstrate **interoperability with Green Dot's existing cybersecurity ecosystem**, including but not limited to: • CrowdStrike Falcon • Cisco Meraki • Palo Alto NGFW • Microsoft 365 / Azure Entra ID • Stellar Cyber SIEM/SOAR • Mimecast (where supported) Vendors must clearly describe how their solution integrates with these platforms, including:

		○ The type of integration: Native, API-based, or dependent on third-party middleware ○ The type of data exchanged (telemetry, events, threat intelligence, contextual enrichment) ○ How the integration supports real-time correlation, root cause analysis, and threat hunting workflows, not just alert forwarding Green Dot Public Schools expects proposed solutions to go beyond basic alert sharing and instead enable deep threat correlation and investigation capabilities through meaningful integration. It is the vendor's responsibility to explain how their solution enhances visibility, detection accuracy, and incident response effectiveness through these integrations.
63	**Threat Response Use Cases** *Reference: Page 4, "Automated containment (e.g., blocking IPs, isolating devices)"* • Please clarify what containment capabilities are expected. Should automated actions be performed by the NDR itself (e.g., via built-in SOAR), or is triggering external systems (e.g., Palo Alto firewalls, CrowdStrike EDR) sufficient?	Vendors must clearly indicate whether and how their proposed NDR solution supports automated containment capabilities in response to identified threats. Green Dot Public Schools does not mandate that containment actions be performed solely by the NDR platform itself. Automated response may be executed either directly within the NDR solution (e.g., via built-in SOAR/playbooks) or via integrations with external platforms such as: • CrowdStrike Falcon (host containment/quarantine) • Palo Alto Networks NGFW (dynamic block lists, IP containment) • Stellar Cyber SOAR • Other API/webhook-capable systems in our security stack

		What is essential is that vendors demonstrate how their solution enables or facilitates automated response, such as: ○ Blocking malicious IPs or domains ○ Isolating compromised endpoints ○ Triggering SOAR workflows ○ Enriching threat context for rapid decision-making Green Dot expects vendors to provide specific details on these capabilities and describe how their solution contributes to real-time threat containment, response coordination, and reduction of incident dwell time.
64	**Security and Background Checks** *Reference: Page 7, "DOJ clearance and TB certification"* • For vendor personnel not physically accessing GDPS campuses, are remote-only workers still subject to DOJ fingerprinting and TB certification?	Vendor personnel who do not physically access GDPS campuses (i.e., remote-only staff) are not required to undergo DOJ fingerprinting or provide TB certification. However, any vendor personnel who will be onsite at GDPS facilities or interacting directly with staff or students must comply with all applicable security clearance requirements, including DOJ Live Scan fingerprinting and up-to-date TB certification, in accordance with California Education Code and GDPS policy. Vendors are responsible for ensuring that only appropriately cleared personnel are assigned to on-site work.

Important Note: All vendors must fully comply with the Cybersecurity Supplemental Terms and Conditions as published in the RFP.