

REQUEST FOR PROPOSALS

IT Equipment, Hardware & Managed Services

Issuing Agency	El Dorado County Fire Protection District
RFP Number	RFP-EDCFD-2026-IT-01
Issue Date	Tuesday, October 13, 2026
Pre-Proposal Conference	Thursday, October 22, 2026, 10:00 AM (Pacific Time); virtual; optional
Written Questions Due	Wednesday, October 28, 2026, 5:00 PM (Pacific Time)
Proposal Deadline	Friday, November 13, 2026, 5:00 PM (Pacific Time)
Anticipated Award	January 21, 2027 (Board of Directors action); contract start on or about February 1, 2027
Contract Period	Three (3) Years with Two (2) One-Year Options
Delivery Address	501 Main St, Diamond Springs, California 95619
Procurement Contact	Brad Gates, Fire Chief
Procurement Email	procurement@eldofire.com (single point of contact for all questions and submissions)

This RFP contains two (2) parts. Specifications define minimum performance and security standards for business-grade equipment and managed IT services. Proposers must meet or exceed all stated specifications. The environment baseline provided in Appendix A represents currently known inventory; the selected provider will establish a Configuration Management Database (CMDB) as an onboarding deliverable. The CMDB is and shall remain a District asset: the District shall have continuous access to the CMDB and the ability to obtain a complete export of its data in a usable format at any time, and the CMDB shall not be dependent upon any particular managed-service provider.

SECTION 1: INTRODUCTION & BACKGROUND

El Dorado County Fire Protection District (ECFPD or "the District") is a California special district providing fire suppression, emergency medical services (including advanced life support ambulance transport), and related public safety services across El Dorado County, operating from administrative offices at 501 Main St, Diamond Springs, CA 95619. In 2026 the District annexed the former Diamond Springs-El Dorado Fire Protection District (DSEDFD), whose legacy IT environment is included in the scope of this RFP.

The District is issuing this RFP to procure IT equipment and hardware (Part I) and ongoing managed IT services, including cloud migration and a walled enterprise AI environment (Part II). The District's reference implementation for the AI environment is Claude (Anthropic); equivalent solutions will be considered (Section 2.13). Proposers may respond to Part I, Part II, or both. The District may award Part I and Part II separately, to the same or different proposers.

SECTION 2: SCOPE OF WORK

PART I: IT Equipment & Hardware

All equipment must be new, current-generation, and covered by manufacturer warranty of no less than three (3) years. All equipment must meet or exceed the specifications below. Proposers shall propose business-grade equipment from established commercial manufacturers (e.g., HP, Lenovo, Dell, or equivalent). Consumer or gaming-grade products will not be accepted.

2.1 Desktop Computers (Quantity: 25)

- Form factor: Small Form Factor (SFF) / Micro PC or equivalent business-grade compact desktop
- Processor: Intel Core i7 (13th Gen or newer) with Intel vPro, or AMD Ryzen 7 PRO equivalent; current generation
- RAM: 16 GB DDR5 minimum
- Storage: 1 TB NVMe SSD minimum
- OS: Windows 11 Pro, 64-bit, licensed
- Color/Finish: Black or neutral professional finish
- Warranty: 3-year minimum, parts and labor

2.2 Laptops (Quantity: 18)

- Form factor: 14" business-grade laptop
- Display: 14" Full HD Plus (1920x1200), 60 Hz minimum, anti-glare. Touchscreen is not required; a touchscreen configuration may be quoted as an option
- Processor: Intel Core i7 with Intel vPro, or AMD Ryzen 7 PRO equivalent; current generation
- RAM: 16 GB minimum, upgradeable to 32 GB (non-soldered memory or an open memory slot). Proposers shall also quote a 32 GB configuration as a separately priced option
- Storage: 1 TB NVMe SSD minimum
- Security: Smart Card Reader, TPM 2.0
- Keyboard: English (US); backlit preferred
- Finish: Professional/business-grade chassis; no consumer or gaming aesthetic
- OS: Windows 11 Pro, 64-bit, licensed
- Warranty: 3-year minimum, parts and labor

2.3 Docking Stations (Quantity: 20)

- Form factor: Universal USB-C / Thunderbolt 4 business-grade docking station
- Dual monitor output (HDMI + DisplayPort)
- USB-A x4 minimum, USB-C x2, Gigabit Ethernet
- Power delivery: 90W minimum to connected laptop
- 3.5mm audio combo jack

2.4 Monitors (Quantity: 70)

The District requires 70 mid-grade monitors suitable for administrative and operational workstations. No specific reference model is designated; proposers are encouraged to propose best-value options that meet or exceed the specifications below.

- Screen size: 27–32 inches (mid-grade commercial or business-grade line preferred)
- Resolution: 1920x1080 (FHD) minimum; 2560x1440 (QHD) preferred

- Panel type: IPS or VA; anti-glare coating required
- Ports: HDMI x1, DisplayPort x1 minimum
- Ergonomic stand: height-adjustable with tilt and swivel preferred
- Warranty: 3 years including panel

2.5 Keyboards & Mouse Sets (Quantity: 35, Open Bid)

- Full-size USB or wireless keyboard (2.4 GHz or Bluetooth)
- Optical mouse, minimum 1600 DPI, ambidextrous
- Wireless sets must use unified receiver or Bluetooth
- English (US) layout; backlit version quoted separately as an option

2.6 Camera & Audio Packages (Quantity: 10, Open Bid)

- Webcam: 1080p minimum (4K preferred), auto-focus, privacy shutter, Teams/Zoom/Meet compatible
- Audio: USB speakerphone with 360° omnidirectional mic OR noise-canceling USB/Bluetooth headset
- Echo cancellation and noise suppression required
- Cables and mounting hardware included

2.7 Migration Labor

- Proposer shall migrate all current system data, user profiles, printers, and software onto new equipment
- Reference scope: 43 units (25 desktops and 18 laptops) at a flat per-unit rate
- Includes configuration of profiles, mapped drives, installed applications, and printer connections
- Work to be performed on-site at the District facilities where equipment is deployed, including the administrative offices at 501 Main St, Diamond Springs, CA 95619 and the District's fire stations (locations provided in Confidential Appendix A-1)
- Proposer to coordinate scheduling with the District IT lead to minimize operational disruption. Work at fire stations shall be scheduled so as not to interfere with emergency response operations

PART II: Managed IT Services

The District seeks a qualified Managed Service Provider (MSP/MSSP) to deliver comprehensive, ongoing IT management, cybersecurity, cloud migration, and AI integration services. Proposers must describe their managed service delivery model in detail. Proposed service frameworks must meet or exceed the requirements described in Sections 2.8–2.18.

Part II Pricing Basis: Definition of Managed Unit

To allow proposals to be compared on an equal basis, monthly per-unit pricing in Exhibit B shall use the following definitions and quantities:

- **Managed Workstation:** each desktop, laptop, or administrative workstation under management. **Pricing basis: 55 units** (ECFPD 46; DSEDFD 9)
- **Managed Server:** each physical server, virtual machine, or backup server/appliance under management. **Pricing basis: 12 units** (ECFPD 7; DSEDFD 5)
- Firewalls, switches, wireless access points, NAS devices, UPS units, printers, and other infrastructure described in Section 2.18 are included in the monthly service and shall not be billed per unit unless the proposer expressly identifies an additional charge in Exhibit B

- Pricing basis quantities are estimates derived from Appendix A. Monthly billing will be based on the device count validated in the CMDB (Section 2.8). Replacement devices shall not be billed in addition to the devices they replace
- Proposers may offer an alternative per-user pricing model as a supplement, but must complete Exhibit B on the per-device basis above for evaluation purposes

2.8 IT Security Onboarding & Initial Assessment (One-Time)

- Cybersecurity assessment performed by an independent third-party firm that is not affiliated with the proposer, identified in the proposal as a subcontractor and subject to District approval, to identify environment deficiencies. The proposer shall remediate deficiencies identified within its scope
- Deliverables: CVE Discovery and Remediation
- Privileged Account Review
- PII and PHI Scan across all District systems
- Roles and Responsibilities documentation
- Communications and Workflow mapping
- Initial Incident Response Plan
- Cyber Awareness Training (all staff)
- Acceptable Use Policy (AUP) development, for District review and adoption
- District-owned CMDB established and delivered to the District within 60 days of go-live, documenting all hardware, software, services, licensing, accounts, and configuration items within the vendor's scope of management
- CMDB shall be maintained as a living document throughout the contract term and transferred to the District or successor vendor upon contract termination
- CMDB ownership and access: the CMDB is and shall remain a District asset. The District shall have continuous access to the CMDB throughout the contract term and may obtain a complete export of all CMDB data at any time, at no additional charge, in a usable, non-proprietary, machine-readable format (e.g., CSV, XLSX, or JSON). The CMDB shall not be dependent upon any particular managed-service provider or proprietary platform; proposers shall identify the proposed CMDB platform and describe how the District's access and export rights will be met

2.9 Core Managed IT Services (Monthly Recurring)

- Remote monitoring and management (RMM) of all District endpoints
- Help desk support (Tier 1–3), Monday–Friday 7 AM–6 PM PT; 24/7 emergency on-call. Minimum service level standards: Critical Outage (system down, life-safety impact), 15-minute response; High Priority (significant impairment), 1-hour response; Medium Priority (partial impairment), 4-hour response; Low Priority (minor issues, requests), 1 business day response. Proposer SLA must meet or exceed these minimums
- Patch management: OS, firmware, and application updates on a monthly cycle, with emergency patching for critical vulnerabilities
- Asset inventory management and CMDB maintenance
- Basic cloud administration (M365 or equivalent)
- Quarterly technology review meetings with District leadership
- Expansion pricing: proposers shall provide unit pricing for contract expansion, including additional managed workstations and servers (per device/month), additional users (per user/month, if applicable), additional stations or facilities, and additional cloud resource tiers. Expansion pricing shall be firm for the base contract period

2.10 Managed Security Services (MSSP) (Monthly Recurring)

- Protection against ransomware, phishing, nation-state actors, and dark web threats
- EDR/MDR (Endpoint Detection & Response / Managed Detection & Response)
- SIEM deployment and 24/7 security event monitoring
- Dark web monitoring for District credentials and data
- Incident response retainer: vendor response within 2 hours of a declared security incident
- Phishing simulation and security awareness training, minimum twice per year
- Compliance documentation support: HIPAA (EMS operations); CJIS Security Policy, only where District systems store, process, or access Criminal Justice Information (CJI)

2.11 Cyber Liability Support Services (Monthly Recurring)

- Ongoing compliance documentation and cyber liability support. Required cybersecurity controls: multifactor authentication (MFA) enforced on all accounts; email security filtering (anti-phishing, anti-spam, sandboxing); DNS filtering; vulnerability scanning (minimum monthly); annual penetration testing performed by a qualified tester independent of the proposer's operations staff (may be subcontracted), with a written report delivered to the District; backup validation testing (minimum quarterly)
- CVE remediation tracking and insurer reporting
- Policy maintenance (AUP, IRP, data handling), for District review and adoption

2.12 Server Migration to Cloud-Based Infrastructure (One-Time Project)

- Full assessment and documentation of existing on-premises servers and applications
- Written migration plan within 45 days of contract award (timeline, risk assessment, rollback procedures)
- Target platform: Microsoft Azure Government or AWS GovCloud; alternates require written justification
- Migrate email to M365 Government Community Cloud (GCC) or equivalent
- Migrate file storage to cloud platform with versioning and access controls
- Geo-redundant backup: 30-day minimum retention, daily snapshots
- Maximum planned downtime per migration event: 4 hours, scheduled off-peak
- No permanent loss of District data. Recovery Time Objective (RTO): systems restored within 4 hours for critical services, 8 hours for non-critical. Recovery Point Objective (RPO): maximum 1 hour data loss for critical systems, 24 hours for non-critical. Annual disaster recovery testing required with written test report delivered to the District. Proposer shall maintain and provide a documented Disaster Recovery Plan within 60 days of contract award
- Decommission on-premises servers upon successful validation, including secure data sanitization of retired storage media
- All services must comply with the HIPAA Security Rule (45 CFR Part 164, Subpart C); the FBI CJIS Security Policy where CJI is stored or processed; and controls consistent with NIST SP 800-53 Rev. 5 (moderate baseline) or an equivalent framework identified by the proposer. All District data shall be stored and processed within the United States

2.13 Enterprise AI Integration: Walled Instance (One-Time Setup + Ongoing Licensing)

- Deploy a private enterprise AI environment accessible only via District intranet/VPN, with contractual guarantees prohibiting District data from being used for model training or disclosed to any party other than the subprocessors identified in the proposal and approved by the District

- Reference implementation: Claude (Anthropic) enterprise deployment. Equivalent enterprise AI solutions that meet every requirement of this section will be considered on an equal basis; a proposer offering an equivalent shall demonstrate how it meets each requirement
- Deployment through the model provider's enterprise API or through an enterprise cloud platform (e.g., Azure Government or AWS GovCloud) under enterprise data-protection terms; consumer-grade AI services shall not be used
- Proposers shall identify the proposed hosting architecture and security boundary for the AI environment, including: (a) data flows for prompts, responses, uploaded documents, and logs; (b) the locations where District data will be processed and stored; (c) retention and deletion periods for prompts, responses, and logs, at both the vendor and model-provider level; and (d) all subprocessors that will process District data
- District data, including prompts and responses, shall not be used for model training by the vendor, the model provider, or any subprocessor
- Existing account: the District currently uses a Claude Team account for a limited group of staff. Proposers shall state whether the proposed environment will incorporate, migrate, or replace that account, and shall identify any licensing overlap
- Role-based access controls (RBAC): tiered permissions for general staff, supervisors, administrators
- SSO integration with the District's Active Directory / Microsoft Entra ID (Azure AD)
- Audit logging: retain full interaction logs for a minimum of 90 days, or longer where required by the District's records retention schedule. Logs shall be accessible to the District IT administrator and exportable to support records retention and California Public Records Act requests
- Content policy configuration appropriate for a public safety environment
- Approved use cases: drafting of incident narratives that contain no protected health information (PHI) or other confidential information, policy Q&A, document summarization, internal knowledge base, training material generation
- Prohibited without separate written approval by the District: entry of PHI or patient care records, access to live CAD/dispatch systems, or access to CJI. Any approved use involving PHI shall be covered by executed Business Associate Agreements with the vendor and model provider
- Proposer to provide a System Security Plan (SSP) for the AI environment prior to go-live
- Ongoing: annual licensing, support, updates

2.14 Hourly Rates

- Standard Rate: \$_____/hr
- After-Hours Rate: included in monthly service tier for covered services; otherwise \$_____/hr
- Holiday Rate: \$_____/hr

Services outside the defined scope of work shall be performed only upon the District's prior written authorization, based on a written estimate with a not-to-exceed amount, and shall be billed at the contracted hourly rates above. The District is not responsible for charges for out-of-scope work performed without prior written authorization.

2.15 Telecommunications & Voice Services

The selected vendor shall manage and support District-owned telecommunications infrastructure including:

- Administrative office telephones, station business lines, and VoIP platform administration
- Voicemail systems, auto-attendants, and related configuration
- Telephone moves, adds, and changes (MACs) for District-owned phone systems

- Carrier coordination and escalation for District-managed voice circuits

Out of Scope. Public safety radio systems, dispatch communications, and alerting infrastructure operated by CAL FIRE, a JPA, or a specialized provider are explicitly excluded from the vendor's management responsibility. The vendor is expected to coordinate with responsible agencies where District IT systems interface with those communications systems.

2.16 Internet & WAN Connectivity

The selected vendor shall manage and support the District's internet and wide-area network connectivity across all stations and facilities. Current connectivity includes commercial broadband, cellular routers, and multiple carrier circuits across field stations; circuit-level detail is provided in Confidential Appendix A-1. Vendor responsibilities include:

- ISP relationship management, circuit monitoring, and carrier escalation for District-managed circuits
- WAN uptime monitoring and monthly availability reporting delivered to the District IT lead
- Cellular failover planning, configuration, and management (existing cellular routers)
- VPN configuration and management for remote access and inter-station connectivity
- Coordination with internet service providers for outage resolution

Out of Scope. Communications circuits owned or operated by CAL FIRE, a JPA, or other governmental agency for dispatch or radio purposes are excluded. The vendor shall coordinate with those entities where District network infrastructure interfaces with their systems.

2.17 Governance, Risk Management & Internal Controls

The District recognizes the principles of the COSO 2013 Internal Control Framework and Government Finance Officers Association (GFOA) best practices. The selected vendor shall maintain and support IT controls that contribute to:

- Protection of public assets and information
- Segregation of duties where appropriate
- Auditability of financial and operational transactions
- Change management controls with documented approval workflows
- Access management controls and privileged account reviews
- System logging and monitoring with tamper-evident audit trails
- Backup and recovery controls with documented test results
- Documentation sufficient to support independent audits
- Risk assessment and mitigation activities

Proposers shall describe how their proposed services support recognized internal control frameworks, including the NIST Cybersecurity Framework (CSF) 2.0, CIS Critical Security Controls v8.1, SOC 2 (AICPA Trust Services Criteria), and principles consistent with COSO 2013.

Annual IT Controls Report. The selected vendor shall provide an annual written report to District leadership summarizing:

- Cybersecurity posture and threat landscape summary
- Vulnerability remediation status and open items
- Backup testing results and recovery validation
- Disaster recovery testing results
- Security incidents, root cause, and corrective actions

- Privileged account review results
- Significant system changes implemented during the year
- Compliance status against applicable frameworks

2.18 Full IT Functional Scope & Boundary of Responsibility

The following defines the complete functional scope of IT services expected from the selected vendor. Proposers must confirm coverage of all areas and identify any exclusions or limitations in their proposal. This scope supersedes any omission in the asset inventory (Appendix A), which represents a best-available baseline rather than a complete inventory.

In Scope. The selected vendor is responsible for:

- Network and internet infrastructure: firewalls, switches, wireless access points, VPNs, internet circuits, and all related equipment within the District's IT environment across all stations and facilities
- Servers and core infrastructure: physical servers, virtual machines, hypervisors, NAS devices, domain controllers, file servers, and backup infrastructure for both the ECFPD and legacy DSEDFD environments
- Domain consolidation: migration of the legacy DSEDFD Active Directory domain into the ECFPD domain following the 2026 annexation, including user account migration, group policy harmonization, and workstation re-joining
- Employee workstations, laptops, printers, and supported endpoints, including bringing unmanaged devices under management and priority replacement of end-of-life equipment
- Microsoft 365, email, identity and access management, multifactor authentication (MFA), and user account administration
- Cloud and SaaS services, software licensing, and individual software account administration as inventoried during onboarding
- District business and public safety applications for which the IT provider has a support or coordination responsibility, including records management and training platforms
- Cybersecurity, patching, endpoint protection, vulnerability management, SIEM monitoring, and incident response
- Backup, recovery, and business continuity for all systems within the provider's scope
- Help desk and day-to-day user support, including staff onboarding and offboarding
- Hardware and software asset management, CMDB maintenance, and change management
- Coordination with the District's other technology vendors, JPAs, governmental agencies, and service providers where their systems interface with or depend upon the District's IT environment
- UPS monitoring and management for network and server infrastructure

Out of Scope. The following are explicitly excluded from the vendor's management responsibility. The vendor is expected to coordinate with responsible agencies where District IT systems interface with these systems:

- Public safety radio systems, communications equipment, and dispatch infrastructure owned, operated, or supported through CAL FIRE, a JPA, or a specialized provider
- CAD / Computer-Aided Dispatch systems operated by CAL FIRE or a JPA
- Station alerting systems operated by or through a specialized provider or JPA
- Any system owned, licensed, or operated exclusively by a partner agency
- Apparatus-mounted or vehicle technology outside the District's IT network

Coordination Requirement. Where out-of-scope systems interface with District networks, computers, applications, or accounts, the vendor shall identify those interfaces during onboarding, document them in

the CMDB, and establish coordination protocols with the responsible agency or vendor. The vendor is not responsible for managing those systems but is responsible for ensuring District-side interfaces function correctly.

SECTION 3: PROPOSAL REQUIREMENTS

3.1 Part I: Equipment & Hardware

1. Cover letter identifying proposer, primary contact, and parts being bid, and acknowledging receipt of all addenda
2. Completed Exhibit A pricing schedule with make/model for all line items
3. Product data sheets confirming that proposed products meet or exceed the specifications in Sections 2.1–2.6
4. Proof of manufacturer authorization or authorized reseller status for each proposed manufacturer (e.g., HP, Lenovo, Dell, or equivalent)
5. Delivery timeline (required: within 30 calendar days of PO issuance to 501 Main St, Diamond Springs, CA 95619)
6. Warranty terms and RMA process
7. Migration labor methodology and staffing plan
8. Three (3) public agency equipment contract references within 5 years
9. If pricing is offered under an existing cooperative purchasing contract (e.g., California DGS, NASPO ValuePoint, Sourcewell), identification of that contract

3.2 Part II: Managed Services

10. Executive summary (2 pages max) describing service delivery approach
11. Technical proposal addressing every requirement in Sections 2.8 through 2.18, with a direct response to each section listed below. This list is provided for reference and does not limit the contractor's responsibility: the full scope stated in Sections 2.8 through 2.18 governs, and any exception or limitation must be expressly identified in the proposal.
 - 2.8 IT Security Onboarding & Initial Assessment (One-Time), including establishment of the District-owned CMDB
 - 2.9 Core Managed IT Services (Monthly Recurring)
 - 2.10 Managed Security Services (MSSP) (Monthly Recurring)
 - 2.11 Cyber Liability Support Services (Monthly Recurring)
 - 2.12 Server Migration to Cloud-Based Infrastructure (One-Time Project)
 - 2.13 Enterprise AI Integration: Walled Instance (One-Time Setup + Ongoing Licensing)
 - 2.14 Hourly Rates
 - 2.15 Telecommunications & Voice Services
 - 2.16 Internet & WAN Connectivity
 - 2.17 Governance, Risk Management & Internal Controls, including the Annual IT Controls Report
 - 2.18 Full IT Functional Scope & Boundary of Responsibility
12. Cloud migration plan outline (preliminary; full plan due within 45 days after award)
13. AI integration architecture diagram and security narrative identifying the proposed hosting architecture, security boundary, data flows, processing and storage locations, retention and deletion periods, and all subprocessors (see Section 2.13)
14. SOC 2 Type II report (issued within the last 18 months) and data handling policy

15. Staffing plan: key personnel, certifications, resumes
16. Draft Service Level Agreement (SLA) with response time commitments and service credits
17. Completed Exhibit B pricing schedule separating one-time and monthly recurring costs, on the pricing basis defined in Part II
18. Three (3) public agency managed IT services references, including at least one cloud migration project
19. Exceptions table: a single table listing every exception to the scope of work, the contract terms in Section 6.10, or the insurance requirements in Section 6.11. Exceptions not listed will be deemed waived

3.3 General Requirements

- Valid business license and authority to do business in California
- Insurance as described in Section 6.11
- Signed Non-Disclosure Agreement (NDA) required before the District provides detailed systems documentation, including Confidential Appendix A-1
- HIPAA Business Associate Agreement (BAA): the selected Part II vendor shall execute the District's BAA before accessing District systems, and shall ensure that cloud, AI, and other subcontractors that create, receive, maintain, or transmit District PHI execute equivalent agreements
- Equipment security: all proposed equipment shall be delivered with current manufacturer firmware and BIOS, and the proposer shall support firmware and security updates through the warranty term
- Subcontractors must be disclosed; the District reserves approval rights
- Background checks: proposer personnel with administrative access to District systems shall pass a background check acceptable to the District. Where access to CJI is required, personnel shall complete the fingerprint-based background checks required by the CJIS Security Policy
- Proposal validity: Part I and Part II pricing shall remain firm for 120 days from the proposal deadline. If awarded, Part II pricing shall remain firm for the base contract period, subject to the annual escalation cap in Exhibit B
- Proposal costs: see Section 6.2

SECTION 4: EVALUATION CRITERIA

Criterion	Part I	Part II
Technical Specification Compliance (meets or exceeds stated specifications)	30%	25%
Total Cost / Price	35%	25%
Vendor Experience & References	15%	20%
Delivery / Implementation Approach & Timeline	10%	15%
Security Posture & Compliance Documentation	10%	10%
AI Integration Capability & Architecture	N/A	5%
Total	100%	100%

4.1 Evaluation Process

- **Responsiveness review.** Proposals will first be reviewed for timeliness and completeness. Proposals that are late or materially incomplete may be rejected
- **Evaluation panel.** An evaluation panel appointed by the Fire Chief, composed of District staff and which may include an outside technical advisor, will score proposals. Panel members will sign conflict-of-interest and confidentiality statements
- **Scoring.** Each non-price criterion will be scored from 0 (not addressed) to 5 (exceptional) and multiplied by its weight, for a maximum of 100 points per Part
- **Price scoring.** The lowest responsive price receives full price points; other proposals receive points in proportion ($\text{lowest price} \div \text{proposer's price} \times \text{price weight}$). Part II price will be calculated as total one-time fees plus thirty-six (36) months of recurring fees on the Part II pricing basis
- **Separate evaluation.** Part I and Part II will be evaluated and scored separately. A proposer bidding both Parts will be scored independently on each
- **Interviews and references.** The District may interview or request demonstrations from the highest-ranked proposers and may adjust scores based on interviews and reference checks
- **Best and final offers.** The District may request best and final offers from the highest-ranked proposers
- **Notice of intended award and protests.** The District will issue a written notice of intended award to all proposers. A proposer may protest the intended award by written notice to procurement@eldofire.com within five (5) business days after issuance of the notice, stating the specific factual and legal grounds. The Fire Chief will respond in writing before the Board considers the award

SECTION 5: PRICING SCHEDULES

Exhibit A: Part I, Equipment & Hardware

Prices must include delivery to 501 Main St, Diamond Springs, CA 95619. Shipping and applicable tax must be itemized. Migration labor quoted per unit. Prices firm for 120 days from the proposal deadline.

Proposer:				
Item	Make / Model / Specifications	Qty	Unit Price	Extended Price
Desktop Computer	Business-grade SFF desktop Intel Core i7 vPro (13th Gen+) or AMD Ryzen 7 PRO 16GB DDR5 1TB NVMe SSD Win 11 Pro Proposed make/model: 	25	\$	\$
Laptop	Business-grade 14" laptop Intel Core i7 vPro or AMD Ryzen 7 PRO (current gen) 14" FHD+ (1920x1200) anti-glare 16GB RAM, upgradeable to 32GB 1TB NVMe SSD Smart Card TPM 2.0 Win 11 Pro Proposed make/model: 	18	\$	\$
Docking Station	Business-grade universal USB-C / Thunderbolt 4 dock Dual monitor 90W PD Gigabit Ethernet Proposed make/model: 	20	\$	\$
Monitor	Mid-grade 27–32" FHD minimum, QHD preferred IPS or VA Anti-glare Ergonomic stand Proposed make/model: 	70	\$	\$
Keyboard & Mouse Sets	Open bid item (Section 2.5) Proposed make/model: 	35	\$	\$
Camera & Audio Packages	Open bid item (Section 2.6) Proposed make/model: 	10	\$	\$
Migration Labor	Device migration and configuration services: migrate user data, profiles, printers, and software from existing systems to new equipment at District facilities (Section 2.7)	43	\$	\$
Shipping				\$
Tax				\$
PART I SUBTOTAL (Quoted Items; excl. keyboards, cameras)				\$

Item	Make / Model / Specifications	Qty	Unit Price	Extended Price
Open Bid Items (Keyboard/Mouse Sets x35 + Camera/Audio x10)				\$
PART I GRAND TOTAL				\$

Optional items (not included in Grand Total; quote per unit):

Option	Unit Price	Proposed Model / Notes
Laptop 32 GB RAM configuration (upgrade cost per unit over base)	\$	
Laptop touchscreen configuration (upgrade cost per unit over base)	\$	
Backlit keyboard and mouse set (per set)	\$	

Exhibit B: Part II, IT Management Services

Separate one-time project fees from monthly recurring costs. Monthly per-unit pricing shall use the Part II Pricing Basis (55 managed workstations; 12 managed servers). Annual escalation capped at 3%.

Proposer:	
------------------	--

Service	Description	Qty / Freq	Price
ONE-TIME PROJECT FEES			
IT Security Onboarding Assessment	Independent third-party cybersecurity assessment and remediation (Section 2.8). Deliverables: CVE Discovery & Remediation, Privileged Account Review, PII/PHI Scan, Roles & Responsibilities, Communications & Workflow, Initial Incident Response Plan, Cyber Awareness Training, Acceptable Use Policy, District-owned CMDB.	1	\$
Server Migration to Cloud	Migration of on-premises server infrastructure to Azure Government / AWS GovCloud, including assessment, migration plan, execution, validation, and decommission of on-premises hardware (Section 2.12).	1	\$
Enterprise AI Integration (Walled Instance)	Deployment of the private enterprise AI environment described in Section 2.13 (Claude reference implementation or approved equivalent), including SSO integration, RBAC, audit logging, content policy setup, and staff onboarding.	1	\$
Staff Training & Onboarding	Department-level new equipment onboarding, cloud platform end-user training, and AI tool introduction sessions. Written user guides included.	1	\$
ONE-TIME SUBTOTAL			\$
RECURRING MONTHLY SERVICES			
Core Managed IT Services: Workstations	RMM, help desk, patch management, asset inventory, basic cloud administration (Section 2.9).	55 units/mo	Per unit: \$ Per month: \$
Core Managed IT Services: Servers	As above, for managed servers.	12 units/mo	Per unit: \$ Per month: \$
Managed Security Services (MSSP): Workstations	EDR/MDR, SIEM monitoring, threat intelligence, ransomware protection, dark web monitoring, incident response retainer (Section 2.10).	55 units/mo	Per unit: \$ Per month: \$

Service	Description	Qty / Freq	Price
Managed Security Services (MSSP): Servers	As above, for managed servers.	12 units/mo	Per unit: \$ Per month: \$
Cyber Liability Support Services	Compliance documentation, policy maintenance, CVE remediation tracking, insurer reporting (Section 2.11).	1/mo	Per month: \$
Cloud Infrastructure Run Rate	Monthly cloud hosting for migrated servers, storage, backup, and M365 GCC licensing. Vendor to itemize.	Monthly	Per month: \$
Enterprise AI Licensing	Ongoing enterprise licensing for the walled AI environment, billed monthly. Support and updates included.	Monthly	Per month: \$
Other recurring charges (itemize, if any)	Any per-unit charge for network devices or other infrastructure (see Part II Pricing Basis).	Monthly	Per month: \$
TOTAL MONTHLY RECURRING			Per month: \$
EVALUATED PART II PRICE (One-Time Subtotal + 36 × Total Monthly Recurring)			\$

Standard Hourly Rate	After-Hours Rate (outside covered services)	Holiday Rate
\$	\$	\$

SECTION 6: TERMS & CONDITIONS

6.1 Reservation of Rights

The District reserves the right to reject any and all proposals; waive informalities; award in whole or in part, including awarding Part I and Part II separately; negotiate with the highest-ranked proposer(s); request best and final offers; cancel this RFP; or purchase any Part I equipment through an existing cooperative purchasing contract, as deemed in the District's best interest.

6.2 Proposal Costs

All costs of preparing and submitting a proposal, attending the pre-proposal conference, and participating in interviews or demonstrations are the sole responsibility of the proposer. The District will not reimburse any proposal preparation, scoping, or presentation costs.

6.3 Payment Terms

Hardware invoices are payable net thirty (30) days after the later of receipt of a correct invoice or the District's acceptance of delivered and installed equipment. Monthly managed services shall be invoiced monthly in arrears for services performed and are payable net thirty (30) days. One-time project fees shall be invoiced according to a milestone schedule agreed at contract execution and are payable upon the District's written acceptance of each milestone deliverable. The District may withhold payment of disputed amounts pending resolution.

6.4 Data Ownership & AI Privacy

All District data, documents, interaction logs, documentation, inventories, network diagrams, configurations, procedures, and operational records generated or developed during this contract remain the sole property of El Dorado County Fire Protection District. Vendor shall not use District data for any purpose, including AI model training, without prior written consent. District data processed through the AI environment shall not be transmitted to, processed by, or stored by any party or system other than those identified in the vendor's proposal and approved in writing by the District, and shall not be used for model training by the vendor, the model provider, or any subprocessor. All District data shall be stored and processed within the United States. Vendor shall comply with HIPAA and the executed Business Associate Agreement with respect to any PHI. Upon contract termination, vendor shall transfer all documentation, password vaults, configuration exports, and asset inventories to the District within 30 days.

6.5 Returns & Cancellation

No restocking fee shall apply to equipment that is defective, damaged in transit, or does not conform to the specifications or the purchase order. Any restocking fee for returns made solely for the District's convenience shall be stated in the proposal and shall not exceed fifteen percent (15%). Termination of managed services is governed by Section 6.10.

6.6 Ethics & Conflict of Interest

Proposers must disclose any current or prior financial, contractual, or personal relationship with District personnel or Board members. Violations may result in disqualification and debarment. If the District determines that the selected vendor or any of its personnel will act as a "consultant" under the Political Reform Act (Government Code § 81000 et seq.) and the regulations of the Fair Political Practices Commission, those individuals shall file a Statement of Economic Interests (Form 700) as required by the District's Conflict of Interest Code.

6.7 Contract Transition Assistance

Upon contract expiration, non-renewal, or termination for any reason, the outgoing vendor shall provide up to ninety (90) days of transition assistance at no additional charge. Transition assistance shall include:

- Transfer of all documentation, network diagrams, system inventories, and operational procedures
- Password vault transfer to the District or successor vendor
- Configuration exports for all managed devices, firewalls, and cloud platforms
- Complete asset inventory in machine-readable format
- Knowledge transfer sessions with incoming vendor or District staff
- Cooperation with successor vendor during parallel operations period

6.8 Non-Collusion & Debarment Certification

By submitting a proposal, the proposer certifies that: (a) the proposal was made without collusion or fraud; (b) the proposer is not currently debarred, suspended, or excluded from federal or state contracting; (c) the proposer has no undisclosed organizational conflicts of interest; and (d) the proposer complies with all applicable equal employment opportunity requirements.

6.9 Public Records Act

Proposers acknowledge that all proposals submitted become public records upon contract award pursuant to the California Public Records Act (Government Code § 7920.000 et seq.). Proposers claiming trade secret protection must specifically identify those portions in writing at the time of submission and provide legal justification for exemption.

6.10 Contract Terms

The selected proposer will be required to execute the District's standard agreement for the applicable Part(s), which will incorporate this RFP and the accepted proposal. Vendor-supplied master services agreements, terms of service, or click-through terms will not govern unless expressly accepted in writing by the District. The agreement will include, at a minimum:

- Termination for convenience by the District on thirty (30) days' written notice, with payment only for services performed and accepted through the termination date
- Termination for cause, with a reasonable cure period
- Non-appropriation: if the Board of Directors does not appropriate funds for any fiscal year, the District may terminate without penalty at the end of the last funded period
- Indemnification, defense, and hold harmless of the District, its Board, officers, employees, and volunteers for claims arising from the vendor's negligence, willful misconduct, breach of data security or confidentiality obligations, or intellectual property infringement
- Service levels and service credits consistent with Section 2.9
- HIPAA Business Associate Agreement (Part II)
- Notice to the District of any actual or suspected security incident involving District data within twenty-four (24) hours of discovery
- Independent contractor status and compliance with all applicable federal, state, and local laws
- Retention of contract records and District audit rights for a minimum of four (4) years after final payment
- California governing law, with venue in the Superior Court of California, County of El Dorado

6.11 Insurance

Before contract execution and throughout the contract term, the vendor shall maintain the following insurance with insurers authorized to do business in California and rated A-:VII or better by A.M. Best:

- Commercial General Liability: \$1,000,000 per occurrence; \$2,000,000 general aggregate
- Automobile Liability: \$1,000,000 combined single limit, covering owned, hired, and non-owned vehicles
- Workers' Compensation: statutory limits; Employer's Liability \$1,000,000 per accident
- Technology Errors & Omissions (Professional Liability), Part II: \$2,000,000 per claim
- Cyber Liability (Network Security & Privacy), Part II: \$1,000,000 per claim, including data breach response, network security failure, privacy liability, and regulatory defense

The District, its Board, officers, employees, and volunteers shall be named as additional insureds on the General Liability and Automobile Liability policies. Certificates of insurance and endorsements are due before contract execution. Vendors awarded Part I only must meet the General Liability, Automobile Liability, and Workers' Compensation requirements.

SECTION 7: PROCUREMENT SCHEDULE & SUBMISSION INSTRUCTIONS

7.1 Procurement Schedule

Activity	Date
RFP issued	Tuesday, October 13, 2026

Activity	Date
Optional virtual pre-proposal conference	Thursday, October 22, 2026, 10:00 AM (Pacific Time)
Written questions due	Wednesday, October 28, 2026, 5:00 PM (Pacific Time)
Q&A addendum issued	Wednesday, November 4, 2026
Proposals due	Friday, November 13, 2026, 5:00 PM (Pacific Time)
Evaluation, reference checks, and interviews (if requested)	November 16 – December 4, 2026
Notice of intended award	On or about Monday, December 7, 2026
Board of Directors consideration of contract award	Thursday, January 21, 2027 (regular Board meeting)
Anticipated contract start	On or about February 1, 2027

Dates following the proposal deadline are anticipated and may be adjusted by the District. Any change to the question deadline or the proposal deadline will be issued by written addendum.

7.2 Procurement Contact

The District maintains a single point of contact for this RFP. All questions, requests for clarification, and proposal submissions shall be sent by email to the procurement mailbox below. Questions or submissions sent to any other address or to individual District personnel may not be received or considered. Only written responses issued by the District by addendum are official.

- Procurement Contact: Brad Gates, Fire Chief
- Email: procurement@eldofire.com
- Reference: RFP-EDCFD-2026-IT-01

7.3 Submission Instructions

- Submit electronically to: procurement@eldofire.com
- Subject line: "RFP-EDCFD-2026-IT-01 - [Company Name] - Part I / Part II / Both"
- Format: single PDF, maximum 25 MB per email. Larger files shall be submitted via a secure file-sharing link, which must be accessible to the District as of the deadline
- Deadline: Friday, November 13, 2026 at 5:00 PM Pacific Time. Late submissions will not be considered
- Pre-proposal conference: optional, virtual, Thursday, October 22, 2026 at 10:00 AM Pacific Time. Request the meeting link from procurement@eldofire.com. Statements made at the conference are not binding unless confirmed by addendum
- Written questions due by Wednesday, October 28, 2026 at 5:00 PM Pacific Time, to procurement@eldofire.com
- Responses to all questions will be issued as a written addendum by Wednesday, November 4, 2026, posted on the District's website (www.eldoradocountyfire.com) and emailed to each proposer that has submitted questions or notified the Procurement Contact of its intent to propose. Proposers are responsible for checking the website for addenda and must acknowledge all addenda in their cover letter

- Confidential Appendix A-1 (detailed IT environment baseline) is available to prospective proposers upon request to procurement@eldofire.com and execution of the District's Non-Disclosure Agreement

APPENDIX A: CURRENT IT ENVIRONMENT (BEST AVAILABLE BASELINE)

This appendix represents the District's best available baseline IT environment as of August 2026, compiled from current asset inventory records maintained by the District's current IT provider. This information is provided to assist proposers in developing responsive proposals and is not warranted as complete or fully reconciled.

Note to Proposers. This baseline is not a complete Configuration Management Database (CMDB). The selected vendor will be required to validate, reconcile, and expand this inventory during the onboarding period and deliver a District-owned CMDB within 60 days of go-live. Proposers should propose based on this baseline and state any assumptions regarding environment complexity.

Confidential Appendix A-1. To protect the security of District systems, this appendix summarizes the environment by category and quantity only. Device-level detail, including makes, models, system and domain names, locations, and circuit information, is contained in Confidential Appendix A-1, which the District will release to prospective proposers upon receipt of a signed Non-Disclosure Agreement (Section 3.3). Requests shall be sent to procurement@eldofire.com.

Workstations: ECFPD

Desktops	27 units; business-class small form factor and workstation models, Windows 11
Desktop Locations	Field stations and administrative offices
Laptops	19 units; mixed business-class fleet from several manufacturers
Laptop Locations	Administrative offices, training, and field staff
Device Status	A small number of laptops are not yet centrally managed or operate in kiosk mode; some units are scheduled for priority replacement
Operating System	Windows 11 is the District standard; remaining legacy units are scheduled for replacement

Workstations: DSEDFD (annexed 2026)

Desktops	5 units; business-class
Laptops	3 units; business-class
IT Admin Workstation	1 unit
Directory	Separate Active Directory domain; integration and migration required
Operating System	Windows 11 standard; remaining legacy units are scheduled for replacement

Servers: ECFPD

Physical Hosts	2
Virtual Machines	4
Backup	1 backup server
Directory Services	On-premises Active Directory
Lifecycle	Several server systems are at or near end of support and are a migration priority (Section 2.12)

Servers: DSEDFD

Domain Controller	1
File Server	1
Virtualization Host	1
Backup	1 backup server
Other	1 additional physical server

Network Hardware: ECFPD Stations

Firewalls	Edge security appliances at connected stations (approximately 7 devices)
Internet Service	Mix of commercial broadband and cellular service; multiple carrier types across stations (vendor to confirm)
Fax	Cloud fax service at multiple stations
Wireless	Business-class wireless access points at all stations
Switches	Managed and PoE switches (2 inventoried; vendor to confirm full count)
Presentation	2 wireless presentation devices

Network Hardware: DSEDFD

Network Storage	4 network-attached storage devices
Switches	2 48-port PoE switches
Wireless	Business-class wireless access points at two locations
Firewall	1 edge security appliance

Uninterruptible Power Supplies (UPS)

ECFPD	3 units supporting server and network equipment
DSEDFD	2 rack-mount units supporting telecom and network equipment

Printers and Copiers

ECFPD	Approximately 10 devices: multifunction printers and copiers, laser printers, and receipt printers across stations
DSEDFD	3 devices: multifunction printers and a receipt printer
Connection Type	All network-connected

Domain & Identity Environment

Directory Services	Two separate on-premises Active Directory domains (ECFPD and DSEDFD); merge and migration required post-annexation
Estimated Managed Units	55 managed workstations (ECFPD 46; DSEDFD 9) and 12 managed servers (ECFPD 7; DSEDFD 5). Some DSEDFD servers may be virtual machines; vendor to confirm. See Part II Pricing Basis

Unmanaged Devices	A small number of laptops, to be brought into management scope
--------------------------	--

Out-of-Scope Systems (Vendor to Coordinate, Not Manage)

The following systems are operated by a JPA, CAL FIRE, or specialized provider and are not within the IT vendor's direct management responsibility. However, where these systems interface with District networks, computers, or accounts, the IT vendor is expected to coordinate with the responsible agency or vendor as necessary.

- Public safety radio systems, communications equipment, and dispatch infrastructure (operated through JPA / CAL FIRE)
- CAD / Computer-Aided Dispatch system (CAL FIRE / JPA operated)
- Station alerting systems
- TargetSafety / other JPA-provided training platforms
- Any system owned, licensed, or operated exclusively by a partner agency

Scope Clarification

The asset information above represents currently known inventory and is not a complete CMDB. The District has not yet fully inventoried all software accounts, SaaS subscriptions, and cloud services. The selected vendor's onboarding deliverable (Section 2.8) shall establish the definitive baseline. Proposers should not exclude services from their proposal simply because a specific item does not appear in this appendix. The functional scope in Sections 2.8–2.18 governs.