REQUEST FOR PROPOSAL

2026-EMA-RFP-001

Technical Infrastructure Modernization & Clean-Slate 911 Systems Deployment

Parke County, Indiana

Issuing Entity: Parke County, Indiana
Project: Public Safety Answering Point (PSAP) Technical Infrastructure Modernization
Procurement Type: Request for Proposals
Authority: Indiana Public Purchasing Code, IC 5-22

TABLE OF CONTENTS

Appendix A – Dispatch and Jail Workstation Diagrams
Appendix B – Cable Color and Identification Standard
Appendix C – Mandatory Compliance Matrix
Appendix D – Pricing Schedule
Appendix E – Acceptance Test Matrix
Appendix F – County-Furnished Equipment and Site Information
Appendix G – Vendor Project Staffing and References

---

1. ADMINISTRATIVE INFORMATION

1.1 Purpose

Parke County, Indiana ("County") is soliciting proposals from qualified technology contractors with demonstrated experience in public-safety communications, PSAP infrastructure, enterprise networking, cybersecurity, virtualization, storage, Microsoft infrastructure, and mission-critical 24x7 support.

The County intends to select a qualified contractor to design, furnish, install, configure, integrate, test, document, and support a modernized technical infrastructure environment for the Parke County Public Safety Answering Point and associated jail operations.

The project is intended to establish a resilient, supportable, secure, and documented infrastructure platform capable of supporting current and future public-safety applications.

1.2 Procurement Method

This solicitation is intended to be conducted as a Request for Proposals under applicable Indiana law and County procurement policies.

The County reserves the right, subject to applicable law and the terms of this RFP, to:

- reject any or all proposals;
- request clarification;
- conduct discussions with one or more offerors;
- request revised proposals or Best and Final Offers if permitted;
- negotiate scope, price, schedule, or contractual terms;
- waive minor informalities where legally permissible;
- cancel or modify the solicitation;

- award all or part of the scope where legally permissible; and
- select the proposal determined to provide the best overall value to the County.

Nothing in this RFP shall be interpreted as requiring award to the lowest-priced proposal.

1.3 RFP Schedule

The County shall insert the following dates before publication:

Event	Date/Time
RFP Issued	9 September 2026
Deadline for Written Questions	16 October 2026 4:00 PM
County Response to Questions	21 October 2026
Proposal Submission Deadline	30 October 2026 4:00 PM
Proposal Evaluation	3-13 November 2026
Interviews/Demonstrations, if applicable	3-13 November 2026
Notice of Intent to Award	13 November 2026
Contract Approval	16 November 2026
Anticipated Project Start	1 December 2026
Project Completion Deadline	1 September 2027

All times shall be Eastern Time unless otherwise specified.

1.4 Questions and Communications

All questions regarding this RFP shall be submitted in writing to:

Christopher O'Brien
Director
Parke County EMA
765-569-5911
em.911@parkecounty.in.gov

Offerors shall not contact County employees, elected officials, PSAP personnel, third-party application vendors, or other persons regarding this solicitation except as specifically authorized by the County.

Unauthorized communications may be considered in accordance with applicable procurement rules.

1.5 Proposal Validity

Proposals shall remain valid for a minimum of one hundred twenty (120) calendar days following the submission deadline unless the County and offeror agree otherwise in writing.

---

2. PROJECT OVERVIEW AND OBJECTIVES

2.1 Statement of Intent

Parke County intends to implement a clean-slate technical infrastructure environment for its PSAP.

The selected contractor shall design and implement a new infrastructure footprint rather than reproducing undocumented legacy architecture.

The clean-slate approach is intended to:

- eliminate undocumented dependencies;
- eliminate unnecessary legacy configurations;
- eliminate obsolete authentication mechanisms;
- establish documented administrative ownership;
- establish modern security controls;
- establish resilient network, compute, storage, and power infrastructure;
- establish recoverable and documented configurations;
- provide a sustainable support model; and
- create a known baseline for future audits, maintenance, and expansion.

The clean-slate requirement applies to the new County infrastructure environment. Existing third-party public-safety applications and equipment that must remain operational shall be integrated only to the extent required by the approved migration architecture.

2.2 Project Objectives

The selected contractor shall provide a complete solution addressing:

1. Enterprise compute and virtualization.
2. Shared resilient storage.
3. Network switching and routing.
4. Redundant perimeter firewalls.
5. Active Directory and DNS.
6. Cybersecurity and privileged access.
7. Workstation replacement.
8. Dispatch multi-monitor and KM/KVM infrastructure.
9. UPS and power protection.
10. Rack and environmental monitoring.
11. GPS-based time synchronization.
12. Backup and disaster recovery.
13. INdigital integration.
14. Cushing CAD integration.
15. WTH GIS integration.
16. IDACS integration.
17. CPC Lockdown integration.
18. Existing Solacom and Mindshare equipment integration.
19. Migration and cutover support.
20. Documentation and training.
21. Five-year support pricing.
22. 24x7x365 emergency support.

2.3 Applicable Standards

The solution shall comply with all applicable laws, regulations, policies, and standards governing the County's environment.

The architectural baseline shall include applicable requirements of:

- NENA i3 Version 3, including applicable published corrections/errata;
- FBI CJIS Security Policy, Version 6.0, as applicable to the County environment;
- applicable Indiana CJIS requirements;
- applicable Microsoft licensing requirements;
- NIST SP 800-88 Rev. 2 for media sanitization;
- applicable manufacturer security and hardening recommendations; and
- other standards specifically identified in this RFP.

NENA describes i3 Version 3 as an IP-based NG9-1-1 architecture incorporating REST/JSON interfaces and updated security and interoperability mechanisms. The contractor shall coordinate with the County and applicable NG9-1-1 providers to determine which i3 capabilities are applicable to the specific PSAP deployment.

Where a County requirement exceeds a baseline regulatory requirement, the County requirement shall apply.

---

3. VENDOR QUALIFICATIONS AND RESPONSIBILITY

3.1 Minimum Qualifications

The prime contractor shall demonstrate:

- at least five (5) years of experience delivering enterprise IT infrastructure;
- demonstrated experience supporting 24x7 mission-critical environments;
- demonstrated public-safety, PSAP, emergency communications, or comparable experience;
- demonstrated experience with enterprise virtualization;
- demonstrated experience with enterprise networking and firewalls;
- demonstrated Microsoft Active Directory experience;

- demonstrated backup and disaster-recovery experience;
- demonstrated experience coordinating with multiple application vendors;
- demonstrated ability to provide four-hour on-site P1 emergency response to the Parke County PSAP;
- appropriate manufacturer certifications for proposed technologies; and
- sufficient financial and technical resources to complete the project.

3.2 Public-Safety Experience

Offerors shall identify at least three (3) substantially similar projects completed within the previous five (5) years.

Each reference shall include:

- customer name;
- customer location;
- project description;
- approximate project value;
- completion date;
- technologies deployed;
- PSAP/public-safety relevance;
- reference contact name;
- reference telephone number; and
- reference email address.

3.3 Project Personnel

The proposal shall identify the personnel assigned to the project, including:

- Project Manager;
- Lead Network Engineer;
- Systems/Virtualization Engineer;
- Cybersecurity Engineer;

- Microsoft/Identity Engineer;
- Field Technician(s);
- Backup/DR Engineer;
- Primary P1 Support Engineer; and
- Secondary P1 Support Engineer.

Resumes or qualifications shall be provided for key personnel.

The County must approve substitutions of key personnel during the project.

3.4 Subcontractors

All proposed subcontractors shall be identified in the proposal.

The prime contractor shall remain fully responsible for all subcontractor performance.

---

4. TECHNICAL INFRASTRUCTURE REQUIREMENTS

4.1 General Architecture

The contractor shall provide a complete infrastructure architecture meeting or exceeding the requirements of this RFP.

"Approved equivalent" equipment may be proposed where the equipment provides equal or superior operational capability, performance, reliability, supportability, security, and lifecycle characteristics.

Brand references are intended to establish a general class of equipment and shall not prevent consideration of technically equivalent alternatives.

The bidder shall identify all proposed makes, models, quantities, licenses, subscriptions, support plans, and relevant technical specifications.

4.2 Virtualized Compute Host Nodes

The contractor shall provide a minimum of two (2) identical enterprise rack-mount server nodes configured as a highly available virtualization cluster.

Acceptable examples include current enterprise platforms from Dell, HPE, Lenovo, Cisco, or approved equivalent manufacturers.

Minimum requirements

Each node shall provide:

- rack-mountable chassis;
- redundant hot-plug power supplies configured for independent power feeds;
- enterprise-class x86-64 processors;
- minimum sixteen (16) physical CPU cores per socket;
- minimum two (2) physical CPU sockets;
- processor performance appropriate for the proposed virtualization and database workload;
- minimum 256 GB DDR5 ECC registered memory;
- memory expansion capability sufficient to support future growth;
- enterprise NVMe boot media;
- redundant boot media configured as RAID 1 or equivalent fault-tolerant architecture;
- independent out-of-band management controller;
- dedicated management network interface;
- HTML5 remote console;
- secure firmware/BIOS configuration;
- hardware/firmware lockdown capability;
- minimum four (4) 10-Gbps-capable network interfaces; and
- manufacturer support for the complete proposed configuration.

The contractor shall submit a workload/performance justification for the selected processor configuration.

The County shall not require a particular processor clock speed or cache-per-core ratio where the bidder can demonstrate equivalent or superior performance.

4.2.1 Boot Architecture

The hypervisor shall boot from dedicated redundant enterprise storage.

Boot media shall not be located on:

- removable USB media;
- a production VM datastore;
- an unprotected single drive; or
- other storage that creates an unnecessary single point of failure.

4.2.2 Out-of-Band Management

The management controller shall provide:

- independent management network connectivity;
- remote console;
- remote power control;
- hardware health monitoring;
- firmware management;
- audit logging;
- secure authentication;
- role-based access; and
- configuration lockdown.

4.3 Shared Storage Array

The contractor shall provide an enterprise shared storage array suitable for the proposed virtualization environment.

Acceptable examples include current enterprise arrays such as Dell PowerVault ME-series, HPE MSA-series, Lenovo ThinkSystem, NetApp, or approved equivalent.

The array shall provide:

- dual redundant storage controllers;
- controller failover without loss of stored data;
- redundant cache protection;
- hot-swappable drives;

- redundant power;
- redundant storage paths;
- multipath support;
- minimum fifteen (15) TB usable capacity after RAID and manufacturer-required overhead;
- capability for future capacity expansion;
- enterprise-grade SSD/HDD media appropriate to the proposed workload;
- snapshots or equivalent point-in-time protection;
- encryption at rest where supported;
- monitoring and alerting; and
- manufacturer support.

The contractor shall identify the proposed RAID or equivalent data-protection architecture and demonstrate that it can tolerate the specified component failures without loss of required availability.

4.3.1 Storage Connectivity

The array shall provide redundant storage connectivity to both compute hosts using:

- 10-Gbps or faster iSCSI;
- 12-Gbps or faster SAS;
- Fibre Channel; or
- another approved enterprise storage protocol.

Each host shall have redundant independent storage paths.

The contractor shall demonstrate multipath operation during acceptance testing.

4.4 Network Switching and Routing

The contractor shall provide two (2) identical enterprise Layer 3 switches configured as a resilient switching pair or stack.

Examples include Cisco Catalyst 9300-class, HPE Aruba CX 6300-class, or approved equivalent.

The switching architecture shall provide:

- redundant operation;
- vendor-supported hardware stacking or equivalent resilient interconnect;
- dedicated inter-switch connectivity that does not unnecessarily consume required client-facing ports;
- minimum 10-Gbps uplink capability;
- hardware-accelerated Layer 3 routing;
- OSPF support where required by the final design;
- policy-based routing where required;
- VLAN support;
- ACL support;
- LACP;
- SNMPv3;
- secure management;
- configuration backup;
- logging; and
- redundant power.

The bidder shall identify the proposed switching architecture and explain its failover behavior.

Where a specific failover time is proposed, the bidder shall identify the manufacturer's documented performance and the method by which it will be validated.

The County's primary requirement is continuity of mission-critical services rather than a particular proprietary switching technology.

4.5 Redundant Perimeter Firewalls

The contractor shall provide two (2) enterprise next-generation firewalls configured in a high-availability Active/Passive or equivalent stateful HA architecture.

Examples include Cisco, Palo Alto Networks, Fortinet, Check Point, or approved equivalent.

The firewalls shall provide:

- stateful failover;
- synchronized connection state;
- redundant power;
- IPS/IDS;
- application control;
- antivirus/malware inspection;
- secure VPN;
- MFA-compatible administrative access;
- logging;
- centralized or secure local management;
- certificate management;
- TLS inspection capability where legally and technically appropriate;
- VLAN/subinterface support;
- routing;
- ACLs/security policies;
- configuration backup;
- role-based administration; and
- manufacturer support.

The proposed platform shall provide at least 1 Gbps of documented security throughput under the County's required security services or shall demonstrate sufficient performance headroom for the proposed environment.

The contractor shall document how throughput is measured and identify which security services are enabled during the manufacturer's published performance measurement.

4.6 Rack and Physical Infrastructure

The contractor shall provide a dedicated 42U lockable rack enclosure.

The enclosure shall include:

- locking front and rear doors;
- perforated ventilation;
- front-to-rear airflow;
- grounding provisions;
- vertical 0U PDU mounting;
- cable-management accessories;
- rack hardware;
- seismic/anti-tip provisions where applicable;
- equipment mounting rails; and
- sufficient capacity for the complete installation and reasonable future expansion.

4.7 GPS Time Synchronization

The contractor shall provide a dedicated GPS-disciplined time source or approved equivalent.

The system shall provide:

- GPS antenna;
- external antenna mounting;
- required cable;
- NTP service;
- redundant or protected power;
- monitoring;
- time-source status;
- secure management; and
- integration with County infrastructure.

The contractor shall coordinate antenna placement with the County and building owner.

The contractor shall not penetrate the roof or building envelope without prior County approval.

4.8 Environmental Monitoring

The contractor shall provide a rack/environmental monitoring system capable of monitoring:

- temperature;
- relative humidity;
- water/leak detection;
- equipment/rack environmental status;
- power status where supported; and
- other critical environmental conditions identified during design.

The system shall provide SNMPv3 and email or equivalent notification capability.

Alarm thresholds shall be documented and approved by the County.

4.9 Workstation Fleet

The corrected total workstation quantity is **eleven (11) physical PCs**.

The contractor shall supply, image, install, configure, and document the following:

Tier	Quantity	Location/Purpose
Tier 1 High-Performance	4	3 Dispatch + 1 Jail Central
Tier 2 Standard	6	Jail Standard Positions
Tier 3 IDACS	1	Dedicated IDACS
Total	**11**	

4.9.1 Tier 1 High-Performance Workstations

Quantity: **4**

Three (3) shall be deployed at dispatch positions and one (1) at Jail Central.

Minimum requirements:

- enterprise SFF or workstation chassis;
- Intel Core i9, Intel Xeon, AMD Ryzen 9, AMD Ryzen Pro, or approved equivalent;
- minimum eight (8) physical performance cores;
- minimum 32 GB RAM;
- TPM 2.0;
- minimum 512 GB NVMe SSD;
- enterprise-grade discrete graphics;
- minimum 4 GB graphics memory;
- sufficient outputs for the assigned display architecture;
- secure firmware;
- Windows 11 Enterprise or County-approved equivalent;
- domain integration;
- wired keyboard and mouse.

The graphics solution shall be capable of driving the displays assigned to the workstation in the final approved dispatch-console architecture.

4.10 Tier 2 Standard Workstations

Quantity: **6**

Deployment:

- Commander;
- Satellite;
- Book-in 1;
- Book-in 2;
- Matron;
- Reports.

Minimum requirements:

- enterprise SFF chassis;
- Intel Core i7, AMD Ryzen 7, or approved equivalent;
- minimum 16 GB RAM;
- TPM 2.0;
- minimum 256 GB NVMe SSD;
- integrated or discrete graphics appropriate to the assigned display;
- Windows 11 Enterprise or County-approved equivalent;
- domain integration;
- wired keyboard and mouse.

4.11 Tier 3 IDACS Workstation

Quantity: **1**

The contractor shall provide one dedicated workstation for Indiana IDACS/NCIC communications to include a display similar to the dispatch position.

The contractor shall coordinate configuration and security requirements with the applicable Indiana Office of Technology/IOT and IDACS authorities.

The workstation shall be isolated and hardened according to applicable state requirements.

The contractor shall not independently modify state-controlled IDACS configuration requirements without authorization.

4.12 Dispatch Display Architecture

There are three (3) primary dispatch positions.

Each position shall accommodate a six-monitor 3-over-3 physical display arrangement.

The contractor shall supply:

- four (4) new displays per dispatch position;
- two (2) existing displays per dispatch position;
- one six-display mounting structure per position;

- one Tier 1 workstation per position;
- one wired keyboard;
- one wired trackball mouse; and
- one dedicated hardware KM/KVM solution.

Total new dispatch displays: **12**

4.12.1 Dispatch Display Requirements

New displays shall be:

- 24-inch or 27-inch;
- LED-backlit;
- 1920×1080 or 2560×1440;
- VESA compatible;
- suitable for continuous professional use;
- thin-bezel;
- compatible with the proposed mounting solution.

The contractor shall verify physical compatibility with the two existing displays at each position.

If existing displays cannot be safely incorporated into the proposed mounting architecture, the contractor shall identify the issue before ordering equipment.

4.13 Dispatch KM/KVM Architecture

Each dispatch position shall receive one dedicated hardware-based KM/KVM solution capable of supporting the four identified computer domains:

1. New Dispatch Domain PC.
2. Existing Sheriff's Department PC.
3. Existing Solacom PC.
4. Existing Mindshare PC.

Software-only switching utilities shall not be used as the primary KM/KVM mechanism.

The proposed system shall provide:

- hardware-based USB HID switching;
- reliable device emulation;
- wired keyboard/mouse connectivity;
- support for the required display configuration;
- audio switching where required;
- configurable target mapping;
- borderless or equivalent mouse-edge switching where supported;
- recovery from target-PC reboot without requiring physical reconnection;
- redundant or protected power where available; and
- documentation of all port assignments.

The contractor shall provide a detailed **Dispatch Console Signal Flow Diagram** showing:

- each PC;
- each monitor;
- each video connection;
- each USB connection;
- each audio connection;
- each KM/KVM port;
- each keyboard/mouse connection; and
- all adapters.

The final solution must be approved by the County before installation.

4.14 Jail Workstations

Jail Central

Quantity: **1**

The contractor shall provide:

- one Tier 1 workstation;
- one 24-inch or larger professional display;
- one heavy-duty monitor mount;
- one wired keyboard;
- one wired mouse.

Jail Standard

Quantity: **6**

The contractor shall provide:

- six Tier 2 workstations;
- six professional displays;
- six single-monitor mounts;
- six wired keyboards;
- six wired mice.

The contractor shall verify actual mounting locations during the site survey.

4.15 Wireless Peripheral Prohibition

Wireless, Bluetooth, RF, and battery-operated keyboard/mouse devices shall not be used at dispatch positions unless specifically approved in writing by the County.

All mission-critical dispatch keyboard/mouse connections shall use physical wired connections.

---

5. CYBERSECURITY, IDENTITY, AND COMPLIANCE

5.1 General Security Requirement

The contractor shall design the environment using defense-in-depth principles.

The solution shall comply with applicable CJIS requirements.

County-imposed security requirements in this RFP are supplemental requirements and shall not be represented as mandatory CJIS controls unless they are directly required by applicable CJIS policy.

5.2 New Active Directory Forest

The contractor shall establish a new Active Directory forest and domain.

The implementation shall not import legacy:

- domain administrator accounts;
- obsolete security groups;
- historical GPOs;
- undocumented service accounts;
- unnecessary trust relationships; or
- obsolete authentication configurations.

All migrated accounts shall be reviewed and recreated according to an approved County identity plan.

5.3 Active Directory Security

The environment shall include:

- secure administrative groups;
- role-based privileges;
- Group Policy;
- Microsoft security baselines;
- account lockout;
- password controls;
- auditing;
- privileged access controls;
- secure service accounts;
- restricted local administrator rights;
- secure DNS;

- time synchronization; and
- documented break-glass access.

NTLM shall be disabled or restricted to the greatest extent technically feasible.

Where a third-party application requires NTLM or another legacy authentication mechanism, the vendor shall document:

- application;
- reason;
- affected systems;
- security risk;
- compensating controls;
- proposed exception duration; and
- County approval.

No permanent exception shall be implemented without County approval.

5.4 Multi-Factor Authentication

Administrative access shall use MFA where supported.

The contractor shall propose a hardware-based or phishing-resistant MFA mechanism appropriate to the County environment.

The proposal shall identify:

- authentication technology;
- Windows integration;
- privileged access implementation;
- recovery process;
- emergency access;
- credential ownership;
- County administrator enrollment; and

- licensing requirements.

5.5 Logging and Monitoring

The solution shall maintain auditable logs for:

- administrative access;
- authentication;
- security events;
- firewall events;
- privileged operations;
- configuration changes;
- system failures;
- backup events;
- security alerts; and
- other events required by applicable policy.

Logs shall be time synchronized and protected from unauthorized modification.

5.6 Certificates and PKI

The contractor shall document all certificates used by:

- firewalls;
- servers;
- applications;
- VPNs;
- monitoring systems;
- NG911 interfaces; and
- other infrastructure components.

Documentation shall identify:

- certificate purpose;
- issuing authority;
- expiration date;
- renewal procedure;
- responsible owner.

County shall retain ownership/control of County-specific certificates and cryptographic keys.

---

6. SOFTWARE, VIRTUALIZATION, AND LICENSING

6.1 Virtualization Platform

The contractor shall provide an enterprise-supported virtualization platform compatible with the proposed two-host architecture.

The proposal shall identify:

- hypervisor;
- version;
- licensing;
- support;
- HA capability;
- live migration;
- storage multipathing;
- backup integration;
- management platform; and
- lifecycle/support dates.

6.2 Windows Server

The baseline operating system shall be Windows Server 2025 where supported by the applicable third-party applications.

Windows Server 2022 may be used where an identified application vendor requires it.

The bidder shall provide a complete Microsoft licensing schedule showing:

- product;
- edition;
- quantity;
- licensing model;
- physical-core calculations;
- VM allocations;
- failover rights;
- Software Assurance/subscription status where applicable;
- support dates.

The contractor shall certify that the proposed configuration is licensed under Microsoft's applicable licensing terms.

The County shall not rely solely on a contractor's narrative statement that a configuration is "fully licensed."

6.3 SQL Server

SQL Server shall be licensed using the licensing model recommended for the final architecture and applicable Microsoft terms.

If SQL Server Standard is proposed under a per-core model, the contractor shall provide:

- number of licensed cores;
- location of licensed workloads;
- failover licensing methodology;
- Software Assurance/subscription status;
- mobility rights where applicable;
- licensing calculations for host failure scenarios.

The contractor shall coordinate the proposed licensing model with Cushing Systems before final implementation.

6.4 Hardware Support

Compute, storage, network, firewall, and other mission-critical infrastructure shall include manufacturer-supported service plans for a minimum of five (5) years where commercially available.

The required support level shall provide:

- 24x7x365 technical support;
- four-hour on-site response for covered P1 hardware incidents;
- parts and labor;
- firmware/software support;
- escalation;
- advanced replacement where available.

The contractor shall provide a written **Keep Your Hard Drive (KYHD)** or equivalent media-retention agreement for applicable failed storage devices.

No failed storage device containing County data shall be removed from County custody without written County authorization.

---

7. THIRD-PARTY APPLICATION INTEGRATION

7.1 General Integration Responsibility

The infrastructure contractor is responsible for infrastructure engineering and coordination.

Third-party application vendors remain responsible for application-specific software configuration, application licensing, proprietary database migration procedures, and application functionality unless expressly included in the contractor's proposal.

The contractor shall maintain a written responsibility matrix.

7.2 INdigital ESInet Integration

The contractor shall coordinate with INdigital to establish the required network handoff.

The architecture shall support the applicable native IP/Ethernet interface.

Legacy serial-to-Ethernet conversion shall not be used unless specifically approved by the County and INdigital.

The contractor shall coordinate:

- VLANs;
- IP addressing;
- firewall rules;
- routing;
- certificates;
- security policies;
- redundant connectivity;
- monitoring;
- test procedures.

The contractor shall include sufficient engineering labor for joint validation with INdigital.

7.3 Cushing CAD

The contractor shall provide infrastructure for the Cushing CAD platform.

The CAD virtual machine shall receive approximately 5 TB of virtual storage, subject to confirmation during detailed design.

The contractor shall provide:

- VM;
- operating system;
- network connectivity;

- storage;
- backup;
- security;
- administrative access;
- database infrastructure as specified;
- coordination with Cushing.

Cushing shall remain responsible for application-specific CAD installation and application configuration unless otherwise stated in the final scope.

7.4 WTH Technology GIS

The contractor shall provide a dedicated VM for the WTH Think GIS platform.

The VM shall provide approximately 300–500 GB of allocated storage, subject to final application requirements.

The contractor shall coordinate migration of:

- application folders;
- GIS data;
- ALI Forwarder;
- required services;
- network configuration.

7.5 IDACS

The contractor shall provide one dedicated IDACS workstation and associated network infrastructure.

The contractor shall coordinate with the Indiana Office of Technology and applicable IDACS personnel.

The contractor shall provide infrastructure support necessary to permit approved IDACS integration with Cushing CAD.

All state-controlled security requirements shall take precedence where applicable.

7.6 CPC Lockdown

The contractor shall coordinate with CPC and Cushing to establish the required Lockdown server and web-client connectivity.

The contractor shall ensure all designated jail positions can reach the approved Lockdown portal.

7.7 Solacom and Mindshare

Existing Solacom and Mindshare systems shall remain operational unless replacement is specifically approved.

The contractor shall:

- document existing interfaces;
- integrate required network connections;
- integrate required KM/KVM functionality;
- coordinate with application/equipment vendors;
- avoid unauthorized configuration changes;
- validate functionality before final acceptance.

---

8. BACKUP, BUSINESS CONTINUITY, AND DISASTER RECOVERY

8.1 3-2-1 Backup Architecture

The solution shall implement a 3-2-1 backup architecture consisting of:

1. Production data;
2. Local backup copy; and
3. Offsite backup copy.

The architecture shall use at least two materially different storage locations/media types.

8.2 Local Immutable Backup Repository

The contractor shall provide a standalone backup repository.

The repository shall:

- be separated from production workloads;
- use a restricted administrative network;
- not rely exclusively on Active Directory authentication;
- support immutable backups;
- prevent unauthorized deletion;
- provide minimum thirty (30) days of immutable retention;
- provide monitoring;
- provide encryption;
- support backup verification.

8.3 Cloud Backup

The contractor shall configure backup replication to a County-owned and County-paid government cloud environment.

Examples include:

- AWS GovCloud (US);
- Azure Government; or
- another County-approved government cloud environment.

The County shall own the cloud tenant/account.

The contractor shall not establish the County's primary cloud backup environment under a contractor-owned tenant.

The solution shall support:

- customer-managed encryption keys where supported;
- US data residency;

- restricted administrative access;
- audit logging;
- MFA;
- immutable retention where supported;
- documented recovery procedures.

8.4 Recovery Objectives

The contractor shall propose and document:

- Recovery Point Objective (RPO);
- Recovery Time Objective (RTO);
- backup frequency;
- retention schedule;
- restoration priorities.

The County shall approve the final values before production implementation.

8.5 Restore Testing

The contractor shall perform documented restoration tests before final acceptance.

At minimum, testing shall include:

- file restoration;
- VM restoration;
- application-consistent restoration where supported;
- database restoration;
- backup repository recovery;
- cloud recovery.

The contractor shall provide test results.

---

9. IMPLEMENTATION, MIGRATION, RELOCATION, AND CUTOVER

9.1 General Approach

The County anticipates using an out-of-county emergency communications relocation period to reduce operational risk during implementation.

The anticipated relocation period is no more than one (1) week.

The contractor shall not assume that the one-week period is automatically sufficient.

The contractor shall submit a detailed schedule identifying all work that must occur during the relocation period.

The contractor shall maintain flexibility in scheduling the installation and implementation activities to accommodate the County's operational requirements and the availability of the designated alternate dispatch location. Installation dates and the final implementation schedule shall be coordinated with the County in advance to ensure continuity of emergency communications operations and minimize operational risk.**9.2 Fallback PSAP Readiness**

Before any local decommissioning activity begins:

- emergency call handling shall be confirmed operational at the fallback facility;
- administrative communications shall be confirmed;
- radio operations shall be confirmed;
- required CAD functionality shall be confirmed;
- County officials shall authorize local infrastructure work.

The contractor shall not begin decommissioning until the County provides written authorization.

9.3 Implementation Phases

Phase 1 – Discovery and Design

The contractor shall conduct a detailed site survey and produce:

- network design;
- rack elevation;
- power design;
- IP addressing plan;

- VLAN plan;
- firewall architecture;
- server/VM architecture;
- storage architecture;
- workstation plan;
- dispatch console design;
- KM/KVM signal-flow diagram;
- backup architecture;
- security architecture;
- migration plan;
- rollback plan.

Phase 2 – Procurement and Staging

Equipment shall be procured, inventoried, and staged.

All serial numbers and asset information shall be documented.

Phase 3 – Clean-Slate Build

The contractor shall install:

- rack;
- UPS;
- PDUs;
- switches;
- firewalls;
- compute;
- storage;
- backup;
- environmental monitoring;
- GPS time source.

Phase 4 – Core Configuration

The contractor shall configure:

- virtualization;
- storage;
- switching;
- routing;
- firewalls;
- AD;
- DNS;
- DHCP;
- security;
- monitoring;
- backup.

Phase 5 – Application Integration

The contractor shall coordinate with:

- INdigital;
- Cushing;
- WTH;
- IOT/IDACS;
- CPC;
- Solacom;
- JES & Sons (Vendor for Mindshare)

Phase 6 – Testing

All acceptance tests shall be completed before production cutover.

Phase 7 – Go-Live Authorization

The County shall determine whether the environment is ready for cutover.

Phase 8 – Cutover

The contractor shall execute the approved cutover plan.

Phase 9 – Stabilization

The contractor shall provide enhanced monitoring and support for a minimum of five (5) business days after cutover, or longer if specified in the final implementation plan.

Phase 10 – Final Acceptance

Final acceptance shall occur only after all required deliverables, tests, documentation, training, and punch-list items are complete.

9.4 Rollback Plan

The contractor shall provide a written rollback plan.

The plan shall identify:

- rollback triggers;
- decision authority;
- maximum acceptable outage;
- configuration restoration;
- DNS rollback;
- firewall rollback;
- network rollback;
- application rollback;
- database rollback;
- emergency communications fallback;
- responsibilities of County and third-party vendors.

The County EMA/911 Director shall retain final authority to authorize or abort production cutover.

10. ENGINEERING, CABLING, AND DOCUMENTATION

10.1 Cabling

All new network cabling shall be Cat6A or fiber as appropriate.

Cables shall be:

- professionally terminated;
- labeled at both ends;
- tested;
- documented;
- routed using appropriate cable management;
- separated according to system utility where appropriate.

10.2 Cable Labeling

Every cable shall be labeled at both ends using machine-printed, durable labels.

Labels shall identify:

- origin;
- destination;
- port;
- system/service.

10.3 Cable Testing

The contractor shall test all new copper and fiber infrastructure.

Test results shall be provided to the County.

10.4 Rack Documentation

The contractor shall provide a final rack elevation showing:

- equipment;
- U positions;
- PDUs;
- patch panels;
- cable-management devices;
- UPS;
- switches;
- firewalls;
- servers;
- storage;
- backup appliance;
- monitoring equipment.

10.5 Configuration Documentation

Final documentation shall include:

- IP address inventory;
- VLAN list;
- routing architecture;
- firewall rules;
- switch configurations;
- server configurations;
- VM inventory;
- storage mappings;
- backup configuration;
- AD structure;
- GPO inventory;

- privileged accounts;
- service accounts;
- certificates;
- licensing;
- support contracts;
- warranty information;
- asset inventory;
- cable matrix.

All final documentation shall be provided electronically in County-approved formats.

10.6 Legacy Media Sanitization

All legacy storage media removed from service shall be sanitized or destroyed according to the applicable County-approved media sanitization procedure and **NIST SP 800-88 Rev. 2**.

NIST SP 800-88 Rev. 2 was finalized in September 2025 and supersedes Rev. 1. It emphasizes selecting appropriate sanitization methods based on media type and sensitivity rather than relying on a universal overwrite count.

The contractor shall provide a serialized Certificate of Sanitization or Certificate of Destruction identifying:

- asset;
- serial number;
- media type;
- sanitization method;
- date;
- technician;
- verification method;
- disposition.

Traditional multi-pass overwrite shall not be required where an appropriate purge, cryptographic erase, or destruction method is more appropriate for the media technology.

---

11. ACCEPTANCE TESTING AND FINAL ACCEPTANCE

11.1 General

The contractor shall develop a detailed acceptance test plan.

No system shall be considered finally accepted solely because equipment has been installed.

11.2 Network Acceptance

Testing shall include:

- VLAN operation;
- routing;
- firewall rules;
- Internet/ESInet connectivity;
- redundant links;
- LACP;
- switch failover;
- firewall failover;
- DNS;
- DHCP;
- VPN;
- management access;
- logging.

11.3 Compute Acceptance

Testing shall include:

- host failure;
- VM migration;
- host reboot;
- management failure;
- network path failure;
- storage path failure;
- restoration of service after failure.

11.4 Storage Acceptance

Testing shall include:

- controller failure;
- storage path failure;
- disk failure;
- multipath operation;
- failover;
- recovery;
- performance validation.

11.5 Security Acceptance

Testing shall include:

- MFA;
- privileged access;
- GPO;

- account controls;
- logging;
- time synchronization;
- firewall policy;
- backup isolation;
- administrative access restrictions.

11.6 Backup Acceptance

Testing shall include:

- backup execution;
- immutability;
- retention;
- restore;
- cloud replication;
- recovery from local backup;
- recovery from cloud backup.

11.7 Dispatch Acceptance

Each dispatch position shall be tested for:

- all six displays;
- monitor arrangement;
- keyboard;
- mouse;
- KM/KVM;
- PC selection;
- audio;

- Solacom connectivity;
- Mindshare connectivity;
- Sheriff's PC connectivity;
- New Dispatch PC connectivity;
- recovery after target PC reboot.

11.8 911/ALI Acceptance

Testing shall be performed in coordination with INdigital and applicable application vendors.

Testing shall verify:

- connectivity;
- ALI delivery;
- CAD receipt;
- firewall behavior;
- redundancy;
- failover;
- logging;
- error handling.

Only authorized test procedures shall be used for emergency communications testing.

11.9 Acceptance Test Documentation

Each test shall include:

Field	Requirement
Test ID	Unique identifier
System	System being tested
Procedure	Test procedure
Expected Result	Required result
Actual Result	Observed result
Pass/Fail	Result
Witness	County/vendor witness
Date	Test date
Corrective Action	If failed

All failed tests shall be corrected and retested.

11.10 Final Acceptance

Final acceptance shall require:

- successful completion of acceptance testing;
- completion of punch-list items;
- final documentation;
- license documentation;
- support documentation;
- warranty documentation;
- credential transfer;

- backup verification;
- training;
- asset inventory;
- media certificates;
- County approval.

Final acceptance shall be documented in writing.

---

12. POST-IMPLEMENTATION SUPPORT AND SERVICE LEVELS

12.1 Support

The contractor shall provide Tier-3 engineering support for:

- servers;
- virtualization;
- storage;
- network;
- firewalls;
- Active Directory;
- DNS;
- backup;
- infrastructure security;
- supported workstation infrastructure.

Third-party application support shall remain subject to the responsibility matrix.

12.2 Incident Classification

P1 – Critical Emergency

Examples include:

- complete CAD outage;

- loss of required emergency call/ALI functionality;
- failure of both perimeter firewalls;
- failure of core switching;
- catastrophic infrastructure failure;
- event causing dispatch shutdown or life-safety risk.

Remote response: within one (1) hour, 24x7x365.

On-site response: within four (4) hours of County incident notification.

P2 – Major Degradation

Examples:

- single compute host failure where HA remains operational;
- single SAN controller failure;
- loss of redundancy;
- localized workstation failure;
- significant non-life-safety degradation.

Remote response: within two (2) hours, 24x7x365.

On-site: next business day if remote remediation is unsuccessful, unless otherwise agreed.

P3 – Routine

Examples:

- routine configuration;
- account creation;
- non-critical GPO changes;
- preventative maintenance;
- standard technical questions.

Response: within four (4) business hours.

12.3 P1 On-Site Requirement

The contractor shall maintain resources capable of providing four-hour physical on-site response to the Parke County PSAP.

The contractor shall identify:

- primary engineer;
- backup engineer;
- service location;
- travel distance;
- emergency contact number;
- escalation manager;
- after-hours procedure.

12.4 SLA Remedies

The final contract may provide for liquidated damages or other remedies for failure to meet mandatory P1 on-site response requirements.

Any liquidated-damages provision shall be subject to review and approval by County counsel and shall establish appropriate exclusions, including circumstances outside the contractor's reasonable control.

If approved, the County may assess a liquidated amount of **$500 per hour or fraction thereof** for failure to meet the contractual P1 on-site arrival requirement, subject to the final executed agreement.

13. WARRANTY, MAINTENANCE, AND RENEWAL PRICING

13.1 Base-Year Support

The proposal shall include twelve (12) months of post-cutover support beginning on the date of final acceptance.

Base-year support shall include:

- 24x7x365 P1 support;
- four-hour P1 on-site response;
- remote support;
- manufacturer escalation;
- covered firmware/software support;
- configuration assistance;
- troubleshooting.

13.2 Renewal Pricing

The bidder shall provide firm pricing for Years 2–5 as requested in the Pricing Schedule.

The County's obligation to exercise any renewal shall be subject to:

- applicable law;
- County approval;
- appropriation;
- satisfactory contractor performance;
- executed renewal documentation.

Any multi-year commitment shall be structured in accordance with applicable Indiana law and County policy.

13.3 Price Escalation

The bidder shall identify all proposed annual price changes.

Unless otherwise approved in the final contract, renewal pricing shall not increase by more than three percent (3%) annually.

The bidder shall provide firm pricing for all hardware maintenance, software support, subscriptions, and services required to maintain the proposed solution.

13.4 Project Warranty

The contractor shall provide a minimum twelve-month workmanship/implementation warranty beginning on final acceptance.

During the warranty period, the contractor shall correct implementation defects at no additional cost.

Manufacturer warranties remain in addition to the contractor's project warranty.

---

14. DATA OWNERSHIP, SECURITY, AND CONFIDENTIALITY

14.1 Data Ownership

All County data, records, configurations, logs, documentation, credentials, certificates, and information generated or maintained under this project shall remain the exclusive property of Parke County to the extent permitted by law.

14.2 Unauthorized Use

The contractor shall not:

- sell County data;
- use County data for advertising;
- use County data for unrelated analytics;
- disclose County data;
- transfer County data to unauthorized parties;
- use County data to train external AI/ML systems;

without written County authorization.

14.3 Credential Ownership

The County shall own and control:

- domain administrator accounts;

- firewall administrative accounts;
- cloud accounts;
- backup accounts;
- encryption keys;
- certificates;
- infrastructure management accounts;
- break-glass credentials.

Vendor personnel may receive delegated access as necessary to perform contractual duties.

14.4 Security Incident Notification

The contractor shall notify the County promptly upon discovery of:

- unauthorized access;
- suspected compromise;
- ransomware;
- malware affecting County systems;
- credential compromise;
- unauthorized disclosure;
- loss of County-controlled media;
- cybersecurity incident affecting County data.

The contractor shall preserve evidence and cooperate with County investigation.

14.5 Data Return and Destruction

Upon contract termination or completion, the contractor shall return or securely destroy County data as directed by the County and applicable law.

Upon request, the contractor shall provide a written certificate documenting destruction.

---

15. PROPOSAL REQUIREMENTS

Each proposal shall contain the following sections.

15.1 Executive Summary

Describe:

- proposed solution;
- project approach;
- major differentiators;
- public-safety experience;
- support model.

15.2 Company Information

Provide:

- legal company name;
- address;
- years in business;
- ownership;
- primary contact;
- relevant certifications;
- financial/organizational qualifications.

15.3 Technical Proposal

Include:

- architecture;
- compute;
- storage;
- network;
- firewall;
- security;

- virtualization;
- workstation;
- KM/KVM;
- backup;
- cloud;
- monitoring.

15.4 Integration Plan

Describe coordination with:

- INdigital;
- Cushing;
- WTH;
- IOT/IDACS;
- CPC;
- Solacom;
- JES & Sons (Vendor for Mindshare).

15.5 Migration Plan

Provide:

- schedule;
- staffing;
- relocation plan;
- cutover plan;
- rollback plan;
- testing plan.

15.6 Support Plan

Provide:

- support organization;

- P1 escalation;
- engineer locations;
- response process;
- subcontractors;
- manufacturer escalation.

15.7 Compliance Matrix

The bidder shall complete Appendix C.

Any exception shall be clearly identified.

Failure to identify an exception may result in the County treating the bidder as having committed to meet the requirement.

15.8 References

Provide at least three comparable references.

15.9 Pricing

Provide all pricing using Appendix D.

All required equipment, licenses, labor, travel, installation, configuration, testing, documentation, training, and support shall be included unless explicitly identified as an optional item.

---

16. EVALUATION AND AWARD

The County intends to evaluate proposals using the following 100-point structure.

Category	Points
Technical Architecture and Resiliency	25
Cybersecurity, Identity, and Compliance	20
Migration, Integration, and Project Management	20
Public-Safety Experience and Qualifications	10

Support, P1 Response, and Service Model	10
Price and Total Cost of Ownership	15
Total	**100**

16.1 Technical Architecture – 25 Points

Evaluation will consider:

- compute;
- storage;
- network;
- firewall;
- resiliency;
- power;
- workstation architecture;
- dispatch console design;
- scalability;
- maintainability.

16.2 Cybersecurity – 20 Points

Evaluation will consider:

- CJIS alignment;
- AD architecture;
- MFA;
- privileged access;
- logging;
- backup security;
- encryption;
- certificate management;

- incident response.

16.3 Migration and Integration – 20 Points

Evaluation will consider:

- migration methodology;
- fallback strategy;
- rollback;
- third-party coordination;
- testing;
- cutover planning;
- project schedule.

16.4 Experience – 10 Points

Evaluation will consider:

- PSAP experience;
- NG911 experience;
- Indiana experience;
- similar project references;
- personnel qualifications.

16.5 Support – 10 Points

Evaluation will consider:

- four-hour P1 response;
- staffing;
- escalation;
- geographic capability;
- manufacturer support.

16.6 Price – 15 Points

Price evaluation shall consider:

- initial project cost;
- Year 2–5 support;
- licensing;
- subscriptions;
- hardware support;
- cloud costs;
- total cost of ownership.

The County may evaluate total five-year cost rather than first-year cost alone.

16.7 Mandatory Responsiveness Requirements

The County may deem a proposal nonresponsive if the bidder:

- fails to submit required pricing;
- fails to provide required references;
- fails to provide a completed compliance matrix;
- cannot demonstrate required P1 response capability;
- refuses a mandatory requirement without an identified exception;
- materially alters the required scope;
- fails to provide required certifications;
- submits materially incomplete information.

---

17. GENERAL PROCUREMENT AND CONTRACT REQUIREMENTS

The final contract shall contain, as applicable:

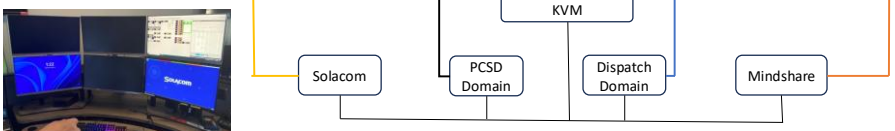
- applicable Indiana law;
- County procurement requirements;
- insurance;
- indemnification;

- confidentiality;
- cybersecurity requirements;
- data ownership;
- public-records provisions;
- termination;
- dispute resolution;
- force majeure;
- assignment;
- subcontracting;
- change control;
- payment terms;
- appropriation requirements;
- warranty;
- audit rights;
- records retention;
- compliance with applicable laws;
- non-discrimination requirements;
- applicable federal/state grant requirements.

APPENDIX A

DISPATCH AND JAIL WORKSTATION DIAGRAMS

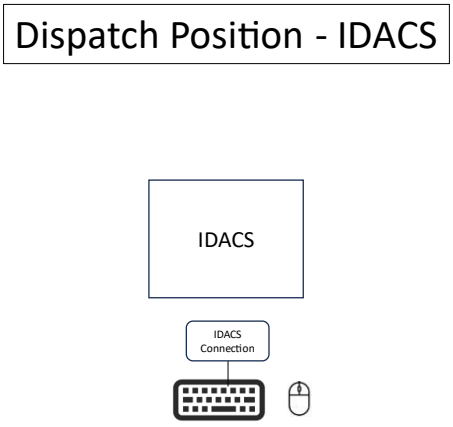
There are three workstations (positions) in the dispatch.



Example Screen Set Up

Contractor will be responsible for the following equipment:

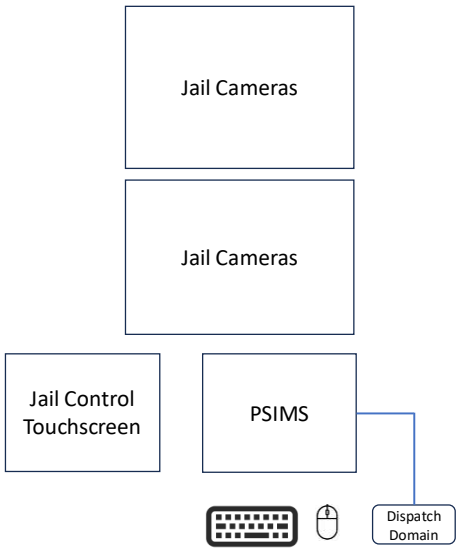
- Terminal PC on the new dispatch domain.
- KVM that connects the 4 PCs with a trackball mouse and keyboard.
- Furniture to mount the six monitors.
- The four monitors (Auxiliary, PCSO Body Cams Map, GIS, and CAD).



Contractor will be responsible for the following equipment:

- PC on IDACS integrated with PSIMS.
- Furniture to mount the one monitor.
- The one monitor.

Jail Position - Central



Contractor will be responsible for the following equipment:

- PC on the new dispatch domain. Same capabilities as the dispatch PC.
- Furniture to mount the one monitor.
- The one monitor (PSIMS).

Jail Position - Standard

Positions

Matron

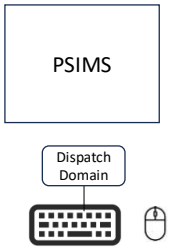
Reports

Commander

Book-In 1

Book-In 2

Satellite



Contractor will be responsible for the following equipment:

- PC on the new dispatch domain. Lessor capabilities than the dispatch and Jail Central PCs.
- Furniture to mount the one monitor.
- The one monitors (PSIMS).
- There are six positions within the Jail.

APPENDIX B

CABLE COLOR AND IDENTIFICATION STANDARD

The contractor shall use the following cable-color scheme unless the County approves an alternative.

Color	**System/Function**
Yellow	911 / INdigital / Call Handling
Gray	IDACS / IOT
Black	Jail Operations / Administrative Phones / Radio as specifically designated
Green	Local Administrative Network
White	Radio Console / Mindshare where designated
Red	County-designated critical or special-purpose connections
Blue	**Do Not Use for New Infrastructure Unless Approved in Writing**

The contractor shall provide a final cable-color legend with the as-built documentation.

Cable color shall not be relied upon as the sole identification method; every cable shall also be labeled at both ends.

APPENDIX C

MANDATORY BIDDER COMPLIANCE MATRIX

RFP Section	Requirement	Comply?	Exception	Make/Model	Supporting Documentation
4.2	Two HA compute hosts				
4.3	15 TB usable shared storage				
4.4	Redundant Layer 3 switching				
4.5	Redundant NGFW				
4.6	42U lockable rack				
4.7	GPS NTP				
4.8	Environmental monitoring				
4.9	11 workstation PCs				
4.12	12 new dispatch displays				
4.13	Hardware KM/KVM				
5.2	New AD forest				
5.4	MFA				
6.2	Windows licensing				
6.3	SQL licensing				
6.4	Five-year hardware support				

7.2	Cushing integration				
7.3	WTH integration				
7.4	IDACS				
7.6	Solacom/Mindshare				
8.2	Immutable local backup				
8.3	County-owned cloud backup				
9	Migration/cutover				
11	Acceptance testing				
12	P1 four-hour response				
13	Five-year pricing				

APPENDIX D

PRICING SCHEDULE

The bidder shall provide fixed pricing for all required components.

D.1 Capital Project

Category	Quantity	Unit Price	Extended Price
Compute Hosts	2		
Shared Storage	1		
Core Switches	2		
Firewalls	2		
Rack	1		
Rack UPS	1		
Rack PDUs	2		
GPS/NTP	1		
Environmental Monitoring	1		
Backup Appliance	1		
Tier 1 PCs	4		
Tier 2 PCs	6		
Tier 3 PC	1		
Dispatch Displays	12		
Jail Displays	7		
Dispatch Mounts	3		

Jail Central Mount	1		
Jail Standard Mounts	6		
KM/KVM Systems	3		
Keyboards	11		
Mice	11		
Cabling	Allowance		
Software/Licensing			
Professional Services			
Training			
Documentation			
Other			
Capital Project Total			

D.2 Support

Year	**Fixed Annual Price**
Year 1	Included
Year 2	
Year 3	
Year 4	
Year 5	

D.3 Optional Items

All optional items shall be separately identified and shall not be included in the mandatory project total.

APPENDIX E

ACCEPTANCE TEST MATRIX

Test ID	Category	Test	Expected Result	Pass/Fail
NET-01	Network	VLAN validation	All VLANs operational	
NET-02	Network	Switch failover	Required services remain operational	
FW-01	Firewall	HA failover	Required sessions/services recover as designed	
STG-01	Storage	Controller failure	Storage remains available	
STG-02	Storage	Path failure	Multipath continues	
VM-01	Compute	Host failure	VMs recover/migrate as designed	
SEC-01	Security	MFA	Unauthorized access prevented	
SEC-02	Security	Privileged access	Least privilege enforced	
BAK-01	Backup	Backup execution	Backup completes	
BAK-02	Backup	Restore	Data restored successfully	
BAK-03	Backup	Immutability	Protected backup cannot be improperly deleted	
DSP-01	Dispatch	Six displays	All displays operational	
DSP-02	Dispatch	KM/KVM	All four targets accessible	
DSP-03	Dispatch	Mouse-edge switching	Target selection operates as designed	
CAD-01	CAD	CAD startup	Application operational	
CAD-02	CAD	Database	Database accessible	

GIS-01	GIS	GIS application	Operational	
ALI-01	911	ALI test	Authorized test delivered correctly	
IDACS-01	IDACS	Connectivity	State-approved connectivity operational	
PWR-01	Power	UPS	Required equipment remains powered	
PWR-02	Power	PDU path	Redundant PSU equipment operates as designed	
ENV-01	Monitoring	Temperature alarm	Alert generated	
NTP-01	Time	NTP	Systems synchronize correctly	
DOC-01	Documentation	Final documents	Complete and accurate	

APPENDIX F

COUNTY-FURNISHED EQUIPMENT AND SITE INFORMATION

Item	County Furnished	Contractor Furnished	Existing/Reused
Solacom			Yes
Mindshare			Yes
Sheriff's PC			Yes
Existing Dispatch Displays		Yes	
Existing Jail Equipment			Yes
ESInet Connection			Yes
Internet Service			Yes
Electrical Circuits			Yes
Generator			Yes
ATS			Yes
Network Pathways		Yes	
Roof Access		Yes	
GPS Antenna Location		Yes	
Physical Security			Yes

The County shall provide available site drawings, electrical information, existing equipment inventories, and known third-party application information to qualified offerors under the County's established solicitation procedures.

APPENDIX G

VENDOR PROJECT STAFFING AND REFERENCES

G.1 Key Personnel

Role	Name	Years Experience	Certification	Availability
Project Manager				
Network Engineer				
Systems Engineer				
Security Engineer				
Microsoft Engineer				
Backup/DR Engineer				
P1 Engineer				

G.2 References

Reference 1

Customer:
Location:
Project:
Completion Date:
Project Value:
Technologies:
Contact:
Phone:
Email:

Reference 2

Customer:
Location:
Project:
Completion Date:

Project Value:
Technologies:
Contact:
Phone:
Email:

Reference 3

Customer:
Location:
Project:
Completion Date:
Project Value:
Technologies:
Contact:
Phone:
Email: