Questions & Answers #5

(Deadline for Questions 09/09/2026 @ 3:00pm EST)

Q&A 3, Answer 30 (Section Reference Correction)
Question 30 of Q&A 3 contains a typographical error in the answer. The answer references "Section 3.11" twice when describing the location of the FSA administrative fee. The correct section is Section 3.21. Amendment #1 correctly references Section 3.21. The fee rate clarification in Answer 30 remains valid — only the section number citation is incorrect. Evaluators should read all references to "Section 3.11" in Answer 30 as "Section 3.21." -mt

50. Battery life, weatherproofing, repair depots (3.9.1, 3.12.1, 4.10.5.2) We have none of these, because we ship nothing physical, and Section 3.1 says software-only bids are welcome. How would you like us to answer them? And how do you score the 50 points at 4.10.5.2 for a software company? Not applicable, scored on the software equivalents such as encryption and uptime, or zero?

Answer: Pursuant to Amendment No. 2, Proposers offering SaaS or software-only solutions in Category 5 may mark physical hardware requirements as "N/A – Software-Only Solution." Under amended Exhibit C (4.10.5.2), evaluators will score software-only submissions based on software reliability equivalents—including cloud availability SLAs, infrastructure redundancy, disaster recovery failover, and encryption standards—ensuring full scoring eligibility without penalty.

51. Evaluation Scenario D (3.14.10) Scenario D says AI analytics belongs here, then asks us to price ten sensor sites with mounting hardware and gateways. We have nothing to mount. Can we price an equivalent software deployment instead, such as an agency of a stated size, and explain the swap without being marked down for it?

Answer: For Evaluation Scenario D (10 Sensor Sites), software-only or SaaS Proposers shall enter their software platform or site/endpoint license fees for the 10 sites and enter $0.00 or "Included" for physical mounting hardware and gateways. Proposers should include a brief explanatory note in their pricing submission detailing the SaaS licensing structure for the 10 sites.

52. **How an empty category is scored (3.14.4, 4.10.6.2) Q&A #26 confirms the six percentages are weighting factors rather than minimum discounts, and Q&A #29 confirms that for software the anchor quantities mean per-license or per-user tiers. Neither answers what happens to a category a bidder does not offer at all. The two hardware categories are 45 percent of the weighting, and we sell no hardware, so we would leave them blank. Do you average only the categories a company actually bids? Or does a blank count as offering a zero percent discount? This one affects our pricing more than anything else here.**

    Answer: Pursuant to Amendment No. 2, leaving non-applicable hardware categories blank (or marking them "N/A") does not count as a 0% discount and will not penalize software-only Proposers. Non-applicable categories are excluded from the Proposer's TCO scoring denominator, weighting the financial score strictly across the software, services, and training categories actually bid.

53. FIPS and CJIS (3.9.2) Two related things. Cloud software generally cannot hold its own FIPS encryption certificate. Ours uses FIPS-validated encryption from Amazon Web Services, and we can document that. Is that enough? Separately, the FBI does not certify vendors against the CJIS Security Policy. No such certificate exists. Would a signed CJIS Security Amendment, our control checklist mapped to the current policy, staff background screening records, our SOC 2 audit, and independent penetration tests satisfy this?

Answer: Regarding FIPS: Proposers may reference cloud infrastructure control inheritance (e.g., AWS FIPS-validated cryptographic modules) to satisfy underlying infrastructure requirements; however, inherited cloud controls do not automatically constitute full application-level CJIS compliance. Valid NIST/FIPS cryptographic module validation certificate numbers must be explicitly provided in the security submission.

Regarding CJIS: The FBI does not issue vendor-level CJIS certifications. A combination of supporting documents — including a signed CJIS Security Amendment, a control checklist mapped to the current CJIS Security Policy, staff background screening records, a SOC 2 Type II audit, and independent penetration tests — collectively satisfies the CJIS documentation requirement for proposal evaluation purposes. Submission of all listed documents is not required simultaneously; a SOC 3 report may be submitted in lieu of a SOC 2 Type II at the proposal stage, with HCSO reserving the right to request the full SOC 2 Type II during evaluation. HCSO will execute a standard NDA to facilitate that review if needed.

Security documentation requirements also vary by solution type: CJIS audit reports, SOC 2 Type II, and FIPS certifications are mandatory for DEMS and BWC systems, but may be marked "N/A" for standalone environmental or situational sensors that do not store or transmit CJI.

Important note: This contract is a cooperative purchasing vehicle. Execution of a CJIS Security Amendment and any required background checks with the applicable Eligible Purchaser are required prior to any vendor personnel being granted access to CJI — but only at the supplemental agreement or local Purchase Order level, not as a pre-award condition of the Master Agreement itself. Full CJIS compliance obligations are fulfilled through individual supplemental agreements with each Eligible Purchaser.

54. Keeping our security reports out of the public record (2.5.4, 5.23) Our SOC 2 and penetration test reports describe how our defenses are built. We normally release them only under a non-disclosure agreement, and publishing them would create a security risk. How would you like us to get them to the evaluation committee? In the unredacted copy only, or another way?

Answer: Proprietary security audits, SOC 2 reports, and penetration tests should be submitted using the Two-Copy Submission Method. Proposers must include the unredacted report in their *Master Unredacted Submission* and include a redacted version (clearly labeled *"Confidential - System Security / Trade Secret"* pursuant to Florida Chapter 119 exemptions) in their *Redacted Public Copy*.

55. Do proposers need to provide three general references that cover as many of the categories as possible, or do proposers need to provide a minimum of three references from the last two year per proposed category?

Answer: Proposers need to provide a minimum of three (3) general professional references total for their overall proposal submission. Proposers are not required to provide three separate references per proposed category. (Note: Per Amendment No. 2, the 2-year utilization threshold is waived for Category 5 AI solutions).

56. Could HCSO confirm which of the 5 categories the Fixed and Mobile surveillance solution fits within?

Answer: Fixed and mobile physical surveillance hardware (cameras, trailers, license plate recognition hardware, sensors) fits primarily under Category 1 (Primary Hardware Ecosystems) or Category 2 (Peripherals & Accessories). Software platforms powering fixed or mobile surveillance fit under Category 3 (Software & SaaS Platforms) or Category 5 (Emerging AI & Predictive Analytics).

57. **Section 4.10.6 / 3.14 – TCO Package and Category Discount Table: The solicitation's discounting model evaluates pricing based on a firm-fixed percentage discount off MSRP by subcategory. Some third-party OEM components integrated into a Proposer's turn-key solutions (e.g., certain sensor, radar, or mitigation hardware) are subject to manufacturer resale restrictions that prohibit line-item discounting, even though the Proposer may offer significant bundled/package pricing when those components are sold as part of an integrated solution SKU.**
    Can HCSO confirm whether the evaluation criteria will recognize and credit bundled or package-level pricing value (i.e., the effective savings realized when hardware, software, and services are procured together as a single integrated solution) as a distinct scored component — separate from, or in addition to, the per-subcategory MSRP discount calculation in Section 4.10.6? If not currently addressed, would HCSO consider clarifying or amending the scoring methodology to account for bundled pricing structures where individual component discounting is contractually restricted by the OEM?

    Answer: Proposers must offer a firm-fixed base percentage discount off MSRP for each awarded subcategory to establish the ceiling contract rate. However, bundled or package-level pricing value is recognized and evaluated via the Mock Quote and Mock Invoice under the TCO Verification Package. Proposers may offer integrated solution SKUs or bundled discounts, provided that every individual component within the bundle meets or exceeds the awarded category discount ceiling.

58. **The solicitation states that HCSO will award contracts based on "Minimum Guaranteed Category Discounts" under a Category-Based Discount Model, rather than fixed SKU-level pricing.**
    Please define "Minimum Guaranteed Category Discounts" — specifically, how categories will be defined, how the minimum discount percentage will be established/verified, and against what baseline MSRP will be measured over the 5-year term.Will the evaluation/scoring methodology account for packaged or bundled pricing that a vendor may propose as a custom solution tailored to an individual agency's needs, or will scoring be based solely on the category discount percentage applied to individual SKUs at MSRP?If bundled/custom pricing is permitted, how will it be normalized or weighted against the standard category-discount pricing for scoring purposes, so that agencies can meaningfully compare bundled offers to standard catalog discount offers?

    Answer: Minimum Guaranteed Category Discounts" represent the binding minimum percentage discount applied off a manufacturer's published MSRP or official commercial list price. Scoring for Relative Financial Value (Section 4.10.6.2) is based on the category discount percentage table. Bundled packages are permitted for agency task orders post-award, provided the bundled price offers savings equal to or greater than the awarded catalog discount rates.

59. Appendix II – TCO Verification Spreadsheet Template: We have identified a discrepancy between the Evaluation Scenario(s) described in the RFP document (Section 3.14) and the corresponding pricing/response structure in the Appendix II template as issued. Can HCSO confirm whether an updated version of Appendix II will be issued to reconcile the scenario details with the pricing package structure, and if so, provide an anticipated release date or Amendment number? If no update is planned, please clarify how Proposers should resolve the discrepancy between the two documents when completing their submission.

Answer: An updated Appendix II TCO Verification Spreadsheet Template will be issued via Amendment No. 2 on DemandStar and teamHCSO.com to ensure exact alignment between Section 3.14 scenario descriptions and spreadsheet tabs.

60. Section 4.10.6 (MSRP List / Catalog Attestation) references a "link to a verifiable MSRP list" and Section 3.14.6 states that suppliers are responsible for "providing and maintaining a current published MSRP" throughout the contract term, consistent with the "living document" intent of the Category Discount model. Our organization does not maintain a publicly hosted, continuously updated MSRP catalog. We are able to provide a current MSRP catalog as a standalone file (e.g., Excel/PDF) at the time of proposal submission and at intervals thereafter upon request, but this would not function as a live, continuously accessible public link.
Can HCSO confirm whether a periodically-updated standalone catalog file (submitted directly to HCSO/FSA and refreshed at defined intervals) satisfies the "MSRP List / Catalog Attestation" requirement, in lieu of a publicly hosted, real-time catalog link?

Answer: Pursuant to Amendment No. 2, Proposers who do not maintain a live public web link may submit their official published MSRP catalog as a standalone digital file (searchable Excel or PDF) with their proposal package. Contractors will be required to provide refreshed catalog files to an Eligible Purchaser upon request at time of subsequent orders requests or quotation for a statement of work.

61. Please clarify whether the cooperative intends to establish awards with multiple qualified vendor based on operational reliability, interoperability, transparency, demonstrated performance, and overall value, thereby allowing Eligible Purchasers to select the solution that best meets their operational requirements; or is the intended procurement model to award primarily by price?

Answer: As clarified in Q&A #4 (Answer 41), HCSO intends to establish multiple vendor awards across categories to provide Participating Entities with a comprehensive catalog of reliable, interoperable solutions. This is a best-value procurement; awards are made to all responsive and responsible Proposers scoring 70% (700 points) or higher across all technical, operational, and financial criteria.

62. **Pricing represents 40% of the overall evaluation, while Technical Specifications—including reliability, MTBF, and security—represent a substantially smaller portion of the available points. Please clarify how the evaluation methodology will ensure that a proposal offering stronger documented reliability,field performance, service, and lifecycle value is appropriately differentiated from a lower-priced proposal that may not provide the same level of operational capability or total cost of ownership?**

    Answer: The evaluation methodology ensures strong differentiation across both operational excellence and financial structure by strictly dividing qualitative evaluation from mathematical pricing calculations:

- **Evaluation Committee Focus (600 Points / 60%):** The Evaluation Committee evaluates operational capability, reliability, and lifecycle value across five non-price sections totaling 600 points. Technical Specifications & Security (4.10.5) represents 90 points of this score, evaluated alongside Corporate Stability & Past Performance (4.10.1 - 100 pts), Ability to Sell & Deliver (4.10.2 - 150 pts), Operations & Logistics (4.10.3 - 100 pts), and Innovation (4.10.4 - 100 pts). High technical performance and field history directly differentiate superior platforms across these 600 points.
- **Financial Evaluation Mechanics (400 Points / 40%):** The Evaluation Committee does not score price tags, equipment costs, or Total Cost of Ownership (TCO) packages. The 400-point TCO package is evaluated separately by HCSO Financial Services Division (FSD) using objective mathematical formulas and audit criteria set forth in Exhibit C (4.10.6):
    - **Financial Transparency & Auditability (150 Points):** Evaluates fee disclosure, Unit of Measure simplicity, and exact consistency between the Mock Quote, Mock Invoice, and narrative descriptions.
    - **Relative Financial Value (250 Points):** Evaluates discount depth relative to MSRP within awarded categories, quantity-tiered anchor discounts, and documented price stability terms (e.g., firm-fixed 5-year pricing).
- **Best Value Overall:** Because 600 of the 1,000 total available points are awarded strictly for qualitative and technical excellence, a proposal offering deep discounts cannot overcome significant deficiencies in reliability, field performance, or operational capability.

63. **What evidence will the Evaluation Committee require to substantiate vendor claims regarding reliability, MTBF, uptime, durability, and field performance? Will technical performance claims be subject to a verification or evidentiary standard comparable to the line-item audit requirements applicable to pricing under Section 4.10.6.1?**

    Answer: Technical performance claims (uptime, MTBF, security compliance) must be substantiated in the proposal by submitting objective documentation, including SOC 2 Type II audit reports, third-party penetration tests, sample SLAs, and verified customer references. Evaluators score Technical Specifications and Security (4.10.5) strictly based on provided third-party documentation rather than self-attestation.

64. **Before a cooperative contract becomes available for statewide use, does HCSO intend to conduct a pilot, trial deployment, demonstration, or proof-of-concept with the highest-ranked Proposer(s) to validate operational reliability, interoperability, usability, and performance under representative conditions? If so, please describe how results would inform the final award decision.**

    Answer: As clarified in Q&A #1 (Answer 6), live demonstrations, pilots, or proof-of-concept evaluations will not be conducted by the Evaluation Committee during the RFP evaluation or BAFO process. However, post-award, participating local agencies may request pilot or proof-of-concept demonstrations directly from awarded vendors prior to issuing local purchase orders.

65. **Beyond the SLAs identified in Section 4.10.3, what mechanisms will be used to monitor and enforce operational performance throughout the contract term? Please clarify whether the cooperative anticipates recurring performance reviews, reliability reporting, remedies for missed SLAs, corrective-action requirements, or other mechanisms that allow performance to remain an active component of vendor accountability after award.**

    Answer: Post-award contract performance is monitored and enforced at the local agency level through binding Service Level Agreements (SLAs) executed under Participating Addenda or Purchase Orders. Remedies for missed SLAs—including service credits, cure notices, and contract termination for default—are governed by Section 2.15 and local purchasing agreements.

66. **Section 4.10.6.2 scores Relative Financial Value based on discount depth and price stability. Please clarify whether this criterion is intended to assess price competitiveness alone or whether it will also consider operational performance, reliability, service/support, lifecycle costs, and other factors that materially affect value over the term of the agreement?**

    Answer: Section 4.10.6.2 strictly evaluates financial competitiveness (discount depth, category discounts, quantity tiers, and price stability). Operational performance, reliability, and service quality are evaluated separately under Section 4.10.2 (Ability to Sell & Deliver), Section 4.10.3 (Operations & Logistics), and Section 4.10.5 (Depth & Breadth of Solutions).

67. Where one Proposer can demonstrate a longer and more substantial record of successful deployments at a comparable scale, while another offers lower pricing but more limited field history, how will the Evaluation Committee account for the relative operational risk and demonstrated performance of each solution in determining overall best value?

Answer: The evaluation methodology strictly separates qualitative technical review from pricing evaluation to ensure objective scoring:

- **Evaluation Committee Focus (600 Points / 60%):** The Evaluation Committee evaluates non-price categories strictly on technical merit, operational capability, and risk. The committee does not evaluate or score the financial TCO package. A vendor with limited field history, unproven deployment scale, or weak references will receive lower scores in Corporate Stability & Performance (4.10.1.1), Past Performance (4.10.1.4), and Technical Specifications (4.10.5), directly reflecting their higher operational risk.
- **Independent TCO Evaluation (400 Points / 40%):** Pricing models and discount tables are evaluated independently using the objective mathematical formulas set forth in Section 4.10.6.
- **Best Value Determination:** Total scores are calculated by combining the committee's independent technical scores with the calculated financial scores. High technical performance and proven operational reliability are heavily weighted (600 points) to ensure that a low price alone cannot compensate for unverified performance or high deployment risk.

68. Section 2.1 states that the solicitation's intent is to provide solutions for the "entire ecosystem of the offering, from physical sensors to the analytical software," and prioritizes "comprehensive, end-to-end solutions" over single-point or piecemeal technologies. Given this stated preference for holistic, fully-integrated ecosystems: Can Proposers offer packaged/bundled solutions that include products or components outside the specific Technology Ecosystem Category (CAT 1–5) being bid, where those additional products support the same operational use case and contribute to a more complete, mission-ready deployment for the Eligible Purchaser? For example, a Proposer may wish to include complementary hardware or software from an adjacent category as part of a single cohesive package to eliminate integration gaps, reduce the number of vendors an agency must manage, and lower total lifecycle cost through consolidated pricing. If cross-category bundling is permitted, please confirm how such packages should be represented in the TCO Verification Spreadsheet (e.g., whether the out-of-category components should be listed under their native category's Discount Table, or attached as a supplemental line within the primary category being bid) so that the cost savings and operational benefit of the holistic package are accurately captured for evaluation purposes.

Answer: Yes, Proposers may include complementary products from adjacent categories to deliver a complete, integrated solution. Out-of-category hardware or software components must be listed under their native Discount Category Table (e.g., hardware under Category 1, software under Category 3) so that appropriate category discounts apply. The complete bundled package price and operational cost savings should be explicitly demonstrated in the Mock Quote and Mock Invoice schedules within the TCO Verification Package. At no time should a quotation provided to an eligible purchaser for a bundled package exceed the price if individual category discounts had been applied.

69. For a category-specific or component-based proposal, will the five-year public-safety experience requirement and the three references using the proposed solution for at least two years be evaluated at the prime-proposer level only, or may qualifying experience and references from an affiliated company, approved subcontractor, or OEM partner be used?

Answer: Yes. While the Prime Proposer maintains ultimate legal, administrative, and performance responsibility under the contract, experience and references from an affiliated parent/subsidiary entity, primary subcontractor, or Original Equipment Manufacturer (OEM) partner may be submitted to satisfy these requirements, subject to the following conditions:

- Direct Support & Deployment: The proposed affiliate, subcontractor, or OEM partner must be actively involved in the delivery, implementation, maintenance, or technical execution of the specific solution component proposed.
- Demonstrated Accountability: The Prime Proposer must clearly document the corporate relationship or binding contractual partnership in their proposal response, establishing how the affiliate or subcontractor's experience directly supports the project scope.
- Reference Scope: References provided for a subcontractor or OEM partner must specifically reflect public safety deployments relevant to the specific product, software, or hardware component they are supplying under this proposal.

70. Please confirm whether HCSO may award a proposer for a software-only subset of Category 1 or Category 5, including an integration, workflow, or analytics platform that interoperates with third-party sensors and evidence systems but does not include proprietary cameras or other hardware.

Answer: Yes. HCSO and the FSA Cooperative Purchasing Program permit and encourage proposals for software-only platforms, integrated workflow tools, and vendor-agnostic analytics solutions within Category 1 (Digital Evidence & BWC Systems) and Category 5 (Situational Awareness & AI).

- Category Scope: Proposers are not required to offer a complete hardware-and-software bundle or proprietary hardware to receive an award in these categories. Software solutions that ingest, manage, analyze, or stream data from third-party hardware, sensors, and existing evidence repositories fully align with the scope of this solicitation.
- Interoperability & Open Architecture: Software-only solutions must demonstrate robust integration capabilities, open APIs, and seamless interoperability with third-party hardware and legacy public safety platforms.
- Pricing & TCO Submission: Proposers submitting software-only solutions should complete the relevant Software/SaaS, Support & Maintenance, and Professional Services lines within the 5-Year Total Cost of Ownership (TCO) evaluation structure, indicating "N/A" for direct hardware components where applicable.

71. **For a Category 5 cloud platform that ingests metadata or operational feeds but is not the system of record for criminal justice information or digital evidence, which certifications and reports are mandatory at proposal submission, specifically CJIS audit documentation, SOC 2 Type II, and FIPS 140-2/140-3 validation?**

    Answer: Any platform that accesses, ingests, or processes CJI streams—regardless of whether it acts as the primary repository—must maintain full CJIS compliance.

72. **Please identify the user counts, data-ingestion volumes, storage and retention assumptions, required third-party connectors, and implementation assumptions that must be included in each five-year TCO evaluation scenario, and confirm whether usage above those assumptions may be priced through disclosed volume tiers.**

    Answer: The baseline scenario assumptions and TCO matrix are designed solely to verify that proposers have accounted for **all necessary product, software, and service categories** required for a fully functional deployment. This ensures that every component of a proposer's solution—across all offered offerings, not just the mock scenarios—is properly priced, cataloged, and within contract scope for any eligible purchasing agency. Only the scenarios which you are propsing as a Primary Technology Category need to be completed.

73. **Does the requirement to adjust agency-specific AI parameters without additional modification, material, licensing, or development fees apply only to configuration options already available in the awarded product, or must vendors include future custom engineering requested through purchaser-specific algorithmic guardrails at no additional charge?**

    Answer: The no-fee requirement applies to configuration options and parameter adjustments available within the awarded product's existing technical capabilities. Vendors are not required to perform future custom engineering or develop new algorithmic functionality at no charge.

    However, it is important to note that this contract is a cooperative purchasing vehicle — the specific AI governance criteria, confidence thresholds, bias-mitigation filters, and data retention triggers for each agency are not addressed at the Master Agreement level. Those terms are defined and negotiated within the individual Supplemental Agreement or Statement of Work executed between the Awarded Supplier and each Eligible Purchaser.

    Agencies requiring custom AI engineering beyond the awarded product's existing capabilities may negotiate those terms, including associated costs, directly within their supplemental agreement.

74. Section 3.11.3 requires DEMS integration with RMS and CAD systems through APIs or standard protocols. Can HCSO identify the RMS and CAD platforms proposers should use when documenting or demonstrating compliance with this requirement?

Answer: HCSO does not designate a specific RMS or CAD platform for proposers to prioritize. Because this contract is available to a wide range of Eligible Purchasers — including law enforcement agencies, municipalities, state and local government entities, and educational institutions — existing technology environments will vary significantly by agency.

Proposers should detail their solution's open-architecture capabilities, standard API and data ingestion options, and ability to integrate with diverse third-party systems so that any participating entity can connect the proposed solution with its existing infrastructure.

Specific RMS/CAD integration requirements will be identified and negotiated at the individual agency level through supplemental agreements or Statements of Work executed between the Awarded Supplier and each Eligible Purchaser.

75. Will a documented open API capable of supporting RMS/CAD integration satisfy the interoperability requirement, or must the DEMS have existing pre-built integrations with specific RMS/CAD platforms?

Answer: A documented open API capable of supporting RMS/CAD integration satisfies the interoperability requirement. The RFP requires that proposed solutions "demonstrate the ability to seamlessly integrate with existing eligible purchaser systems, including Records Management Systems (RMS) and Computer-Aided Dispatch (CAD) software via APIs or standard protocols."

Pre-built integrations with specific platforms are not mandated.

Proposers with pre-built integrations to major public safety platforms will receive higher scores under Section 4.10.4.1 (Interoperability, 30 points), while open API documentation without pre-built connectors will be scored in the mid-tier range.

Specific integration requirements will be identified and negotiated at the agency level through individual supplemental agreements or Statements of Work executed between the Awarded Supplier and each Eligible Purchaser.

76. For purposes of the unlimited cloud storage requirement, can HCSO clarify whether the required pricing must include both native evidence generated by the proposed BWC system and unlimited third-party evidence ingested into the DEMS, including evidence originating from other video systems, citizen-submitted media, documents, and other external sources?

Answer: The TCO Verification Spreadsheet distinguishes between two types of unlimited storage that must be separately defined and priced:

- Unlimited Native Storage refers to data generated exclusively within the Proposer's own technology ecosystem (e.g., their own body cameras or LPRs).
- Unlimited Third-Party Storage (CAT-3) is explicitly defined as data generated related to an investigation from technology outside the vendor's ecosystem, such as private citizen cell phone video, documents, or exports from other law enforcement agencies.

Proposers must price and define both storage types separately within their CAT-3 Software/SaaS line items. "Unlimited" storage must be explicitly defined in the proposal — vague or undefined storage terms will be evaluated accordingly under the Simplicity of UOM scoring criteria.

Specific storage configurations, volume thresholds, and any fair-use policies applicable to a particular agency's deployment will be negotiated at the individual agency level through supplemental agreements or Statements of Work executed between the Awarded Supplier and each Eligible Purchaser.

77. Can HCSO clarify whether "unlimited cloud storage" requires a fixed price regardless of evidence volume, file size, or quantity, and whether any storage limitations or fair-use thresholds are permissible if clearly disclosed?

Answer: Unlimited" storage must be explicitly defined in the proposal. Proposers offering unlimited storage must clearly state what is included and any applicable conditions. Vague or undefined storage terms will be penalized under the Simplicity of UOM scoring criteria, which deducts 10 points for every "usage-based" or "estimated" fee (e.g., "starts at," "variable data fees").

A fixed price per unit of measure is strongly preferred. Proposers may disclose fair-use thresholds or tiered volume structures, provided they are clearly defined with fixed units of measure (e.g., per TB, per user, per agency). Any storage limitation or threshold not explicitly disclosed in the Category Discount Table is deemed waived for the life of the contract.

Specific storage configurations, volume assumptions, and any fair-use policies applicable to a particular agency will be negotiated at the individual agency level through supplemental agreements or Statements of Work executed between the Awarded Supplier and each Eligible Purchaser.

78. For the AI-assisted audio and video redaction requirement, must the DEMS automatically identify content requiring redaction, or will assisted redaction tools that automate portions of the workflow while retaining human review satisfy the requirement?

Answer: Assisted redaction tools that automate portions of the workflow while retaining human review satisfy the requirement. The RFP evaluates "AI-assisted redaction" as a value-added capability under Section 4.10.4.3, and the solicitation does not mandate fully autonomous redaction without human oversight.

Full automation is not required — tools that assist authorized personnel in identifying and applying redactions will be scored accordingly. Proposers offering more advanced automated identification capabilities will receive higher scores under the Innovation and Value-Added Attributes criteria.

The specific redaction workflow, including the degree of automation and human review thresholds required by a particular agency, will be defined and negotiated at the individual agency level through supplemental agreements or Statements of Work executed between the Awarded Supplier and each Eligible Purchaser.

79. Does HCSO expect the DEMS to automatically identify exemptions under Florida public-records law and recommend or apply redactions, or is the requirement satisfied by tools that enable authorized personnel to perform and document compliant redactions?

Answer: The requirement is satisfied by tools that enable authorized personnel to perform and document compliant redactions. The RFP does not mandate fully autonomous identification of Florida public-records exemptions. Proposers offering AI-assisted redaction tools — including automated identification suggestions with human review — satisfy the requirement and will be scored under Section 4.10.4.3 (Advanced AI Tools).

Proposers offering more advanced automated exemption identification capabilities may receive higher scores under the Innovation and Value-Added Attributes criteria, but full automation is not a threshold requirement.

The specific redaction workflow, including the degree of automation, exemption categories applicable to a particular agency, and human review requirements, will be defined and negotiated at the individual agency level through supplemental agreements or Statements of Work executed between the Awarded Supplier and each Eligible Purchaser. Florida Statute § 119.071 public records exemptions applicable to a given agency's data will be addressed at that level.

80. Do the AI governance requirements and associated scoring criteria apply to AI-assisted capabilities within the DEMS, such as transcription, search, or redaction, or only to solutions proposed under Category 5, Situational Awareness & Artificial Intelligence?

Answer: The AI governance requirements apply to any solution utilizing Artificial Intelligence, machine learning, or automated decision-making logic — regardless of category. This includes AI-assisted capabilities within a DEMS (such as transcription, search, or redaction) proposed under Category 1, as well as solutions proposed under Category 5.

Proposers offering AI-assisted capabilities within their DEMS must demonstrate the technical ability to adjust AI parameters to meet agency-specific requirements and must confirm that algorithmic guardrails are adjustable without additional modification, licensing, or development fees in order to receive full credit under Section 4.10.4.2 (AI Governance Documentation, 20 points).

The specific AI governance criteria — including confidence thresholds, bias-mitigation filters, and data retention triggers — are not addressed at the Master Agreement level. Those terms are defined and negotiated within the individual Supplemental Agreement or Statement of Work executed between the Awarded Supplier and each Eligible Purchaser.

81. For the DEMS requirements, can HCSO clarify whether CJIS audit reports, SOC 2 Type II, and FIPS certifications must apply directly to the DEMS application, or whether applicable certifications/validations of the underlying cloud environment and cryptographic modules satisfy the requirement?

Answer: Certifications and validations of the underlying cloud environment and cryptographic modules may be used to satisfy portions of the requirement; however, they do not automatically constitute full application-level compliance. Proposers may reference cloud infrastructure control inheritance (e.g., Azure Government or AWS FIPS-validated cryptographic modules) for underlying infrastructure requirements, but must also provide independent validation demonstrating that their specific application stack, software interfaces, data flows, administrative controls, and personnel management fully adhere to CJIS Security Policy and FIPS 140-2/140-3 requirements.

Valid NIST/FIPS cryptographic module validation certificate numbers must be explicitly provided in the security submission.

It is important to note that this contract is a cooperative purchasing vehicle. The Master Agreement establishes an administrative contract vehicle and does not inherently grant access to CJI. Full CJIS compliance obligations — including execution of a CJIS Security Amendment and required background checks — are fulfilled at the supplemental agreement or local Purchase Order level with each individual Eligible Purchaser, not as a pre-award condition of the Master Agreement itself.

82. Does HCSO require the DEMS itself to hold a FIPS validation, or is use of FIPS 140-2/140-3 validated cryptographic modules sufficient?

Answer: Use of FIPS 140-2/140-3 validated cryptographic modules is sufficient — the DEMS application itself is not required to hold a standalone FIPS validation. Proposers must explicitly provide valid NIST/FIPS cryptographic module validation certificate numbers in their security submission to substantiate this compliance.

Proposers relying on cloud infrastructure (e.g., Azure Government or AWS GovCloud) may reference platform-level FIPS-validated cryptographic modules for underlying infrastructure; however, this does not automatically constitute full application-level compliance. Independent validation of the application stack, data flows, and administrative controls must also be demonstrated.

As a reminder, this contract is a cooperative purchasing vehicle. The Master Agreement establishes an administrative contract vehicle and does not inherently grant access to CJI. Full FIPS and CJIS compliance obligations are fulfilled at the supplemental agreement or local Purchase Order level with each individual Eligible Purchaser.

83. Must the DEMS calculate and retain a SHA-256 cryptographic hash for every evidence file at ingestion, or will equivalent technical controls or other industry-standard cryptographic hashing methods satisfy the evidence-integrity requirement?

Answer: Equivalent technical controls or other industry-standard cryptographic hashing methods satisfy the evidence-integrity requirement. The RFP references SHA-256 as the standard for chain-of-custody documentation, but the evaluation criteria under Section 4.10.4.4 reference "hashing algorithms (SHA-256), or similar."

Proposers utilizing equivalent industry-standard hashing methods should clearly identify the algorithm used and explain how it ensures evidence integrity.

Proposers implementing SHA-256 or stronger hashing algorithms at ingestion will receive the highest scores under the Chain of Custody criteria.

The specific chain-of-custody and evidence integrity requirements applicable to a particular agency's deployment — including acceptable hashing standards and audit trail retention policies — will be defined and negotiated at the individual agency level through supplemental agreements or Statements of Work executed between the Awarded Supplier and each Eligible Purchaser.

84. For the immutable audit-trail requirement, can HCSO clarify which evidence interactions must be captured, such as viewing, playback, downloading, sharing, metadata changes, redaction, export, and deletion?

Answer: At minimum, the immutable audit trail must capture all interactions that affect the integrity, accessibility, or disposition of evidence. This includes, but is not limited to: viewing/playback, downloading, sharing, metadata changes, redaction, export, and deletion. The RFP requires "immutable audit trails" as part of the Chain of Custody documentation evaluated under Section 4.10.4.4.

Proposers should describe in their submission which specific interactions are captured and logged. More comprehensive audit trail coverage will receive higher scores under the Chain of Custody criteria.

The specific audit trail requirements applicable to a particular agency's deployment — including which interaction types must be logged and retention periods for audit records — will be defined and negotiated at the individual agency level through supplemental agreements or Statements of Work executed between the Awarded Supplier and each Eligible Purchaser.

85. When evidence reaches the end of its retention period and is permanently deleted, must associated audit and chain-of-custody records also be deleted, or may audit records documenting the existence and disposition of the evidence be retained?

Answer: Audit and chain-of-custody records documenting the existence and disposition of evidence may be retained after the underlying evidence is permanently deleted. The RFP requires "immutable audit trails" as part of the Chain of Custody documentation, and the purpose of those records is to document what happened to evidence throughout its lifecycle — including its final disposition.

Deleting audit records upon evidence deletion would undermine the integrity and auditability of the chain of custody.

Proposers should clearly describe their data purge and retention policies in their submission, including how audit records are handled upon evidence deletion. The RFP requires "proof of automated deletion capabilities for non-investigatory data as applicable" under the Data/Purge Policies scoring criteria.

The specific retention periods for both evidence and associated audit records applicable to a particular agency's deployment will be defined and negotiated at the individual agency level through supplemental agreements or Statements of Work executed between the Awarded Supplier and each Eligible Purchaser, in compliance with applicable Florida Statute retention requirements.

86. When evaluating Category 1 submissions, may functionality provided through integrated non-BWC products within the same vendor ecosystem be considered when scoring interoperability, common operating picture, analytics, and value-added capabilities?

Answer: Yes. Proposers may include complementary products from adjacent categories to deliver a complete, integrated solution. Out-of-category hardware or software components must be listed under their native Discount Category Table so that appropriate category discounts apply. The complete bundled package price and operational cost savings should be explicitly demonstrated in the Mock Quote and Mock Invoice schedules within the TCO Verification Package.

Functionality provided through integrated non-BWC products within the same vendor ecosystem will be evaluated and scored under the applicable Innovation and Value-Added Attributes criteria (Section 4.10.4), including Interoperability (30 points) and Advanced AI Tools (10 points), provided the integrated solution is clearly documented and priced within the proposal.

The specific integration scope, including which ecosystem products will be deployed for a particular agency, will be defined and negotiated at the individual agency level through supplemental agreements or Statements of Work executed between the Awarded Supplier and each Eligible Purchaser.

87. May the BWC, in-car video system, and DEMS be provided by different manufacturers as an integrated solution, provided interoperability and a unified evidence workflow can be demonstrated?

Answer: Yes. The RFP encourages proposals that offer the broadest selection of technology and does not require that the BWC, in-car video system, and DEMS be provided by a single manufacturer. Proposers utilizing multiple manufacturers must clearly identify all parties involved, including any subsidiary companies, distributors, resellers, or subcontractors, and demonstrate that the combined solution delivers a unified evidence workflow.

The Awarded Supplier remains the single point of accountability for the performance of all products and services provided, regardless of the delivery model or number of manufacturers involved.

The specific integration requirements, interoperability standards, and unified workflow expectations for a particular agency's deployment will be defined and negotiated at the individual agency level through supplemental agreements or Statements of Work executed between the Awarded Supplier and each Eligible Purchaser.

88. Is secure transfer through docking, wireless, or network-based workflows acceptable, or is direct cellular upload from the camera required?

Answer: Secure transfer through docking, wireless, or network-based workflows is acceptable. The RFP does not mandate direct cellular upload from the camera as the exclusive transfer method. Proposers should clearly describe their evidence transfer methodology and demonstrate that it maintains chain of custody and data integrity throughout the transfer process.

Proposers offering multiple transfer options (docking, wireless, cellular, and network-based) will be evaluated more favorably under the Depth & Breadth of Solutions criteria (Section 4.10.5).

The specific transfer method required for a particular agency's deployment — including any requirements for direct cellular upload, docking station infrastructure, or network-based transfer — will be defined and negotiated at the individual agency level through supplemental agreements or Statements of Work executed between the Awarded Supplier and each Eligible Purchaser.

89. May evidence initially transfer to an agency-controlled local/on-premises system before being transferred or synchronized with the cloud DEMS?

Answer: Yes. The RFP does not mandate a cloud-only transfer path. Hybrid deployment models — including evidence that initially transfers to an agency-controlled local or on-premises system before synchronization with the cloud DEMS — are acceptable, provided the proposed solution satisfies all data sovereignty, CJIS security, and public records custody requirements.

Proposers should clearly describe their data transfer and synchronization architecture, including how chain of custody and data integrity are maintained throughout the transfer process, whether on-premises, cloud, or hybrid.

The specific deployment model — including whether an agency requires local/on-premises staging prior to cloud synchronization — will be defined and negotiated at the individual agency level through supplemental agreements or Statements of Work executed between the Awarded Supplier and each Eligible Purchaser.

90. For the 10 dual-camera systems in Scenario A, what camera configuration does HCSO expect, and may additional camera channels be proposed?

Answer: Scenario A is designed as a standardized evaluation baseline to verify that proposers have accounted for all necessary product, software, and service categories required for a fully functional deployment. The baseline scenario assumptions are not intended to restrict the configuration a proposer may offer.

Proposers may propose additional camera channels beyond the 10 dual-camera baseline, provided the additional channels are clearly itemized and priced within the TCO Verification Package. Any configuration proposed beyond the baseline scenario should be presented as an optional add-on with transparent per-unit pricing consistent with the awarded Category Discount structure.

The specific camera configuration required for a particular agency's deployment — including the number of channels, mounting requirements, and integration with in-car video systems — will be defined and negotiated at the individual agency level through supplemental agreements or Statements of Work executed between the Awarded Supplier and each Eligible Purchaser.

91. Are automated recording triggers, including emergency-light activation and coordinated BWC activation, required, preferred, or considered value-added?

Answer: Automated recording triggers — including emergency-light activation and coordinated BWC activation — are considered value-added capabilities. The RFP does not mandate automated triggers as a threshold requirement for responsiveness. Proposers offering automated recording triggers will be evaluated more favorably under the Innovation and Value-Added Attributes criteria (Section 4.10.4) and the Depth & Breadth of Solutions criteria (Section 4.10.5).

Proposers should clearly describe any automated trigger capabilities in their submission, including the types of triggers supported and how they integrate with in-car video and BWC systems.

The specific automated recording trigger requirements for a particular agency's deployment — including which trigger events are required and how they integrate with existing fleet and dispatch systems — will be defined and negotiated at the individual agency level through supplemental agreements or Statements of Work executed between the Awarded Supplier and each Eligible Purchaser.

92. Does the month-36 refresh require complete replacement of the BWC/in-car hardware, or can current-generation equivalent hardware be provided under the lifecycle program?

Answer: Current-generation equivalent hardware may be provided under the lifecycle refresh program. The RFP does not mandate complete like-for-like replacement of BWC or in-car hardware at the month-36 refresh. Proposers should clearly describe their hardware lifecycle and refresh program in their submission, including what constitutes an eligible refresh unit and how equivalency is determined.

Proposers offering more comprehensive lifecycle programs — including guaranteed replacement with current-generation or better hardware — will be evaluated more favorably under the Depth & Breadth of Solutions criteria (Section 4.10.5).

The specific hardware refresh requirements applicable to a particular agency's deployment — including whether complete replacement or equivalent hardware is acceptable, and the standards for determining equivalency — will be defined and negotiated at the individual agency level through supplemental agreements or Statements of Work executed between the Awarded Supplier and each Eligible Purchaser.

93. Can the BWC/in-car hardware portion of Category 1 be proposed in conjunction with a technology partner providing the DEMS, provided the combined solution meets the Category 1 requirements?

Answer: Yes. Proposers may propose the BWC/in-car hardware in conjunction with a technology partner providing the DEMS, provided the combined solution meets all Category 1 requirements and delivers a unified evidence workflow. The Awarded Supplier remains the single point of accountability for the performance of all products and services provided, regardless of the delivery model.

Proposers utilizing a technology partner for the DEMS must clearly identify all parties involved, including any subsidiary companies, distributors, resellers, or subcontractors, and document the corporate relationship or binding contractual partnership in their proposal response.

The specific integration requirements between the BWC/in-car hardware and the DEMS — including interoperability standards, chain-of-custody continuity, and unified workflow expectations — will be defined and negotiated at the individual agency level through supplemental agreements or Statements of Work executed between the Awarded Supplier and each Eligible Purchaser.

94. For a Software-as-a-Service solution delivered on a major cloud platform (e.g., Microsoft Azure / Azure Government), security controls follow the standard cloud shared-responsibility model, under which certain attestations are held at the platform level.

a. Under the shared-responsibility model, will the Agency recognize platform-level (cloud-provider) SOC 2 Type II, FIPS 140-validated cryptographic modules, and CJIS Security Policy-aligned controls toward the Security & Encryption score in Section 4.10.5.3?

b. When combined with a Proposer's own information-security certification (e.g., ISO/IEC 27001:2022), are these sufficient for full credit — or does the Agency require certifications issued specifically in the Proposer's name?

Answer: Platform-level certifications (e.g., Azure Government SOC 2 Type II, FIPS 140-validated cryptographic modules) may be referenced to satisfy underlying infrastructure requirements under the shared-responsibility model; however, they do not automatically constitute full application-level compliance. Proposers must provide independent validation demonstrating that their specific application stack, software interfaces, data flows, administrative controls, and personnel management fully adhere to CJIS Security Policy and FIPS 140-2/140-3 requirements. Valid NIST/FIPS cryptographic module validation certificate numbers must be explicitly provided.

A Proposer's own information-security certification (e.g., ISO/IEC 27001:2022) combined with platform-level certifications may be sufficient for partial credit, but certifications issued specifically in the Proposer's name — particularly a SOC 2 Type II — are required for maximum scoring under Section 4.10.5.3. A SOC 3 report may be submitted initially, with HCSO reserving the right to request the full SOC 2 Type II during evaluation.

As a reminder, this contract is a cooperative purchasing vehicle. The Master Agreement establishes an administrative contract vehicle and does not inherently grant access to CJI. Full CJIS compliance obligations are fulfilled at the supplemental agreement or local Purchase Order level with each individual Eligible Purchaser, not as a pre-award condition of the Master Agreement itself.

95. For a privately held company:

a. Will the Agency accept reviewed or unaudited financial statements — supported by bank references, a Dun & Bradstreet report, and proof of insurance — for the Corporate Stability criterion in Section 4.10.1?

Answer: Yes. Submitting reviewed or unaudited financial statements does not disqualify a privately held company from award consideration. Unaudited statements that demonstrate basic solvency remain eligible for evaluation and scoring under the mid-level point tiers. Supporting documentation such as bank references, a Dun & Bradstreet report, and proof of insurance may be submitted to supplement unaudited financials and will be considered by evaluators.

Five years of audited financial statements are preferred but not strictly required for a proposal to be considered responsive. Evaluators will score financial submittals based on the duration of operational history, level of financial verification, and demonstrated fiscal stability.

The specific financial documentation requirements applicable to a particular agency's supplemental agreement will be negotiated at the individual agency level.

96. For a Proposer offering software for Category 1 (Digital Evidence Management) and Category 5 (Situational Awareness & AI) but no hardware:

a. May a Proposer bid only the software elements of these categories?

b. Can such a Proposer be awarded at the subcategory level without offering cameras, drones, or sensors?

Answer: Yes to both. HCSO and the FSA Cooperative Purchasing Program permit and encourage proposals for software-only platforms, integrated workflow tools, and vendor-agnostic analytics solutions within Category 1 and Category 5. A Proposer offering software only may bid the software elements of these categories and may be awarded at the subcategory level without offering cameras, drones, or sensors.

Software-only Proposers in Category 5 may mark physical hardware requirements as "N/A – Software-Only Solution" and will be scored on software reliability equivalents — including cloud availability SLAs, infrastructure redundancy, disaster recovery failover, and encryption standards — ensuring full scoring eligibility without penalty.

The specific software components, integration requirements, and deployment scope applicable to a particular agency will be defined and negotiated at the individual agency level through supplemental agreements or Statements of Work executed between the Awarded Supplier and each Eligible Purchaser.

97. So that storage pricing uses a fixed unit of measure, which format does the Agency prefer?

a. A flat rate per agency?

b. A set price per terabyte?

c. A customer-provided (bring-your-own) storage option?

Answer: All three storage pricing formats are acceptable, provided the unit of measure is clearly and explicitly defined within the Proposer's Category Discount Table. The Category Discount Table defines what is within scope for Eligible Purchasers — any storage component not listed there is deemed outside the scope of the contract and unavailable for purchase.

Proposers should select the format that best reflects their actual pricing model and define it clearly. A flat rate per agency and a set price per terabyte are both acceptable fixed-unit formats. A customer-provided (bring-your-own) storage option is also permissible, provided it is disclosed and any associated integration or management fees are transparently itemized within the Category Discount Table. Vague or usage-based storage terms will be penalized under the Simplicity of UOM scoring criteria.

The specific storage configuration applicable to a particular agency will be negotiated at the individual agency level through supplemental agreements or Statements of Work.

98. If a Proposer teams with a hardware partner or reseller:

a. Must the partner be named and approved at the time of bid submission?

b. Or only if the Proposer is awarded the contract?

Answer: Proposers intending to utilize a hardware partner, authorized distributor, or regional reseller should identify them within their proposal submission. While inclusion in the proposal establishes vendor capabilities at the overarching agreement level, any subsequent task orders or purchase agreements issued under the contract remain subject to specific review and written approval of designated subcontractors by HCSO or the individual Eligible Purchaser prior to project execution.

Participating agencies reserve the right to accept, reject, or require replacement of proposed subcontractors for specific local engagements.

The specific hardware partner or reseller applicable to a particular agency's deployment will be confirmed and approved at the individual agency level through supplemental agreements or Statements of Work executed between the Awarded Supplier and each Eligible Purchaser.