

Sample RFP Response

Worked example — major transport-hub and public-realm policing (Dubai profile)

HumanityAI'd — July 2026

CONFIDENTIAL — ILLUSTRATIVE SAMPLE, NOT A SUBMITTED BID

Note: This is a worked example showing how a tender response reads when Patrol Sight is mapped onto a flagship security authority's requirements. It uses publicly reported facts about Dubai's existing AI-surveillance programme to make the example concrete. It is **not an actual submission**, no engagement is implied, and all commercials are indicative.

1. Executive summary

Dubai Police launched its Oyoon AI surveillance programme in January 2018, connecting tens of thousands of cameras with facial recognition to a central command centre, and publicly credited AI cameras with 319 arrests in the programme's first year. Facial recognition has since been extended to Dubai Metro stations to identify wanted persons. The capability, the command infrastructure and the institutional confidence in facial recognition are all established.

What remains unaddressed is the last fifty metres. Recognition today happens where the cameras are — at fixed points the subject walks past — and the result reaches an officer by radio, after the encounter. **Patrol Sight closes that gap: it puts recognition into the officer's own line of sight, returning a colour-coded identification into the lens of their AR glasses in approximately 68 milliseconds**, while the person is still in front of them.

The entire system runs on a server inside the authority's own network. The watchlist is the authority's, enrolled by the authority's own personnel, searchable only by named operators, with every query logged. No face image, faceprint or alert leaves the premises — which satisfies UAE PDPL treatment of biometric data as sensitive personal data by construction rather than by contractual assurance.

2. Understanding of requirements

We understand the authority requires: a capability that improves outcomes for officers deployed on foot in high-footfall public realm and transport environments; identification fast enough to act on during an encounter; complete control of watchlist content and access; strict data residency; integration with the existing command-and-control estate rather than a parallel silo; a defensible audit trail; and demonstrable reliability at the scale of a 24-hour operation.

We also understand what the authority is **not** asking for: an autonomous system. Every match Patrol Sight produces is presented to an officer for verification. The system informs a human decision; it never authorises or executes one.

3. Proposed solution

- Patrol officers wear AR glasses streaming hardware-encoded H.264 over the authority's dedicated 5 GHz network to an on-premises GPU server.

- The server detects faces (SCRFD), computes 512-dimension ArcFace embeddings on TensorRT FP16, and searches the authority's watchlist using GPU FAISS.
- A colour-coded category label returns into the officer's lens — **measured ~68 ms typical (49-103 ms range)** at 14-20 effective recognition frames per second. Categories (wanted, banned, missing person, person of interest, staff) are the authority's own, colour-mapped so an officer reads category at a glance rather than parsing a name.
- A two-layer tracker answers 97.6% of frames from an identity cache without re-searching — the design decision that makes continuous patrol recognition affordable on a single GPU.
- The command console gives the control room live per-device frame rate, latency and face counts with annotated preview, the alert stream, tracking history per person and per device, role-based operator accounts and a complete audit trail. Alerts publish on an internal message bus for consumption by the authority's existing command-and-control platform.

4. Compliance matrix (illustrative extract)

Req.	Requirement	Compliance	Evidence
R1	Identification delivered to the officer during the encounter	Comply	Measured ~68 ms glasses-to-label, stage-by-stage budget provided
R2	Watchlist scale $\geq$ 50,000 persons	Comply	93,728 persons in live production; measured 80-130 ms at 13M
R3	Hands-free operation for foot patrol	Comply	No officer interaction required; continuous recognition
R4	Data residency — on-premises processing of biometric data	Comply	Full on-prem stack; operable air-gapped; zero egress verifiable by the authority's network audit
R5	Authority-owned watchlist, no vendor database	Comply	Enrolment by authority personnel; no scraped or supplied face data
R6	Human verification before action	Comply — by design	No automated enforcement capability exists in the product
R7	Full audit trail of searches and matches	Comply	Audit middleware; operator audit view; exportable
R8	Integration with existing command-and-control	Partially — integration scoped separately	Alerts publish on internal bus; per-system integration effort quoted
R9	Encrypted transport on the wearable link	Roadmap — Q1 2027	Costed in Technical Due-Diligence Report Phase 2. Until then specified as an isolated VLAN with no uplink — a documented control
R10	Independent accuracy benchmark (NIST FRTE)	Not held	We do not hold an FRTE ranking and will not imply one. We offer measured accuracy testing in the authority's own environment during the pilot, and provide our internal 0-90° pose benchmark
R11	Recognition at ranges beyond 10 m	Does not comply	Reliable to ~5 m, 6-7 m in good light, 8-10 m in long-range mode. Beyond that a head-worn camera cannot deliver the pixels; fixed cameras remain the correct tool
R12	Concurrent devices per server	To be measured	Bounded by decode and detection, not search. Measured during pilot; contracted on the measured figure

Rows R8 through R12 are deliberately honest. A security authority's engineers will find these limits in evaluation; finding them disclosed, dated and costed builds the credibility that carries the rest of the bid.

5. Data sovereignty, security & privacy

All detection, recognition, watchlist storage, alerting and audit logging execute on the authority's on-premises server. The deployment functions with no internet connectivity. Biometric data is sensitive personal data under UAE PDPL with restricted cross-border transfer; because nothing transits outside the authority's network, the transfer question does not arise.

Internal security: zero-trust per-service authentication on the message bus, AES-256-GCM payload encryption between the device hub and the console, TLS termination, JWT and API-key authentication, IP allowlisting on the device stream port, and configurable retention with purge capability.

Disclosed hardening in progress: credential rotation and per-device provisioned tokens, reduction of the published network surface to a single ingress, and encryption of the wearable transport. These are Phases 0–2 of a costed plan detailed in the accompanying Technical Due-Diligence Report and would be complete before operational deployment. Until the wearable transport is encrypted, the glasses network is specified as an isolated VLAN with no internet uplink.

6. Governance & lawful use

- The authority holds the lawful basis for each watchlist entry; the platform records provenance and enforces the authority's retention policy.
- Every search and match is attributable to a named operator or a specific device, with timestamp and confidence, and is exportable for oversight or judicial review.
- No emotion inference, no demographic profiling, no covert-operation features, no automated action.
- We will support the authority's Data Protection Impact Assessment during the pilot and supply the audit evidence it requires.

7. Implementation plan

Week 0: kick-off, RF survey of the pilot patrol area, server installation, information-security review and DPIA initiation, KPI sign-off. Week 1: stack deployment, glasses provisioning, threshold calibration against a consented volunteer cohort, zero-egress network audit by the authority. Week 2: information-security sign-off, limited live watchlist load, operator console training. Week 3: officer induction and **shadow running — alerts to the control room only, no officer action — to establish the baseline false-positive rate**. Weeks 4–5: live operation under the authority's own verification procedure, daily alert review. Week 6: measurement against agreed KPIs, audit-log review with the data-protection function, readout and rollout proposal covering additional patrol areas and transport nodes.

8. Hardware, network & fleet

Ten AR glasses for the pilot with a 10% spare ratio, a charging and provisioning station, and one on-premises GPU server (16–24 GB GPU recommended for fleet headroom; the measured reference deployment runs on an 8 GB RTX 4060 Ti).

Network requirement, stated as a critical dependency: a dedicated 5 GHz SSID across the patrol area with wireless power-save disabled, at least two access points, and approximately 20 Mbps per streaming device. In our own measurements, moving from a 2.4 GHz link with power-save enabled to 5 GHz WiFi 6 with power-save disabled changed the network round trip from roughly 100 ms to roughly 4 ms. **The wireless network determines the officer's experience more than the AI does**, and we would rather specify it plainly than have the pilot judged on a radio problem.

9. Commercials (indicative)

Site licence at the tier matching watchlist size and device count (USD 150k–400k per year), glasses fleet and on-premises server as CAPEX, implementation including RF survey and watchlist onboarding, and a Priority or Mission-critical SLA. Command-and-control integration quoted per target system. Full schedule per the Pricing & Packaging document. All figures indicative pending scoping.

10. Why HumanityAI'd

- The only offering combining AR-glasses capture, fully on-premises inference, an authority-owned watchlist and GCC-compliant data residency. The nearest regional precedent — a 50-unit smart-glasses deployment in UAE security operations in 2019 — proved the concept on 2019 hardware and left the category open.
- A live production deployment as proof, with published measurements rather than claims.
- A neutral supply chain: neither dependent on cloud services nor exposed to the sanctions position of the largest surveillance vendors.
- A governance posture designed to survive scrutiny, because in this category the buyer's reputational risk is as real as their operational need.

11. Assumptions & exclusions

Authority-provided wireless network, power and rack space; authority holds lawful basis, watchlist content, officer verification procedure and enforcement policy; glasses fleet lead time 6–8 weeks; command-and-control integration quoted separately per system; concurrent-device capacity per server established during the pilot; recognition ranges beyond 10 metres excluded and served by existing fixed-camera infrastructure.

Administrative envelope (supplier registration, trade licence, SIRA licensing where the deployment involves private-security systems, ICV documentation for federal or Abu Dhabi scope, bid and performance bonds) to be completed per the authority's procurement requirements — see RFP Response Template §16.