

RFP / RFB Response Template

Patrol Sight — reusable tender response

HumanityAI'd — July 2026

CONFIDENTIAL — INTERNAL SALES TEMPLATE

How to use this template

GCC security technology is procured through the operating authority — a police force, ministry of interior, airport operator, giga-project security function, or a private estate's security division — via formal tender or, for pilots, a direct award or limited tender. This template maps Patrol Sight onto the sections almost every security-technology RFP contains.

Three rules for using it:

1. **Replace every bracketed prompt.** A tender response that reads like a template loses on evaluation.
2. **Keep the honest posture.** Where we are on roadmap, say "Roadmap" with a date. A compliance matrix with three honest "Roadmap" rows and a costed plan scores better than one with thirty green ticks that collapse under technical questioning — and it matches the disclosures in our Technical Due-Diligence Report, which the buyer's engineers will read.
3. **Never bid without the administrative envelope confirmed** — see §16. In Saudi Arabia this means an Etimad-registered local partner; in Abu Dhabi an ICV certificate materially affects scoring; in Dubai private security, SIRA licensing applies to the systems and the company.

1. Executive summary

[2–3 paragraphs: recognition delivered into the patrol officer's line of sight, fully on the authority's premises, in about 68 milliseconds. Name the specific authority, its operating environment (transport hub, stadium, district, border, event), and the operational gap you are closing — the gap between what the control room knows and what the officer on the ground knows.]

2. Understanding of requirements

[Restate the authority's stated goals in our words: officer capability, response time, watchlist control, data residency, integration with existing command-and-control, auditability, KPIs. Demonstrate that we read the brief and understand their concept of operations — not just their technical specification.]

3. Proposed solution

- Patrol officers wearing AR glasses streaming hardware-encoded H.264 to an on-premises GPU server

- Face detection (SCRFD) and ArcFace 512-dimension recognition executed on TensorRT FP16; GPU FAISS search over the authority's own watchlist
- Colour-coded category labels returned into the officer's lens — measured **~68 ms typical, 49-103 ms range**, at 14-20 effective recognition frames per second
- Two-layer tracking eliminating 97.6% of vector searches, which is what makes continuous patrol recognition viable on a single GPU
- Command console: live per-device monitoring, alert stream, tracking history, role-based operator access, full audit trail
- Watchlist owned and enrolled entirely by the authority; bulk enrolment at 40-60 images/second, live index hot reload
- **No cloud dependency, no vendor-supplied face database, no automated enforcement action**
- Architecture diagram: [insert from Technical Due-Diligence Report §3]

4. Compliance matrix

[Table: each requirement → Comply / Partially / Roadmap → evidence. Cite measured figures, not marketing claims. Be honest; "Roadmap Q1 2027" with a costed plan beats overclaiming.]

Req. ID	Requirement	Compliance	Evidence / Notes

5. Performance & accuracy

- **State the recognition envelope plainly:** reliable identification to approximately 5 metres, maximum 6-7 metres in good lighting, 8-10 metres in long-range mode at reduced frame rate. Faces below the minimum pixel threshold are rejected rather than guessed at.
- Latency: measured stage-by-stage budget available (capture, transit, decode, detect, embed, search, return, render).
- Scale: measured recognition latency by watchlist size — 100k → 50-70 ms, 1M → 60-90 ms, 13M → 80-130 ms.
- Off-angle performance: ArcFace R50 selected after a 0-90° yaw benchmark showing approximately 60% fewer false negatives at extreme pose than the lightweight alternative.
- **Independent benchmarking:** we do not currently hold a NIST FRTE ranking and will not imply one. [State the current position on an FRTE submission if asked, and offer measured accuracy testing in the authority's own environment during the pilot as the substitute evidence.]
- **Accuracy will be measured in the authority's environment during the pilot, and the contracted figures will be the measured ones.**

6. Data sovereignty, security & privacy

- Fully on-premises; recognition, watchlist, alerts and audit trail never leave the authority's network; the system is operable fully air-gapped
- Biometric data is sensitive personal data under [UAE PDPL / Saudi PDPL / applicable regime]: in-country processing is satisfied by construction
- Customer-owned watchlist; no scraped, purchased or vendor-supplied face database
- Zero-trust internal service authentication; AES-256-GCM payload encryption between device hub and console; TLS termination; API-key and JWT authentication; IP allowlisting on the device stream
- Configurable retention, purge capability, and a complete audit trail of every search and match, exportable for regulatory or judicial review
- Privacy mode: transmit only the 512-number faceprint (~2 KB) rather than the image
- **Security hardening in progress and disclosed:** credential rotation and per-device tokens, network-surface reduction, and encrypted glasses transport are Phase 0-2 of a costed hardening plan [state completion date]. Until encrypted transport ships, the glasses network is specified as an isolated VLAN with no internet uplink — a documented security control, not an omission
- [Address the authority's specific regime: UAE Information Assurance / NES, Saudi NCA ECC, SIRA requirements for Dubai private security, GDPR-equivalent obligations where applicable]

7. Governance & lawful use

This section wins security tenders and is usually written badly by competitors. State it directly:

- Every match is presented to a human officer for verification. **The system informs a decision; it never authorises or executes one.**
- The authority holds the lawful basis for each watchlist entry; the platform records provenance and supports the authority's retention policy.
- Every search and every match is attributable to an operator or device, and exportable.
- No emotion inference, no demographic profiling, no covert-operation features.
- We will support a Data Protection Impact Assessment during the pilot and provide the audit evidence it requires.

8. Implementation plan

- Phase 0 (Week 0): kick-off, RF site survey, server installation, information-security review and DPIA initiation, success metrics signed
- Phase 1 (Week 1): stack deployment, glasses provisioning, threshold calibration on a consented test cohort, zero-egress network audit
- Phase 2 (Week 2): information-security sign-off, limited live watchlist load, operator training
- Phase 3 (Week 3): officer induction and shadow running to establish the baseline false-positive rate
- Phase 4 (Weeks 4–5): live operation with verified action, daily alert review
- Phase 5 (Week 6): measurement against agreed KPIs, audit review, readout, rollout plan
- [Insert milestone table / Gantt]

9. Integration

- Alert publication on an internal message bus for consumption by the authority's existing command-and-control or video-management platform
- [Name the authority's existing systems and state the integration approach and effort per system]
- Glasses configuration managed through a dedicated settings service and console

10. Hardware & fleet

- AR glasses: model, quantity, 10% spare ratio, charging and provisioning station
- On-premises GPU server: minimum 8 GB GPU (the measured reference), 16–24 GB recommended for fleet headroom; 32 GB RAM, 8+ cores, 512 GB SSD, NVIDIA driver 550+
- **Network requirement (critical):** dedicated 5 GHz SSID across the patrol area with wireless power-save disabled, ≥ 2 access points, ~ 20 Mbps per streaming device. The reference glasses are 5 GHz only. Wireless quality determines end-user latency more than the AI does
- Fleet sizing per GPU: measured during the pilot and contracted on the measured figure

11. Operations & support

- Single-command deployment, health, update and teardown tooling; unattended recovery after reboot
- Tiered SLA (Standard / Priority / Mission-critical): response targets, spare-unit pool, threshold and index tuning reviews
- Remote support through a customer-controlled channel that can be disabled entirely; on-site or customer-mediated log export for air-gapped sites
- Training: officer induction (1 hour), operator console training, watchlist administrator training, IT handover

12. Analytics & reporting

- Per-device utilisation, frame rate and latency; alert volumes and outcomes; tracking history per person and per device
- False-positive tracking and periodic accuracy review
- Exportable reports for the authority's own KPI and oversight reporting

13. Team & experience

- HumanityAI'd overview; the live production deployment as reference (93,728 enrolled persons, measured ~68 ms glasses-to-label)
- Key personnel and roles
- [Named integrator partner for installation, fleet operations and first-line support — do not bid national-scale operations alone]

14. Risk & mitigation

[Table from BRD §8 plus the Technical Due-Diligence hardening plan. Naming risks and owning them demonstrates maturity; security buyers assume undisclosed risk is worse than disclosed risk.]

15. Commercial

- Licence + hardware + implementation + support, structured to the authority's budget cycle
- CAPEX-owned hardware option
- [Insert priced schedule from Pricing & Packaging]

16. Administrative envelope — confirm before bidding

- **Saudi Arabia:** Etimad platform registration; local partner required for government tenders
- **Abu Dhabi / federal UAE:** valid ICV certificate (absent certificate scores zero; ICV weighting is material in Abu Dhabi evaluation)
- **Dubai private security:** SIRA licensing of the company, systems and personnel
- Trade licence, bid and performance bonds, insurance, local support presence
- [Confirm the authority's specific supplier-registration portal and prerequisites]

17. Assumptions & exclusions

[State clearly: authority-provided wireless network and power; authority holds lawful basis and watchlist content; glasses lead time 6–8 weeks; enforcement policy and officer procedure are the authority's; integration effort per external system quoted separately; model-licensing status if not yet resolved at bid time.]

Attachments to include

Company one-pager · Master pitch deck · Case study · Technical Due-Diligence Report · Deployment & Operations Guide · POC Playbook · Pricing schedule