

Outreach Sequence Guide

How to run the sale — what to send, to whom, when

HumanityAI'd — July 2026

CONFIDENTIAL — INTERNAL SALES ENABLEMENT

1. The motion in one line

Reference-first, sovereignty-led, partner-backed. Win a fast private-estate or venue reference, lead every conversation with data residency and the officer-level gap, and co-bid government work with a licensed regional integrator who already holds the relationship and the fleet-operations capability we lack.

2. Sequence the buyers — do not start with the biggest

This is the single most important judgement in the plan. Government law enforcement is the largest prize and the slowest, most clearance-gated buyer. Going there first with no live security reference wastes a year.

Order	Buyer class	Why here	Cycle
1st	Private estates & venues (Emaar, Majid Al Futtaim, stadium and district operators)	Commercial decision, real security operation, SIRA-licensed but not clearance-gated. Produces the reference everything else needs	3-6 months
2nd	Transport & event operators (Dubai Airports, Abu Dhabi Airports, venue authorities)	Deadline-driven, already fluent in biometrics, large foot-patrol estates — the strongest "last fifty metres" story	6-12 months
3rd	Giga-project security functions (NEOM, Diriyah, RCU, Red Sea Global)	Procure directly as corporates outside Etimad; greenfield with security designed in	6-12 months
4th	Government law enforcement & ministries (Dubai Police, MOI UAE/KSA, SDAIA)	Highest value, deepest cycle — enter with a reference, an integrator and completed hardening	12-24+ months

In parallel from day one: engage an integrator partner (\$4) and complete the administrative envelope — ICV certification for Abu Dhabi/federal UAE, SIRA licensing for Dubai systems, an Etimad-registered local partner for Saudi government work. These take months and cannot be started when the tender drops.

3. Which document at which stage

Stage	Goal	Send / show
1. First touch	Get a meeting	One-Pager + a two-line "last fifty metres" hook
2. Discovery call		Master Pitch Deck

Stage	Goal	Send / show
	Qualify: their FR estate, patrol model, watchlist ownership, data-residency stance	
3. Live demo	Create the "wow" — glasses on their head	Glasses demo + Demo Script; leave the Case Study
4. Technical & security vetting	Satisfy their information-security function	Technical Due-Diligence Report + Deployment & Operations Guide
5. Governance review	Satisfy legal / data protection	PRD §8 (out of scope), Deployment Guide §7, RFP Template §7 (Governance & lawful use)
6. Business case	Justify budget	BRD + PRD + Feature Matrix & Roadmap
7. Pilot proposal	Get a signed pilot	POC Playbook + Pricing & Packaging
8. Formal tender	Win the bid	RFP Response Template + Sample Response; attach the kit
Throughout	Positioning	Market Analysis + Competitor Analysis to frame every conversation

Send the Due-Diligence Report. It discloses our security debt and the model-licensing item. That feels counterintuitive; do it anyway. A security buyer's engineers will find these in evaluation, and disclosed-and-dated beats discovered-and-hidden every time. Undisclosed risk is the one thing that ends a security sale permanently.

4. The integrator conversation — run it before the customer conversation

We cannot credibly bid fleet operations at national scale alone, and our own due-diligence report says so. Approach MVP Tech, Al-Futtaim Technologies, TCC or SAMI as **partners, not resellers**:

"You hold the customer relationship and the fleet-operations capability. We hold a wearable recognition capability that runs entirely on-premises and that nobody in your portfolio can currently offer. Neither of us can bid this alone."

That framing works because it is true. IDEMIA's 2025 memoranda with TCC and SAMI show this is the established entry model for a foreign recognition vendor in Saudi Arabia.

5. The five messages that win

- 1. The last fifty metres** — your cameras know; your officer doesn't, until afterwards. That gap is the product.
- 2. Measured, not claimed** — ~68 ms glasses-to-lens, 93,728 enrolled, P95 search 8.5 ms, published stage by stage. Nobody else in this category publishes a latency budget.
- 3. Sovereign by construction** — biometric data never leaves the building. Cloud recognition cannot follow under UAE and Saudi data-protection law.
- 4. Your list, your server, a human decides** — no scraped database, recorded lawful basis, mandatory human verification, complete audit trail. The governance posture is the sales asset.
- 5. Neutral supply chain** — not cloud-dependent, not exposed to the sanctions position of the largest surveillance vendors, without regional sourcing sensitivities.

6. First-touch email skeleton

Subject: Recognition in the officer's line of sight — fully on your premises

Dear [name],

[Organisation] already runs facial recognition on fixed cameras. So this is the only question I want to put to you: when one of your officers is standing three metres from someone on your watchlist, does the officer know — or does the control room find out afterwards?

We've built Patrol Sight to close that gap. An officer wearing AR glasses gets a colour-coded identification in their lens in about 70 milliseconds, matched against your own watchlist, on a server inside your building. No cloud, no vendor-held face data, and every match goes to the officer to verify — it informs a decision, it never makes one.

It's running in production today against a 93,000-person index. I'd like to show you a live demo and propose a contained six-week pilot at one site, measured against numbers we agree together — including the false-positive rate.

Are you open to a 30-minute call?

[signature — HumanityAI'd, Artificial Intelligence for Smart Glasses]

What not to write. No claims of NIST ranking. No unquantified accuracy figures. No suggestion of covert use, automated action, or that we can supply a face database. No mention of ranges beyond 10 metres. Each of these would be found out in evaluation and would cost the deal.

7. Handling the four predictable objections

Objection	One-line answer	Backing doc
"NEC/IDEMIA already supply our biometrics."	They supply the fixed points a subject walks to; we supply the officer who walks. We deploy beside them.	Competitor Analysis §3
"What's your NIST ranking?"	We don't have one and won't imply one — here's our measured end-to-end pipeline and an offer to measure accuracy in your own environment during the pilot.	Due-Diligence Report; POC Playbook §7
"Facial recognition is a legal and reputational risk."	The risk lives in scraped data, cloud processing and automated action. We have none of the three, and we'll support your DPIA.	Deployment Guide §7; RFP Template §7
"Can a vendor your size support us at national scale?"	Not alone, and we don't claim to — we bid with [integrator] for installation, fleet operations and first-line support.	Contacts §4

8. Cadence

- Day 0: first-touch email with the One-Pager attached.
- Day 5: follow up with one concrete measurement (the latency budget or the 97.6% cache-elision figure) — technical specificity gets replies from security buyers where marketing language does not.
- Day 12: the sovereignty angle written for their specific regulatory position (UAE PDPL, Saudi PDPL, SIRA).
- Day 21: offer the demo unconditionally — "thirty minutes, we bring the glasses, you wear them."
- Day 30: close-the-file email. Often the highest reply rate.
- On any reply: discovery call, then a live demo within two weeks. **The demo converts this product; get to it fast.**

Run the integrator track on its own parallel cadence — it does not wait for a customer reply.

9. Region-specific notes

- **Dubai:** SIRA licensing applies to the company, the systems and the personnel — treat SIRA engagement as a market-entry project, not a customer conversation. Dubai Police is the most FR-experienced buyer in the region and correspondingly the most demanding.
- **Abu Dhabi / federal UAE:** obtain ICV certification early — an absent certificate scores zero and the weighting is material. Expect to bid with or through a UAE-licensed partner.

- **Saudi Arabia:** government sales require Etimad registration and a local partner. The giga-projects (NEOM, Diriyah, RCU, Red Sea Global) procure directly as corporates and are the faster, more realistic entry point. SDAIA is both a potential buyer and an AI-governance approval path — engaging them early is worth more than a single deal.
- **Qatar:** Monaqasat for government; venue operators procure directly. The 2022 World Cup FR legacy means the concept needs no explanation.
- **Events pipeline:** Expo 2030 Riyadh and World Cup 2034 specify security years ahead of opening. Being in those conversations in 2026–27 is how a 2030 deployment happens.

10. Two internal gates — know them before you promise anything

1. **Model licensing.** The recognition weights derive from a research-licensed lineage. Discovery, demos and pilots under an evaluation arrangement can proceed; **a paid production deployment cannot close until this is resolved.** Do not let a deal reach signature ahead of it.
2. **Security hardening Phase 0-1** (credential rotation, per-device tokens, network-surface reduction, encrypted wearable transport — roughly 4-5 engineer-weeks). Required before any government operational deployment. Disclose the plan and its dates; do not describe it as complete.

Both are stated plainly in the Technical Due-Diligence Report, which is the document that makes disclosing them an asset rather than a liability.