core-intel.io

GOVERNMENT SECURITY TECHNOLOGY

Government Security Technology Profile

Security infrastructure planning for ministries, checkpoints, public facilities, field teams and command-room operations.

Document status	Prepared for preliminary review and scope confirmation
Version	Review v1.0
Use	Briefing, due diligence, procurement, pilot planning or tender invitation
Confidentiality	No public references or project names without written approval

Audience

Prepared for ministries, public security teams, facility operators, procurement officers and IT/security departments evaluating a confidential security pilot.

Decision supported

Use this document to decide whether Core-Intel should be invited to a briefing, site survey, technical proposal, pilot scope discussion or tender response.

Recommended next step	Request a 30-minute briefing, send tender requirements or request a confidential pilot discussion.
Contact	core-intel.io | info@core-intel.io | +964 785 333 2770

Mission Fit

Start with one strategic gate, building or perimeter

Security projects should begin with a controlled site survey and limited pilot before wider procurement. Core-Intel focuses on operational control, reporting and procurement-ready documentation rather than public claims.

Ministries

Sensitive entrances, internal access flows, public reception areas and leadership reporting.

Police and courts

Facility access, evidence logging, incident routing and controlled reporting.

Checkpoints and city entrances

Vehicle flow, operator tasks, incident notes, search status and command visibility.

Airports and energy zones

Perimeter readiness, access planning, operational dashboards and escalation notes.

Public events

Temporary command visibility, field team coordination and incident summaries.

Command rooms

Central dashboards, workload queues, incident status, evidence packages and monthly reporting.

Security Solutions

Modular capabilities after site survey

Modules are selected after scope confirmation. Core-Intel does not claim fixed brands or models before site conditions, procurement rules and approved supplier options are reviewed.

Perimeter intelligence

Visibility around strategic gates, buildings, facilities and sensitive perimeters with agreed reporting and escalation paths.

Checkpoint control

Entry, inspection, assignment and incident workflows for checkpoints, city gates, facility entrances and controlled access points.

Command room monitoring

Operational dashboards for incident queues, device status, operator workload and executive summaries.

Field operations

Mobile workflows for patrols, inspectors and supervisors with tasks, checklists, location notes and daily summaries.

Evidence reporting

Controlled capture, classification, review and export of incident evidence, photos, notes and documents.

Access control

Role, location and zone-based access planning for staff, visitors, contractors and sensitive operational areas.

ANPR/VMS readiness

Planning for number plate recognition and video management systems aligned with approved hardware and procurement rules.

Site survey and scope

Vendor-neutral site survey material, constraints, equipment notes, installation scope and procurement recommendations.

30-Day Security Pilot

Site Survey -> Pilot Setup -> Monthly Report -> Expansion Recommendation

The 30-day path creates operational evidence for leadership and procurement without requiring a public announcement or large first commitment.

Step	Output	Decision value
1. Site survey	Risks, access points, existing equipment, constraints and target workflow.	Confirms realistic scope before purchase.
2. Pilot setup	Roles, dashboards, reporting model, equipment assumptions and acceptance criteria.	Creates a reviewable pilot plan.
3. Monthly report	Findings, usage notes, incident categories, gaps and improvement list.	Shows operational value without public disclosure.
4. Expansion recommendation	Procurement path, support model, training plan and next deployment scope.	Supports a controlled tender or next phase.

Deployment Bundles

Procurement-friendly security packages

Bundles help technical and procurement teams compare scope without locking the organization into unsupported brand claims.

Perimeter Intelligence Bundle

- Perimeter map
- Camera/alarm assumptions
- Incident categories
- Monthly report

Checkpoint Bundle

- Access flow
- Operator roles
- Vehicle/person notes
- Command dashboard

Field & Evidence Team

- Mobile checklist
- Photo/document evidence
- Supervisor review
- Export package

RF + Command Room Readiness

- Visibility requirements
- Connectivity assumptions
- Dashboard layout
- Escalation model

Procurement and Confidentiality

Designed for sensitive public-sector evaluation

Core-Intel can prepare site survey notes, installation scope, approved-model assumptions, supplier confirmation material, training notes and operational reports after scope confirmation.

Vendor-neutral delivery

Core-Intel can work with approved suppliers and models after site survey and procurement review.

No public references

No public project names, logos, photos or case studies without written approval.

NDA-ready

Private briefings and confidential pilot discussions can be handled under NDA.

Tender ready

Available for ministries and enterprise tenders, site surveys, technical proposals and phased delivery.

Important note

This document is prepared for early evaluation and scope discussion. It is not a certification, legal opinion or final contract. Final commitments, service levels, hosting, security controls, pricing and timelines must be confirmed in a signed proposal or agreement.