



MARKET INTEREST EVENT

'Smart Basing - Access Control'

24 April 2024 - 10:30 to 12:30

This presentation's audio will be recorded on MS Teams.

CONTENTS

- 1 Participating suppliers
- 2 Aim of Market Interest Event
- 3 Introduction & Context
- 4 Background
- 5 Aims
- 6 Requirements
- 7 Results
- 8 Deliverables
- 9 Delivery Plan
- 10 Commercial Brief
- 11 Clarification Questions
- 12 Next steps

THESE ARE SUPPLIERS PARTICIPATING IN THE MARKET INTEREST EVENT

Steadfast Security	Identec	Johnson Controls
Eagle Automation Systems Ltd	Reliance High-Tech Ltd	Chubb Fire & Security Ltd
Hunter Communication Services	Acre Security	TIS Group
BT	Knight Protection Ltd	Captec Ltd
Tensor plc	Motorola Solutions	T2 Security Ltd
Eclipse Digital Solutions	Serco	Electranet UK Ltd
Fortinet	Electranet UK Ltd	Plextek
CDS Systems Ltd	Mytec Group	Total Security Protection Ltd
Taylor Woodrow	MIG Security and Events Ltd	Kings Security Systems Ltd
Aceda	Akhter Computers Ltd	Security Solutions
Siemens plc	Synectics Security Ltd	Dual-Stream Ltd
North	Nedap	Vysiion
Obvious Technologies	Sovereign Fire and Security Ltd	BDR Group
Kubus	Reflex	Evolution (Electronic Security Systems) Ltd
Mitie	Verkada	
PA Consulting		

THE AIM OF THE MARKET INTEREST EVENT IS:

To provide the context of the Army's 'Smart Basing - Access Control' Project.

- To give an overview of the requirement and the opportunity for industry to ask Clarification Questions (CQs).
- To give a broad overview of MOD commercial processes / timelines.
- Issue a Request for Information (RFI) post event to all attendees (detail outlined in commercial brief).

Project Team attendance:

SRO - Brigadier Andy Cox

Project Director - Colonel Tom Robinson

Commercial Officer - Mr James Racheter

Project Team - Mr Gary Joynson, Lt Col Mike Pimm

SME reps - Legal, Infrastructure, Security, Finance, Information

British Army's 'Smart Basing - Access Control' Project

SRO – Brigadier Andy Cox

Chief-of-Staff Home Command

CONTEXT: BRITISH ARMY'S 'SMART BASING - ACCESS CONTROL' PROJECT

What

The British Army's 'Smart Basing - Access Control' project aims to automate pass issue and access control at Main Entry Points (MEPs) across the Army estate (88 total sites).

Why

The project believes that automated access control and pass issue will:

1. Improve the lived experience for site users.
2. Reduce the volume of required human intervention at the front gates.
3. Maintain at least the current level of site security, if not enhance it.
4. Reduce cost to allow re-investment.

How

The project seeks to do this by installing an integrated system using technology which will allow authorised users to access sites efficiently and securely with limited human intervention required.

Currently, MEPs to sites across the army estate are manned by guards who must manually issue passes and verify that each vehicle and individual attempting to enter a site has permission to enter. Each site has its own pass and there is no centralised database.

This project has identified the following key pain points in the current system:



The system is costly in terms of guarding resource and requires our civilian and military guard force to spend time on low value-adding tasks.



There is no way to check permissions between sites, meaning that if a security risk is identified, sites are not automatically updated.



Verification of car registrations, human ID and pass expiry dates is prone to human error, and guarding duties are not always completed to the security standard required.



There is a lack of evidential CCTV to support live threat identification or after-action review.



The lived experience of civilian and military personnel is impacted by delays at gates, whilst waiting for passes and by backfilling guarding tasks.

AIMS: AUTOMATION OF TASKS

The project aims to automate 2 security tasks:

Task	Details	Types of guard who can carry out this task			
		Field Army	MPGS	MGS	Contractor
Supervisors	Manage workforce / shift patterns / assurance ¹	✓	✓	✓	
Guard Comd	Responsible for managing team during shift Coordinates incident response Ensures duties correctly carried out	✓	✓		
Control of Entry	Check pedestrian / vehicle passes Open gate Restrict access to unauthorised personnel	✓	✓	✓	
Pass issuer	Issue temporary / permanent vehicle / pedestrian passes	✓	✓	✓	✓
QRF	Armed response to incidents Perimeter / base patrol Reserve workforce	✓	✓		
Armed cover	Static armed guard to cover entry points	✓	✓		
CCTV	Monitor CCTV feeds Alert guard force to incidents / suspicious activity	✓	✓	✓	✓
RiP	Reserve workforce to enable others to go on breaks	✓	✓		
Dog handler	Patrol with security dog				✓
MCC	Provide access control to Military Court Centres	✓	✓	✓	

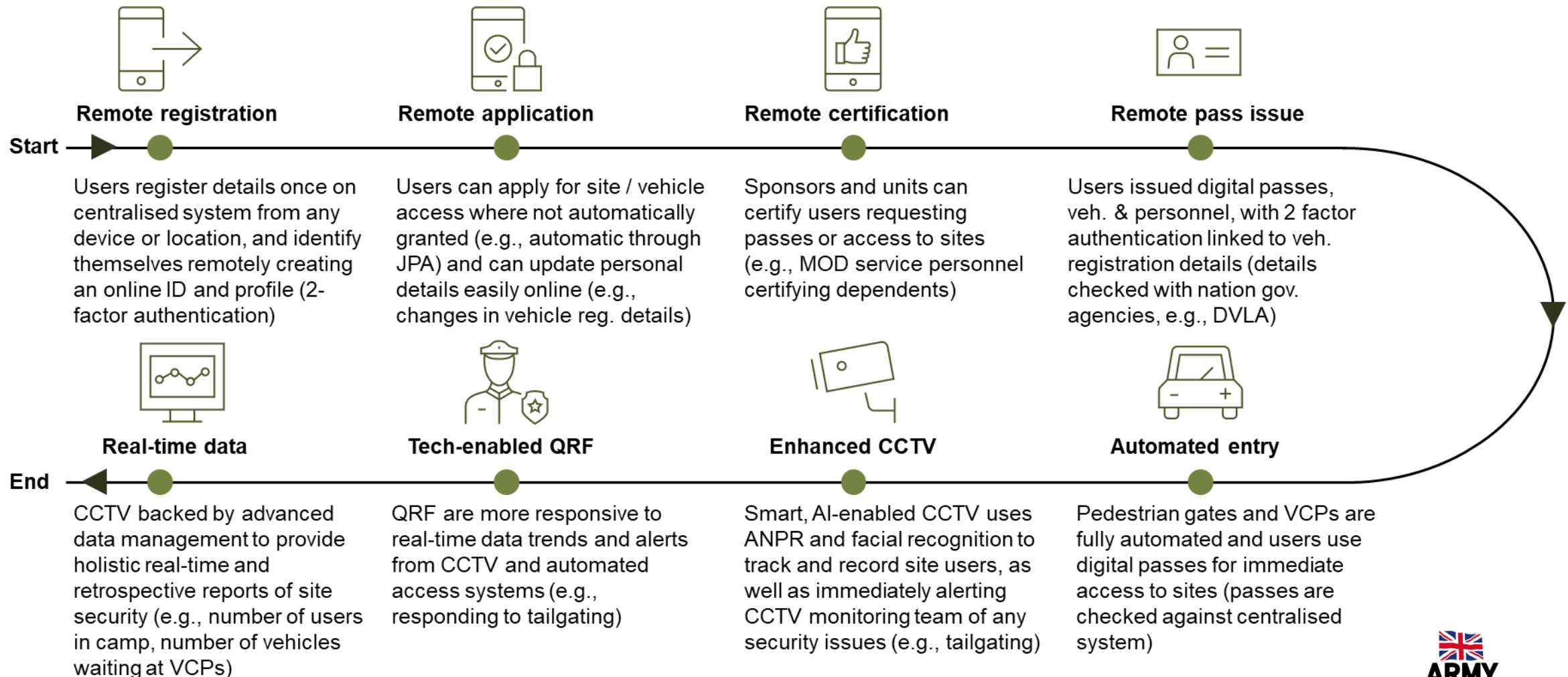
Automated Task
Armed role

NB: A guard force presence will continue at each site.

AIMS: THE AUTOMATED JOURNEY

5

The project aims to create a fully automated end to end journey for entry and exit into the 88 identified army sites



REQUIREMENTS

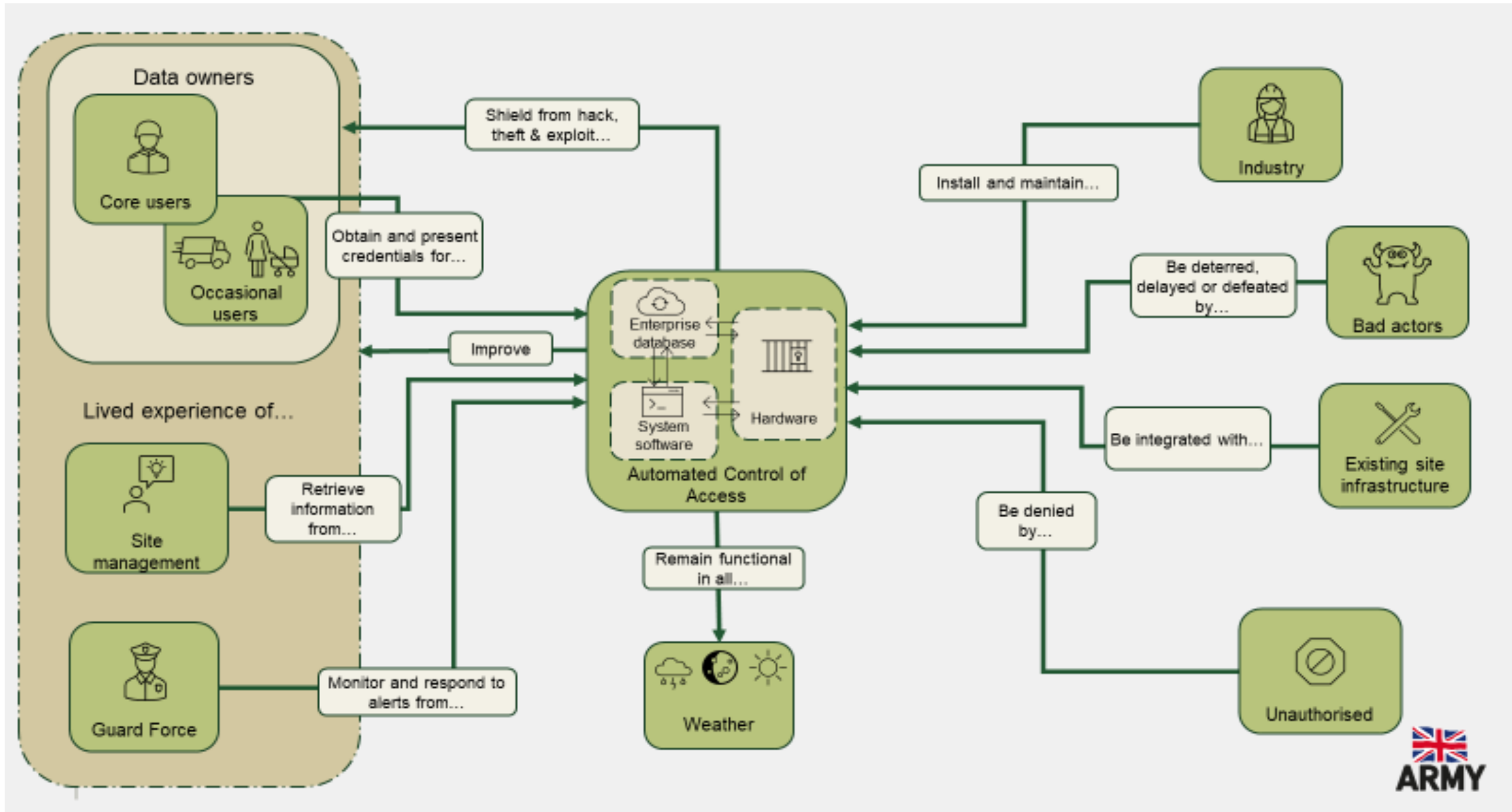
6

The following high-level requirements have been identified. A full detailed list of User Requirements will be shared.

It should be noted that the list below is not prescriptive or exhaustive, and the project is open to other solutions presented by industry.

Requirement	Detail
ANPR	Immediately recognises and logs veh. registration (triggering raising of barrier) in central data system, able to alert QRF / guard for specific vehicles of interest.
Centralised portable CCTV facilities	Wi-Fi enabled and portable CCTV capable of being centralised across multiple sites.
Online pass application and issue system	All MOD site users able to create secure cloud-based pass with real-time details of security clearance, site accesses granted, virtual ID, veh. reg, dependents, etc., (able to link with existing virtual MOD and government systems, e.g., JPA, DVLA).
Automated barriers	Both pedestrian and vehicle gates admit only one user at a time and require 2-factor authentication to ensure security integrity.
Gate surveillance and alerts	Provides immediate alerts of suspicious activity at gates to CCTV monitor / Gd. Comd., e.g., tailgating, users covering faces, pre-ID'd suspicious vehicles.
Resilience and dedicated support	Across all technologies resilience will need to be inbuilt in case of power / Wi-Fi outage, a security incident or tech failure (e.g., in-built battery, on stand-by engineer capability).
Facial recognition	Uses facial recognition cameras and cross references with information in virtual IDs to certify users prior to automated access.
Vehicle thermal imaging	Thermal camera scans all cars for non-declared passengers in vehicles, able to differentiate between human, animal, etc.
Under vehicle scanning	Conducts quick scans of underside of vehicles providing immediate alerts to CCTV monitor/QRF of suspicious items.
Secure by Design (SbD)	Solutions must employ the MOD's Secure by Design principles throughout.

REQUIREMENTS – BOUNDARY DIAGRAM



RESULTS: BETTERMENT

7

Beyond our efficiency target, the project wishes to deliver betterment across capabilities and the user experience.

Opportunity	Type
1. No requirement for separate car passes – all on one user profile.	User experience
2. Ability to manage access remotely – revoking or limiting passes.	Capability
3. Faster entry to camp with no requirement to park and book in.	User experience
4. No requirement to repeat the manual paper process for each visit to a (new) camp – passes can be valid for multiple / all camps and easily edited and controlled online.	User experience / capability
5. Guard force can more easily track visitor / contractor access in and out of camp.	Capability
6. Reduced requirement for Field Army to provide guard force / control of entry.	User experience
7. Potential to improve security with 100% pass check and facial recognition / ANPR to ensure correct identity / vehicle.	Capability
8. Ability to ensure all vehicles are correctly MOT'd and insured before access is granted.	Capability

RESULTS: SECURITY

The project wishes to provide:

- Accountability and an accurate audit trail, delivering traceability for vehicles on site and greater confidence in personnel access.
- At least maintain, if not improve security in access control with 100% pass check and facial recognition / ANPR to ensure correct identity / vehicle, with no degradation to the remaining security processes.

Principles	Deter	Detect	Delay	Deny
Extant Access Control Security	• Barriers • Guard • Passes / ID checks • Cameras – not universal	• Passes / ID Checks • Cameras • Guard	• Fences • Barriers • Physical checks • Guard	• Guard / QRF
Automated Access Control Security	• Single/Double barrier • Cameras • Automated ID pass checks • ANPR / 2 factor authentication • Guard (where threat state dictates)	• Automated ID Database checks • Time bounded access authorisation • Cameras • ANPR / 2 factor authentication • Guard (where threat state dictates)	• Fences • PAS 68 (crash rated) barriers • ANPR / 2 factor authentication • Guard (where threat state dictates)	• Guard / QRF (where threat state dictates) • Automated ID Database checks • Time bounded access authorisation • PAS 68 (crash rated) barriers • ANPR / 2 factor authentication

RESULTS: WORKFORCE

The project wishes to impact:

- **Gapping.** Currently the Army / establishments are holding guard force gaps. This has numerous impacts on establishments and the units housed there, not least an increased guarding requirement passed onto Fd Army troops.
- **Automation.** 'Smart Basing – Access Control' will focus on two core guarding tasks: access control and pass issue. In practice, these tasks are the least desirable for troops to carry out and are tasks that we have identified as appropriate for automation.
- **Flexibility.** We therefore envisage that in the initial phases of the project we will be able to free up MPGS and MGS for other tasks at their existing station, or they could be used at other locations which are holding guard force gaps.
- **Fd Army.** This should result in a release of Fd Army troops from some guarding tasks.

The Army requires an Industry Partner to deliver technology and infrastructure to meet the outlined aims and requirements and deliver the specified results.

Please note, is it not essential that one provider covers the whole scope. Multiple providers (e.g. consortium) can deliver the scope. Equally, Access Control and Pass Issue specific contractors may need to work in conjunction with existing contractors on the army estate at specific sites.

Automation	Description
Control of entry	Install technical solution and accompanying infrastructure that enables automation of: • Checking of pedestrian and vehicle passes • Confirming that they match the person / vehicle • Confirming passes are valid for the site • Opening / unlocking barrier / gate • Monitoring for unauthorised access • Locking down access as required
Pass issue	Rollout a solution that automates pass issue across all sites for all users by: • Accrediting user identity, linking with MOD and other government databases • Providing 2 factor authentication • Issuing passes that are compatible with entry and exit system, across all 88 army sites

DELIVERY PLAN

The project aims to deliver 6 entry points as a pilot and proof of concept in Year 1 (FY24/25)

Shortlist Sites	Region	PFI/PPP	Complexity
Catterick Munster Bks	North	N	L
Minley Gibraltar Bks	SE	Y	L
Cottesmore Kendrew Bks	Central	N	L
Tidworth Station	SW	Y	L
Larkhill Royal Artillery Bks	SW	Y	L
Stafford Beacon Bks	Central	N	L

Sites were selected based on multiple criteria to ensure they can be delivered within the pilot timeline (1 year) and represent a suitable cross section of UK wide sites in terms of geographic location, challenges faced (infrastructural, environmental etc) and site size and type.

Complexity was the primary driver of deliverability within a year timescale, based on the estimated volume of work required at each site to achieve automated access control and pass issue.

- Following the pilot, an assessment phase will be completed to determine the success of the delivery method and solution, with a go/no go decision for implementation across the remaining sites.
- For the pilot phase, suppliers will be required to deliver all necessary infrastructure. This will then be reviewed, and we reserve the right to change this after the pilot.
- The remaining 82 sites will undergo automation across the subsequent 5 years.

JAMES RACHETER

D INFO COMMERCIAL TEAM LEAD

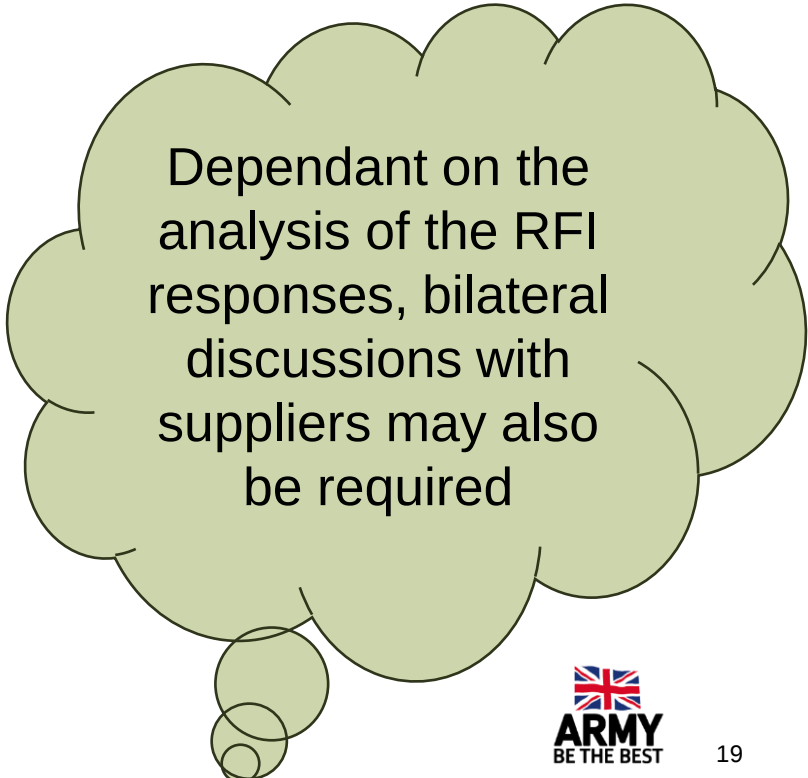
We have not yet determined the Commercial Model we will employ for 'Smart Basing - Access Control', but features will include:

- Competition.
- A role for SMEs, where possible.
- Flexibility to accommodate the pilot sites in year 1.
- Appropriate contract change control provision.
- Interoperability.
- Iterative development.
- Maintenance / through-live sustainment.

INDUSTRY INPUT TO THE COMMERCIAL STRATEGY

Responses to the Request for Information (RFI) will inform the Commercial Strategy by:

- Providing an opportunity for industry to advise MOD on perceived barriers to doing business.
- Make suppliers aware of a procurement, to engage and gain their opinion on the viability of the concept.
- Gaining insight to the market possibilities.
- Understanding risks and issues not previously considered.
- Prevent potentially unachievable procurements from being formally launched.
- Gaining a formal understanding of the potential supply base (including SMEs) and determine the amount of interest in the requirement.
- Gauging market appetite for risk and capacity to deliver the required outputs.



Dependant on the analysis of the RFI responses, bilateral discussions with suppliers may also be required

KEY INDICATIVE COMMERCIAL MILESTONES

- Early Market Engagement – now.
- OBC completion followed by Army, MOD and Cabinet Office Approval.
- ITT – August '24.
- Tender period – est. 3-4 months but dependant on Route-to-Market.

Disclaimers:

- Route-to-market yet to be determined.
- Timings are indicative and subject to internal scrutiny / approvals to proceed to the tender stage.
- No obligation for the MOD to continue with the requirement following the Market Interest Event. If suppliers choose to act on any answers and/or information they receive from this event, it is entirely at their own risk.
- Any resulting procurement procedure will be conducted competitively.

CLARIFICATION QUESTIONS

Format:

- **Raise (virtual) hand.** – Please state name and company you're representing before posing question.
- **Type question in Teams Q&A tab.** – Please include name and company in question.
- **Unanswered questions.** Where able, any unanswered questions will be responded to as part of the clarification question response.

NEXT STEPS

12

The following documentation will be issued to all suppliers who have contacted us regarding the market interest event (whether they join today or not):

- A copy of this presentation.
- DRAFT User Requirements Document (including KURs).
- Clarification Questions and Authority responses.
- RFI (issued as a separate notice on the DSP) with a 2-week response time.
- Suppliers may be invited to participate in bilateral discussions with the Authority (should analysis of the RFI responses dictate), estimated 10 – 24 May 24.

THANK YOU FOR YOUR PARTICIPATION