SMART BASING – AUTOMATED CONTROL OF ACCESS

USER REQUIREMENT DOCUMENT

Revision History

Version	Revision Date	Summary of Changes	Changes Marked
v1.0		XXXXX	
v1.1-v1.4		XXXXX	
v1.5	21 Mar 24	XXXXX	
v1.6	3 Apr 24	XXXXX	
v.1.7	17 Apr 24	XXXXX	

17 Apr 2024

USER REQUIREMENT DOCUMENT FOR SMART BASING AUTOMATED CONTROL OF ACCESS

CONTENTS

PART 1

General Description

1. This document is the repository for the user requirements that articulate the military effects and operational outcomes required to be delivered by the Automated Control of Access (ACA) Capability. Although the user requirements have been developed against assumptions and implications for Defence in the post-2024 timeframe, for Capability Planning purposes they can be considered 'enduring' for as long as Land Concepts envisage the need for those aspects of ACA and effects described in this document. Changes to the capability's definition may occur periodically as the threat it is designed to counter changes, and Defence and/or foreign policy is revised in response to shifts in the global geo-political situation. Additionally, the user requirements outlined within this document are a generic set of requirements which will be generally applicable across most sites. However, site-specific variations may prove necessary depending on either existing contracts at some sites, or where the projected cost and scale of any wholesale changes to site layout and architecture exceeds the approved budget. Pragmatic compromise between the user and service provider on an ad hoc basis may be necessary to determine a solution of 'best fit' within constraints of the candidate sites.

Single Statement of Need (SSON)

2. The Army seeks to replace its current arrangements for site access and pass issue with a networked, automated solution governing both pedestrian and vehicle traffic. If trials at our six selected pilot sites indicate a high likelihood of a successful wider rollout, the solution will be adopted at over 80 Main Entry Points (MEPs) throughout the UK, and will at least maintain and at best enhance the physical security of all sites where it is installed. This safeguards business critical assets and the personal safety of site users. The project will improve the lived experience amongst the core user groups by reducing local idiosyncratic access control measures and will streamline and simplify site access across the estate for any approved personnel. It is anticipated that automation of elements of the guarding role may necessitate a review of the demand signal for workforce requirement at candidate sites. The technical solution will incorporate available measures as advised by the selected industry partner that best meets the user's specified requirements. Any solution that facilitates and enhances the typical user journey as illustrated in Figure 3 will be given due consideration for adoption.

Background

3. Access to sites across the Army estate is presently controlled by personnel employed in the guarding role[1]. Guards are responsible for manually issuing passes according to local access policy, and must verify that each vehicle and individual presenting themselves for site access has both a legitimate need and are an approved person. This project aims to address the following shortcomings of the present

[1] The Army currently employs guards from three main populations: the Military Provost Guard Service (MPGS), who offer an armed guarding capability and are uniformed service personnel; the MOD Guard Service (MGS) unarmed civil servants predominantly employed to check and issue passes and control access. The third and smallest guarding workforce is provided by UKTAP who typically guard their own sites where MPGS or MGS are unavailable. Smaller bespoke arrangements exist in both Northern Ireland and Germany.

arrangements:

a. The system is costly in workforce terms and requires our guard force to allocate resource towards tasks of low cognitive complexity.

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

c. Verification of car registrations, personal credentials and associated expiry dates is prone to human error, so guard duties are not always completed to the standard required.

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

e. The lived experience of civilian and military personnel is adversely affected by delays at peak times and by the requirement to obtain a new vehicle pass at every site, even when an occasional visitor.

Operational Context

4. There are ten distinct tasks conducted by guard force at sites, although few sites will see the guard force perform all of these. This project aims to automate two of these tasks whilst ensuring that the Army retains the requisite SQEP (Suitably Qualified and Experienced Personnel) to perform the remaining components of the guarding role. We anticipate that the project will potentially yield opportunities for centralisation of the CCTV function and with a smaller workforce. Any potential reductions will be confirmed after completion of the pilot phase.

PRELIMINARY

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	✓	✓	✓	

Armed role

Number of supervisors is driven by the size of the guard force, so changes in headcount elsewhere will also affect supervisor numbers

Automated Tasks

1. Some supervisors will also be guard commanders. MGS supervisors often cover multiple sites

Figure 1 – Guarding Tasks

5. Although the technical solution will be operated on a site basis, it will feature networked capabilities that allows it to be upgraded and updated. A single permissions database will be created, maintained and queried regardless of the site to which a

prospective user is seeking access. A boundary diagram of the key relationships with external factors is shown at Figure 2.

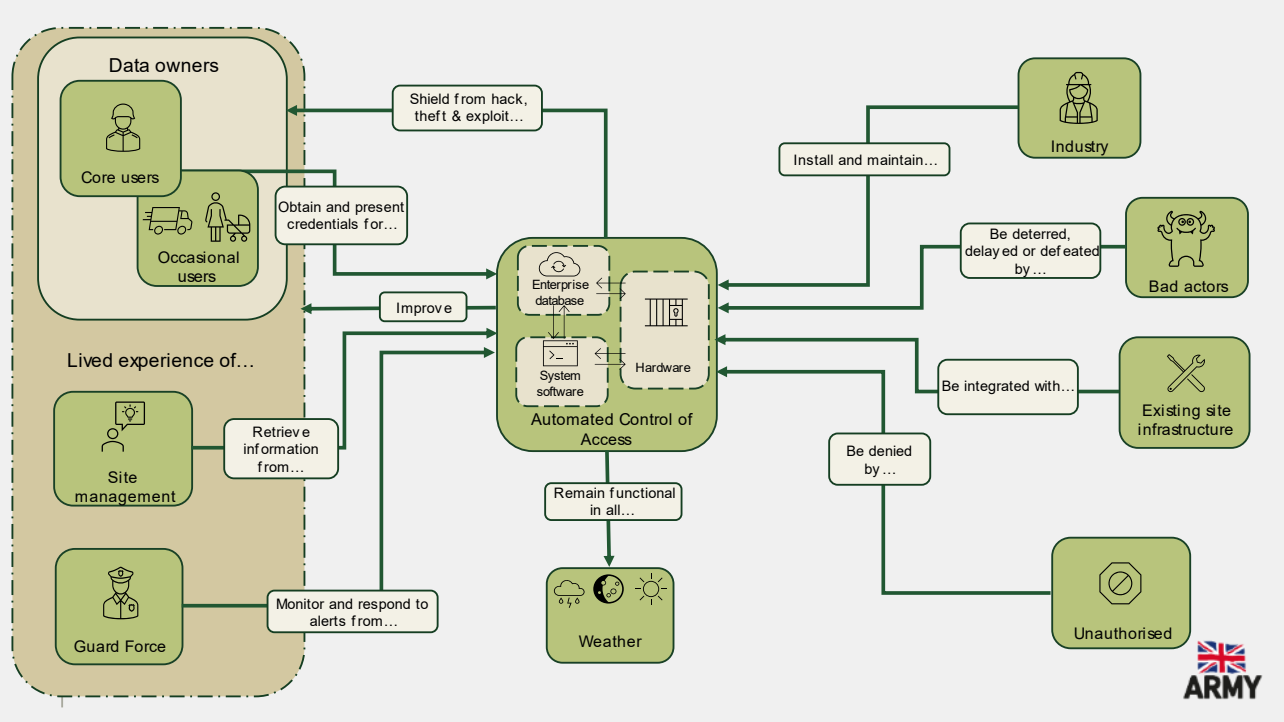

Figure 2 – Boundary Diagram

Operating Environment

6. The capability must deliver pass issue and ACA to all users of Army sites. A total of 33 distinct user personas have been identified, and for ease of reference these have been allocated to one of five ‘user journeys’ to better understand risks and pain points:

User persona	Access requirement	User	ID card
UK military personnel	based on site, requiring vehicle pass	Journey 1	MOD 90
Foreign military personnel	based on site, requiring vehicle pass	Journey 1	Foreign
MOD employee	based on site, requiring vehicle pass	Journey 1	Civil Service
VIP (including foreign)	based on site, requiring vehicle pass	Journey 1	Foreign
Foreign civil servant	based on site, requiring vehicle pass	Journey 1	Foreign
Contractors working for MOD	based on site, requiring vehicle pass	Journey 1	Photo ID
MOD spouse/partner, adult	based on site, requiring vehicle pass	Journey 1	Photo ID
UK military personnel	based on site, no vehicle pass required	Journey 2	MOD 90
UK military personnel	visitor, no vehicle pass required	Journey 2	MOD 90
Foreign military personnel	based on site, no vehicle pass required	Journey 2	Foreign
Foreign military personnel	visitor, no vehicle pass required	Journey 2	Foreign
MOD employee	based on site, no vehicle pass required	Journey 2	Civil Service
MOD employee	visitor, no vehicle pass required	Journey 2	Civil Service
Foreign civil servant	based on site, no vehicle pass required	Journey 2	Foreign
Contractors working for MOD	based on site, no vehicle pass required	Journey 2	Contractor
Contractors working for MOD	visitor, no vehicle pass required	Journey 2	Photo ID
VIP (including foreign)	visitor, no vehicle pass required	Journey 2	Foreign
External agency worker	approved list, vehicle pass required	Journey 3	Photo ID
Foreign military personnel	visitor, vehicle pass required	Journey 3	Foreign
Civilian military employee	visitor, vehicle pass required	Journey 3	Civil Service
Contractors working for MOD	visitor, vehicle pass required	Journey 3	Contractor
MOD immediate family, child	visitor, accompanied	Journey 4	N/A

MOD immediate family, child	based on site, accompanied	Journey 4	N/A
MOD Immediate family	escorted pass required	Journey 4	Photo ID
MOD family/friend	escorted pass required	Journey 4	Photo ID
Civilian emergency services	escorted pass required	Journey 5	Issued ID
UK military personnel	visitor, vehicle pass required	Journey 5	MOD 90
Foreign military personnel	escorted pass required	Journey 5	Foreign
Foreign civil servant	escorted pass required	Journey 5	Foreign
Contractors working for MOD	escorted pass required	Journey 5	Photo ID
VIP (including foreign)	escorted pass required	Journey 5	Foreign
External agency worker	escorted pass required	Journey 5	Photo ID
Guest groups	escorted pass required	Journey 5	Photo ID

Table 1 – User populations and types of access

Operating Process

7. To help visualise the end goal for the ACA project, Figure 3 shows how a user will interact with the system at various touchpoints, demonstrating a multi-layered system that demands strong multi-factor credentials paired with an automatic point of entry.

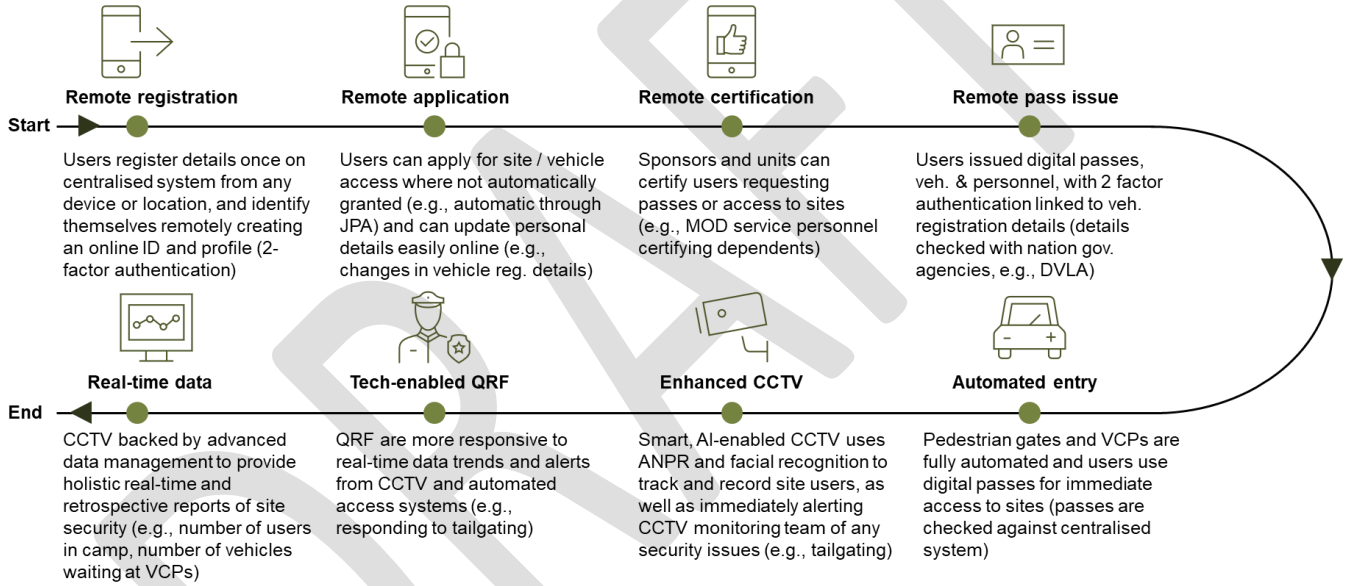

Figure 3 – Specimen user journey

Applicable Acquisition Strategy

8. The commercial strategy is still under development, with a decision point on 24 Apr 24. The Army will host an Industry Interest Day online with a view to raising awareness about the pending project amongst potential commercial partners. Once this initial engagement has taken place and the future direction is better understood, further detail will be incorporated into the FBC.

Required IOC and FOC Dates

9. It is envisaged that IOC and FOC dates will be contingent on the progress made towards installation at our selected pilot sites. There are numerous project milestones between the date of this document and the IOC date, however the aspiration is to have working access points in our six pilot sites NLT the end of 2024. Timings for the commencement of Year 2 builds will depend on the progress of the first phase of the pilot

where , but we accept that some work will have to be taken at risk. Further clarity on likely achievable dates will be provided as we better understand possible frictions associated with gaining approval from Cabinet Office and working through the non-discretionary project design processes such as Secure by Design (SbD) and Construction Design Management (CDM).

Capability Milestone	**Required Date**	**Measure of Effectiveness**	**High Level Measures of Performance**	
IOC	Start of Pilot	Six sites with one automated and functional VCP each. Guard force to remain in place	*Training*	*Site users and guards at pilot sites trained on use of automated access system plus reversionary method and pass issue.*
			Equipment	*Six automated VCPs (one automated VCP at each pilot site). Exact equipment TBD by suppliers.*
			Personnel	*No change*
			Information	*Comms to be issued to all pilot site users in advance of IOC date.*
			Doctrine	*n/a*
			Organisational	*n/a*
			Infrastructure	*Installation of new gates (and any other infra TBD by supplier) at six pilot sites.*
			Logistics	*Maintenance and support contract in place at pilot sites.*
FOC	End of Pilot	Six sites with one automated VCP each. Access control and pass issue personnel withdrawn. System ready to be rolled out at up to up a total of 83 entry points across 72 sites following selected CoA plan. Commencement of Year 2 builds will occur whilst the pilot is ongoing.	*Training*	*Site users and guards at pilot sites trained on use of automated access and pass issue. Training to commence at next sites due to receive automation.*
			Equipment	*Six automated VCPs (one automated VCP at each pilot site). Exact equipment TBD by suppliers. Equipment ready to be implemented at next sites due to receive automation.*
			Personnel	*Access control and pass issue personnel withdrawn and re-tasked or re-roled.*
			Information	*Analysis of pilot site traffic and throughput complete at each of the three phases. Messaging about outcome of pilot to be issued Army wide. Further comms to be issued to next sites due to receive automation.*
			Doctrine	*Remote CCTV room and QRF concept tested and exercised. New SOPs written and distributed to guard force.*
			Organisational	*Changes to organisational structures may be necessary at sites where ACA indicates that the demand for pass issue and access control is reduced.*
			Infrastructure	*Installation of new gates (and other infrastructure TBD by supplier) at six pilot sites. Infra ready to be*

				implemented at next sites due to receive automation.
			Logistics	*n/a*

Table 2 – IOC and FOC conditions

Planned OSD

10. To be determined on discussion with the chosen supplier once the component parts of the system have been identified and selected. Some elements of the system will be unsophisticated and have a long lifespan, whereas others are more likely to require routine updates and upgrades. At the OSD, ACA will be replaced by a system with similar capabilities, recognising that new technology may be available. Further clarity about the anticipated lifespan of the equipment procured will be incorporated into the FBC once engagement with industry has commenced.

Interoperability

11. The system may be dependent on Army Estate Wide Internet Access (AEWIA). Engagement with industry partners will confirm this dependency. The system will also be dependent on some existing MOD or other Government digital systems and security architecture[2]. Engagement with industry partners will confirm this. The system should avoid the use of or be protected against interference from parts of the EM spectrum commonly employed by civilian or military communications devices.

Constraints

12. The ability to alter the layout of certain sites and their approach roads to the extent required to implement a fully featured ACA solution may not be feasible in all situations. It is also recognised that for various reasons some sites may be unsuited to the introduction of ACA[3], and these have been removed from consideration during the scoping phase of the project. The system must conform to NPSA and NCSC standards.

The system adopted must be safe to use and must comply with Army and MOD SHEF policy to protect users. Construction Design Management principles as stipulated by the Health and Safety Executive will be followed throughout. Legal constraints, such as the prohibition on use of mobile phones by the driver of a vehicle, will also constitute a constraint in that we must develop solutions other than the most straightforward one for the envisaged use case. The implications of compliance with the full range of regulations, including but not limited to GDPR and RIPA have been considered, and mitigations incorporated into the user requirements listed to protect the Authority from liability and specify a solution that is compliant in all three areas.

[2] Including but not limited to: Defence ID Cards, DVLA databases, JPA, MyHR, Defence Gateway, HM Passport Office, Digital Identity for Defence.

[3] Due to the skewed user population that typically access Army Ph1 training establishments and some remote sites, a series of MJPs (Military Judgement Panels) will sit after the pilot rollout to determine whether it is feasible to implement a version of ACA without compromising security provision.

Priorities

Priority	Meaning
Key	A User Requirement that may drive design and/or cost and which may require innovation or technology update (with the associated risk) to achieve the aim. A Key User Requirement (KUR) may not be traded below the Threshold without major implications for Capability/project feasibility.
Mandatory	A User Requirement, generally a User Constraint, designated as such for legal or safety reasons and which may not be traded.
Priority 1	Highest priority reflecting a primary user requirement that may drive design and/or cost and which may tolerate acceptable levels of risk to achieve the aim. Trade-off below Threshold will require approval of the SRO.
Priority 2	A secondary user requirement, which may have design and/or cost implications but will not tolerate project risk to achieve the aim. Trade-off below the Threshold will require approval of the OF5 Project Lead.
Priority 3	Lowest priority reflecting a tertiary user requirement, which may have design implications but will not have cost implications and which will not tolerate project risk to achieve the aim. Trade-off below the Threshold will require the approval of the SO1 Project Lead.

Table 3 – Priority definitions

Capability Model

13. A general representation of how the capability might work is provided at Figure 3. Although it demonstrates a possible example of one of the ways in which the possible technical solution that might be provided, it should not constrain thinking about alternatives which might achieve the same outcome.

Capability Users

14. The Automated Control of Access system will be used by:

a. All individuals and vehicles entering sites where the capability is installed.

b. Guard force and QRF.

c. Monitoring teams.

d. Site management.

e. Maintenance and support teams.

Capability Stakeholders

15. **Sponsor.** The programme sponsor is Comd Home Command.

16. **Senior Responsible Owner.** The Senior Responsible Owner is COS Home Command.

17. **Other Stakeholders.** The hierarchy of other areas with a vested interest throughout the life cycle of the project is represented in Figure 4.

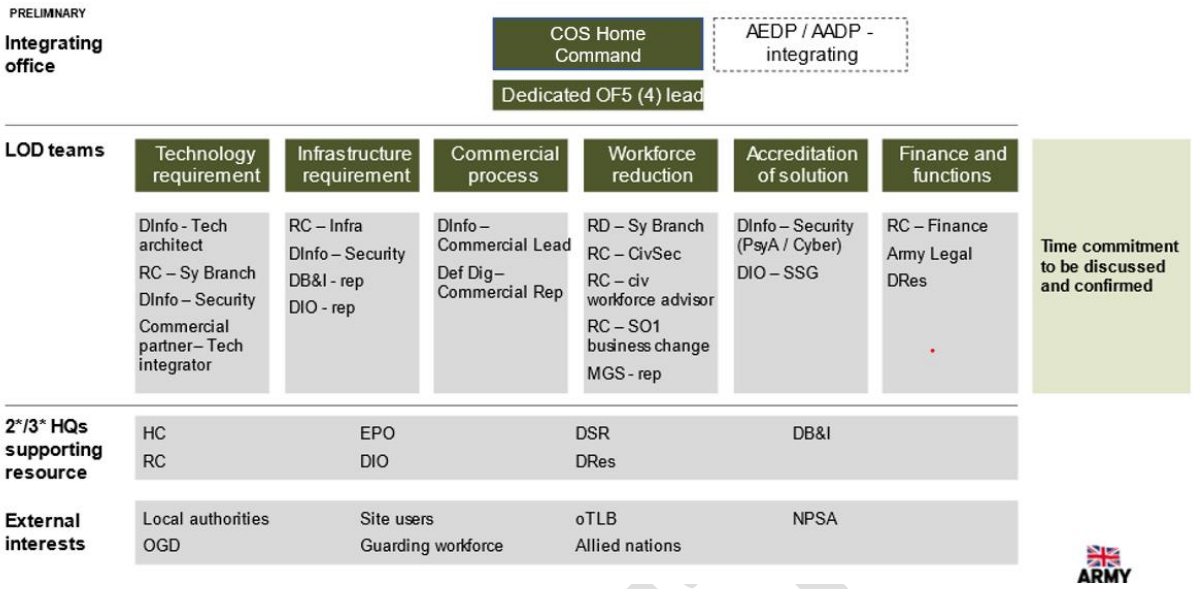

Figure 4 – Stakeholder hierarchy

Dependencies

18. This project is linked to Home Command's Pj IRONSIDE and is one of the strands within IRONSIDE to realise efficiencies that might be made by adopting smarter ways of working and so reduce the overall cost associated with providing and sustaining the Army's Firm Base. As such, the SmartBasing concept is dependent on the direction of travel of IRONSIDE, but also on the subordinate dependencies outlined in Table 4.

	Dependencies	**Comments**
D1	DBI rollout	To implement the tech solution, sites need to have access to reliable and fast internet. This is already complete at most sites through DBI, but this must underpin ACA.
D2	Enterprise Data access	For the team to assist in optimisation activities, the HC PMO will require access to data from throughout the enterprise, including Army and DIO.
D3	Empowerment of HC to drive commercial / DIO prioritisation	This project will require that commercial resource and site infrastructure works are prioritised to deliver in the required timeframe. HC will need to be empowered to draw on dedicated commercial resource and influence DIO priorities.
D4	Engagement with project implementation	Delivery of the project benefit is subject to the implementation of changes to process, tools and commercials. The implementation of these changes would need to be led from RC rather than any AEDP team.
D5	Stakeholder attendance at meetings	The project will require stakeholders from RC and Army HQ to attend regular project governance and deep dive working sessions. This includes but a monthly sponsor group and bi-weekly governance group.
D6	SME time commitment	This project will require a time commitment from SMEs across MOD including. DInfo, Army Commercial, Defence Digital, Regional Command Infra and Security. The core team/AEDP will endeavour to minimise the time commitments required.
D7	Access to AADP sprint teams to support delivery	The responsibility for the completion of business cases will largely fall to AADP and AEDP team members.

		Recruitment is underway for a dedicated HC team to project manage pilot and longer term roll out. Both teams will be able to draw on support from x-DLoD SMEs for the duration of their involvement in the project.
D8	Op HIDAGE	Proposed solution needs to account for Op HIDAGE redeployment of personnel.
D9	RC Infra validation of assumption	For the cost model to be validated prior to submission to the AIC, there is a requirement for RC Infra to validate the VROM Infra Cost assumptions contained in the model. Work has been conducted by HC Infra to confirm the assumptions included below at Infra 1 – 6 inclusive.
D10	RC Security	For the cost model to accurately predict workforce benefits, RC Security must provide insight into natural wastage tempo and help determine sites where ACA is unlikely to be an adequate replacement for the status quo.
D11	Local authority engagement	To set the conditions for a successful rollout of ACA, some sites may need elements of their MEP (Main Entry Point) redesigned, and this may have an impact on the pace and volume of traffic on public roads. Planning permission for changes may be required.
D12	Government certification	The solution procured will need to conform to NPSA standards and NCSC regulations.

Table 4 – Project Dependencies

Assumptions

19. Assumptions have been made throughout the scoping and planning phase of the project and are listed below against each of the DLoDs in Table 5.

Ser. (MDAL)	Assumption Title	Data/ Assumption	Source
Training			
T-1			
Equipment			
E-1	Tech costs per establishment	Tech cost per establishment: £168,927	Quote from industry provider
E-2	Tech costs per site	Tech cost per site: £12,775	Quote from industry provider
E-3	Tech costs per entry point	Tech cost per entry point: £33,664	Quote from industry provider
E-4	Tech cost centralised system	Tech cost for centralised pass system: £2,000,000	DInfo Business Assumption
E-5	Tech Opex	Annualised tech running costs: £3,000,000	DInfo Business Assumption
E-6	CCTV cameras per Entry Point	5	Business Assumption
E-7	Initial set up fee per CCTV camera	£1,000	Industry Benchmarking
E-8	Equipment Cost per CCTV camera	£2,000	Industry Benchmarking
E-9	Annual Monitoring per CCTV camera	£1,800	Industry Benchmarking
Personnel			

P-1	Rollout task elimination	Rate of task elimination through year of automated rollout: 50%	AEDP Analysis
P-2	WF Fin Control Total Headcount	WF Control Total based on planned MPGS headcount of 1337	TLB WF Fin Team
Information			
I-1			
Concept and Doctrine			
C+D-1	Risk adjustment level	Risk adjustment to stated 10yr Net Efficiencies: 70% (ML3)	Defence Maturity Level Framework
Organisation			
O-1	Headcount complementing ratios	Ratios have been used to determine the headcount complement for shift tasks - the ratios are listed in the Assumptions Reference tab	RC Security
O-2	Supervisor Scaling Factors	Scaling factors are used to determine supervisor numbers based on staffing levels at each establishment - the scaling factors are listed in the Assumption References tab	RC Security
O-3	Grade split per task	The grade split per guarding task can be found in the Assumption References tab	RC Security
Infrastructure			
Infra-1	Infra costs - Low Complexity	Low complexity entry points incur a VROM Infra Cost of £272,720	SPONS, Historic Examples
Infra-2	Infra costs - Medium Complexity	Medium complexity entry points incur a VROM Infra Cost of £553,977	SPONS, Historic Examples
Infra-3	Infra costs - High Complexity	High complexity entry points incur a VROM Infra Cost of £728,064	SPONS, Historic Examples
Infra-4	Infra cost - CDEL vs RDEL	Infra costs incurred will be CDEL	AH Infra Finance
Infra-5	PFI CAPEX	Infra CAPEX costs will be multiplied by 1.568 at PFI sites	DIO Contract Management team
Infra-6	PFI OPEX	Infra OPEX costs will be calculated by applying a 1.110 multiplier to PFI capex costs	DIO Contract Management team
Logistics			
L-1			
Interoperability			

Inter-1			
Unofficial DLOD	**DATA/ ASSUMPTION**		
CP1	General Inflation Rate	10yr average annual inflation rate: 2.5%	Indigo
CP2	Construction Inflation	Construction inflation rates for New Work as listed on Indigo	Indigo
CP3	Rollout start date	Start of rollout: FY25/26	Implementation Plan
CP4	Public Interest sites out of scope	Those sites which attract significant public interest will not be automated under this program because it is likely that guarding will need to be retained at the entry points - there are five sites listed out of scope for this reason, listed in the Assumption References Tab.	RC Security Branch
CP5	Net benefit threshold	Sites where the 10yr net benefit gained from automation is <£150k will be out of scope.	AEDP Analysis
CP6	Government Furnished Assets	The project will not make use of Government Furnished Assets.	AEDP Analysis
CP7	VAT Recovery	All cost estimates included in this model are exclusive of VAT. It is anticipated that most of the VAT incurred on the costs can be recovered, in line with policy stated in JSP 916 'MOD Tax and Duty manual'. Annex A to JSP 916 Part 2 Chapter 5 outlines the eligible services for VAT refund.	JSP 916

Table 5 – Project planning assumptions list

PART 2

Key User Requirements

20. Four KURs have been identified: Security, Networked, Reliability and Throughput. Table 6 outlines why each element is essential, and documents how the effect of each will be measured.

KUR	Description	Threshold MOE	Objective MOE	Justification
Title of KUR	*A text descriptor of the KUR*	*The minimum level of acceptable capability*	*The preferred level of capability needed/the level of capability beyond which there is point in investing*	*Why the KUR is needed and why the threshold level is set at a particular level*
Security	The authority requires the capability to safeguard its selected sites from unauthorised access through an automated entry point whilst simultaneously providing a seamless and intuitive user experience for authorised personnel.	Personnel who are not pre-authorised to enter a site should not be afforded access through an automated entry point by bypassing, brute forcing or surreptitiously circumventing the procured system.	A database of approved personnel and vehicles will be maintained. Personnel whose access authority status changes will have their credential withdrawn or flagged immediately. Vehicles that fail to comply with site access regulations will be similarly subject to flagging and restricted from entry via the automated system.	The capability will only be procured across the Army estate if it can be demonstrated that the present levels of security provided by the human guard force is maintained or can be improved upon.
Networked	The authority requires the capability to incorporate a single 'authorised person' database which allows for remote ID verification as well as site access patterns across the Army estate to be interrogated	Users should be able to apply once by verifying their identity with a government issued ID[4]. This will generate a credential which will be accepted by the ACA system across all sites on	As for threshold, but the system should allow for pan-estate banned lists of both personnel and vehicles, and 'flag up' attempts to access sites by banned personnel to all sites on the network. The network should cater for the push of updates and security patches	The current solution sees sites operate in isolation, maintaining local lists of banned vehicles. It relies on the manual distribution of security warnings to inform the guard force at each site of the possibility that persons of interest will attempt access to Army sites. Adoption would ensure an 'all informed net' and allow for updates to be pushed to all sites using the network.

[4] MOD 90, UK, EU or Commonwealth passport, UK or EU driving licence, PASS card, Voter Authority Certificate or similar.

	by a super-user population (TBD). The method of obtaining a credential for the first time should be available on a range of personal or issued devices and in any location with internet access, including at the point of need.	the network. The network and its component parts must be protected against remote denial of service attack or other exploit that might permit illegitimate access to either the system itself or the Army sites where ACA is installed. Personal data of those registered for ACA will be protected, and the system as a whole shall conform to the MOD Secure by Design (SbD) principles.	and have the capacity to handle all the sites at which ACA will eventually be adopted.	
Reliability	The authority requires the capability to be reliably used 24/7 in all weather conditions likely to be encountered within the British Isles. It must also conform both in hardware and software terms, to relevant NPSA and NCSC standards, and be protected and hardened against brute force attacks and potential spoofing.	The system shall achieve a minimum of 90% uptime in any given rolling 30-day period. A manual or remote activation method should be incorporated into the design allowing for guard force to occasionally override the system.	As for Threshold, except that the system shall achieve a minimum of 95% uptime in any given rolling 30-day period. Each component (pedestrian or vehicle) shall be capable of completing 1,000 cycles per working day without more than routine, scheduled maintenance periods that still meet the uptime criteria.	The ability of the authority to surge personnel to replace a broken system should not be relied upon. Nevertheless, a reversionary means of operation is still required.
Throughput	The capability should be able to accommodate anticipated peak access demands at sites where it is installed to the same or	The system shall be able to cycle and admit a vehicle before resetting to receive credentials for the next within 15 seconds.	As for Threshold, except that the automated vehicle access system should complete its cycle within ten seconds.	Analysis indicates that at some busy sites in excess of 700 vehicles per hour may enter within peak times. Therefore, in order to avoid causing congestion and queues on the access roads, the system must be

	better standard achievable with a human guard force.	Personnel entering sites via a pedestrian gate should be able to enter within ten seconds of presenting their credential to the sensor.		designed to cope with the volume of entry attempts without compromising security.

Table 6 – Key user requirements

PART 3

Detailed User Requirements

21. There are currently 68 proposed URs, documented below.

ID	User Requirement	Remarks	Measure of Effectiveness			Requirement Type	Candidate Priority	Justification	Owner	Proposed Validation Method	Status
			Threshold	Objective	Status						
UR 1.1	As a [user], I must be able to apply for and receive vehicle and personnel [system credential]s through a secure online service.	Service must be accessible for all users (military and non-military) as an application on MODNET and FDIS through browser from any internet-enabled device (computer, phone, tablet, etc).	Service available on internet enabled devices (browser).	Service available on all mobile devices and via all internet enabled devices (app and browser).	TBC	Functional	Priority 1	JSP 440	D Info	[System credential] issuing service must be compatible with multiple mobile platforms (both iOS and Android) as well as accessible to users via any internet browser on different internet enabled devices (e.g., both app for mobile pass and users accessing through browser on laptops). The ability to apply in advance of arrival, or at the point of need should be supplied. It should be generated in pdf or similar to allow for screenshots or hardcopy printing.	Candidate
UR 1.2	As a [user], I must be able to apply for and receive vehicle and personnel [system credential]s	System should issue permission to enter in two minutes or less and be available 24/7.	[System credential] should be issued in less than three minutes and the facility to register and apply be available 24/7.	[System credential] should be issued in less than two minutes and the facility to	TBC	Functional	Priority 1	JSP 440	D Info	Application, authorisation (including multi factor and interfacing with other platforms) and granting of	Candidate

ID	User Requirement	Remarks	Measure of Effectiveness			Requirement Type	Candidate Priority	Justification	Owner	Proposed Validation Method	Status
			Threshold	Objective	Status						
	through a secure online service.			register and apply be available 24/7.						permission (and pass printing is required) should be complete in less than two minutes.	
UR 1.3	As a [user], I must be able to apply for and receive vehicle and personnel [system credential]s through a secure online service.	Service must have a user-friendly interface, accessible equally by all [user] groups.	n/a	n/a	TBD	Functional	Priority 2	JSP 440	D Info	The service must guide the [user] intuitively through a minimal number of steps to apply for a [system credential], download any passes, update profile details and use passes when reaching sites. All [user]s must be able to easily use system (including ability to update and apply for new [system credential] or permissions).	Candidate
UR 1.4	As a [user], I must be able to apply for and receive vehicle and personnel [system credential]s through a secure online service.	Service must have unique [user] profiles and visible to [guard force], [system administrators] and [site management], ensuring registration needs to be completed once. One profile is necessary per [user] across the	n/a	[User] must only have to create a profile once unless it is deleted (automatic deletion in timeframe specified by Data Protection Act, GDPR, 2018, where use policy directs)	TBC	Functional	Priority 1	JSP 440	D Info	The service will manage [user] profiles in accordance with The Data Protection Act, GDPR, 2018 and use an authorised source to validate credentials against. [User]s register initially and a profile is created, [user]s can add information to this profile when	Candidate

ID	User Requirement	Remarks	Measure of Effectiveness			Requirement Type	Candidate Priority	Justification	Owner	Proposed Validation Method	Status
			Threshold	Objective	Status						
		whole network; not site specific. Profiles should be regularly matched against definitive personnel database(s) and accounts declared moribund or pass withdrawn if legitimate need for access changes.								required (e.g., upon completion of driving test [user]s can add their driver's license details and [user vehicle] details), profile remains for set period (e.g., two years) or deleted when they request deletion, and is visible to authorized users only (profile only shows relevant non-GDPR protected information). The service must comply with MOD policy on the retention of personal information and be able to securely store OFFICIAL-SENSITIVE PERSONAL data in accordance with JSP 440.	
UR 1.5	As a [user], I must be able to apply for and receive vehicle and personnel [system credential]s	Service should be customisable on a global and site basis through permissions based access controls	n/a	[System administrator] profiles must have edit and authorisation access to accounts	TBC	Functional	Mandatory	JSP 440	D Info	Service will have the ability for [system administrator]s to manage all passes and impose blanket constraints on	Candidate

ID	User Requirement	Remarks	Measure of Effectiveness			Requirement Type	Candidate Priority	Justification	Owner	Proposed Validation Method	Status
			Threshold	Objective	Status						
	through a secure online service.	authorised by the [authority].								passes (e.g., all passes / permissions must be renewed annually), also approved administrators are able to authorise this at the individual site-level (e.g., for some sites special permissions must be sought, vehicle passes are only valid for one day)	
UR 1.6	As a [user], I must be able to apply for and receive vehicle and personnel [system credential]s through a secure online service.	System must provide a security role-based model to permit assignment of administrators and other security roles as set by the [authority].	n/a	Administrator profiles must have edit and authorisation access to accounts.	TBC	Functional	Priority 1	JSP 440	D Info	Service must have the ability allow centralised administrators to assign local administrators who have authority to approve and sponsor applicants for specific sites or military units.	Candidate
UR 1.7	As a [user], I must be able to apply for and receive vehicle and personnel [system credential]s through a secure online service.	Service must have the ability to automatically authorise access if certain key criteria are reached (group assignment model).	Require one senior approval for access.	Automatically authorise access.	TBC	Functional	Priority 1	JSP 440	D Info	The [access control system] will incorporate a group assignments model to enable management of group access based on validation criteria, where required. E.g., [system administrator]s for a	Candidate

ID	User Requirement	Remarks	Measure of Effectiveness			Requirement Type	Candidate Priority	Justification	Owner	Proposed Validation Method	Status
			Threshold	Objective	Status						
										certain site state that anybody who works for the MOD can have unlimited vehicle and personal access, thus any [user] applying who has already had their MOD status verified is automatically granted a [system credential]. The system should identify what type of permission is required and issue a [system credential] that is easily visually distinguishable by [guard force] to identify [user] type.	
UR 1.8	As a [user], I must be able to apply for and receive vehicle and personnel [system credential]s through a secure online service.	[User] must be able to change vehicle details and update personal details as required, using the secure online service and application. Routine updates to personnel data (name, capbadge and rank changes) should be automatically uploaded to the	[System administrator] can change details at request.	[User]s can change details of their profile	TBC	Functional	Mandatory	JSP 440	D Info	This is to ensure that information such as vehicle registration and security vetting details can be updated when needed by the user without the requirement to re-apply for permissions (details should be able to be cross checked / authorised, where relevant, e.g.,	Candidate

ID	User Requirement	Remarks	Measure of Effectiveness			Requirement Type	Candidate Priority	Justification	Owner	Proposed Validation Method	Status
			Threshold	Objective	Status						
		[access control system].								security clearance check against SC Database or JPA). Frequent vehicle changes will prompt a user alert to allow manual checks.	
UR 1.9	As a [user], I must be able to apply for and receive vehicle and personnel [system credential]s through a secure online service.	[Access control system] must comply with GDPR and data privacy regulations and notify [user]s of required usage and consent required.	n/a	[Access control system] must comply with GDPR and data privacy regulations.	TBC	Non-functional	Mandatory	JSP 440, Information Commissioner's Office Guidelines incl. GDPR guidance, Data Protection Act 2018, Data Protection Act Guidance Note 11: CCTV and Data Protection Considerations.	D Info	The [access control system] must prompt and record [user]s signing any required authorisations for use of personal data as stipulated in data protection legislation.	Candidate
UR 1.10	As a [user], I must be able to apply for and receive vehicle and personnel [system credential]s through a secure online service.	[Access control system] generates automated alert to notify registered [user]s of changes to their [system credential] / access rights.	[Access control system] confirms [user] of change on screen once change has been made.	[Access control system] issues a post change notification via another method of communication.	TBC	Functional	Priority 1	JSP 440	D Info	If [user] permissions or details are changed or updated, then system will push an automated notification to the [user] on their contact platform of choice (e.g., through app, SMS, email) – service should ensure [user]s do not have to log in to service to check if changes have taken place.	Candidate

ID	User Requirement	Remarks	Measure of Effectiveness			Requirement Type	Candidate Priority	Justification	Owner	Proposed Validation Method	Status
			Threshold	Objective	Status						
UR 2.1	As a [user] I must be able to verify my identity and authority for site access, linking with MOD and other government databases as required and human authorising agents, generating a [system credential].	[Access control system] must be able to accredit users who provide government issued identification digitally (e.g., MOD 90, passport, driving license).	[Access control system] must accredit users within 1 minute using at most 2 forms of ID.	[Access control system] must accredit users in less than 30 seconds using 1 form of ID.	TBC	Functional	Priority 1	JSP 440	D Info	[Access control system] must enable rapid and secure verification of MOD or gov issued documents, similar to virtual passport or driver's license applications and renewals now, to confirm [user] identity (able to scan identity documents, then take or upload self-picture that is checked against government databases, DVLA, Insurance DB, Digidentity, JPA).	Candidate
UR 2.2	As a [user] I must be able to verify my identity and authority for site access, linking with MOD and other government databases as required and human authorising agents, generating a [system credential].	[Access control system] must be able to interface with existing MOD or .gov. digital systems.	[Access control system] must interface with critical MOD or .gov digital systems.	[Access control system] must have the ability to interface with all MOD or .gov digital systems	TBC	Functional	Priority 1	JSP 440	D Info	[Access control system] must be able to check and work alongside existing MOD digital systems to confirm [user] details and site permissions where relevant, ie through API to JPA. It is expected that this will include integration with MOD Cloud through a secure gateway. This may include DVLA and .gov	Candidate

ID	User Requirement	Remarks	Measure of Effectiveness			Requirement Type	Candidate Priority	Justification	Owner	Proposed Validation Method	Status
			Threshold	Objective	Status						
										database verification as required.	
UR 2.3	As a [user] I must be able to verify my identity and authority for site access, linking with MOD and other government databases as required and human authorising agents, generating a [system credential].	[Access control system] must allow [user]s registering and / or applying for a[system credential] to be verified by sponsors.	Allow [user]s to be verified by one sponsor per site.	Allow [user]s to be verified by nominated sponsor	TBC	Functional	Priority 1	JSP 440	D Info	[Users] whose identity is accredited are then able to have their details validated for access by approved sponsors who can vouch for them, through automated email to that sponsor (e.g., a civilian contractor has identity confirmed and then sends request for access to their MOD employing contact at site, who confirms they are needed at site, then their [system credential] can be authorised by site).	Candidate
UR 2.4	As a [user] I must be able to verify my identity and authority for site access, linking with MOD and other government databases as required and human authorising agents, generating	[Access control system] must allow [site management] to set what information / identification is required to allow access.	Allow one main [system administrator] to set what information is required	Allow a set of [system administrator]s to set what information is required.	TBC	Functional	Priority 1	JSP 440	D Info	[System administrator]s may need to change the identity / information requirements for [user]s and should be easily able to do so (e.g., may be decided that when registering a [user vehicle] they must provide insurance	Candidate

ID	User Requirement	Remarks	Measure of Effectiveness			Requirement Type	Candidate Priority	Justification	Owner	Proposed Validation Method	Status
			Threshold	Objective	Status						
	a [system credential].									and driver's license details – which can be verified through DVLA link).	
UR 2.5	As a [user] I must be able to verify my identity and authority for site access, linking with MOD and other government databases as required and human authorising agents, generating a [system credential].	[Access control system] is to replace the existing Army SISYS system.	n/a. Data transfer from SISYS desirable.	Removal of SISYS.	TBC	Functional	Mandatory	JSP 440	D Info	Army currently utilising SISYS which will be superseded by proposed [access control system]. Data transfer from SISYS desirable to facilitate referral database/history upon which to draw for streamlined site access.	Candidate
UR 2.6	As a [user] I must be able to verify my identity and authority for site access, linking with MOD and other government databases as required and human authorising agents, generating a [system credential].	[User]s and [system administrator]s must have the ability to use multi-factor authentication.	Support one time code texted to device	Support muti factor authorisation such as biometric authentication (fingerprint, face recognition) or one-time passwords / codes, ANPR.	TBC	Functional	Mandatory	JSP 440	D Info, PsyA	Sites and users must have the ability to print [system credential]s if necessary for inspection by [guard force] if necessary (ie if the threat state increases), Administrators should also be able to access details of user's permission levels and print a temporary [system credential] for [user]s (if required). The [access control system] should be viable for multi-factor	Candidate

ID	User Requirement	Remarks	Measure of Effectiveness			Requirement Type	Candidate Priority	Justification	Owner	Proposed Validation Method	Status
			Threshold	Objective	Status						
										authentication, where regular access requirement is facilitated by a proximity chip reader, and casual access is facilitated by a one-time code texted to a mobile device- see 3.2 below.	
UR 2.7	As a [user] I must be able to verify my identity and authority for site access, linking with MOD and other government databases as required and human authorising agents, generating a [system credential].	[Access control system] must allow varied access levels and time allowances	[Access control system] must allow for 5 different user types	[Access control system] must allow for 10 or more different types of users	TBC	Functional	Priority 1	JSP 440	D Info	The [access control system] will support multiple access levels, allowing different [user]s to have varying levels of access based on their permissions, e.g., differentiating between [pedestrian]s, vehicle owners, residents, visitors, and service personnel. Service should allow [system administrator]s and [site management] to set time-based access control rules, detailing specific time periods during which certain [user]s or [user] groups are granted ingress or egress,	Candidate

ID	User Requirement	Remarks	Measure of Effectiveness			Requirement Type	Candidate Priority	Justification	Owner	Proposed Validation Method	Status
			Threshold	Objective	Status						
										ensuring enhanced security and control and sending notifications to [site management] with a duty of care.	
UR 2.8	As a [user] I must be able to verify my identity and authority for site access, linking with MOD and other government databases as required and human authorising agents, generating a [system credential].	[Access control system] should allow customisable access permissions for temporary [user]s.	Allow set [user] groups to have set permissions.	Allow [system administrator]s to assign and change permissions against all [user] groups.	TBC	Functional	Priority 1	JSP 440	D Info	The service should allow [system administrator]s to set specific access permissions for temporary [user]s, such as service personnel or delivery drivers, based on their specific roles or tasks, ensuring fine-grained control.	Candidate
UR 2.9	As a [user] I must be able to verify my identity and authority for site access, linking with MOD and other government databases as required and human authorising agents, generating a [system credential].	[Access control system] must ensure a maximum expiry date of 3 years and be linked to security clearance dates, with the ability to automatically withdraw passes if no longer serving or employed by MOD.	n/a	Link [system credential] to SC dates and expire in no more than 3 years.	TBC	Non-functional	Mandatory	JSP 440	D Info, PsyA	JSP 440 states that passes need to be linked to security clearance and expiry dates and for no more than three years.	Candidate
UR 2.10	As a [user] I must be able to verify my identity and authority for site	Service must allow for immediate / real-time pass	Cancellation of [system credential] in less than 5 minutes, with markers on the	Cancellation of [system credential] in	TBC	Functional	Mandatory	JSP 440	D Info	In the event of emergency then [system credential]s can be immediately	Candidate

ID	User Requirement	Remarks	Measure of Effectiveness			Requirement Type	Candidate Priority	Justification	Owner	Proposed Validation Method	Status
			Threshold	Objective	Status						
	access, linking with MOD and other government databases as required and human authorising agents, generating a [system credential].	cancellation for individuals or multiple [user] groups.	system alerting other sites to the cancellation, preventing automated entry to other sites.	less than one minute.						cancelled for [user]s (e.g., if they are banned from sites), or for [user] groups en masse.	
UR 3.1	Generated [system credential]s must be compatible with automated entry and exit system and incorporate two-factor individual authentication.	[Access control system] fully integrated with Pedestrian Digital Pass Service.	Enable [pedestrian] access on a separate system.	Enable [pedestrian] access using the same vehicle access authorisation and system.	TBC	Functional	Priority 1	JSP 440	D Info	The [access control system] should seamlessly integrate with a mobile [system credential] issuing service, allowing [pedestrian]s to authenticate and access the gate system using their mobile devices or printed document. The system should retain a real time 'site census' to list the population at risk by [user] groups and enable Op WIDEAWAKE, or compliance with fire or Martyn's Law regulation.	Candidate
UR 3.2	Generated [system credential]s must be compatible with automated entry and exit system and incorporate	[Access control system] should ensure secure access / exit through multi factor	Support one time code texted to device.	Support muti factor authorisation, including but not limited to biometric	TBC	Functional	Mandatory	JSP 440	D Info, PsyA	The system should ensure secure authentication of users through the mobile [system credential] service,	Candidate

ID	User Requirement	Remarks	Measure of Effectiveness			Requirement Type	Candidate Priority	Justification	Owner	Proposed Validation Method	Status
			Threshold	Objective	Status						
	two-factor individual authentication.	authentication. This is required to maintain accurate site records, and confirm entry / exit of contractors.		authentication (fingerprint, face recognition) or one-time passwords / codes / ANPR.						preventing unauthorized access or tampering. It should support multi-factor authentication methods, such as biometric authentication (fingerprint, face recognition) or one-time passwords / codes, to enhance security and prevent unauthorized access.	
UR 3.3	Generated [system credential]s must be compatible with automated entry and exit system and incorporate two-factor individual authentication.	System must have resilience in place to mitigate against [system credential]s not working or access being denied.	[Users] to reverse / use exit lane away from barrier and exit – exit without entering site.	[User] to exit without needing to reverse, impacting other drivers – exit without entering site.	TBC	Functional	Priority 1	JSP 850	HC Infra	If a [user] is denied access, then they must be able to turn around and exit vicinity securely. Direction to a designated help-point (potentially the guard room) should also be included.	Candidate
UR 3.4	Generated [system credential]s must be compatible with the [access control system] and incorporate two-factor individual authentication.	System must identify other [user]s in [user vehicle] other than the driver and notify [user] to ensure that all occupants scan [system credential] for entry.	Incorporate a robust technical solution to identify multi-occupant vehicles and reconcile number of valid [system credential]s presented at point of entry with expected number, flagging up [user vehicle] for remote interaction if required.	Technical solution to identify how many [user]s are in a [user vehicle] and reject access if same number of [system credential]s are not presented and warn driver	TBC	Functional	Priority 1	JSP 440	D Info	System will be able to identify and discriminate between single and multi-occupant vehicles. It will demand valid [system credential]s from all occupants and passengers in the vehicle and reject when an	Candidate

ID	User Requirement	Remarks	Measure of Effectiveness			Requirement Type	Candidate Priority	Justification	Owner	Proposed Validation Method	Status
			Threshold	Objective	Status						
				reason for rejection.						unexpected number of passes are scanned. User feedback prompts driver to scan all other passengers in the vehicle (barrier still rises if they do not but an alert and details are sent to central control room for assessment).	
UR 4.1	All [user]s must be able to use the automated entrance and exit system to allow [user vehicle]s and [pedestrian]s timely entrance / exit to and from ACA equipped sites.	System must include autonomous [vehicle ID solution] and be linked to pass issue [system credential]s.	n/a	[User vehicle]s should be identified regardless of the VRN/plate type, size, location. Motorcycles and pedal cycles and their riders will be catered for.	TBC	Functional	Mandatory	JSP 440, BSEN 62676-4:2015 Video surveillance systems for use in security applications.	D Info	[Vehicle ID solution] at equipped gates will confirm with system that vehicle has a [system credential] and once two-factor personal identification without resorting to presenting [system credential]s on a mobile device is complete, allow [user]s and [user vehicle]s access to site. Solution accommodates military plates and overseas as required.	Candidate
UR 4.2	All [user]s must be able to use the automated entrance and exit system to allow [user vehicle]s and	System should complete one cycle of authentication, barrier up, vehicle passage, barrier	Process to be complete in ten seconds and be available 24/7.	Process to be complete in less than ten seconds and be available 24/7.	TBC	Functional	Priority 1	JSP 440, JSP 850	D Info, HC Infra	Two-factor authentication and [user vehicle] identification system will activate a complete cycle of	Candidate

ID	User Requirement	Remarks	Measure of Effectiveness			Requirement Type	Candidate Priority	Justification	Owner	Proposed Validation Method	Status
			Threshold	Objective	Status						
	[pedestrian]s timely entrance / exit to and from ACA equipped sites.	down in ten seconds or less and be available 24/7. System downtime must not exceed 5% in any rolling 30 day period.								the barrier, allowing access for one vehicle, from presentation of [system credential]s, within ten seconds. This will allow up to six [user vehicle]s per minute to use one automated lane. This process must be able to be used 24/7. The throughput achieved by current workforce during peak times at each site should be bettered or maintained.	
UR 4.3	All [user]s must be able to use the automated entrance and exit system to allow [user vehicle]s and [pedestrian]s timely entrance / exit to and from ACA equipped sites.	System must include a space for [user vehicle]s to park before approaching the barriers, which is capable in both size and layout to handle typical site-specific peak flow for [user] groups without [system credential]s.	Include a lay-by for vehicles.	Include a temporary car-park for vehicles.	TBC	Functional	Priority 1	JSP 850	HC Infra	The system should include a lay-by/car park/holding area where visitors and other [user]s without a [system credential] can park before approaching the barriers. This will allow them to obtain a [system credential] without disrupting the flow of traffic. It will also reduce instances of [user]s being rejected at the barriers, which may	Candidate

ID	User Requirement	Remarks	Measure of Effectiveness			Requirement Type	Candidate Priority	Justification	Owner	Proposed Validation Method	Status
			Threshold	Objective	Status						
										cause delays. This space may need to be created by moving the boundary fence near the VCP inwards, towards the camp, to avoid congesting main road.	
UR 4.4	All [user]s must be able to use the automated entrance and exit system to allow [user vehicle]s and [pedestrian]s timely entrance / exit to and from ACA equipped sites.	System must allow [user]s to exit the entry point after being denied access without disrupting traffic, requiring human intervention, or being admitted on to camp in order to turn around.	[User]s to reverse away from barrier and exit – exit without entering site.	[User]s to exit without needing to reverse, impacting other drivers – exit without entering site.	TBC	Functional	Priority 1	JSP 850	HC Infra	There must be enough space for [user]s to exit the automated entry and exit system without being admitted on to camp and without disrupting traffic at the entry point or on nearby public roads.	Candidate
UR 4.5	All [user]s must be able to use the automated entrance and exit system to allow [user vehicle]s and [pedestrian]s timely entrance / exit to and from ACA equipped sites.	System must be able to accommodate large commercial and military vehicles.	Accommodate the entry of large commercial and military vehicles.	Accommodate the parking, turning and entry of large commercial and military vehicles.	TBC	Functional	Priority 1	JSP 850	HC Infra	The specific size of military vehicles that will pass through the system will depend on the nature of each site with an SVR being the largest (turning circle of 30.5m). All systems at all sites will be required to accommodate a TCV as a minimum.	Candidate
UR 4.6	All [user]s must be able to use the automated	System must deter and alert against	System must prevent unauthorised vehicle and pedestrian	System must prevent unauthorised	TBC	Functional	Mandatory	JSP 440, BS EN 12464-2:2014 Lighting Outdoor	D Info, PsyA, HC Infra	Gates should be designed in a way to deter	Candidate

ID	User Requirement	Remarks	Measure of Effectiveness			Requirement Type	Candidate Priority	Justification	Owner	Proposed Validation Method	Status
			Threshold	Objective	Status						
	entrance and exit system to allow [user vehicle]s and [pedestrian]s timely entrance / exit to and from ACA equipped sites.	unauthorised entry.	access, immediately alarming [guard force].	vehicle and pedestrian access, immediately alarming [guard force] and initiate audible alarms, lighting etc.				Workplaces, CIBSE LG06/16 Lighting Guide for The Outdoor Environment, BSEN 60839-11-1:2013 Alarm and electronic security systems. Electronic access control systems. STaMP – JSP 440 Part 2 Leaflet 3A.		unauthorised access at both pedestrian and vehicle gates (from tailgating, jumping brute force, or surreptitious circumvention or bypass of physical security or cyber safeguards, etc). Visible cameras, flood lighting and message boards should be incorporated. Any instance of unauthorised access or a non-trivial attempt should provide an immediate alert to [guard force].	
UR 4.7	All [user]s must be able to use the automated entrance and exit system to allow [user vehicle]s and [pedestrian]s timely entrance / exit to and from ACA equipped sites.	System must deliver Hostile Vehicle Mitigation up to NPSA standards, up to PAS 68 where required.	n/a	Hostile Vehicle Mitigation up to NPSA standards, up to PAS 68 where required – site specific.	TBC	Non-functional	Mandatory	JSP 850, National Protective Security Authority	HC Infra	Vehicle barriers should deliver mitigation against hostile vehicle ramming and tailgating. Barriers should be able to withstand vehicle impacts to the standard dictated for each site by DIO's Security Services Group.	Candidate

ID	User Requirement	Remarks	Measure of Effectiveness			Requirement Type	Candidate Priority	Justification	Owner	Proposed Validation Method	Status
			Threshold	Objective	Status						
UR 4.8	All [user]s must be able to use the automated entrance and exit system to allow [user vehicle]s and [pedestrian]s timely entrance / exit to and from ACA equipped sites.	System must prevent unauthorised [pedestrian] access, and be non-pass back through [pedestrian] access points.	System must prevent unauthorised vehicle and [pedestrian] access, immediately alarming [guard force].	System must prevent unauthorised vehicle and pedestrian access, immediately alarming guard force and initiate audible alarms, lighting etc.	TBC	Functional	Mandatory	JSP 440, BSEN 60839-11-1:2013 Alarm and electronic security systems. Electronic access control systems. STaMP – JSP 440 Part 2 Leaflet 3A	D Info, HC Infra, PsyA	Pedestrian barriers should prevent tailgating, jumping, climbing etc. and should detect any attempt at unauthorised entry. If any attempt is detected the system must alert the [guard force] immediately. The process for safeguarding against surreptitious attack (STaMP) should be followed.	Candidate
UR 4.9	All [user]s must be able to use the automated entrance and exit system to allow [user vehicle]s and [pedestrian]s timely entrance / exit to and from ACA equipped sites.	System must have a redundancy access help point in place that is away from the main gate and allows [user]s to contact central monitoring / [guard force].	Call button to central monitoring [guard force] at gate.	Call button to central monitoring [guard force] set away from gate	TBC	Functional	Mandatory	JSP 440	D Info	In the event of [user]s being unable to access site or [system credential]s not working, [user]s are able to pull away from the flow of traffic and contact guard room for help (e.g., an intercom with camera that [guard force] could use to speak to guard room and confirm identity visually. [Guards force] then able to manually open gate for said user).	
UR 4.10	All [user]s must be able to use the	System must have a secure	n/a	Manual override for [guard force]	TBC	Functional	Mandatory	JSP 440, JSP 850	D Info, HC Infra	[Guard force] should be able to remotely	Candidate

ID	User Requirement	Remarks	Measure of Effectiveness			Requirement Type	Candidate Priority	Justification	Owner	Proposed Validation Method	Status
			Threshold	Objective	Status						
	automated entrance and exit system to allow [user vehicle]s and [pedestrian]s timely entrance / exit to and from ACA equipped sites.	manual override to allow [guard force] to operate gates physically if necessary (both from central guard room and at gate).		and emergency services required. Must be able to be initiated remotely/not physically at gate.				STaMP – JSP 440 Part 2 Leaflet 3A		access and control the gate system using authorised devices that are not exploitable via theft, loss, spoofing, or mimicking RF signals and which permit operation from a distance (e.g., in the event of emergency). Loss of ability to use gates will prevent entry and exit from sites and therefore mitigation of this is critical.	
UR 4.11	All [user]s must be able to use the automated entrance and exit system to allow [user vehicle]s and [pedestrian]s timely entrance / exit to and from ACA equipped sites.	System should be accessible for all [user]s.	n/a	System must be compliant with Equalities Act 2010	TBC	Non-functional	Mandatory	JSP 440, JSP 850	D Info	The system should incorporate accessibility features, such as support for assistive technologies, visual indicators, or audible cues, to ensure equitable access for users with disabilities and be compliant with the Equalities Act 2010.	Candidate
UR 4.12	All [user]s must be able to use the automated entrance and exit system to allow [user vehicle]s and	System should be fully compliant with expected safety standards whilst remaining reliable and	Gate system should comply with relevant safety standards and regulations and meet standard life expectancy timelines.	Gate system should comply with relevant safety standards and regulations and	TBC	Non-functional	Mandatory	JSP 850, Health and Safety at Work Act 1974	HC Infra	The [access control system] should comply with relevant safety standards and regulations to ensure the safety of	Candidate

ID	User Requirement	Remarks	Measure of Effectiveness			Requirement Type	Candidate Priority	Justification	Owner	Proposed Validation Method	Status
			Threshold	Objective	Status						
	[pedestrian]s timely entrance / exit to and from ACA equipped sites.	durable – 95% serviceable.		exceed standard life expectancy timelines.						users and minimize potential risks, whilst simultaneously remaining reliable and durable, capable of withstanding various weather conditions and heavy usage over an extended period. Note, these standards may change throughout implementation period and therefore tech and infra implemented across the project may change with time as policies and standards change.	
UR 4.13	All [user]s must be able to use the automated entrance and exit system to allow [user vehicle]s and [pedestrian]s timely entrance / exit to and from ACA equipped sites.	[User]s must be able to access the camp on foot or in a vehicle through separate entry points.	n/a	Separate [pedestrian] and vehicle access points that all comply with H&S standards.	TBC	Functional	Priority 1	JSP 850	HC Infra	Both entry points must be governed by the [access control system] and there must be a clear demarcation between each entrance to comply with H&S standards and separate [pedestrian] and vehicle access points appropriately.	Candidate
UR 4.14	All [user]s must be able to use the automated	System should be easily scalable	Requirement for <30% change in	Requirement for <20% change in	TBC	Functional	Priority 2	JSP 850, JSP 440	D Info, HC Infra	The system should be scalable, allowing for easy	Candidate

ID	User Requirement	Remarks	Measure of Effectiveness			Requirement Type	Candidate Priority	Justification	Owner	Proposed Validation Method	Status
			Threshold	Objective	Status						
	entrance and exit system to allow [user vehicle]s and [pedestrian]s timely entrance / exit to and from ACA equipped sites.	across single and multiple sites.	design between each site.	design between each site.						expansion and routine upgrades or integration with additional gates or access points as the need arises. System should also be easy to scale across different sites once supporting digital infrastructure is installed.	
UR 5.1	Centralised monitoring system must allow [guard force] and [site management] oversight of all entry and exit locations as well as list of newly issued [system credentials] for site.	Monitoring system should link with entry access and exit systems to track all site [user]s. System to incorporate and multi-factor authentication on exit to provide real time assurance of on-site personnel.	Provide ability to list all vehicles and individuals on site.	Provide ability to list all vehicles (and owners) and individuals on site, along with the times of their exits/entries.	TBC	Functional	Priority 2	JSP 440, BSEN 62676-4:2015 Video surveillance systems for use in security applications.	D Info, PsyA	System tracks all [user]s entering and exiting sites and records details centrally. [User] access is logged so that full site use history is available. It will be Able to provide a real-time readout for administrators on who is currently on site or away, including providing alerts if [user]s have stayed on site but their [system credential] are no longer valid (e.g., immediate alert to [guard force] with [user] details, including contact details, so [guard force] are able to	Candidate

ID	User Requirement	Remarks	Measure of Effectiveness			Requirement Type	Candidate Priority	Justification	Owner	Proposed Validation Method	Status
			Threshold	Objective	Status						
										call and confirm location / if [user] is still on site)	
UR 5.2	Centralised monitoring system must allow [guard force] and [site management] oversight of all entry and exit locations as well as list of newly issued [system credentials] for site.	System should allow data export.	Allow all data to be exported directly to MOD systems.	Allow all data to be exported directly to MOD systems in usable/user friendly formats.	TBC	Functional	Priority 1	JSP 440	D Info	The system should have the ability to securely share data for other organisations effectively democratising the data for exploitation in other use cases. As an example, 'clocking in' data for travel to work claims.	Candidate
UR 5.3	Centralised monitoring system must allow [guard force] and [site management] oversight of all entry and exit locations as well as list of newly issued [system credentials] for site.	System must allow 24/7 real-time monitoring of entrance and exit points with advanced analytics capabilities.	n/a	24/7 real-time monitoring of entrance and exit points with advanced analytics capabilities.	TBC	Functional	Mandatory	JSP 440, BSEN 62676-4:2015 Video surveillance systems for use in security applications.	D Info, PsyA	System must provide a live feed to [guard force] and should also provide automated instantaneous alerts of suspicious activity (e.g., provides an alert when a particular vehicle tries to access camp, when individual leaves a bag unattended, in the event of tailgating).	Candidate
UR 5.4	Centralised monitoring system must allow [guard force] and [site management] oversight of all	System must include a customisable alerting and notification system.	n/a	Sites must be able to customise alerts based in incident severity with	TBC	Functional	Mandatory	JSP 440	D Info, PsyA	System must include customisable alert thresholds based on the severity of incidents, and must	Candidate

ID	User Requirement	Remarks	Measure of Effectiveness			Requirement Type	Candidate Priority	Justification	Owner	Proposed Validation Method	Status
			Threshold	Objective	Status						
	entry and exit locations as well as list of newly issued [system credentials] for site.			notifications being shared across network or parts thereof.						allow integration with various communication channels (email, SMS, mobile apps) to notify local [site management], [guard force] and relevant authorities.	
UR 5.5	Centralised monitoring system must allow [guard force] and [site management] oversight of all entry and exit locations as well as list of newly issued [system credentials] for site.	System must enhance incident response coordination.	n/a	Provision of standard procedure to follow during incident response.	TBC	Functional	Mandatory	JSP 440	PsyA	System provides automated incident response workflows to guide the [guard force] through predefined steps in handling specific types of incidents (Op WIDEAWAKE, vehicle intruder, suspicious activity outside perimeter etc.)	Candidate
UR 5.6	Centralised monitoring system must allow [guard force] and [site management] oversight of all entry and exit locations as well as list of newly issued [system credentials] for site.	Retrospective data available for trend analysis and investigation.	Keep a record of all data for one year.	Keep a record of data for as long as GDPR restrictions allow.	TBC	Functional	Priority 1	JSP 440, Data Protection Act 2018, Information Commissioner's Office Guidelines incl. GDPR guidance.	D Info	System records all activity on gates and can provide advanced data and analytics capabilities, including historical data for forensic purposes (e.g., micro view with all videos of entry from a particular vehicle or user, macro view of traffic flow data across multiple gates and across	Candidate

ID	User Requirement	Remarks	Measure of Effectiveness			Requirement Type	Candidate Priority	Justification	Owner	Proposed Validation Method	Status
			Threshold	Objective	Status						
										different time horizons).	
UR 5.7	Centralised monitoring system must allow [guard force] and [site management] oversight of all entry and exit locations as well as list of newly issued [system credentials] for site.	System should ensure data privacy and protection. NCSC guidance on incorporation of hardware and software produced by 'vendors of concern' should be followed.	n/a	Data privacy ad protection must adhere to GDPR rules. Role based access required.	TBC	Non-functional	Mandatory	JSP 440, Data Protection Act 2018, Information Commissioner's Office Guidelines incl. GDPR guidance. NCSC 'Advice on high risk vendors in UK telecoms'.	D Info, PsyA	The system should prioritise data privacy and protection, implementing appropriate measures to secure [user] data and prevent unauthorised access or misuse. Role-based access permissions should limit [user]s to specific functionalities based on their responsibilities. Unauthorised access and/or loss of OS data is a critical issue. All data must be securely backed-up to avoid loss.	Candidate
UR 5.8	Centralised monitoring system must allow [guard force] and [site management] oversight of all entry and exit locations as well as list of newly issued [system	System should have the ability to seamlessly integrate and manage surveillance systems from diverse sites with different hardware and	All sites must be able to be centrally monitored, either by [site management]. [guard force] or [system administrator]s.	All sites must be able to be centrally monitored, integrating with existing technology and systems.	TBC	Functional	Mandatory	JSP 440, JSP 850, BSEN 62676-4:2015 Video surveillance systems for use in security applications, BS 7671 IEE Regulations for	D Info, PsyA, HC Infra	System must allow for monitoring of different sites to be centralised (e.g., one physical CCTV / video monitoring location overseeing the entrance and exit points for multiple sites). Surveillance and	Candidate

ID	User Requirement	Remarks	Measure of Effectiveness			Requirement Type	Candidate Priority	Justification	Owner	Proposed Validation Method	Status
			Threshold	Objective	Status						
	credentials] for site.	software configurations.						Electrical Installations.		other add-ons need to sit upon an open architecture/LOSA to permit plug and play.	
UR 5.9	Centralised monitoring system must allow [guard force] and [site management] oversight of all entry and exit locations as well as list of newly issued [system credentials] for site.	System must support, and be capable of interfacing with, a wide range of surveillance cameras, sensors and other monitoring devices.	System must support: security cameras, night-capable security cameras, perimeter sensors, motion-activated security lights.	System must support: security cameras, night-capable security cameras, perimeter sensors, motion-activated security lights and more.	TBC	Functional	Mandatory	JSP 440, BSEN 62676-4:2015 Video surveillance systems for use in security applications.	HC Infra, PsyA	System must support a wide range of sensors, including but not limited to: security cameras, night-capable security cameras, perimeter sensors, motion-activated security lights etc.	Candidate
UR 5.10	Centralised monitoring system must allow [guard force] and [site management] oversight of all entry and exit locations as well as list of newly issued [system credentials] for site.	Any system installed and the way in which it can be used must not require RIPA assurance.	Avoid requirement for RIPA assurance where possible – if required, train personnel on requirements.	Avoid requirement for RIPA assurance.	TBC	Non-functional	Mandatory	JSP 440, Regulation of Investigatory Powers Act 2000 (RIPA).	PsyA	Any solution should not be one that requires RIPA authorisation. Additionally, if contractors are going to be required to operate the surveillance systems, then they must understand RIPA and operate the Smartbasing systems in accordance with the Code (and be responsible for training their staff on the same).	Candidate

ID	User Requirement	Remarks	Measure of Effectiveness			Requirement Type	Candidate Priority	Justification	Owner	Proposed Validation Method	Status
			Threshold	Objective	Status						
UR 6.1	The system must be designed to be reliable, able to operate outdoors in a range of inclement weather conditions. It will include through-life support and a service-management package.	The system must be back online within a designated SLA timeframe in (TBD) in the event of an outage.	System must be back online within 30 minutes.	System must be back online within 1 hour. This must be adjustable depending on times of day and threat levels.	TBC	Functional	Mandatory	JSP 440	D Info	Clearly defined SLAs between the Army and the provider (specifics of maintenance arrangements TBD), outlining expected response times, system availability, and resolution times for incidents. Note, response times may need to be different for different sites and at different times.	Candidate
UR 6.2	The system must be designed to be reliable, able to operate outdoors in a range of inclement weather conditions. It will include through-life support and a service-management package.	The system must have appropriate in-built resilience to continue operation in the event of a power or network failure.	The gates must be able to operate for existing [system credential] holders in the event of a power cut.	As for threshold, however [system credential] issue must also be available in the event of a power or network failure.	TBC	Functional	Mandatory	JSP 440, JSP 850	HC Infra	In the event of lack of power or network connection, system must be able to operate independently on a UPS, for defined time period (e.g., 12 / 24 hrs.) and notify allocated site representatives of the failure.	Candidate
UR 6.3	The system must be designed to be reliable, able to operate outdoors in a range of inclement weather conditions. It will include through-life support and a service-	[User]s and [guard force] should be provided with training and onboarding materials.	n/a	All [user]s and [guard force] must be trained.	TBC	Non-functional	Mandatory	JSP 440, JSP 850	D Info, HC Infra	The system should provide comprehensive training materials, including manuals, tutorials, and onboarding resources, to ensure both [user]s and [guard force]	Candidate

ID	User Requirement	Remarks	Measure of Effectiveness			Requirement Type	Candidate Priority	Justification	Owner	Proposed Validation Method	Status
			Threshold	Objective	Status						
	management package.									are given the right level of awareness of and can interact with the system to the extent required by their role.	
UR 6.4	The system must be designed to be reliable, able to operate outdoors in a range of inclement weather conditions. It will include through-life support and a service-management package.	System should be robust and provide maintenance and diagnostics info.	The system should provide a 90% serviceability rate.	The service should provide a 95% serviceability rate.	TBC	Functional	Priority 1	JSP 440, JSP 850	D Info, HC Infra	The gate system should provide maintenance and diagnostic features, allowing [system administrator]s to monitor the system's health, receive alerts for potential issues, and perform regular maintenance tasks to ensure optimal performance. System must provide a 95% serviceability rate (% for discussion with Infra).	Candidate
UR 6.5	The system must be designed to be reliable, able to operate outdoors in a range of inclement weather conditions. It will include through-life support and a service-management package.	System should be regularly maintained and serviced and updated throughout service life.	Maintenance should be carried out at a regular cadence of once a year.	All maintenance and servicing issues should be immediately (within a pre-agreed timeframe). Exceeding the SLA timeframe may result in penalties.	TBC	Functional	Priority 1	JSP 440, JSP 850	D Info, HC Infra	System must be evergreen, supported with regular maintenance to ensure ongoing functionality. A solution composed of COTS technology rather than incorporating bespoke technology would be preferred.	Candidate

ID	User Requirement	Remarks	Measure of Effectiveness			Requirement Type	Candidate Priority	Justification	Owner	Proposed Validation Method	Status
			Threshold	Objective	Status						
UR 6.6	The system must be designed to be reliable, able to operate outdoors in a range of inclement weather conditions. It will include through-life support and a service-management package.	System being implemented may require change with time due to several reasons including policy changes, standards changes, site and Army requirement. A change request process is required to facilitate this.	n/a	A change request process is required.	TBC	Non-functional	Mandatory	n/a			
UR 6.7	The system must be designed to be reliable, able to operate outdoors in a range of inclement weather conditions. It will include through-life support and a service-management package.	The system must be able to withstand all possible environmental conditions.	System should meet environmental robustness industry standards.	System should perform above environmental robustness industry standards.	TBC	Functional	Mandatory	Ministry of Defence Climate Change and Sustainability Strategic Approach, Environmental Planning Regulations as advised by the DIO Planning and Environmental Planning Team.	HC Infra	The solution must be able to withstand rain, wind, snow, heat etc to required industry standards.	Candidate
UR 7.1	All installed hardware must be appropriately accredited for use on a military establishment and be able to integrate with existing systems.	System must comply with MOD, Army and NPSA security standards.	n/a	System must comply with MOD, Army and NPSA security standards.		Non-functional	Mandatory	JSP 440, JSP 850 STaMP – JSP 440 Part 2 Leaflet 3A	PsyA	The Policy and Standards Tab provides a non-exhaustive list of policy, guidance, standards and legislation that the system should adhere to. SbD	Candidate

ID	User Requirement	Remarks	Measure of Effectiveness			Requirement Type	Candidate Priority	Justification	Owner	Proposed Validation Method	Status
			Threshold	Objective	Status						
										compliance is essential.	
UR 7.2	All installed hardware must be appropriately accredited for use on a military establishment and be able to integrate with existing systems.	System (hardware and software) should be able to integrate with existing security systems.	Service must interface with critical MOD or .gov digital systems and infrastructure.	Service must have the ability to interface with all MOD or .gov digital systems and infrastructure.	TBC	Functional	Priority 1	JSP 440, JSP 850, BSEN 60839-11-1:2013 Alarm and electronic security systems. Electronic access control systems.	D Info, HC Infra, PsyA	The system should integrate seamlessly with existing security systems, such as surveillance cameras or alarms, to enhance overall security and provide a comprehensive solution.	Candidate
UR 8.1	The centralised monitoring service, [access control system]and [system credential] issue software should be securely cloud hosted.	[Site management] and [system administrator]s should be security cleared and vetted.	n/a	[Site management] and [system administrator]s should be security cleared and vetted.	TBC	Non-functional	Mandatory		PsyA	All personnel, including cloud service providers (CSP) staff, undergo appropriate security clearance and vetting processes to handle sensitive defence information.	Candidate
UR 8.2	The centralised monitoring service, [access control system]and [system credential] issue software should be securely cloud hosted.	Cloud providers must be official accredited and compliant with government security standards.	n/a	Cloud providers must be official accredited and compliant with government security standards.	TBC	Non-functional	Mandatory	JSP 440	D Info, PsyA	The solution must use cloud services that are certified under the G-Cloud framework, which is designed to simplify the procurement of cloud services within the UK public sector, including defence.	Candidate
UR 8.3	The centralised monitoring service, [access control system]and	The solution must adhere to relevant	n/a	The solution must adhere to relevant	TBC	Non-functional	Mandatory	JSP 440	D Info, PsyA	The solution must include a robust encryption mechanism for data	Candidate

ID	User Requirement	Remarks	Measure of Effectiveness			Requirement Type	Candidate Priority	Justification	Owner	Proposed Validation Method	Status
			Threshold	Objective	Status						
	[system credential] issue software should be securely cloud hosted.	encryption standards.		encryption standards.						in transit and at rest, adhering to UK government encryption standards for classified and sensitive information.	
UR 8.4	The centralised monitoring service, [access control system]and [system credential] issue software should be securely cloud hosted.	The solution must comply with NCSC guidelines.	n/a	The solution must comply with NCSC guidelines.	TBC	Non-functional	Mandatory	JSP 440, National Cyber Security Centre	PsyA	The solution must adhere to guidelines provided by the National Cyber Security Centre (NCSC) for securing cloud services, including best practices for configuration and access controls. Aggregation of data will be a cyber risk so must be considered in data record design.	Candidate
UR 8.5	The centralised monitoring service, [access control system]and [system credential] issue software should be securely cloud hosted.	The solution must include network security measures and isolation practices.	n/a	The solution must utilise network security measures that meet industry standard mitigation measures to secure and encrypt cloud data.	TBC	Non-functional	Mandatory	JSP 440	D Info, PsyA	The solution must utilise network security measures such as Virtual Private Clouds (VPCs) and network segmentation, to isolate defence-related services from other non-defence workloads.	Candidate
UR 8.6	The centralised monitoring service, [access control	The solution must include robust	Keep a record of all data for one year and	Keep a record of data for as long as GDPR	TBC	Functional	Priority 1	JSP 440, Data Protection Act Guidance Note	D Info	The solution must include robust logging, auditing,	Candidate

ID	User Requirement	Remarks	Measure of Effectiveness			Requirement Type	Candidate Priority	Justification	Owner	Proposed Validation Method	Status
			Threshold	Objective	Status						
	system]and [system credential] issue software should be securely cloud hosted.	auditing and monitoring.	complete analysis against this data.	restrictions allow, completing ongoing analysis of this data.				11: CCTV and Data Protection Considerations, Information Commissioner's Office Guidelines incl. GDPR guidance, Data Protection Act 2018.		and monitoring mechanisms to track and analyse activities within the cloud environment, enabling quick detection of potential security incidents.	
UR 8.7	The centralised monitoring service, [access control system]and [system credential] issue software should be securely cloud hosted.	The solution provider must follow secure development practices.	n/a	The system must follow industry best practices and secure coding standards.	TBC	Non-functional	Mandatory	JSP 440	D Info	The solution provider must follow secure development practices for any custom applications or services deployed in the cloud, following industry best practices and secure coding standards.	Candidate
UR 8.8	The centralised monitoring service, [access control system]and [system credential] issue software should be securely cloud hosted.	The solution provider must have robust disaster recovery and business continuity procedures.	An industry standard disaster recovery system must be in place.	A better than industry standard disaster recovery system must be in place.	TBC	Functional	Mandatory	JSP 440, JSP 850	D Info	The cloud provider must have robust disaster recovery and business continuity plans in place to minimise downtime and data loss in the event of a disruption.	Candidate
UR 8.9	The centralised monitoring service, [access control system]and [system credential] issue software	The solution provider must comply with all necessary regulation.	n/a	The cloud provider must comply with relevant defence and government	TBC	Non-functional	Mandatory	JSP 440	D Info, PsyA	The cloud provider must comply with relevant defence and government regulations, including adherence	Candidate

ID	User Requirement	Remarks	Measure of Effectiveness			Requirement Type	Candidate Priority	Justification	Owner	Proposed Validation Method	Status
			Threshold	Objective	Status						
	should be securely cloud hosted.			regulations, including adherence to the Security Policy Framework (SPF).						to the Security Policy Framework (SPF).	
UR 8.10	The centralised monitoring service, [access control system]and [system credential] issue software should be securely cloud hosted.	The solution must be accompanied by a suitable exit strategy.	n/a	An exit strategy to transition to another provider without cessation of the service must be provided.	TBC	Non-functional	Mandatory		D Info	The solution must be accompanied by a clear exit strategy that includes data migration plans and procedures in case there is a need to transition to a different cloud provider or hosting solution.	Candidate
UR 8.11	The centralised monitoring service, [access control system]and [system credential] issue software should be securely cloud hosted.	All data must be shared with the Army.	Allow all data to be exported directly to MOD systems.	Allow all data to be exported directly to MOD systems in usable/user friendly formats.	TBC	Functional	Priority 1	JSP 440, Data Protection Act Guidance Note 11: CCTV and Data Protection Considerations, Information Commissioner's Office Guidelines incl. GDPR guidance, Data Protection Act 2018.	D Info	Data collected on all software must be available to the Army to use as they wish within the boundaries set within the GDPR rules.	Candidate

Table 6 – Detailed user requirements

Status	Meaning

Candidate	On first addition to the URD, or re-instatement.
Traded	If the need is still valid but satisfaction is deferred indefinitely, typically as a consequence of trade-off activity.
Transferred	If relocated out of the URD into another URD, typically as a consequence of trade-off activity.
Cancelled	If no longer valid because the operational need has changed.

PART 4

Context Documents

22. The following work feeds into this URD:

- DCGS Smartbasing IRTB
- ACGS DRes Smartbasing IRTB

23. All policies and documents used to produce the listed user requirements:

Ser	Document	Relevant Section
	Overarching Documents	
1	JSP 850 Part 1: Policy	Security
2	JSP 850 Part 2 Standards and Guidance	Infrastructure Security Standards
3	JSP 440: The Defence Manual for Security	Leaflet 3A Infrastructure/Project Works/STaMP
4	JSP 440: The Defence Manual for Security	Leaflet 3D Perimeter Security, including Hostile Vehicle Mitigation and Lighting
5	BPS 6.0 Guardrooms, Pass Offices and Access Control Facilities	Access and External Facilities
6	Government Functional Standard 007: Security	All sections
7	Data Protection Act Guidance Note 11: CCTV and Data Protection Considerations	Ref CIO-3-27-1-2
8	National Protective Security Authority	Operational Requirements
9	HMG Cabinet Office Security Policy Framework	Overarching Principles; Physical Security
10	Information Commissioner's Office Guidelines incl. GDPR guidance	UK GDPR guidance and resources

11	Data Protection Act 2018	
12	Investigatory Powers Act 2016	
13	Regulation of Investigatory Powers Act 2000 (RIPA)	
14	Health and Safety at Work Act 1974	
15	ACSO 2007	
NPSA Standards and Guidance		
16	Guide to security fences-pedestrian perimeter barriers	
17	CCTV within the perimeter of a site	
18	Security Lighting	
19	Integrated Electronic Security	
20	Catalogue of Security Equipment	
British and European Standards and Guidance		
21	BS 1722-10-2019-Fences – Specification for anti-intruder fences in chain link and welded mesh	
22	BS 7671 IEE Regulations for Electrical Installations	
23	BS 1722-14:2017 Fences Specification	
24	BS 5489-1:2020 Code of practice for design of road lighting.	
25	PD CEN/TR 13201-1:2014 Road Lighting Performance Requirements	

26	BS EN 12464-2:2014 Lighting Outdoor Workplaces	
27	CIBSE LG06/16 Lighting Guide for The Outdoor Environment	
28	BSEN 62676-4:2015 Video surveillance systems for use in security applications.	
29	BSEN 60839-11-1:2013 Alarm and electronic security systems. Electronic access control systems.	
30	ISO/IEC 27001	
31	Environmental Planning Regulations as advised by the DIO Planning and Environmental Planning Team	
32	NIST 800-160 vol 1-2	
33	NIST 800-37 section 2.8	

PART 5

Glossary of Abbreviations and Terms

24. Glossary of Terms. Terms enclosed in [square brackets] are used consistently throughout Part 3, and are defined in the table below.

Ser	Term	Definition
1	Access control system	The capability offered by the combination of the hardware and software being procured through this project in order to facilitate automated pedestrian and vehicle access to selected sites.
2	Authority	The procuring entity; in this case the Army TLB, but delegated to Home Command.
3	Guard force	Personnel employed in the armed or unarmed guarding role, responsible for protecting the site to which an access control system has been fitted.
4	Pedestrian	A user entering a site on foot, via the pedestrian access point only.
5	Site management	Personnel responsible for ensuring that the policy governing site access for users is complied with. Ultimately responsible for the security and safety of their designated site.
6	System administrator	Personnel employed to manage and maintain the access control system's software, having been granted special permissions on the database.
7	System credential	The virtual token generated by and logged within the access control system database once identity is satisfactorily verified, and which will grant the authorised user access through an automated gate.
8	User	The population of people who may require and seek access to a site, as specified in Table 1 above.
9	User vehicle	A vehicle containing one or many users, any combination of whom may or may not possess a system credential.

25. Glossary of Abbreviations.

Ser	Term	Definition
1	AADP	Army Advanced Development Team

2	ACA	Automated Control of Access
3	ACSO	Army Command Standing Order
4	AEDP	Army Efficiency Delivery Partner
5	DInfo	Director – Information
6	DRes	Director – Resources
7	GDPR	General Data Protection Regulations
8	JSP	Joint Service Publication
9	KUR	Key User Requirement
10	MEP	Main Entry Point
11	NCSC	National Cyber Security Centre
12	NPSA	National Protective Security Authority
13	PSyA	Principal Security Advisor. *The Army's senior security SME; post held by Assistant Head (OF5) within Information Directorate.*
14	QRF	Quick Reaction Force. *Guarding personnel held at immediate readiness to respond to emerging events or incidents.*
15	SbD	Secure by Design. *The process by which MOD ensures that security is accounted for from the commencement of major projects.*
16	SISYS	The in-service Defence Site Access Management System
17	STaMP	Surreptitious Threat Mitigation Process
18	VCP	Vehicle Check Point