Crown
Commercial
Service

RM6100 Technology Services 3 Agreement
Framework Schedule 4 - Annex 1
Lots 2, 3 and 5 Order Form

Order Form

This Order Form is issued in accordance with the provisions of the Technology Services 3 Framework Agreement RM6100 dated [ ] between the Supplier (as defined below) and the Minister for the Cabinet Office (the "**Framework Agreement**") and should be used by Buyers after making a direct award or conducting a further competition under the Framework Agreement.

The Contract, referred to throughout this Order Form, means the contract between the Supplier and the Buyer (as defined below) (entered into pursuant to the terms of the Framework Agreement) consisting of this Order Form and the Call Off Terms. The Call-Off Terms are substantially the terms set out in Annex 2 to Schedule 4 to the Framework Agreement and copies of which are available from the Crown Commercial Service website RM6100 Technology Services 3. The agreed Call-Off Terms for the Contract being set out as the Annex 1 to this Order Form.

The Supplier shall provide the Services and/or Goods specified in this Order Form (including any attachments to this Order Form) to the Buyer on and subject to the terms of the Contract for the duration of the Contract Period.

In this Order Form, capitalised expressions shall have the meanings set out in Schedule 1 (Definitions) of the Call-Off Terms

This Order Form shall comprise:

1. This document headed “Order Form”; roadmap
2. Attachment 1 – Services Specification;
3. Attachment 2 – Charges and Invoicing;
4. Attachment 3 – Implementation Plan;
5. Attachment 4 – Service Levels and Service Credits;
6. Attachment 5 – Key Supplier Personnel and Key Sub-Contractors;
7. Attachment 6 – Software;
8. Attachment 7 – Financial Distress;
9. Attachment 8 - Governance
10. Attachment 9 – Schedule of Processing, Personal Data and Data Subjects;
11. Attachment 10 – Transparency Reports; and
12. Annex 1 – Call Off Terms and Additional/Alternative Schedules and Clauses.

The Order of Precedence shall be as set out in Clause 2.2 of the Call-Off Terms being:

.1.1 the Framework, except Framework Schedule 18 (Tender);

.1.2 the Order Form;

.1.3 the Call Off Terms; and

.1.4 Framework Schedule 18 (Tender)

Section A
General information

Contract Details	
Contract Reference:	C9667 - B
Contract Title:	Crossing the Border Products and Services
Contract Description:	Provision of run, maintain and sustain services for the Border Crossing (BX) and Helios applications
Contract Anticipated Potential Value: this should set out the total potential value of the Contract	£36,623,042
Estimated Year 1 Charges:	[redacted]
Commencement Date: this should be the date of the last signature on Section E of this Order Form	1st December 2025

Buyer details
Buyer organisation name Secretary of State for the Home Department, acting on behalf of the Home Office (referred to as "Buyer")
Billing address 2 Marsham Street, London, SW1P 4DF
Buyer representative name [redacted]

Buyer representative contact details

[redacted]

Buyer Project Reference

Project_9667

Supplier details

Supplier name

BAE Systems Applied Intelligence Limited (referred to as “Supplier”)

Supplier address

[redacted]

Supplier representative name

[redacted]

Supplier representative contact details

[redacted]

Order reference number or the Supplier’s Catalogue Service Offer Reference Number

Itt_77424

Guarantor details

Guidance Note: Where the additional clause in respect of the guarantee has been selected to apply to this Contract under Part C of this Order Form, include details of the Guarantor immediately below.

Guarantor Company Name

Not Applicable

Guarantor Company Number

Not Applicable

Guarantor Registered Address

Not Applicable

Section B
Part A – Framework Lot

Framework Lot under which this Order is being placed

1.	TECHNOLOGY STRATEGY & SERVICES DESIGN	☐
2.	TRANSITION & TRANSFORMATION	☐
3.	OPERATIONAL SERVICES	
	a: End User Services	☐
	b: Operational Management	X
	c: Technical Management	☐
	d: Application and Data Management	☐
5.	SERVICE INTEGRATION AND MANAGEMENT	☐

Part B – The Services Requirement

Commencement Date
See above in Section A

Contract Period

Lot	Maximum Term (including Initial Term and Extension Period) – Months (Years)
2	36 (3)
3	60 (5)
5	60 (5)

Initial Term Months
48 months

Extension Period (Optional) Months
12 months

Minimum Notice Period for exercise of Termination Without Cause (183 Calendar days)	6 months

Sites for the provision of the Services

The Supplier shall provide the Services from the following Sites**:**
Buyer Premises:

All Home Office Sites

Supplier Premises:

[redacted]

Third Party Premises:

[redacted]

Buyer Assets
Home Office POISE Laptops

[redacted]

Additional Standards

Additional standards will be agreed by the Parties, acting reasonably, prior to the start of the Year 1 Implementation Period.

Buyer Security Policy

disposal-and-decommissioning-policy.doc

disposal-and-decommissioning-requireme

cyber-security-email-policy.docx

cyber-security-external-email-configuratior

secure-use-of-social-media-and-messaging

audit-and-compliance-policy.docx

cyber-security--2c2r-policy.docx

it-service-continuity-standard.docx

backup-and-restore-standard.docx

cyber-risk-management-and-governance (

cyber-security-and-information-assurance.(

cyber-security--offshoring-policy.docx

cyber-security--publicly-accessible-content

cyber-security--security-training-and-awar

cyber-security--third-party-assurance-polic

Buyer ICT Policy

cyber-security--build-and-configuration-pc

cyber-security--build-and-configuration-st

cyber-security--cryptography-policy.docx

cyber-security--cryptography-standard.doc

cyber-security--firewall-policy .docx

cyber-security--forensic-readiness-policy.d

physical-and-environmental-security-for-c

protective-monitoring-policy.docx

cyber-security--secure-development-policy

cyber-security-patching-policy (1).docx

cyber-security--technical-vulnerability-man

cyber-security-technical-vulnerability-mana

cyber-security--wifi-security-policy.docx

Insurance

Third Party Public Liability Insurance (£) - £5,000,000

Professional Indemnity Insurance (£) - £1,000,000 and in the annual aggregate

Buyer Responsibilities

Please find below the dependencies on the Buyer for the BX and Helios Discovery and Mobilisation Period of 1st December 2025 – 27th March 2026.

A full list of dependencies for Implementation will be agreed by the Parties, acting reasonably, prior to the start of the Year 1 Implementation Period.

Annual check points will be undertaken throughout the contract lifecycle where the outcomes of the following year will be agreed. These are referred to in this Order Form as conformance points; the first conformance point is November 10th 2026, approximately seven months after the end of the Mobilisation period. In addition to annual conformance points the Parties will meet monthly to review Supplier performance and once every three months during the Implementation Period to establish if the agreed scope of services still meets the Buyer's needs or whether the Change Request process shall be followed pursuant to Schedule 5 (Change Control Procedure).

The Buyer will meet the following responsibilities listed in the table below. In the event that any of these Buyer Responsibilities are not met then:

The Supplier is relieved from liability for achieving the affected deliverables by the relevant due dates; and

The Parties shall, acting reasonably, agree on adjustment to dates, deliverables or financial envelope as applicable.

ID	Dependency	Description
BR1	Security Clearances and POISE devices	The Buyer will provide POISE laptops to Supplier team members once they have achieved security clearance
BR2	Access to information	Supplier will have full and timely access to all relevant information, documentation and systems necessary to deliver the scope set out in this document
BR3	Access to personnel	Key Buyer and CtB supplier personnel, including subject matter experts, process owners and decision makers will be available for meetings and workshops as required
BR4	Buyer contacts	Responsive Buyer contacts for different aspects of the engagement will be agreed to ensure efficient communication and ownership
BR5	Buyer policies and procedures	The Buyer will provide policies and clear guidance to ensure the Supplier adheres to relevant policies and procedures
BR6	Timely sign-off	The Buyer will review and sign off all deliverables following a review and sign off process, within 15 working days

Goods

N/A

Governance – Option Part A or Part B

Governance Schedule	Tick as applicable
Part A – Short Form Governance Schedule	□
Part B – Long Form Governance Schedule	X

The Part selected above shall apply this Contract.

Change Control Procedure – Option Part A or Part B

Change Control Schedule	Tick as applicable
Part A – Short Form Change Control Schedule	□
Part B – Long Form Change Control Schedule	X

The Part selected above shall apply this Contract. Where Part B is selected, the following information shall be incorporated into Part B of Schedule 5 (Change Control Procedure):

- Not applicable

Section C

Part A - Additional and Alternative Buyer Terms

Additional Schedules and Clauses

Part A – Additional Schedules

Additional Schedules	Tick as applicable
S1: Implementation Plan	x
S2: Testing Procedures	x
S3: Security Requirements (either Part A or Part B)	Part A □ or Part B x
S4: Staff Transfer	x
S5: Benchmarking	x
S6: Business Continuity and Disaster Recovery	x
S7: Continuous Improvement	x
S8: Guarantee	□
S9: MOD Terms	□

Part B – Additional Clauses

Additional Clauses	Tick as applicable
C1: Relevant Convictions	x
C2: Security Measures	x
C3: Collaboration Agreement	x

Where selected above the Additional Schedules and/or Clauses set out in document RM6100 Additional and Alternative Terms and Conditions Lots 2, 3 and 5 shall be incorporated into this Contract.

Part C - Alternative Clauses

The following Alternative Clauses will apply:

Alternative Clauses	Tick as applicable
Scots Law	□
Northern Ireland Law	□
Joint Controller Clauses	□

Where selected above the Alternative Clauses set out in document RM6100 Additional and Alternative Terms and Conditions Lots 2, 3 and 5 shall be incorporated into this Contract.

Part B - Additional Information Required for Additional Schedules/Clauses Selected in Part A

Additional Schedule S3 (Security Requirements)

The security management plan will be revised, as required, to ensure compliance with Home Office security requirements, security aspects letter and security policies.

Additional Schedule S4 (Staff Transfer)

Additional Clause C1 (Relevant Convictions)

Participation in a criminal organisation

- Participation offence as defined by section 45 of the Serious Crime Act 2015
  - Conspiracy within the meaning of:
  - section 1 or 1A of the Criminal Law Act 1977; or
  - article 9 or 9A of the Criminal Attempts and Conspiracy (Northern Ireland) Order 1983, where that conspiracy relates to participation in a criminal organisation as defined in Article 2 of Council Framework Decision 2008/841/JHA on the fight against organised crime.

Corruption

- Corruption within the meaning of section 1(2) of the Public Bodies Corrupt Practices Act 1889 or section 1 of the Prevention of Corruption Act 1906;
- The common law offence of bribery;
- Bribery within the meaning of sections 1, 2 or 6 of the Bribery Act 2010, or section 113 of the Representation of the People Act 1983.

Terrorist offences or offences linked to terrorist activities

- Any offence:
  - listed in section 41 of the Counter Terrorism Act 2008;
  - listed in schedule 2 to that Act where the court has determined that there is a terrorist connection;
  - under sections 44 to 46 of the Serious Crime Act 2007 which relates to an offence covered by the previous two points.

Money laundering or terrorist financing

- Money laundering within the meaning of sections 340(11) and 415 of the Proceeds of Crime Act 2002
- An offence in connection with the proceeds of criminal conduct within the meaning of section 93A, 93B or 93C of the Criminal Justice Act 1988 or article 45, 46 or 47 of the Proceeds of Crime (Northern Ireland) Order 1996.

Child labour and other forms of trafficking human beings

- An offence under section 4 of the Asylum and Immigration (Treatment of Claimants etc.) Act 2004;
- An offence under section 59A of the Sexual Offences Act 2003
- An offence under section 71 of the Coroners and Justice Act 2009;
- An offence in connection with the proceeds of drug trafficking within the meaning of section 49, 50 or 51 of the Drug Trafficking Act 1994
- An offence under section 1, 2 or section 4 of the Modern Slavery Act 2015.

Non-payment of tax and social security contributions

- Breach of obligations relating to the payment of taxes or social security contributions that has been established by a judicial or administrative decision.
- Where any tax returns submitted on or after 1 October 2012 have been found to be incorrect as a result of:
  - HMRC successfully challenging the Supplier under the General Anti – Abuse Rule (GAAR) or the “Halifax” abuse principle; or
  - a tax authority in a jurisdiction in which the Supplier is established successfully challenging it under any tax rules or legislation that have an effect equivalent or similar to the GAAR or “Halifax” abuse principle;

- a failure to notify, or failure of an avoidance scheme which the Supplier is or was involved in, under the Disclosure of Tax Avoidance Scheme rules (DOTAS) or any equivalent or similar regime in a jurisdiction in which the Supplier is established.

Other offences

- Any other offence within the meaning of Article 57(1) of the Public Contracts Directive as defined by the law of any jurisdiction outside England, Wales and Northern Ireland.
- Any other offence within the meaning of Article 57(1) of the Public Contracts Directive created after 26th February 2015 in England, Wales or Northern Ireland.

Additional Clause C3 (Collaboration Agreement)

[redacted]

Subject to the agreement by all parties to the Collaboration Agreement on the terms of the Collaboration Agreement, including limits of liability and the timetable for agreeing the collaboration plan, an executed Collaboration Agreement shall be delivered from the Supplier to the Buyer within the first thirty (30) Working Days from the Contract Commencement Date

Section D
Supplier Response

Commercially Sensitive information

The following information, relating to the Supplier and any of the Supplier's subcontractors, is Commercially Sensitive Information:

- Details of the Supplier's and any subcontractor's methodologies, approaches, policies and processes.
- All information relating to limits of liability, daily fee rates, pricing and charging mechanisms, and any negotiated discounts, which is not publicly available.
- The terms of the Supplier's and any subcontractor's insurance, which are strictly confidential.
- All details relating to personnel including but not limited to staff personal data, the numbers of resources with specific skills, numbers of security cleared staff, staff terms and conditions of employment and staff selection methods.

Section E
Contract Award

This Call Off Contract is awarded in accordance with the provisions of the Technology Services 3 Framework Agreement RM6100.

SIGNATURES

For and on behalf of the Supplier

Name	[redacted]
Job role/title	[redacted]
Signature	[redacted]
Date	**23rd December 2025**

For and on behalf of the Buyer

Name	[redacted]
Job role/title	[redacted]
Signature	[redacted]
Date	**23rd December 2025**

Attachment 1 – Services Specification

1. PURPOSE

1.1 This is an order form for provision of services to develop, maintain and support the Crossing the Border (CTB) Product Family. The Crossing the Border Product Family includes Border Crossing (BX), Helios, and Borders Platforms. The requirements detailed in this Lot 1 are for the development, maintenance and support in relation to BX and Helios.

1.2 Border Crossing (BX) is made up of several parts. At the Passenger Control Point (PCP) BX allows Border Force officers to search passenger records using biometrics and documents. In addition, checks take place on the passport chip to verify its validity. In the back-office BX Tools allows Border Force officers to investigate passengers more thoroughly, either before, during or after they have crossed the border. The BX admin tool provides authorised users with access to BX audit and performance data.

1.3 Helios is used for the ingest, maintenance and sharing of watchlist data. This data then supports the end-to-end passenger journey - from visa applications and pre-departure checks right through to crossing the border.

1.4 The purpose of this contract is to provide a full suite of technology-driven service operations for the run, maintain, sustain, iteration, tech debt and any fresh development required of existing or new products for border operations and to provide the services outlined in this document for the initial contract term of 48 months with the option to extend for a period of 12 months (48 + 12).

1.5 The Parties acknowledge that the services specification and associated requirements may change as a result of the activity within the Discovery and Mobilisation Period and that this Order Form may need to be updated and agreed accordingly.

2. BACKGROUND TO THE BUYER

2.1 The first duty of the Government is to keep citizens safe and the country secure. The Home Office plays a fundamental role in the security and economic prosperity of the UK. The Home Office is the lead Government Department for immigration and passports, drugs policy, crime, fire, counter terrorism and police.

2.2 Further detail can be accessed here: Home Office - GOV.UK (www.gov.uk)

3. BACKGROUND TO REQUIREMENT/OVERVIEW OF REQUIREMENT

3.1 Crossing the Border (CtB) is the steady state services and products which control the flow of people and services across the borders. This is done principally via the Primary Control Points, mediated by a Border Force officer, or via an e-gate indirectly supervised by an officer. Information from ports is processed by a central collection of systems, hosted in the cloud and on premise. These systems are built on top of a number of infrastructure platforms, leveraging a hybrid cloud model.

3.2 The central systems support 24 hours a day 365 days a year operations, requiring high degrees of resilience and availability. The existing applications run on diverse technological stacks and have been delivered over a 3 year programme and are expected to evolve over the next 5 years in line with government policy and operational need. The system is critical national infrastructure, incorporating official and secret data sets and related processes.

3.3 Within the Home Office Digital (HO Digital) directorate at the Home Office, the Migration and Borders Technology Portfolio (MBTP) encompasses all technology delivery and support for Migration, Asylum, and Border control. This includes the delivery of major technology programmes which make up part of the CtB Product Family, including but not limited to Immigration Platform Technology (IPT), Future Borders and Immigration System (FBIS) and the New Plan for Immigration (NPI). MBTP is organised in a product-centric way, with business requirements met where possible by leveraging a set of strategic technology products. These products are organised across sets of related ‘product families’ with the Crossing the Border Product Family being one of these.

3.4 The requirements in this document detail the Services to be delivered by a Supplier who will work with the Buyer in alignment with the HO Digital strategy, roadmap, and priorities of the Crossing the Border Product Family and for the Supplier to over the lifespan of the Contract to provide digital services teams who will deliver the scope of requirements as detailed below;

3.4.1 Deliver a flexible, responsive and predictable service provision, supporting the delivery of the objectives and priorities set out in the Crossing the Border roadmap.

3.4.2 Provide teams with the ability to flex resources up or down over the course of the Contract in line with business needs.

3.4.3 Create collaborations and partnerships that ensure delivery teams are supported and agreed repeatable processes in place.

3.4.4 Ensure alignment with exiting delivery strategies but devises improvements and enhancements, based on analytics to deliver a quality service and value for money.

3.4.5 Support the live services (including dedicated Level 3 Support for the products) and operational support teams.

3.4.6 Support critical national infrastructure, with appropriate onshore facilities, providing 24X7 monitoring and ability to facilitate responses to incidents within target Service Level Agreements.

3.4.7 Continuously improve the processes, and delivery methods of products, driven by user insights and performance analytics, to enhance the live service, drive value for money and efficiency.

3.4.8 Build new features to maintain the relevance of the live services in a digital landscape.

3.4.9 Work in partnership with all stakeholders in HO Digital and its partners in an atmosphere of openness and transparency. Buyer HO Digital expects all stakeholders, partners, and suppliers to work collaboratively, transparently and in partnership to successfully achieve its outcomes.

3.4.10 Drive the convergence and the use of shared technology, resource, and content.

3.4.11 Commitment to use and integrate relevant Buyer toolsets, where supplied, or their successor(s) for tracking and managing incidents, service requests, changes and problems.

3.5 These outcomes will be more specifically measured in terms of:

3.5.1 Adherence to HO Digital flexible working methodologies

3.5.2 Delivery of requirements to plan

3.5.3 Adherence to IT service management processes

3.5.4 Compliance with all required security measures

3.5.5 Compliance with all policy and legislative requirements

3.5.6 Compliance with Government standards, notably the Service Standard

3.5.7 Use of best industry practice

3.6 The Supplier is required to structure their teams and organisation as necessary to meet the requirements to deliver the Services. The Buyer's expectation is that the Supplier will provide multiple, multi-disciplinary teams, working in parallel, developing designs, and delivering change into live service.

3.7 It is important to note that we expect that there will be some fluctuation, both up and down, in terms of number of resources and role types in each team, as well as number of teams, over the course of the Contract as products and services move from development into delivery and BAU.

3.8 The Buyer will require the Supplier to flex to their needs as requirements evolve over the course of the Contract. The Buyer will work with the Supplier to review the delivery roadmap and discuss the skills mix and resources required and have an open dialogue on the best way to proceed in the best interest of meeting the objectives of the Crossing the Border family.

3.9 The Buyer requires the Suppliers personnel to have as a minimum National Security Vetting to SC level prior to deployment on delivery of the Services and starting work on development or production related activities. There may also be a requirement for further vetting for access to police information requiring NPPV3.

3.10 The Supplier will work with other development and support teams, collaboratively, cooperatively and in partnership to ensure the integrity of the overarching digital services capability HO Digital provides to its customers, end users and partners. Specifically, but not limited to:

3.10.1 BAU Live Services operational teams

3.10.2 UKVI customer support and service resolution teams

3.10.3 Build teams in other product families

3.10.4 Improvement teams in other product families

3.10.5 MBTP support teams

3.10.6 Government Partner teams

3.10.7 User-centric design teams

4. DEFINITIONS

4.1 The following definitions apply to this Attachment 1 only

Expression or Acronym	Definition
Approval to Operate	means a process of Certification and Accreditation so an IT system can be granted an Buyer to Operate (ATO) by the Home Office
Buyer	means the Home Office
Buyer Corporate Security Function	means the Home Office Corporate Security Function responsible for assuring the security of all products and services used within the Home Office and that the appropriate security measures are in place within any third party provider delivering services to the Home Office
Buyer Data	means and documentation, information or data provided by the Home Office or accessed by any third party provider to enable the delivery of the Services
Availability Management Process	means the process of ensuring the agreed levels of service availability are achieved and maintained in line with relevant Buyer strategy.
BAU	means business as usual

BFO	means Border Force Officer
Border Platforms	means the O and S platforms used to host the products within the CtB Product Family
Border Force	means the Buyer directorate responsible for control of the UK border
BPSS	means the government Baseline Personnel Security Standard as detailed at National security vetting: clearance levels - GOV.UK (www.gov.uk)
BX	means the Border Crossing (BX)product which is made of several parts - Primary Control Point (PCP) allows Border Force Officers to search passenger records using biometrics and documents. BX Tools allows Border Force Officers to investigate passengers more thoroughly, either before, during or after they have crossed the border. BX admin tool provides authorised users with access to BX audit and performance data.
CCS Technology Services 3 Framework	means the Crown Commercial Service Technology Services 3 framework agreement RM6100
CIS	means critical security control measures in place to help identify, manage and mitigate cyber security threat
CMDB	means configuration management database
Commencement Date	means the date specified as such in the Order Form in Section A
Components	means the individual parts of a service or application
Configuration Items	means a fundamental unit of a configuration management system that has distinct requirements, functionality and/or product relationships
Contract	means the contract between the Preferred Provider and the Buyer for the delivery of the Services
Contract Term	means the term of the contract in this instance an initial term of 4 years plus an optional 1 year extension
CSV	means comma separated values
CtB	means Crossing the Border
CtB Product Family	means the wider range of products and services as detailed at Appendix 4 which combined provide the digital products used to secure the UK Border
Customer Data	means any documentation, information or data provided by the Home Office or generated, processed, stored or transmitted by any third party provider acting on behalf of the buyer which must be handled in line with the Data Protection Act 2018

Cyber Security Operations Centre	means the systems and processes in place to monitor the health of cyber space and co-ordinate incident response
Data Operations	means the Buyer Data Operations Team
HO Digital	means the Home Office Digital directorate which provides the Buyer internal and external facing IT and digital services
DDOS	means distributed denial of service
DevOps	means the software development methodology that combines and automates the work of software development (Dev) and IT operations (Ops) teams to accelerate the delivery of higher-quality applications and services
Discovery and Mobilisation Period	means the period following contract award where the Supplier will complete a deep dive to establish the detail required for transition of Services and develop the final service delivery plan and is a distinct phase prior to transition of the services into BAU
DV	means developed vetting check as detailed at National security vetting: clearance levels - GOV.UK (www.gov.uk)
EBSA	means the Authorities Environment Build Support Administration platform
Facility Security Clearance	means the measures in place to ensure the Preferred Provider meets and maintains the required protective security controls to safeguard classified assets. It provides the Buyer with assurance that these assets will be appropriately protected.
FBIS	means Future Borders and Immigration Systems, the UK's digital products and services used for management of immigration services
GNIB	means Garda Northern Ireland Immigration Bureau
Government Partner Teams	means the teams from other government departments and organisations who provide information for the protection of the border via the CtB products and services
Government Secure Intranet	means the intranet used by the government for classified information
Government Security Classification Marking	means the security marking used to classify the sensitivity of information and the security measures to be used when handling such information as detailed at Government Security Classifications - GOV.UK (www.gov.uk)
Helios	Helios means the system used for the ingest, maintenance and sharing of watchlist data. This data then supports the end-to-end passenger journey - from visa applications and pre-departure checks right through to crossing the border.

HMG Security Policy Framework	means the framework which sets out the expectation of how Government organisations and third parties handling Government information and other assets will apply protective security to ensure effective, efficient and secure working as detailed at Security policy framework - GOV.UK (www.gov.uk)
HMPO	means HM Passport Office
HO Digital Problem Management Operations Model	means Buyer ITIL compliant documentation outlining the processes, procedures, resources and toolsets for managing problems within the Home Office environment
I-LEAP	International Law Enforcement Alerts Platform
IDS/IPS	means Intrusion Detection Systems and Intrusion Prevention Systems which are both means of network security. IDS is a network traffic monitoring solution. IPS is a preventative solution, which blocks delivery of certain documents/information, acting in a similar way to a firewall.
Impex	means import and export data from O to S data centres.
IPT	means Immigration Platform Technology
ITIL	means Information Technology Infrastructure Library
JIRA	means the project management software which is used to manage projects and track bugs.
KPI	means Key Performance Indicator. KPI’s are used as measurable performance metrics which will allow the Buyer to track and manage performance against these set metrics.
Level 2 Support	means IT technical Support to provide assistance on issues that level 1 support have been unable to resolve. Level 2 support involves in-depth troubleshooting, technical, and backend analysis
Level 3 Support	means IT technical Support that Level 2 is unable to resolve. It is the highest level of IT technical support. Providing in depth examination of incidents and issues.
MBTP	means the Home Office Migration and Borders Technology Portfolio which deliver a digital and technology services for the protection of the UK border
Negative Immigration	means an Immigration watchlist, one of the watchlists within Helios

National Cyber Security Centre	means the UK government agency that provides cyber security advice, guidance and support to industry and the public
National Security Vetting	means the security checks required to provide services to government as details at National security vetting: clearance levels - GOV.UK (www.gov.uk)
New Plan for Immigration	means the new controls of our legal immigration system by ending free movement and introducing a new points-based immigration system. This means that the decision on who comes to our country is based on the skills people have to offer
NPPV3	means Non Police Personnel Vetting level 3. It permits access to Secret level material. As detailed: About the Police National Vetting Service | Warwickshire Police
O Side	means the cloud based platform used to hold data marked as Official
Parties	means the Buyer and the Supplier
Persistent Volumes	means configuration of persistent data locations for stateful applications which allows containerised applications to store data beyond the lifecycle of individual containers or pods. This makes it possible to retain data even after a pod restart or update.
PKI Certificates	means Public Key Infrastructure (PKI) certificates. These are electronic documents that are used to prove the validity of a public key. They include information about the public key, the identity of the owner, and are digitally signed by a trusted entity.
PNR Data	means passenger name record (PNR) data, information collected by airlines and other passenger service operators as part of their normal course of business and includes information required to complete and process a booking
PPPT	Police & Public Protection Technology within the Home Office
Problem Management	means the process of identifying, managing and finding solutions for the root cause of incidents on an IT service.
Product Family	means all the digital services and programmes associated with the Borders and Migration Portfolio which include but not limited to BX, Helios, FBIS, MBTP, ATLAS, Core Cloud, Border Vision, ETA’s, E Visas and EBSA

Product Manager	means the person(s) responsible for the strategic direction of products and services for the Buyer;
Product Owner	means the Person(s) responsible for ensuring that product development is following the agreed roadmap and delivering value. This person works with the Product Manager to set direction and priorities
RACI	means the document for identifying key stakeholders and their responsibility or level of activity in relation to a project or programme of works
RAID	means Risk, Assumptions, Issues and Dependencies log
Registered Traveler Data	means the data held for all persons registered as a member of the Registered Traveler Scheme
Registered Traveler Scheme	means the membership service which allows faster and more convenient entry through the UK border
Root Cause Analysis	means the process of identifying and solving problems/issues after occurrence.
RPO/RTO	means recovery point objective and recovery time objective
Secure by Design Principles	means principles developed by the Central Digital Data Office to drive outcomes and their adoption is mandatory across central government and ALBs. They promote consistent and coherent security ways of working in digital delivery. Organisations which already have a local Secure by Design approach - or elements of one - will be expected to adhere to the principles, although they may wish to develop additional ones (and activities) to cater for their own circumstances.
Security Check or SC	means the security clearance level for individuals with access to information classified as OFFICIAL SENSITIVE
Semaphore	means the system used to electronically collect passenger and crew travel document information in advance of travel either into or out of the UK
Service Acceptance and Assurance	means the service acceptance criteria used to meet service requirements including functionality, operational support, performance, security to meet functional/non-functional requirements. These activities are undertaken to ensure new releases can be properly supported as part of the Live Service
Service Standard	means the Digital Service Standard is a set of 14 criteria to help government create and run good digital services.

Service Transition	means Service transition lifecycle stage makes sure that changes to services and service management processes are carried out in a coordinated way. The Buyer team is responsible for working with delivery teams on transitioning releases into live support
SFTS	means Secure File Transfer Services
SIEM	means security, information and event management
SLA	means service level agreement, the service levels to be met by the Preferred Provider to deliver the Services to the required standards
S Side	means the Buyer platform used to hold data marked as Official Sensitive and above
Supplier	means BAE Systems Applied Intelligence Limited
SWG	means security working group
SyOps	means systems operation and IT operations management
The Services	means the services outlined in this Attachment 3 Service Requirements document
UI	means user interface
UK EYES ONLY	means the security classification applied to information and data of a level of sensitivity that cannot be viewed by any individual that is not a UK national
UKVI	means UK Visas and Immigration
VPN	means virtual private network
WAF	means web application firewall
Working Day	means between the hours of 08:00 to 17:00 on any day other than a Saturday, Sunday or public holiday in England and Wales

5. SCOPE OF REQUIREMENT

5.1 The table below has a brief description of each in scope product or service that is managed across the Border Crossing and Helios teams. Where a service is described as “Shared” in the “Managed by” column below, the Supplier will have some responsibility as part of scope, the detail of which will be determined during the Discovery and Mobilisation Period.

Component Part	Managed by	Description
CtB Helios Application	Helios	CtB Helios Application is the service and screen used to upload documents to attach to records on the watchlists on the S CtB system. It requires users to use the SPaaS Thin Client to access it
CtB S BX Admin (User Admin)	Helios	CtB BX Admin (user admin) is the service and screen used to administer the users on the CtB Helios system on S
CtB CRS Ingest	Helios	Technical service to enable the loading of CRS data into Helios O. Comprises application services for SFTS service (including the UI part used by Data Operations), subsystem
CtB MIDA Ingest	Helios	Technical service to enable the loading of CRS data into Helios O. Comprises application services for SFTS service (including the UI part used by Data Operations), subsystem. The receipt of the data file is manual, and loading is triggered manually via O BX admin
CtB PNC Ingest	Helios	Technical service to enable the automated receipt and loading of PNC data into Helios O. Compromises of application services for SFTS service, S3 bucket, the data feed file and the Ingress subsystem
CtB Garda Ingest	Helios	Technical service to enable the receipt and loading of Garda data (GNIB Negative Immigration) into Helios S. Depends on Garda File store, the application services for SFTS service, S3 bucket, the data feed file, Impex and the ingest subsystem on S. The receipt of the data file is automatic, but the loading is triggered manually via O BX admin
CtB HOSOL Ingest	Helios	Technical service to enable the receipt and loading of HOSOL data (Home Office Serious Offenders List) into Helios S. Depends on application services for SFTS service, S3 bucket, the data feed file, Impex and the ingest subsystem on S. The receipt of the data file is automatic, but the loading is triggered manually via O BX admin.
CtB MSMR2	Helios	MSMR2 (successor to MSMR-Lite) is responsible for carrying out the search functionality from upstream interfaces such as PCP-UI, and e-gates; then federating the search to downstream services to be then aggregated, and sorted into a response back to the original consumer to provide a Border Force Officer with the relevant information to make an informed decision
CtB HMPO Ingest	Helios	Technical service to enable the receipt and loading of HMPO data into Helios S. Depends on application services for the Data Operations email mailbox, the data feed file, Impex and the ingest subsystem on S. The receipt of the data file is via email and the loading is triggered manually via O BX admin.
CtB Registered Traveller Ingest	Helios	Technical service to enable the loading of Registered Traveller data into Helios S. Depends on application services for the data feed file, Impex and the ingest subsystem on S. The receipt of the data

		file is manual a portal on the 'Registered Traveller Scheme' business service and the loading is triggered manually via O BX admin.
CtB Garda Extract	Helios	Technical service to enable the automated creation and transmission of the Garda data file extract (Negative Immigration) to Garda from Helios O. Depends on application services for the data extract file, S3 bucket, SFTS service and the ingest subsystem (that creates the extract file).
CtB Semaphore Extract	Helios	Technical service to enable the automated creation (but not transmission) of the Semaphore extract file from Helios S. Depends on application services for the data extract file, Semaphore Extract subsystem (that creates the extract file) and the Persistent Volumes and file stores into which the file is placed. The transmission of the file is carried out manually via other business services.
CtB O Report Generator	Helios	Technical service to enable the automated running and creation of reports on the O side of CtB / BX / Helios. The reports are CSV text file extracts. The reports are then stored for viewing or transmission by users who then use "CtB O BX admin (reports)".
CtB S Report Generator	Helios	Technical service to enable the automated running and creation of reports on the S side of CtB / BX / Helios. The reports are CSV text file extracts. This technical service also then copies the report files via Impex to the O CtB / BX / Helios system. The reports are then stored on O for viewing or transmission by users who then use "CtB O BX admin (reports)".
CtB S Kibana	Shared	CtB S Kibana is the CtB instance of Kibana, used for view S side alerts and monitoring, build upon the SPaaS Kibana service.
CtB S Grafana	Shared	CtB S Grafana is the CtB instance of Grafana, used for view S side alerts and monitoring, build upon the SPaaS Grafana service.
CtB Garda file store	EBSA	CtB Garda file store is the file store into which Garda place the "CtB Garda data feed file". It is from this file store that the "CtB NI SFTS Service" picks up for data feed file as part of the "CtB Garda Ingest" technical service. Also, the "CtB Garda Extract" technical service created and transmits the Garda extract to the "CtB Garda file store". This file store is not provided by the Buyer, but if there is an incident relating to it that stops the "CtB Garda Ingest" or the "CtB Garda Extract" an incident should be raised against this service for tracking (whilst it is communicated to Garda).
CtB BX eGates	BX	CtB BX eGates is a primary impacted service that sits under the BX solution. providing an automated check of chipped passports through physical eGates
CtB BX eGates infrastructure	BX	Infrastructure technical service that underpins the eGates service. This infrastructure is all in port.
CtB BX Port Office Infrastructure	BX	CtB BX Port Office Infrastructure (BX POI) Service to support the Border Crossing POISE Primary Contact Point (PCP) End User Devices (EuDs) and peripherals

		The POI EuD Service offers a managed service for all POI EuD devices used to access POISE. The devices offered are Windows Laptops, Desktops, Document Scanners and Passport Scanner. Devices provided allow HO Border Force users to access and consume existing data, tools and Buyer applications on POISE. The Service offers BX POI hardware Incident Management of assets across the Border Crossing estate. Is the primary hardware support team for BX POI End User Devices, any queries or escalations should be sent to the EUC Service Manager.
CtB BX Application URL	BX	CtB BX Application URL is the link and associated configuration that is installed on the PCP end user devices. The link is used by Border Force Officers to access the "CtB BX Application" that is the service that enables Border Force Officers to check passengers and passports at PCPs in ports. CtB BX Application URL depends on the "CtB BX Ports and Offices" business service.
CtB BX PCP UI	BX	At the Passenger Control Point (PCP) BX allows Border Force officers to search passenger records using biometrics and documents. In addition, checks take place on the passport chip to verify its validity.
CtB BX Training Environment	BX	Training environment for BX.
CtB O BX Admin (User admin)	BX	CtB O BX Admin (User admin) is the service and screen used to administer the users on the CtB BX system.
CtB O BX Admin (Site admin)	BX	CtB O BX Admin (Site admin) is the service and screen used to administer the sites on the CtB BX system.
CtB O BX Admin (Content admin)	BX	CtB O BX Admin (Content admin) is the service and screen used to administer the help and screen content on the CtB BX system.
CtB O Kibana	Shared	CtB O Kibana is the CtB instance of Kibana, used for view O side alerts and monitoring, building upon the EBSA Kibana service.
CtB O Grafana	Shared	CtB O Grafana is the CtB instance of Grafana, used for viewing O side alerts and monitoring, building upon the EBSA Grafana service.
CtB O Dynatrace	Shared	CtB O Dynatrace is the CtB instance of Dynatrace, used for viewing O side alerts and monitoring, building upon the EBSA Dynatrace service.
CtB BX LAN	Enterprise Services	The new Port Office Infrastructure is known as CtB BX LAN - provides a resilient replacement for the legacy WI infrastructure in ports and back-office sites in order to support BX, ECU and eGates at Ports both functionally and non-functionally.
CtB PCP Offline Data Capture	BX	CtB PCP Offline Data Capture (ODC) is a disaster recovery and business continuity for the BX Application at Border Crossing primary control points (PCPs).

		The capability is available on selected devices only and, in certain locations, supplemented by additional offline stop list functionality.
CtB PCP ODC Harvest	BX	CtB PCP ODC Harvest is the service that enables suitable users to harvest the data from ODC mode following an ODC event.
CtB BX Tools URL	BX	BX Tools is a suite of applications to be used by Border Force and other security agencies for two very high-level use case: 1. For further investigation into a person of interest that was previously prevented from going through border patrol, and logging such instances where this occurs. 2. For agencies both inside and outside of Border Force to carry out background checks on individuals as part of their business processes when undertaking activities such as processing applications. CtB BX Tools URL is the link and associated configuration that is installed on the certain end user devices. The link is used by Border Force Officers to access the "CtB BX Tools" applications. CtB BX Tools URL depends on the "End User Device" business service."
CtB BX Tools (Document number search)	BX	CtB BX Tools (Document number search) is part of the suite of business services that is CtB BX Tools. CtB BX Tools (Document number search) is the business service that enables the Border Force Officer (normally in the port back office) to search the watchlist using a document number or a person's details. If that functionality does not work, the Incident should be recorded against this business service.
CtB BX Tools (Watchlist Record Lookup)	Helios	CtB BX Tools (Watchlist Record Lookup) is part of the suite of business services that is CtB BX Tools.
CtB BX Tools (Record number search)	BX	CtB BX Tools (Record number search) is part of the suite of business services that is CtB BX Tools. CtB BX Tools (Record number search) is the business service that enables the Border Force Officer (normally in the port back office) to search the watchlist using a watchlist record number or an address.
CtB BX Tools (Investigation Log)	BX	For further investigation into a suspicious person that was previously prevented from going through border patrol, and logging such instances where this occurs

CtB BX Tools (Bulk Search)	BX	CtB BX Tools (Bulk Search) is part of the suite of business services that is CtB BX Tools. CtB BX Tools (Bulk Search) is the business service that enables a user (normally the Immigration Service Crosscheck Team, or those checking the Passenger Transit Report after ODC use) to upload a file which is then used to perform a bulk search against the watchlists.
I-LEAP integration	Shared	International Law Enforcement Alerts Platform. Strategic solution for CTB source of Interpol data. Platform managed by PPPT. Integration point jointly managed by PPPT and CTB.
Match Engine	Helios	Software or systems designed to facilitate matching or comparison tasks. For instance, in the context of databases, a match engine could be used to identify and match records based on specific criteria (currently unpriced to be discussed during Discovery and Mobilisation Period)

6. THE REQUIREMENT

6.1 The Supplier will be required to complete a Discovery and Mobilisation Period during which they will work with the Buyer, incumbent suppliers, Buyer HO Digital stakeholders and any other stakeholders, as deemed necessary, to develop a detailed roadmap and delivery plan, including service levels and acceptance criteria which will be agreed with the Buyer.

6.2 The acceptance criteria provided below is for information to inform Suppliers of the levels of service they will be expected to deliver as a minimum. Please note that additional deliverables and acceptance criteria will be agreed throughout the term of the Contract.

Deliverable	**Description of work to be carried out**	**Delivery Test / Acceptance Criteria**
Source code	Source code checked into the Customer's source code repository, including functional code, configuration, automated tests and deployment scripts	Passing of user acceptance tests against agreed technical acceptance criteria for relevant user stories or upon moving into live production, whichever occurs first
Machine readable code	Binaries for the Service deployed onto the Authorities infrastructure	Passing of user acceptance tests against agreed technical acceptance criteria for relevant user stories or upon moving into live production, whichever occurs first
Delivery plan	Development and documentation of delivery plan	Work effectively managed by development teams, reviewed and agreed with Buyer Delivery Lead at relevant governance forums

Operational documentation	Documentation of the release and technical procedures required to maintain and operate the Service on the Customer's Confluence collaboration suite	On receipt of the documentations which will be released by Preferred Provider, these shall be accepted through the relevant operational acceptance tickets in JIRA or its successor
Design & Test documentation	Documentation of the technical design and test plans for the Service on the Customer's Confluence collaboration suite	On receipt of the documentations which will be released by Preferred Provider these shall be accepted through the relevant operational acceptance tickets in JIRA or its successor. Test documentation is made readily available on Confluence or its successor without need for a JIRA ticket

7. CONTINUOUS IMPROVEMENT REQUIREMENTS

7.1 The Supplier will be expected to continually improve the way in which the required Services are to be delivered throughout the duration of the Contract. This includes run, maintain and sustain support, continuous improvement of products, management of tech debt, iterative changes, integration fresh development and preventative and remedial activities required, in line with the Authorities priorities and to ensure critical national infrastructure in scope of this contract remains fit for purpose.

7.2 Where the Supplier wants to propose new ways of working these should be presented to the Buyer during monthly/quarterly Contract review meetings.

7.3 Changes or improvements to the way in which the Services are to be delivered must be agreed by the Buyer prior to any changes being implemented.

8 ARCHITECTURE REQUIREMENTS

8.1 The Supplier must ensure that all systems are operated in such a manner that;

8.2 The Supplier shall enable the CtB Product Family with the capabilities required to allow the Buyer or nominated parties to monitor the operational health and usage of the applications and services to ensure services meet any agreed Non-Functional Requirements.

8.3 The Supplier must comply with the Buyer's policies and the EU Directive on PNR Data and any applicable legislation.

8.4 The Supplier is required to collaborate with the Buyer to establish cost monitoring processes and where appropriate cost controls for cloud capabilities within the product.

8.5 The Supplier is required to follow and support the Buyer architectural and design governance practices.

8.6 The Supplier is required to follow the Buyer's architectural and design standards.

8.7 The Supplier is responsible for maintaining a technical debt register and review of the technical debt register with an appointed Buyer representative on a regular basis to report, manage, plan, and deliver remediation of technical debt.

8.8 The Supplier is required to support and input to the architectural risk register which will be reviewed with an appointed Buyer representative monthly to report, manage and plan remediation of risk.

8.9 Unless deemed an emergency the Supplier will be required to schedule any downtime for the CtB capability within agreed low traffic windows.

9 TEST REQUIREMENTS

9.1 The Supplier will be required to:

9.2 Ensure that all tests are included with the correlated code and configuration changes within the source and version control process.

9.3 Ensure relevant testing activities are included within the automation pipeline with configuration criteria defining the scope and content of the test execution.

9.4 Test automation code coverage across all environments and regression packs at all times must meet, or exceed the KPI standard set out in this contract, with the remainder being auto assisted on manual intervention. Manual regression steps are to be agreed with the Buyer by exception.

9.5 Adopt the Buyer's security testing processes and adopt a shift left approach in the delivery pipeline.

9.6 Ensure that code, test and requirement coverage metrics are agreed and measured per component.

9.7 Ensure that no component is delivered that exceeds the defect threshold and criteria agreed with the Buyer for the related test phase.

9.8 Utilise the Buyer's defect classification model and record all related defect information within the Buyer's JIRA instance. Where the security classification of the defect prevents the utilisation of JIRA the Buyer will agree an alternate method with the Supplier.

9.9 Maintain and evidence test plans, execution results and completion reports for each iteration and at each tier of test for which the Supplier has responsibility. The format and content of said artifacts with be collaboratively agreed with the Buyer's test assurance team.

9.10 Follow the Buyer's overarching test strategy and collaborate on any changes or enhancements required to support the product.

9.11 Collaborate with the Buyer to review and execute the test strategy and RACI for test stages (including support for Buyer test stages).

10. OUT OF HOURS EXPEDITED DELIVERY PROVISION

10.1 The Supplier will provide delivery team engineers to support expedited delivery as requested by the CtB delivery lead.

10.2 Out of hours overtime for expedited delivery is only applicable during exceptional circumstances and where agreed with the Buyer and will not be applied as an extension to regular, planned activity. Expedited delivery will operate between 20:00 – 06:59 + 1 day Monday to Sunday and 07:00 – 06:59 + 1 day on public holidays. This will only be in addition to standard working hours (i.e. a working day that has been altered to start at 10am and finish at 7pm will not accrue overtime).

10.3 Payments of out of hours overtime for expedited delivery cannot exceed the cap agreed with the Buyer for this Contract or any associated statement of work. Any cap to be agreed during the Discovery Period.

11. OUT OF HOURS 24/7 ON CALL SERVICE REQUIREMENTS

11.1 Engineers with suitable experience and minimum National Security Vetting to SC level will be available "on-call" 24 hours to provide subject matter expert and engineering expertise for the duration of this Contract and any associated statement of work.

11.3 The Supplier must provide an On-Call Support rota for those services covered by this contract. Engineers must be capable of:

11.3.1 Querying and analysing data in Dynatrace and Kibana, or their successors.

11.3.2 Performing code analysis into symptoms

11.5 OOH OT for on-call support response is applicable at all times outside of the Working Day, Monday to Friday 08:00 – 17:00.

11.6 Payments of out of hours overtime for on-call support response cannot exceed the cap for this contract or associated SOW.

12. INCIDENT MANAGEMENT, PROBLEM MANANGEMENT AND AVAILABILITY.

12.1 The Supplier will provide their services as a Level 3 support capability in accordance with the Authorities HO Digital's MBTP incident management processes.

12.2 These issues will be triaged and resolved by Level 2 Support teams, based on instructions for known errors

12.3 If Level 2 are unable to resolve an incident because it would require a change in the source code or a change in the way the product functions, data errors, or is overall too technically complex; the incident will be raised to the Level 3 support team to conduct a root cause analysis. The Supplier will be responsible for;

12.3.1 Root Cause Analysis – Provide an impact assessment on the cause of the issue, the impact to end users and recommendations on the resolving the issue

12.3.2 Code Change –Should an incident require a code change from the applications team to resolve, this will need to be done in collaboration/support of the Buyer's Quality Assurance, release and product (Service ownership) team(s).

12.3.3 Design Changes – If an incident highlights an issue in the original design, the application architecture team will need to make a design decision on any changes that needs to be made to the design.

12.3.4 Data Corrections – if Data needs to be patched then the Supplier team is responsible for identifying the changes needed and seeking the test evidence and approvals to run these data corrections in Production if they have access or raising a ticket with the appropriate team to run more large scale / complex data corrections.

12.3.5 Work Instructions – If the problem is one that may occur again and a work instruction for Level 2 can be written so Level 2 can resolve these in future without Level 3 input if Level 2 cannot create the work instructions then the Level 3 team is responsible for writing a Work Instruction in line with shift left principles.

12.3.8 Collaborating with other teams on incident management

12.3.9 Facilitating the restoration of normal service operation

12.3.10 As per 11.2 As part of their Level 3 support and development activities or in their regular monitoring of the system, the Suppliers responsible for raising any issues they see in Production with the Level 2 Support teams so appropriate triage and incident management processes can start.

12.9 .

13. SERVICE LEVEL MANAGEMENT

13.1 The purpose of service level management is to define, document, agree, monitor, measure, report and review the level of IT services.

13.2 The Supplier will advise and assist in the definition, documentation, agreement, monitoring, measuring, reporting and review of Service Level Agreements (SLAs).

13.3 There will be a requirement to input into Monthly Service Management review. Other key activities will include ensuring the agreed SLAs are delivered, Triage of allocated tickets, providing updates on incidents and problems on the HO service management tooling.

14. INCIDENT RESOLUTION

14.1 The Supplier will be assigned incidents for investigation within Level 3 support activities and as investigation progresses, the Supplier will provide updates.

14.2 The Supplier will provide updates within the Buyer ITIL Toolset following access being granted during transition.

14.3 Within the scope of the working hours agreed for the Supplier service, the Supplier will provide support to Level 2 teams to meet the stated Incident Resolution Times and their agreed service level agreements. All incident start times are measured from the moment the incident record is registered in the Buyer ITIL Toolset following access being granted during transition.

PRIORITY DESCRIPTION RESOLUTION TARGETS

Priority	Description	Response Target	Resolution Target
P1	P1 means an Incident: a) that results in a complete or substantial loss of the Service; or (b) that results in an essential part of the Service being unusable for all End Users; or (c) that results in all End Users being unable to access the Service.	100% <= 15 mins	100% <= 4 hours
P2	P2 means an Incident: (a) where the Service is materially adversely affected, but can be circumvented; or	100% <= 30 mins	100% <= 8 hours

	(b) where the Service remains operable, but certain material aspects of the Service are disabled; or (c) where a large group of End Users is unable to access the Service; or certain material aspects of the Service.		95% <= 2 Working Days 100% <= 5 Working Days
P3	P3 means an Incident: (a) that results in a minimal business impact for the Service where non-critical functions or procedures are down, unusable, or difficult to use; or (b) affecting a single or small group of End Users.	100% <= 24 hours	
P4	P4 means an Incident:	100% <= 48 hours	95% <= 3 working days

	(a) that results in little or no material impact on the Service or the Customer's business; or (b) where the Service is determined to be functioning as designed but the Incident may result in a Change Request to modify or enhance the Service; or (c) raised in response to questions, compliments, complaints, escalations, or queries from the Customer.		100% < 5 working days

14.4 Service level detailed are subject to change and may evolve over the life of the Contract.

15. SERVICE AVAILABILITY AND SUPPORT HOURS

15.1 Crossing the Border (CtB) is the digital “front door” into the UK at the Border and as such is a critical service and must be available 24 hours a day 365 days of the year meeting the agreed availability target for service availability. The system has been delivered through mature flexible methods that optimise the delivery of new technical products, driving throughput and velocity.

15.2 Any planned release must be in accordance with non-impacting release arrangements to ensure service availability.

15.3 The Supplier will provide third line support in the form of resolutions to incidents found in the service in live operation 24/7 (support hours).

16. PROBLEM MANAGEMENT

16.1 The Supplier is required to deliver a HO Digital aligned, and collaborative capability providing both proactive and reactive problem management support under the governance of the enterprise's HO Digital Service Desk, in accordance with HO Digital Problem Management operating model.

16.2 The Supplier will:

16.2.1 Perform a Root Cause Analysis (RCA) and collaborate with other teams during this process to resolve the root cause

16.2.2 Develop workarounds until the fix can be released to production

16.3 The Supplier will adopt a proactive approach to Problem Management, seeking to resolve known errors and eliminate the root causes of incidents.

16.4 Report the success of proactive problem management through enhanced reporting in the monthly service performance pack, reviewed at the monthly Service Review Board.

17. EVENT MANAGEMENT

17.1 As part of any development, the Supplier will work with HO Digital, Level 2 Support, the operational support teams, site reliability engineering and service transition teams to ensure that appropriate and necessary thresholds, triggers and alerts have been implemented as part of the solution within each feature's release.

17.2 The Supplier will ensure that monitoring alerts are captured appropriately and disseminated to the required tools and teams as part of their developmental activities. All alerts will be fully documented with their resolution scripts, and these provided to Level 2 teams as part of knowledge transfer as required, with expectation the transition activities for knowledge transfer will be from the Level 2 exiting supplier.

17.3 Further integration of where monitoring and alerts appear may be required if tooling changes or requirements change.

18. CHANGE MANAGEMENT

18.1 Relevant change management processes can be found at Appendix 3

19. SYSTEM AND OPERATIONS MANAGEMENT

19.1 In the day-to-day systems management and operational support of the CtB Product family, the Supplier shall work in a Level 3 support capacity in line with requirements assigned to them by the relevant Level 2 teams.

19.2 The Supplier will be responsible for ensuring an effective capacity for supporting the live service in production.

20. RELEASE AND DEPLOYMENT MANAGEMENT

20.1 Release assurance and integration activities deliver enhancements, maintenance, and new services to the enterprise, but they can also present risk to the controlled environments and services of the Buyer Live Services estate.

20.2 The Supplier will be required to work with the Buyer HO Digital Change & Release Management Team for that team to raise all the required release and deployment approvals.

20.3 The Supplier will be required to work with Buyer Office HO Digital and ensure compliance with the Authorities non-impacting release strategy to ensure planned releases and maintenance do not affect overall system availability.

20.4 The Supplier will prepare and test release packages and support for deployment across non-production and production environments as per the CtB release operating model.

21. RELEASE AND DEPLOYMENT SCHEDULE

21.1 The Supplier shall provide deployment support to operational teams. This may be outside of the core hours by agreed exception.

21.2 In accordance with the change and release processes the Supplier will deploy all approved and tested releases or action the deployment schedule as part of a continuous delivery approach through agreed pipeline release cycles.

22. APPLICATION AND INFRASTRUCTURE MANAGEMENT

22.1 The Supplier shall provide support into the application and infrastructure operational teams as determined by the instructions the Supplier developed as part of the transition of changes and releases into the production environment. This includes creating and then supporting scripts developed as a result of incidents and / or problems for which the Supplier provided the resolution.

23. GOVERNANCE

23.1 The Supplier is required to provide designated, named, and suitably qualified, point of contact, as a Service Delivery Manager, through whom delivery of the Services will be managed with the Buyer’s lead Delivery Manager on a day-to-day basis

23.2 The Supplier will allow access to all documentation and data required for the Buyer to review or audit the Supplier’s operational processes at any time throughout the duration of the Contract.

23.3 The Supplier is required to align to ISO/EIC 20000 accreditation standards in delivery of their services for the duration of the Contract as part of the CtB systems wide ISO/EIC 20000 accreditation.

23.4 The Supplier is required to;

23.4.1 Participate in the monthly and ad-hoc service reviews.

23.4.2 Promptly respond to all requests from the Buyer which may cover all aspects of system operations.

23.4.3 Engage cooperatively and proactively in review of service data and remediation or improvement activities for the entire end to end services in scope of this Contract including underperforming components which may be in scope for improvement.

23.4.4 The Supplier is required to provide a named point of contact to attend governance meetings as set out by the Buyer and provide input to such meetings covering topics such as status, plans, actions.

23.4.5 Participate in scheduled and ad-hoc delivery and service reviews, SWGs, change boards, and any other meetings as deemed necessary by the Buyer.

23.4.6 Promptly respond to all requests from the Buyer which cover all aspects of delivery and system operations.

23.4.7 Engage cooperatively and proactively in review of service data and remediation or improvement activities for the entire end to end services in scope of this Contract, including underperforming components which may be in scope for improvement.

23.4.8 The Supplier will advise and assist in the definition, documentation, agreement, monitoring, measuring, reporting and review of Service Level Agreements (SLAs).

23.4.9 There will be a requirement to input into monthly service management review. Other key activities will include ensuring the agreed SLAs are delivered, triage of allocated tickets, providing updates on incidents and problems on the HO service management tooling.

24. KEY MILESTONES AND DELIVERABLES FOR DISCOVERY

24.1 During the Discovery and Mobilisation Period the Supplier will work with the Service Integrator to identify and assess business analysis activity required for the delivery of the CtB services. Findings will be presented to HO Digital and agreed between all Parties how this activity will be delivered and managed under which CtB contract throughout the contract term.

24.2 During the Discovery and Mobilisation Period the Supplier will provide the Buyer with the following Deliverables detailed in the table below which will be reviewed and accepted or returned by the Buyer.

Activity/Artefact	Responsible Owner	Due Date for Delivery (from 1st Dec start date)	Notes

Detailed Roadmap	**Delivery Lead**	27/02/2026	Dependent on HO to deliver roadmap
Detailed Implementation Plan	**Delivery Lead**	31/03/2026	
Service Levels and Acceptance Criteria / Service Design / Service Model	**Service Architect**	27/02/2026	
Test Strategy	**Test Lead**	30/01/2006	
Test RACI	**Test Lead**	30/01/2006	
RAID definition	**Delivery Lead**	31/12/2025	
Performance Management Strategy (KPI)	**Delivery Lead**	30/01/2026	Dependent on KPMG to facilitate for all suppliers
Security Management Plan	**Security Lead**	31/12/2025	In reality this is completed and with HO
Business Continuity and Disaster Recovery Plan (BCDR)	**Service Architect**	31/03/2026	
Continuous Improvement Plan	**Solution Architect**	31/03/2026	
Collaboration Agreement	**Solution Architect**	30/01/2026	Dependent on KPMG to facilitate for all suppliers
Quality Plans	**Solution Architect**	31/03/2026	
Exit Plan	**Delivery Lead**	31/03/2026	

New Integration Analysis/Requirements Gathering	**Business Analyst**	30/01/2026	
New Integration Design	**Solution Architect**	27/02/2026	
New Integration Estimation Review	**Solution Architect**	27/02/2026	
Tech Debt Analysis/Estimation Review	**Engineering Lead**	30/01/2026	
Transition Management	**Delivery Lead**	31/03/2026	
Knowledge Transfer	**Delivery Lead**	31/03/2026	
Service Process Set up	**Service Architect**	31/03/2026	
Service Technical Set up	**Service Architect**	31/03/2026	
Onboarding/Mobilisation	**Account Team**	31/03/2026	
Orientation	**Account Team**	31/03/2026	

24.3 Throughout the delivery of the Service, the Supplier is required to take responsibility for software development and test activities within the lower environments for the duration of this Contract. All release management and integration test activities are the responsibility of the Buyer with support from the Supplier and any deliverables supplied must reflect the Supplier’s responsibilities.

24.4 Post contract award the Supplier must provide an implementation plan(s) consisting of a schedule, forecasts, deliverables and acceptance criteria; for the coming PI which will be elaborated and will be iterated on a PI-by-PI basis to provide a long-term implementation plan.

25. MANAGEMENT INFORMATION/REPORTING

25.1 Reporting requirements will be captured in the governance schedules under transparency reporting, and these will be defined and agreed during the Discovery and Mobilisation Period.

25.2 Operational reporting and associated management processes such as RAID etc will be defined and agreed during the Discovery and Mobilisation Period.

26. VOLUMES

26.1 Volumes will be determined during the Discovery and Mobilisation Period.

27. SUSTAINABILITY / SOCIAL VALUE

27.1 The Supplier must demonstrate their commitment to social value by ensuring that throughout the Contract Term they have activities and processes in place that will show how they can deliver additional environmental benefits in the performance of the contract, including working towards net zero greenhouse gas emissions. Illustrative example: conducting pre-contract engagement activities with a diverse range of organisations in the market to support the delivery of additional environmental benefits in the performance of the contract.

27 QUALITY

27.1 The Supplier will provide a list of accreditations held that are relevant to the scope of the Supplier's solution.

27.2 Buyer technical standards and principles will be followed (including NCSC, and GDS published standards).

28 STAFF AND CUSTOMER SERVICE

28.1 The Supplier shall provide a sufficient level of resource throughout the duration of the Contract in order to consistently deliver a timely and best value, quality service.

28.2 The Supplier's staff assigned to the Contract shall have the relevant qualifications and experience to deliver the Contract to the required standard.

28.3 The Supplier shall ensure that staff understand the Buyer's vision and objectives and will provide excellent customer service to the Buyer throughout the duration of the Contract.

29 SERVICE LEVELS AND PERFORMANCE

29.1 The Buyer will measure the quality of the Supplier's delivery by adherence to the KPI's that will be discussed and agreed during the Discovery phase. The early view of the KPI's that may become applicable is as follows:

	KPI	POOR	UNSATIS-FACTORY	IMPROVE	ON TARGET	ABOVE TARGET

1	IT Governance – Unauthorised changes per month				0	
2	IT Governance – Failed release working group/Go no go checks per month				0	
3	IT Governance – Failed phase gate reviews per month				0	
4	Performance Management – Critical processes with agreed goals and metrics	80%	85%	90%	95%	100%
5	Performance Management – Defect resolution times				To Target	Quicker than agreed target
6	Enterprise architecture Workstreams using enterprise architecture services				100%	
7	Service Management - % of services with defined SLA	<80%	80%	90%	>90%	
8	Compliance with defined service levels	<90%	90%	95%	100%	
9	Compliance with existing DORA metrics	<90%	90%	95%	100%	
10	Delivery of outcomes to agreed quality standards	<90%	90%	95%	100%	
11	Use of tooling, adherence to WoW, standards	<90%	90%	95%	100%	
12	Availability of requirement information through agreed tooling	<90%	90%	95%	100%	
13	Supplier leads the understanding and defining of requirements	<90%	90%	95%	100%	
14	Transparency on SOW activities and ways of working	<90%	90%	95%	100%	

29.2 The Supplier must adhere to an Incentives Mechanism and Service Credit regime which will be in force until the end of the contract. The process will be further defined during the Discovery and Mobilisation Period.

29.3 A performance management strategy will be developed during the first 6 months after contract commencement which will include processes for management of poor performance.

30 SECURITY AND CONFIDENTIALITY REQUIREMENTS

30.1 The Supplier will be required to hold Cyber Essentials, ISO27001 or an equivalent accreditation as per the terms of the CCS Technology Services 3 Framework RM6100. The Buyer will require a copy of the accreditation certificate prior to start of mobilisation of the services.

30.2 The Supplier must ensure that all individuals supporting delivery of the services must hold SC clearance as minimum. All individuals deployed in the delivery of the services must hold National Security Vetting at Security Cleared (SC) level as a minimum. For further details please see below; www.gov.uk/government/organisations/united-kingdom-security-vetting

30.3 Supplier should be advised that where an individual has held SC vetting but has not been engaged on a contract delivering services to government for 12 months or longer, then regardless of the expiry date of the vetting this vetting will no longer be valid.

30.4 Please note valid SC vetting must be in place prior to start of the services and the Supplier will be responsible for sponsoring all vetting and costs for vetting.

30.5 The Supplier must ensure that all data shared or produced in the delivery of the Contract carries the relevant Government Security Classification Marking and is treated in accordance with the Government Security Classification Policy, for further details please see below.

30.6 The Buyer will require all SC vetting for individuals deployed in the delivery of the Services to be transferred to the Buyer for the duration of the Contract Term. Prior to start of the services the Supplier will be required to complete a security clearance transfer form for each individual with SC vetting to be deployed on the Contract. www.gov.uk/publications-security-classifications.

30.7 The Supplier must ensure compliance at all times with the requirements of the Government Security Policy Framework. Please see below for further details. www.gov.uk/government/publications/security-policy-framework.

30.8 The Supplier must ensure that any data produced or shared in the delivery of this Contract is not held Offshore. Where the Supplier has a requirement for data to be stored or accessed Offshore then approval must first be sought from the Buyer.

31 SECURITY MANAGEMENT

31.1 The Supplier shall ensure appropriate Security Assurance is conducted on any 3rd party suppliers used to provide the service before being provided access protected the Buyer's ICT services.

31.2 The Supplier shall be ISO/IEC 27001 and Cyber Essential Plus compliant. The Supplier shall ensure that they have active ISO/IEC 27001 certification throughout the duration of the Contract for any of their locations used to provide any services in scope of this Contract.

31.3 The Supplier shall support the service with SC security cleared staff with caveat of UK EYES ONLY that are skilled and competent and have undergone additional Buyer's onboarding checks and security briefings before engaging them on design or delivery of services. Suppliers Personnel who are unable to obtain the required security clearances must be prevented from accessing systems, which store, process or are used to manage the Buyer's Data except where agreed with the Buyer in writing.

31.4 The Supplier shall be subject to pre-employment checks that are compliant with ISO/IEC 27001 and ISO/IEC 27002, the Security Policy Framework, and HMG Personnel Security Controls and shall include the verification of, as a minimum: identity, unspent criminal convictions and right to work.

31.5 The Supplier may choose the method of assessment, but it must conform to Good Industry Standards or CPNI ‘Personnel Security Risk Assessment’ available at: https://www.cpni.gov.uk/

31.6 The Supplier shall ensure that Supplier Personnel that have the ability to access Customer Data or systems holding Customer Data shall sign SyOps documents that commit them to standard security related requirements, undergo regular training on secure information management principles and undergo any required Buyer led training. Unless otherwise agreed with the Buyer in writing, this training must be undertaken annually.

31.7 The Supplier shall immediately inform the Buyer if the Supplier's environment is subject to a Cyber Attack during the term of the Contract. The Supplier shall also make the Buyer aware of any cyber attacks it has experienced within the last year, with full details where appropriate of what information was obtained and what was carried out to mitigate the risk.

31.8 The Supplier shall report any non-compliance with the Buyer's security policies and procedures appropriately.

31.9 The Supplier shall support the Buyer's Protective Monitoring Service by sharing information such as threat intelligence, vulnerabilities, and less structured information, such as lessons learned reports, with the Cyber Security Operations Centre for situational awareness and tuning. The Supplier will log all such information by utilising the relevant the Buyer's audit logging and monitoring standards.

31.10 The Supplier shall ensure that any data that they generate is retained legally in compliance with statutory or legal obligations such as the Data Protection Act 1998, so that information assurance standards are understood and adhered to in order to manage risk effectively.

31.11 The Supplier shall comply with the requirements of any codes of connection, multilateral or bilateral international agreements and community or shared services security policies to which the Buyer are signatories (e.g., Government Secure Intranet); so that specific aspects of information assurance are understood and adhered to in order manage risk effectively.

31.12 The Supplier shall ensure that Buyer information, Buyer data and information assets are transmitted in such a way as to ensure that no unauthorised person has access to them and that information assurance standards are understood and adhered to in order manage risk effectively.

31.13 The Supplier shall ensure that there is an efficient system of reporting, recording and investigating breaches of security, which the Buyer security staff can monitor, in accordance with HMG Security Policy Framework, so that the Buyer is informed of the risks and security incidents so that it can respond.

31.14 The Supplier shall ensure that all systems are operated in such a manner to support the Buyer's compliance with HMG Security Policy Framework located at: https://www.gov.uk/government/publications/security-policy-framework.

31.15 The Supplier shall ensure National Cyber Security Centre (NCSC) good practice is followed.

31.16 The Supplier shall support product teams in their work to maintain all systems and information assets to the appropriate accreditation levels, including scheduled regular IT health checks and management of outstanding risks agreed as part of service acceptance.

31.17 The Supplier shall ensure that all reasonable steps are taken to minimise security breaches in the physical, procedural, or technical domains of any asset under the Suppliers control. This shall include encryption of all Buyer data in transit end-to-end, using methods as proposed by the Supplier and agreed with the Buyer.

31.18 The Supplier shall maintain a register of security certificates across all in-scope services in live production environments, including renewals and key updates to the agreed tooling.

31.19 The Supplier shall provide support via technical means from agreed locations aligned to security and policy requirements. The Supplier will safeguard the Buyer data under the UK Data Protection regime and must be able to state the physical locations in which data may be stored, processed, and managed from, and what legal and regulatory frameworks the data will be subject to at all times.

31.20 The Buyer data shall not be subject to offshoring arrangements.

31.21 The Supplier shall gain and maintain the Buyer’s approval to operate for the combination of sites, infrastructure and processes used to deliver the Services.

31.22 The Supplier shall support with agreeing with the Buyer a document setting out security risks relevant to the Services, and the way in which they are addressed, together with an assessment of any remaining risks which may need to be accepted, and clear statements regarding any relevant assumptions and external security dependencies.

31.23 The Supplier shall ensure that Suppliers Personnel shall be granted increased IT privileges or access rights only to the extent necessary to carry out their duties. When Supplier Personnel no longer need elevated privileges, The Supplier shall revoke their access rights within one (1) Working Day.

32 PRODUCT SECURITY REQUIREMENTS

32.1 The Supplier must ensure application development takes place in a secure development environment which controls changes to source code and the release through a pipeline into development/testing/staging environments prior to being released into live production to minimise the risks of unauthorised/untested changes and prevents leaking of production information into the non-productive environments.

32.2 Threat and vulnerability management (TVM) - the Supplier must ensure the system uses up to date and supported versions of products and software, unless agreed with the Buyer, it is regularly screened for new vulnerabilities and configuration errors and security patches from vendors are applied on a regular basis to minimise the risk of known vulnerabilities being exploited. The Supplier must support with the reporting of any critical or high-risk issues to the Buyer at the next SWG

32.3 Network security - the network must provide sufficient network separation between application/system components depending on their information classification and exposure with strong and robust controls (to include firewalls, WAF, proxies, VPN, IDS/IPS, DDOS) regulating the information flows across the network boundaries.

32.4 Anti-malware - the system must be protected against malware infection and any anti-malware software must be automatically updated at least daily to ensure it remains effective.

32.5 Encryption – the system should ensure information is encrypted in transit on both internal and external networks, at rest as appropriated for it classification using strong ciphers, PKI certificates are from trusted sources and private keys are secured and managed.

32.6 Hardening – the Supplier should ensure that operating systems and applications are security hardened in accordance with CIS level 1 benchmarks as a minimum and where appropriate CIS level 2.

32.7 IAM - users and services must be uniquely identifiable and authenticated by a centrally managed identity store with robust role-based access controls for users, developers and administrators following the principals of least privilege and segregation of duties. User access to production applications must be restricted to only Buyer authorised devices from authorised locations. Administrator access to production environments must be restricted to only Buyer authorised devices/locations and be timebound.

32.8 Logging and monitoring - security logging must be enabled to support incident investigations, forensics and provide continuous security monitoring to detect suspicious user, administrator, or erroneous network activities. Logs must be made available to the Buyer Tooling/Platform   ) to provide monitoring of the environment against defined security use cases. Logs data will be identified as part of the secure by design process in collaboration with the MBTP cyber security team.

32.9 Backup / recovery – data must be backed up to allow recovery of information destroyed or corrupted by a malicious user, accidentally or through a system failure to meet the RPO/RTOS for the system.

32.10 Resilience - the system should be resilient to single points of failure.

32.11 Governance - the security and information risks must be actively governed with monthly reporting on security KPI to the Buyer SWG in order to steer and continuously improve the security of the system. At a minimum this should cover risks, security incidents, vulnerabilities and remediation status, security patching, system upgrades and new capabilities. The Supplier will support with providing the relevant information to the Buyer where required.

33 SECURITY PROCESSES

33.1 The Supplier will support the Buyer in managing the CMDB: The Supplier will not directly change the CMDB.

33.2 An onboarding and off-boarding process must exist to ensure only authorised users are provided with access to the system and the access is terminated when the user changes roles or leaves the company. The Supplier will assign resources to provide support services and when necessary they will request production access to the system

33.3 All changes/releases deployed into the pre-production/production environments must be controlled through a robust change management process.

33.4 A process should exist for controlling the regular deployment of patches into the production environments in a timely manner.

33.5 All security incidents must be recorded, tracked through to closure and communicated to stakeholder following a security Incident Management Process. The Supplier will support the Buyer's security incident management where required.

33.6 The system must have a business continuity plan which is periodically tested to ensure the system can be recovered following a major incident, and the Supplier will contribute to the Business Continuity Plan as required.

33.7 Application security incident management - the Supplier will report, manage an actual or suspected breach of information security of the service in line with Buyer HO Digital policy.

35. SECURITY MONITORING

35.1 The Supplier shall contribute to identifying the systems, Configuration Items, or other service components that should be monitored and establishing the Security monitoring strategy.

35.2 The Supplier shall provide logs to the Buyer's SIEM (Security Incident and Event Management) monitoring tools where relevant.

35.3 The Supplier shall support with establishing and maintaining thresholds and other criteria for determining security events, and choosing criteria to define each type of event (informational, warning, or exception).

35.4 The Supplier shall contribute to establishing and maintaining policies for how each type of detected event should be handled to ensure proper management. All high priority alerts must be raised in the mandated tools.

35.5 The Supplier shall support implementing processes required to operationalise the defined thresholds, criteria, and policies.

35.6 Regular checks to ensure the application has not breached or an application not being attacked.

36. SECURITY TOOLING

36.1 The Supplier will support the Buyer in the use of their security tooling, utilising them appropriately throughout the project lifecycle. Tooling includes:

36.2 SIEM Tools: Splunk or any successor to it that the Buyer wishes to use

36.3 Vulnerability scanning includes: Tenable.io, SonarQube, Trivy etc.

36.4 AV: MS Defender or Buyer tools as required

36.5 IAM:- RedHat SSO

37. DESIGN SECURITY

37.1 The Supplier shall work collaboratively with the MBTP cyber security architects to ensure any design is secure and aligns to secure by design principles.

38. PAYMENT AND INVOICING

38.2 Invoices should only be raised for works delivered and approved by the Buyer as per the statement of work approval process.

38.3 Payment will only be processed on receipt of a valid invoice containing the relevant purchase orders details.

38.4 Payment can only be made following satisfactory delivery of pre-agreed certified products and deliverables.

38.5 Before payment can be considered, each invoice must include a detailed elemental breakdown of work completed and the associated costs., in line with the milestone payment plan

38.6 Invoices should be submitted to: [redacted]

39. CONTRACT MANAGEMENT

39.1 The Supplier will be required to attend regular contract management meetings (monthly) where the following areas will be discussed; (Please note this list is not exhaustive)

39.1.1 Review and agreement of works to be completed under a statement of works

39.1.2 Supplier performance/KPI review

39.1.3 Review of delivery against key milestones and agreed deliverables

39.1.4 Risks, Issues and Dependencies

39.2 Attendance at Contract Review meetings shall be at the Supplier's own expense.

40. LOCATION

40.1 The Services will be carried out remotely with occasional travel required to Home Office locations within the UK. This includes, but is not limited to;

40.1.1 Face to face planning sessions

40.1.2 Buyer HO Digital events

40.1.3 Collaborative working sessions with Buyer HO Digital, incumbent supplier, suppliers within the CtB ecosystem, Buyer stakeholders and any other stakeholders as deemed appropriate by the Buyer.

40.1.4 The Supplier will be responsible for all costs for travel which is required to enable the successful delivery of the Services, including out of hours requests.

Attachment 2 – Charges and Invoicing

Part A – Milestone Payments and Delay Payments

This table will be completed using the payment profile in our milestone payment plan. M1 revised as per customer requirements for this period for application support.

#	Milestone Description	Milestone Payment amount (£GBP)	Milestone Date	Delay Payments (where Milestone) (£GBP per day)
M1	Discovery and Mobilisation	[redacted]	[redacted]	[redacted]
M2	Year 1 BAU Service Delivery (01/04/2026 – 30/09/2026)	[redacted]	[redacted]	[redacted]
M3	Year 2 Delivery (01/10/2026 – 31/03/2027). Milestones to be agreed in line with PI planning and Payment in line with contract value will be agreed by the end of milestone M2.			
M4	Year 2 Delivery (01/04/2027 – 30/09/2027). Milestones to be agreed in line with PI planning and Payment in line with contract value will be agreed by the end of milestone M3.			
M5	Year 3 Delivery (01/10/2027 – 31/03/2028). Milestones to be agreed in line with PI planning and Payment in line with contract value will be agreed by the end of milestone M4.			
M6	Year 3 Delivery (01/04/2028 – 30/09/2028). Milestones to be agreed in line with PI planning and Payment in line with contract value will be agreed by the end of milestone M5.			
M7	Year 4 Delivery (01/10/2028 – 31/03/2029). Milestones to be agreed in line with PI planning and Payment in line with contract value will be agreed by the end of milestone M6.			
M8	Year 4 Delivery (01/04/2029 – 30/09/2029). Milestones to be agreed in line with PI planning and Payment in line with contract value will be agreed by the end of milestone M7.			
M9	Year 5 Delivery (01/10/2029 – 31/03/2030). Milestones to be agreed in line with PI planning and Payment in line with contract value will be agreed by the end of milestone M8.			
M10	Year 5 Delivery (01/04/2030 – 30/11/2030). Milestones to be agreed in line with PI planning and Payment in line with contract value will be agreed by the end of milestone M9.			

Part B – Service Charges

Service charges are not applicable for Discovery and Mobilisation Period. Service charges for the contract term from 01/04/2026 – 30/09/30 will be agreed during the Discovery and Mobilisation Period.

Charge Number	Service Charges

Part C – Early Termination Fee(s)

Early termination fees will be calculated as 6 x the Supplier's agreed monthly run rate. The Supplier's monthly run rate will be agreed ahead of each contract year.

Attachment 3 – Outline Implementation Plan

Outline%20Implementation%20Plan%20-

Attachment 4 – Service Levels and Service Credits

Service levels and service credits will be agreed during the Discovery and Mobilisation Period.

Service Levels and Service Credits

Service Levels				Service Credit for each Service Period
Service Level Performance Criterion	Key Indicator	Service Level Performance Measure	Service Level Threshold	

Service Credit Cap

The Service Credit Cap shall be agreed by the end of the Discovery and Mobilisation Period.

Critical Service Level Failure

Critical metrics will be agreed by the end of the Discovery and Mobilisation Period.

Attachment 5 – Key Supplier Personnel and Key Sub-Contractors

.1.1 The Parties agree that they will update this Attachment 5 periodically to record any changes to Key Supplier Personnel and/or any Key Sub-Contractors appointed by the Supplier after the Commencement Date for the purposes of the delivery of the Services.

Part A – Key Supplier Personnel

Key Supplier Personnel	Key Role(s)	Duration
[redacted]	Delivery Manager	Full contract term
[redacted]	Transition Manager	1 Year
[redacted]	Commercial Manager	Full contract term

Part B – Key Sub-Contractors

Key Sub-contractor name and address (if not the same as the registered office)	Registered office and company number	Related product/Service description	Key Sub-contract price expressed as a percentage of total projected Charges over the Contract Period	Key role in delivery of the Services
CACI	[redacted]	Border Crossing (BX)	30%	Delivery and Support of Border Crossing (BX)

Attachment 6 – Software – Not Applicable

Attachment 7 – Financial Distress

For the purpose of Schedule 7 (Financial Distress) of the Call-Off Terms, the following shall apply:

PART A – CREDIT RATING THRESHOLD

Entity	Credit Rating (long term)	Credit Rating Threshold
BAE Systems Applied Intelligence	[redacted]	[redacted]
	[redacted]	[redacted]
CACI	[redacted]	[redacted]
	[redacted]	[redacted]

PART B – RATING AGENCIES

- Dun and Bradstreet

100-86	Minimal Risk
85-51	Lower than average risk
50-11	Greater than average risk
10-0	High Risk

- Company Watch

100-36	Low risk
35-26	Greater than average risk
25-0	High risk

Attachment 8 – Governance

PART A – SHORT FORM GOVERNANCE – Not Used

PART B – LONG FORM GOVERNANCE

Long form governance will be agreed once the Discovery and Mobilisation Period has concluded. Annual check points will be undertaken throughout the contract lifecycle where the long form governance for the following year will be agreed. During the course of Discovery and Mobilisation the Parties will operate at a minimum of two governance boards:

Attachment 9 – Schedule of Processing, Personal Data and Data Subjects

This Attachment 9 shall be completed by the Controller, who may take account of the view of the Processors, however the final decision as to the content of this Schedule shall be with the Buyer at its absolute discretion.

1.1.1.1 The contact details of the Buyer's Data Protection Officer is [redacted]

1.1.1.2 The contact details of the Supplier's Data Protection Officer is [redacted]

1.1.1.3 The Processor shall comply with any further written instructions with respect to processing by the Controller.

1.1.1.4 Any such further instructions shall be incorporated into this Attachment 9.

Description	Details
Identity of Controller for each Category of Personal Data	**The Buyer is Controller and the Supplier is Processor** The Parties acknowledge that in accordance with Clause 34.2 to 34.15 and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of the Personal Data set out in this table. No such Personal Data will be held on Supplier Devices or Supplier Networks. Access to Personal Data is not guaranteed and only arises if support scenarios present themselves. In this case, access to Personal Data is incidental.
Duration of the processing	For the full duration of the contract.
Nature and purposes of the processing	The Home Office processes personal information to provide for the administration and effective handling of the actions required, these include, but is not limited to: immigration including visa applications, nationality including citizenship applications and border functions (both in to and out of the UK, Customs Duties, policing databases to assist in the detection, investigation and prevention of crime; data that is held and processed for policing and judicial purposes-in order to provide investigative policing which includes detection of crime, apprehension and prosecution of offenders and the maintenance of law and order; the protection of the UK and UK citizens from terrorism; personal information that is held and processed in order to support criminal and coronial proceedings relating to major historic enquiries; personal information that is processed with regard to the prevention and detection of fraud; personal information used to verify an identity; the undertaking of statistical and analytical analysis, and the fulfilment of legal requirements and responsibilities. The processing is not consent based due to the nature of the data held and the purposes for processing. Specifically, the nature and processing for the Supplier is in order design, build and validate a functional solution, and provide on-going support and maintenance including patching and upgrades.

	N.B. For further detailed description of the overarching Controllers processing purposes, then refer to the DSAB DPIA documents which can be request from the DPO.
Type of Personal Data	[redacted]
Categories of Data Subject	Members of the public
Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	Not applicable as the Personal Data is not held or transferred to Supplier network or devices.

Attachment 10 – Transparency Reports

During the Discovery and Mobilisation Period a weekly status report will be delivered in PowerPoint format to an agreed list of Buyer stakeholders. Transparency Reports for the Implementation Period will be agreed once the Discovery and Mobilisation Period has concluded.

Annex 1 – Call Off Terms and Additional/Alternative Schedules and Clauses

RM6100-Lots-2-3-and-5-Call-Off-Terms-v3 011025.docx

RM6100-Lots-2-3-and-5-Additional-and-Alternative-Terms-and-Conditions-v2.00 .odt