Schedule 2.1 – Statement of Requirements

Department for Work & Pensions

STATEMENT OF REQUIREMENTS

[REDACTED]

CONTENTS

1. DEFINITIONS

2. INTRODUCTION

3. VALUES & BEHAVIOURS

4. IMPLEMENTATION

5. TRANSFORMATION

6. OPERATION

7. GENERAL MANAGEMENT

LIST OF SERVICE ELEMENTS

8. HEALTH AND SAFETY & RISK MANAGEMENT

9. BUSINESS CONTINUITY AND DISASTER RECOVERY

10. SECURITY THREAT AND RISK ASSESSMENT & SECURITY PLAN

11. WORK ORDER MANAGEMENT

12. CONTROL AND MONITORING FACILITY

13. SECURITY SYSTEMS

a) CCTV SYSTEM

b) AUTOMATED ACCESS CONTROL SYSTEM (AACS)

c) FIRE DETECTION SYSTEMS

d) INTRUDER DETECTION SYSTEMS AND PANIC ALARM BUTTONS

e) LONE WORKER SOLUTION

f) SECURITY SYSTEM NETWORK

g) BODY WORN CAMERAS (Additional Operational Services)

14. TRIALLING

15. TESTING, COMMISSIONING AND HANDOVER REGIME

16. SUPPORT AND MAINTENANCE REQUIREMENTS

17. SECURITY OFFICERS

18. VISITOR MANAGEMENT

19. INCIDENT MANAGEMENT

20. KEY MANAGEMENT

21. CAR PARK MANAGEMENT

22. ADDITIONAL SECURITY PROVISION

23. REPORTING REQUIREMENTS

24. SECURITY PROJECTS & CAPITAL PROGRAMME

25. SUSTAINABILITY

26. RESPONSE TO HEIGHTENED THREAT

27. UNACCEPTABLE CUSTOMER BEHAVIOUR (Incl. Database additional requirement)

28. CONTRACT IMPROVEMENT AND DEVELOPMENT

29. EXIT

ANNEX A – List of Solutions Required

1 DEFINITIONS

1.1. In this Schedule, defined terms shall have the definitions prescribed to them in Schedule 1 and as follows:

Additional Operational Services	the Services described as such in this Schedule 2.1 (Statement of Requirements) which are to be provided by the Supplier if instructed by the Authority in accordance with Clause 5.11 of the Agreement (Additional Operational Services);
Alarm Receiving Centre or **ARC**	EN 50136-1:2012 clause 4.1.2: Continuously manned centre to which information concerning the status of one or more alarm systems are reported;
Appropriate Vehicles	vehicles provided by the Supplier to undertake the duties identified under the Service Elements;
Area Relief Officer	existing Security Officer role as specified in the Transferring Former Supplier Employee Notional Data;
Asset Verification and Condition Survey	survey exercise, completed by the Supplier as early as reasonably possible following the Approval of the Existing Systems Detailed Solution in line with the Approved Existing Systems Detailed Solution;
Asset Verification and Condition Survey Report	the report created as part of the Asset Verification and Condition Survey as further described in Paragraphs 16.8 and 16.9 of this Schedule 2.1;
Assignment Instructions	BS 7499:2013. Operational document detailing specific contractual duties to be executed by each member of the Supplier Personnel that details roles, responsibilities and duties;
Authorised Persons	persons authorised either by the Authority or other persons so authorised to be working on the Affected Property;
Authorised Vehicles	vehicles authorised to enter the Affected Property having first obtained approval to do so as per the process approved by the Authority within the Car Park Management Detailed Solution defined in Annex A to this Schedule 2.1 (Statement of Requirements);
Authority Core Business	the business of dealing with members of the public, claimants and potential claimants to administer the work and pensions policies of the UK Government;
Authority Customer	members of the public who may access the Authority's services or receive benefits;
Authority Personnel Escort	escort to be provided by appropriately trained Security Officers to accompany Authority Personnel whilst performing their duties such as an off-site visit with Authority Customers as requested by the Authority or

	determined as required following a [REDACTED] determining temporary additional security provision commensurate to the risk profile;
Authority Personnel	all directors, officers, employees, agents, consultants and contractors of the Authority;
Authority Network	has the meaning given in Paragraph 13.64 of this Schedule 2.1;
Authority Opening Hours	the opening hours for each Affected Property which shall be determined by the Authority, subject to change from time to time and defined within each Affected Property's Security Plan;
Authority Visitors	those individuals visiting the Affected Property as agreed by an authorised member of Authority Personnel. This shall not include Authority Customers;
Car Parks	those secure areas within the Affected Property utilised for parking Authorised Vehicles in line with the Approved Car Park Management Detailed Solution;
CCTV	closed circuit television system used around the Perimeter of Affected Properties, within Public Waiting Areas and at vulnerable/key points;
Control and Monitoring Facility	a central control facility to provide the monitoring, management and communication required to deliver the requirements of this Schedule 2.1 (Statement of Requirements) which shall include but not be limited to an Alarm Receiving Centre and Remote Video Response Centre;
Customer Care Officer	existing Security Officer role as specified in the Transferring Former Supplier Employee Notional Data;
Customer Support Officer	existing Security Officer role as specified in the Transferring Former Supplier Employee Notional Data;
Emergency	a state of heightened security or business risk as a result of an Incident or the notification or alert generated by the Supplier System;
Emergency Services	Police, Fire Brigade or Ambulance Services;
Energy Management Solution	Authority Policy created and managed by the Supply Chain Integrator and provided to the Supplier;
Enrolment	the procedures to be executed by the Supplier relating to the creation, addition and amendment of data utilised by the Replacement Automated Access Control System;
Excluded Existing Systems Parts Register	has the meaning given in Schedule 2.2 (Performance Levels);

Existing Systems	has the meaning given in Schedule 1 (Definitions);
Existing Systems Obsolescence/Unavailability Report	the report completed by the Supplier during the Implementation Phase as part of the Asset Condition and Verification Survey in accordance with Paragraph 16.10 of this Schedule 2.1 (Statement of Requirements);
External Patrol	appropriate Supplier Personnel undertaking a patrol by foot or vehicle of the Perimeter of an Affected Property as determined within the Affected Property's Security Plan;
Factory Acceptance Testing or **FAT**	the test which shall be conducted by the Supplier to determine and document that the relevant equipment, hardware and software operates according to its specification, covering the following key areas: (a) functional; (b) fault management; (c) communications; (d) interface requirements;
Financial Transparency Objectives	has the meaning given it in Schedule 7.5 (Financial Reports and Audit Rights) of the Agreement;
First Aid	response by appropriately trained Supplier Personnel to provide help to a sick or injured person until full medical treatment is available (e.g. attendance by the Emergency Services);
Government Response Level	additional and sustainable protective security measures reflecting the broad nature of the threat combined with specific business and geographical vulnerabilities and judgements on acceptable risk;
HMG Baseline Personnel Security Standard	those security standards as set out in HMG Baseline Personnel Security Standard, (Version 5.0 dated 30/10/2014 including any subsequent updates / amendments to this version). For the avoidance of doubt, this Standard requires the Supplier to check and verify details relating to Supplier Personnel such as: a) Identity; b) Employment history (for a minimum of past 3 years); c) Nationality and immigration status; and d) Criminal record (unspent convictions only), except that in relation to any sexual offences or other offences with a safeguarding element or indicating risk to persons with vulnerabilities or at risk. Spent convictions and relevant offender lists may also be considered;
HR Database	the Authority's existing human resources database, the Single Operating Platform (SOP) which is owned and managed by Shared Services Connected Ltd (SSCL);

	SOP is an oracle based system which supports many Government Departments providing: a) HR; b) Finance (organisation wide); c) Purchase to Pay; d) Payroll; and e) Expenses; SOP includes a comprehensive set of details on Authority Personnel that the Authority may permit the Supplier access to at its absolute discretion and subject to completing all required security checks, clearances and fully satisfying all security technical requirements;
Incident	activity that includes but is not limited to BS 7958:2015 any activity that raises cause for concern that an offence has been, is being or is about to be committed, or that an occurrence has taken place warranting specific action by the Supplier;
Information Security Policy	BS ISO/IEC 27001:2013 Information Security Management Part 2, Specification for Information Security Management Systems, or the equivalent Authority publication when available;
Internal Patrol	appropriate Supplier Personnel undertaking a patrol by foot of the internal demise of an Affected Property as determined within the Affected Property's Security Plan;
Mobile Patrol	BS 7499:2013 Assignment whereby a Security Officer performs various duties but is not solely assigned to one location or premises;
Network Diagnostic Test	test performed by the Supplier in accordance with the Approved Existing Security Systems Support and Maintenance Detailed Solution or Replacement Security Systems Support and Maintenance Detailed Solution (as applicable) to assess the performance and availability of the Authority Network and/or Supplier Network (as applicable).
Nominated Authority Contacts	those named member of Authority Personnel who are authorised to act on behalf of the Authority as notified to the Supplier from time to time;
Operational Readiness Completion Date	has the meaning given in Schedule 1 (Definitions) of the Agreement;
Other Government Departmental Colleagues or **OGD Colleagues**	the personnel of other Governmental departments who may occupy or use the Affected Property;
Panic Alarms	all devices, including desk mounted, screen mounted, personal (portable) devices and pendant alarms utilised by Authority Personnel to raise alarm in the event of an Incident or Emergency;

Perimeter	the external boundary of each Affected Property;
Permit to Work System	the system provided and operated by the Supply Chain Integrator for the control and management of access to and right to work on the Affected Properties for all Supplier Personnel in the delivery of the Services and Authority Supply Chain Member personnel in the delivery of the Authority Supply Chain Services;
Plan (and any term suffixed by **Plan** or **plan**)	those plans listed throughout Schedule 2.1 (Statement of Requirements) as specifically used in Annex A;
Principle Contractor	the Principle Contractor role and all associated responsibilities as defined in the Construction (Design and Management) Regulations 2015;
Principle Designer	the Principle Designer role and all associated responsibilities as defined in the Construction (Design and Management) Regulations 2015;
Private Mobile Radio or **PMR**	a radio system including hand portable, vehicle and desk mounted equipment which enables radio communications. The protocols used must be industry standard allowing use of terminal equipment from a number of equipment manufacturers. This shall include either traditional PMR systems or emerging smartphone based systems as proposed by the Supplier;
Process (and any term suffixed by **Process** or **process**)	those processes required to satisfactorily perform the Services listed throughout Schedule 2.1 (Statement of Requirements);
Project	works including all construction, refurbishment activities and work involving replacement of assets or increasing the permanent value of the asset and/or extends its life beyond the originally anticipated life-cycle;
Public Waiting Areas	the areas within Affected Property's that are open to the public (specifically Authority Customers), from which the Authority delivers the Authority Core Business;
Remote Video Response Centre or **RVRC**	BS 8418:2015 clause 3.1.30: Continually manned remote centre capable of receiving multiple concurrent CCTV images from remote locations for the purpose of interacting with supervised premises to provide security and related services;
Replacement Automated Access Control System or **Replacement AACS**	the electronic system and associated equipment utilised to centrally control access and egress to the Affected Property and which forms part of the Replacement Security System;
Report (and any term prefixed or suffixed by **Report** or **report**)	those reports required by the Authority listed throughout Schedule 2.1 (Statement of Requirements);
Response	response to alarms by a combination of appropriately trained Supplier Personnel and the Supplier System,

	which for physical on-site attendance, shall include an Internal Patrol and External Patrol of the Affected Property;
Response Protocol	has the meaning given in Paragraph 17.7 of this Schedule 2.1;
Security Incident Classification	the agreed classification to be applied to categorisation of all Incidents. For the avoidance of doubt, the Security Incident Classification is to be developed by the Supplier and submitted to the Authority for approval within the Incident Management Detailed Solution defined in Annex A to this Schedule 2.1 (Statement of Requirements);
Serious Incident Review Group	the escalation group for the review of all Serious Incidents with representatives from the Authority, Supply Chain Integrator, Supplier, trade unions and other Authority Supply Chain Members;
Security Officer Team Leader	those Security Officers responsible for the management and leadership of Security Officer teams;
Security System Network	the network infrastructure (including WAN and LAN) used by the Supplier to provide the Services, which may be the Authority Network and/or Supplier Network (as applicable);
Security Systems	those electronic and physical systems installed, maintained and operated on the Affected Property as detailed in Paragraph 13: Security Systems of this Schedule 2.1 (Statement of Requirements);
SIA	Security Industry Authority or any regulating authority which may replace it;
Site Acceptance Testing	the second phase of the testing process during which the Authority and system End Users will test the system to determine and document that the equipment hardware and software operates according to the specification, covering the following key areas: (a) functional; (b) fault management; (c) communications; (d) support systems; and (e) interface requirements. The procedure shall be developed by the Supplier for Approval including pass/fail criteria;
Supplier Network	has the meaning given in Paragraph 13.65 of this Schedule 2.1;
Supply Chain Integrator System	the system to be provided by the Supply Chain Integrator for the use of all Authority Supply Chain Members to be

	used in the receipt, tracking and management of all Work Orders and the production of Reports as required by the Authority;
Target Fix Times	has the meaning given it in Schedule 2.2 (Performance Levels) of the Agreement;
Training	all role-specific and SIA licence training (including but not limited to training for new SIA licences, or SIA licences in addition to those SIA licences already held) provided by the Supplier to the Supplier Personnel;
User Acceptance Testing	the last phase of the testing process during which the Authority and system End Users will test the system to make sure it can handle required tasks in real-world scenarios to ensure full operational capability. For the avoidance of doubt, the User Acceptance Testing process and methodology shall be proposed by the Supplier and approved by the Authority;
Visitor Escort	escort to be provided by appropriately trained Security Officers for a visitor to an Affected Property, as requested by the Authority;
Westminster Government Secure Zone	the defined geographical secure zone within Westminster, Central London that is subject to additional security requirements as specified by the relevant Government Bodies to include but not limited to: Metropolitan Police, Government security services and GCHQ; and
Work Order	means a formal notification of activity required as issued by the Supply Chain Integrator via the System to the Authority Supply Chain Members. This shall include reactive work required from time to time and also all planned work (including statutory work and testing) scheduled to be undertaken throughout the Term.

2 INTRODUCTION

2.1 The Authority requires the Supplier, using the standard of care required by the Agreement, to carry out all activities, operations and functions expressly stated in or reasonably to be inferred as required by this Schedule 2.1 (Statement of Requirements) in order to deliver the comprehensive security Services.

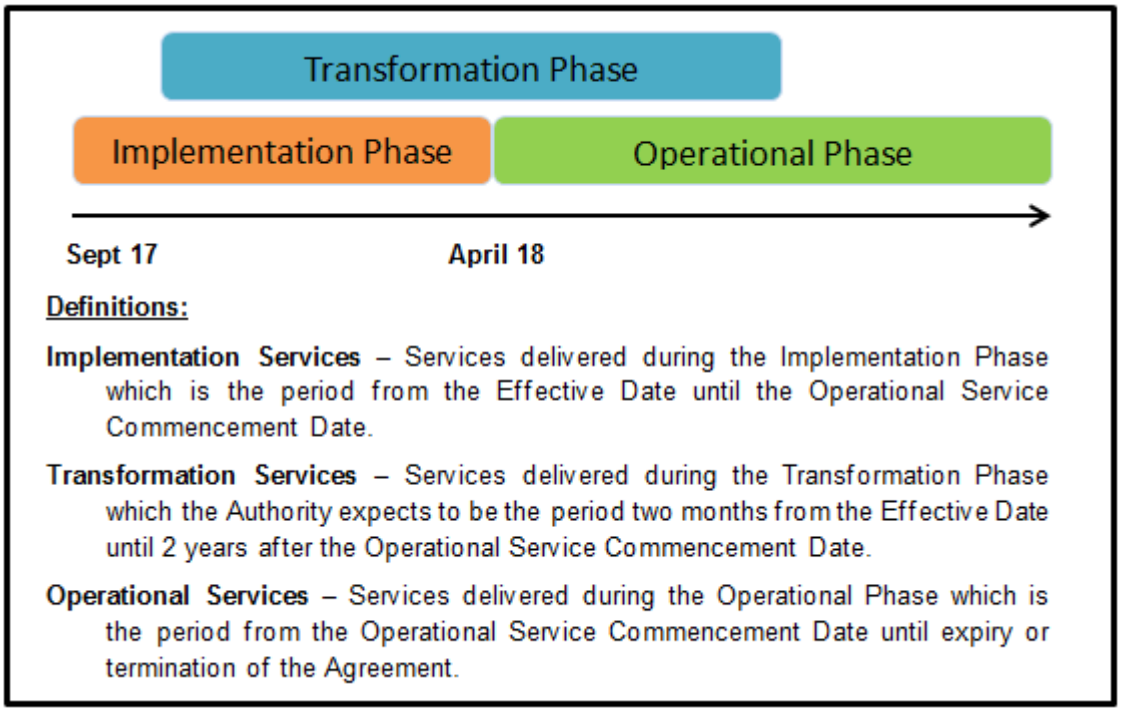
2.2 The Services include the Implementation Services, Transformation Services and Operational Services:

a) the Implementation Services are services rendered during the Implementation Phase;
b) Transformation Services are services rendered during the Transformation Phase; and

c) Operational Services are services rendered from the Operational Service Commencement Date to the expiry of the Term in accordance with the Detailed Solutions developed by the Supplier.

2.3 The Services shall be rendered during the appropriate phase and anticipated timeline as detailed with Fig. 1; see below.

2.4 Fig. 1: Phase Diagram and Anticipated Timeline



2.5 The Services consist of all the individual Service Elements as listed in Paragraph 8 (Health and Safety & Risk Management) through to Paragraph 29 (Exit) (inclusive) and defined within this Statement of Requirements.

2.6 The Authority requires the Supplier to deliver the Services to satisfy the following strategic objectives:

a) Deliver effective security services, reducing the frequency and seriousness of incidents effecting all occupiers and users of the Affected Property;
b) Deliver more efficient security services, significantly reducing unit costs per full time employee through alignment with site specific risk profiles across the Affected Properties making the optimal use of the Supplier System and Security Officers;
c) Provide expert assessment of security risk fully compliant with recognised industry standards for the delivery of Security Threat and Risk Assessments across the Affected Property;
d) To align security services with changes in the Authority Estate, through re-assessment in order to satisfactorily deal with new threats and other emerging vulnerabilities and exploit new and emerging technologies / capabilities;
e) To enable the delivery of the declared transformational objectives (as set out in Paragraph 5.2) and continue to deliver value for money throughout the Term of the Agreement;

f) To enable a smooth transition and successful exit from the PRIME Contract and a managed transition to the target operating model; and

g) By working closely with Authority Personnel, ensure customer service as measured by the Satisfaction Surveys, performance monitoring and people engagement is protected throughout the Term of the Agreement.

2.7 In addition to delivery of this Statement of Requirements, to ensure the Authority's objectives are met, the Authority requires the following outputs:

a) Developing a Security Threat and Risk Assessment methodology and Security Plan processes for approval by the Authority;

b) Completion of site specific Security Threat and Risk Assessments and Security Plans;

c) Management of a professional Security Officer workforce deployed flexibly across the Affected Properties;

d) Management of Incidents and Emergencies as they occur across the Affected Properties;

e) Provision and maintenance of a comprehensive range of Security Systems;

f) Provision of a Supplier System capable of integrating and/or interfacing with other related systems including but not limited to those of the Authority and Authority Supply Chain Members, where required;

g) Delivery of the Services as required to support changes to the Authority's business operations including but not limited to extended operating hours and digital transformation;

h) Management of Work Orders associated with the Affected Properties utilising the Supply Chain Integrator System or an alternative system that has the required functionality and capability to interface effectively with the Supply Chain Integrator System (including, but not limited to, the Supply Chain Integrator's Work Order management system and reporting on the progress of completion of services required from such Works Orders;

i) Support to enable a potential future state in which the Government Property Unit (**GPU**) or other Government entities may provide some or all estate services across the entire Government estate;

j) Compliance with all statutory, regulatory and any relevant policies, processes and standards; and

k) Royalty free use by the Authority of all systems, design, processes and ways of working, procedures and service models created and undertaken by the Supplier in performing the Services.

SUPPLY CHAIN INTEGRATOR'S ROLE

2.8 The Supply Chain Integrator will act as the Authority's programme manager, project manager and contract administrator in relation to the Agreement. It is intended that the Supply Chain Integrator will act as the Authority Representative and, where applicable, may act as the Authority's agent under the Agreement.

2.9 The Supply Chain Integrator will monitor and manage the Authority Supply Chain Members to ensure:

a) compliance by Authority Supply Chain Members of their respective contractual obligations under the relevant Authority Supply Chain Contracts; and

b) that the relevant programmes and project plans to be delivered by the Authority Supply Chain Members are being adhered to in terms of cost and time and the integration of design, construction, commissioning, procurement, scheduling and cost management across the whole of the Authority's supply chain.

3 VALUES & BEHAVIOURS

3.1 The Supplier shall operate on behalf of the Authority and as such uphold, promote and live the Authority's following values:

a) **Achieving the Best** - using all our resources efficiently so that high and consistent standards of service are provided;
b) **Respecting People** - by treating the Authority Customers, the Authority Personnel and Authority Supply Chain Members with respect, welcoming diversity and valuing other's ideas and responding fairly to individual needs;
c) **Making a Difference** - by providing the Services so that Authority Personnel can support, challenge and inspire the Authority's Customers to improve their lives and help each other to make a difference; and
d) **Looking Outwards** - by working with others and learning how to get better at what we do.

3.2 In addition, the Supplier shall interact with the Authority, Authority Personnel, other Government departments and Other Government Departmental Colleagues, the Authority Supply Chain Members, Authority Customers and the general public ensuring behaviours are in line with the Authority's following values:

a) The health and safety of individuals is the Authority's primary concern. The Supplier shall deliver the Services and utilise best endeavours to collaborate with each Authority Supply Chain Member in the delivery of the Authority Supply Chain Services, including complying with the highest possible level of health and safety and the Authority's policies, processes and ways of working with regards to health and safety;
b) Ethical and transparent business dealings, ensuring Supplier Personnel uphold the highest possible level of integrity and probity. The Authority's supply chain will operate on an Open-Book basis;
c) A full recognition that a successful supply chain will require high levels of cooperation between the Authority, Supply Chain Integrator, Supplier and Authority Supply Chain Members;
d) Protecting and upholding the brand values and reputation of the Authority and ensuring that this is not in any way damaged, compromised or bought into question; and
e) Shall not use the Authority's brand and the relationship as a supplier to the Authority for any advertising and or promotional purposes without the prior written permission from the Authority.

3.3 The Supplier shall also comply and actively support Authority policy, Authority strategy and relevant legislation regarding non-discriminatory employment and health and wellbeing policy. These include 'disability confident' and 'health and wellbeing' initiatives as well as other such current and future Authority Policies (see schedule 2.6 (Authority Policies) and the Agreement.

4 IMPLEMENTATION

IMPLEMENTATION SERVICES

4.1 Implementation Services shall be delivered during the Implementation Phase which is the period from Effective Date until the Operational Service Commencement Date. Implementation Services are described as such in Schedule 2.1 (Statement of Requirements) within each relevant Service Element.

4.2 The Affected Properties are currently serviced via the PRIME Contract, which is a 20 year, Private Finance Initiative (PFI), Expanded Private Resource Initiative for Management of the Estate (PRIME) agreement and which provides the Authority with a fully serviced estate including comprehensive security services.

4.3 The Authority requires the Supplier's full support, resources and expertise in the exiting of the PRIME Contract, which is a complex and long-standing arrangement and in the subsequent implementation of the Services. The Services to be provided are business critical to the Authority and, as such, the Authority requires a seamless, controlled and planned implementation of the Services.

4.4 By the time stated in Annex A, the Supplier shall provide for Approval a draft overall "Implementation Plan Detailed Solution" in line with Good Industry Practice, detailing how the Supplier will execute and control an implementation exercise of this size and scale, at all times minimising the impact of the implementation on Authority Core Business, Authority Personnel and Authority Customers. An indicative list of items to be included in this overall Implementation Plan Detailed Solution is included in Annex A.

4.5 Upon instruction by the Authority, the Supplier shall execute, utilising Supplier Personnel, the approved overall "Implementation Plan Detailed Solution" in line with the values and behaviours referred to in Paragraph 3.

5 TRANSFORMATION

TRANSFORMATION SERVICES

5.1 Transformation Services shall be delivered during the Transformation Phase in accordance with the timeframes specified in this Agreement or as otherwise instructed by the Authority. Transformation Services are described as such in Schedule 2.1 (Statement of Requirements) within each relevant Service Element.

5.2 In addition to the delivery of the Operational Services, the Authority intends to undertake a significant transformation in the delivery of security services to meet the following transformation objectives:

a) Introduce industry best practice, technology and innovation to improve the current service delivered whilst maximising value for money;
b) To better utilise the Supplier System to reduce the Authority's requirement for Security Officer hours without negatively impacting the security and health and safety of Authority Personnel and Authority Customers;
c) Redesign and significantly improve the quality of Security Threat and Risk Assessments and site specific Security Plans across the Affected Properties;
d) Better protect Authority Personnel, Authority Customers and the Affected Properties by implementing the recommendations of the Security Plans;

e) To transition from Existing Systems some of which are “closed protocol” or proprietary to commercially available off the shelf Security Systems in order to increase flexibility and improve consistency in technology across the Affected Properties;
f) To support and assist the re-distribution of certain delivery tasks including facilities management and receptionist duties within the Authority Supply Chain Members, for improved service delivery; and
g) To deliver significant savings to the Authority throughout the Term of the Agreement.

5.3 The Authority expects Transformation to take place in a phased manner, which shall involve the installation of Replacement Security Systems. The Authority does not guarantee that installation of Replacement Security Systems will take place across all the Affected Properties concurrently or that Transformation will take place at all Affected Properties during the Term.

5.4 The Authority requires that Trial Success is achieved in respect of Trials as described in Paragraph 14 of this Statement of Requirements prior to Transformation being undertaken.

6 OPERATION

OPERATIONAL SERVICES

6.1 Operational Services shall be delivered throughout the Operational Phase. Operational Services are described as such in Schedule 2.1 (Statement of Requirements) within each relevant Service Element.

7 GENERAL MANAGEMENT

ACCOUNT MANAGEMENT

ACCOUNT MANAGEMENT TEAM

7.1 The Authority requires a dedicated account management team that consistently performs to the highest standards of management to support the achievement of the Authority’s strategic and transformation objectives. The Account Management Personnel shall have the skills and capability to liaise with and work alongside the Supply Chain Integrator with minimal day to day involvement by the Authority. The Supplier will provide the Services in a proactive manner identifying and implementing current legislation and industry best practices.

7.2 The Supplier shall:

ACCOUNT MANAGEMENT IMPLEMENTATION SERVICES

7.3 by the time stated in Annex A, provide for Approval a draft “Account Management Detailed Solution” in accordance with Good Industry Practice, detailing who will be accountable for the delivery of the Service Elements contained within this Statement of Requirements and specifically the performance management of the Security Officer workforce. An indicative list of items to be included in this Account Management Detailed Solution is included in Annex A;

7.4 upon instruction by the Authority, execute, utilising Supplier Personnel, the approved “Account Management Detailed Solution” in line with the values and behaviours referred to in Paragraph 3;

ACCOUNT MANAGEMENT OPERATIONAL SERVICES

7.5 ensure that all Supplier Personnel have the appropriate communications devices which will enable them to effectively carry out their duties. In support of this, all contact details including telephone numbers and email addresses for the Account Management Team as detailed within the approved Account Management Detailed Solution and all Security Officer Team Leaders shall be provided to the Authority and maintained by the Supplier;

7.6 provide the Authority with advice and data on all aspects of the Services to control business risk, especially where this may have an impact on the use and operation of the Affected Properties by the Authority. Attend meetings acting as the Authority's advisor on Security matters. These meetings may include (but are not limited to), local, business, departmental, operational and corporate centre safety committees, the Serious Incident Review Group and the authority risk management group, details of which will be provided by the Authority; and

7.7 work collaboratively with the Authority, Supply Chain Integrator and Authority Supply Chain Members to integrate the delivery of Services with other Authority Supply Chain Members to maximise operational efficiencies, ensure value for money for the Authority and taking into account the Authority's Financial Transparency Objectives.

HELPDESK

7.8 The Authority requires that the Supplier provides a helpdesk function for the management of all Work Orders and to liaise with the Supply Chain Integrator in the management of the Services.

7.9 The Supplier shall:

HELPDESK IMPLEMENTATION SERVICES

7.10 during the Implementation Phase, work with the Supply Chain Integrator to develop, agree and implement a helpdesk function including all associated systems functionality;

HELPDESK OPERATIONAL SERVICES

7.11 provide a 24/7 helpdesk function available by phone and email;

7.12 utilise the Supply Chain Integrator System or an alternative system that has the required functionality and capability to interface effectively with the Supply Chain Integrator System, for the provision of the helpdesk (including, but not limited to, the Supply Chain Integrator's Work Order management and computer-aided facility management (CAFM) systems;

7.13 manage and administer all Car Park pass requests; and

7.14 manage and administer all AACS pass requests.

SUPPLIER PERSONNEL

7.15 The Authority requires that the Supplier provides highly competent and professional Supplier Personnel to enable the delivery of the Services and the achievement of the Authority's strategic objectives and transformation objectives. The Supplier shall be a member of the SIA Approved Contractor Scheme.

7.16 The Supplier shall:

SUPPLIER PERSONNEL IMPLEMENTATION SERVICES

7.17 by the time stated in Annex A, the Supplier shall provide for Approval a draft “Human Resources Detailed Solution” in line with Good Industry Practice, detailing how the Supplier shall manage, motivate and retain a professional workforce. An indicative list of items to be included in this Human Resources Detailed Solution is included in Annex A;

SUPPLIER PERSONNEL OPERATIONAL SERVICES

7.18 upon instruction by the Authority, execute, utilising Supplier Personnel, the approved “Human Resources Detailed Solution” throughout the Term in line with the values and behaviours referred to in Paragraph 3;

7.19 provide all Supplier Personnel required to deliver the Services at all times and shall ensure that all Supplier Personnel are suitably competent and experienced to deliver the Services. At all times the Authority shall determine suitability and have the right to instruct the Supplier to remove any Supplier Personnel in accordance with the Agreement;

7.20 ensure, prior to commencing any work for the Authority, all Supplier Personnel are subject to as a minimum HMG Baseline Personnel Security Standard security clearance. For certain Affected Properties (to be advised by the Authority), further levels of Supplier Personnel assessment may be required. This will typically require individuals to hold Security Check (SC) clearance in line with the latest HMG personnel security controls (https://www.gov.uk/government/publications/hmg-personnel-security-controls). There may be certain roles that require interaction with vulnerable groups, access higher levels of sensitive information, or due to the systems access capability, (for example database administrators, etc.), may be required to be subject to higher levels of personnel security vetting. The Authority shall advise on these roles during the Implementation Phase. All security clearance documents shall be made available at all times to the Authority; and

7.21 deploy Supplier Personnel and other resources flexibly in order to ensure the Authority benefits from the scope and scale of the Supplier’s organisation.

COMMUNICATIONS

7.22 The Authority requires that the Supplier ensures regular communication between Supplier Personnel and Authority Personnel. The Authority requires that the Supplier manages all communications in the delivery of Services in a professional and timely manner to support the achievement of the Authority’s strategic objectives and transformation objectives.

7.23 The Supplier shall:

COMMUNICATIONS IMPLEMENTATION SERVICES

7.24 by the time stated in Annex A, provide for Approval a draft “Communication Plan” within the "Account Management Detailed Solution” in line with Good Industry Practice, detailing how the Supplier will ensure and manage regular communication throughout the Term. An indicative list of items to be included in the Account Management Detailed Solution is included in Annex A;

7.25 upon instruction by the Authority, execute, utilising Supplier Personnel, the approved “Account Management Detailed Solution” in line with the values and behaviours referred to in Paragraph 3;

COMMUNICATIONS OPERATIONAL SERVICES

7.26 ensure those individuals identified within the approved Account Management Detailed Solution make regular visits to all Affected Properties and that contact is made with Authority Personnel (specifically local managers) to discuss contract performance and any issues;

7.27 ensure that Security Officer Team Leaders regularly hold service delivery meetings with local managers to discuss local service delivery, areas that are working well and areas for improvement. The Supplier shall ensure that actions are recorded and improvements made throughout the Term of the Agreement; and

7.28 at all times, maintain appropriate processes and procedures, including the provision of all required equipment (including Supplier Equipment), to ensure communication of changes to the UK Threat Level to all active Supplier Personnel within 2 hours and all other Supplier Personnel at start of day or on commencement of their next shift to ensure that the relevant Supplier Personnel are fully informed of new arrangements prior to such Supplier Personnel working in connection with this Agreement.

QUALITY MANAGEMENT

7.29 The Authority requires that the Supplier designs and implements a robust quality management system assuring the Authority that all Service Elements contained within this Statement of Requirements are delivered consistently and in compliance with all relevant legal requirements.

7.30 The Supplier shall:

QUALITY MANAGEMENT IMPLEMENTATION SERVICES

7.31 by the time stated in Annex A, provide for Approval a draft “Quality Management Detailed Solution” in line with Good Industry Practice, detailing how the Supplier will implement the required quality management system. An indicative list of items to be included in this Quality Management Detailed Solution is included in Annex A; and

QUALITY MANAGEMENT OPERATIONAL SERVICES

7.32 upon instruction by the Authority, execute, utilising Supplier Personnel, the approved “Quality Management Detailed Solution” throughout the Term in line with the values and behaviours referred to in Paragraph 3.

DOCUMENT MANAGEMENT

7.33 The Authority requires the Supplier to provide a document management service for the accurate reporting of data and document storage for information and details of Affected Properties. This will interface with the Supply Chain Integrator System to be accessed by the Authority and Supply Chain Integrator for timely and robust document management.

7.34 The Supplier shall:

DOCUMENT MANAGEMENT IMPLEMENTATION SERVICES

7.35 by the time stated in Annex A, provide for Approval a draft “Document Management Detailed Solution” in line with Good Industry Practice, detailing the process to be executed in delivery of a professional document management service. An indicative list of items to be included in this Document Management Detailed Solution is included in Annex A; and

DOCUMENT MANAGEMENT OPERATIONAL SERVICES

7.36 upon instruction by the Authority, execute, utilising Supplier Personnel, the approved Document Management Detailed Solution in line with the values and behaviours referred to in Paragraph 3.

VACANT MANAGEMENT SOLUTION

7.37 The Authority may require that the Supplier provides a vacant management solution to be implemented upon request by the Authority when an Affected Property is vacant or underutilised. The Supplier's vacant management solution shall provide an efficient solution to the security of the Affected Property, fully satisfying the Authority's requirements e.g. statutory and contractual whilst maximising value for money.

7.38 Where such vacant management solution is required by the Authority, it shall be effected via the Change Control Procedure if required.

7.39 Where required, the Supplier shall:

VACANT MANAGEMENT IMPLEMENTATION SERVICES

7.40 develop a vacant management solution to be implemented upon request to satisfy the Authority requirement as defined at 7.37; and

VACANT MANAGEMENT OPERATIONAL SERVICES

7.41 upon request, provide a vacant management solution for Affected Properties as per the Approved vacant management solution demonstrating value for money in the provision of this service.

8 HEALTH AND SAFETY, RISK MANAGEMENT AND FIRE RISK ASSESSMENTS

8.1 The Authority requires that the Supplier, in its undertakings and duties, exercises robust Health and Safety & Risk Management policies to protect Authority Personnel and those Authority Customers, Authority Visitors and other third parties who might be affected by the delivery of the Services from risk and harm.

8.2 The Authority requires that the Supplier shall at all times control and manage the risks associated with the delivery of the Services as contained within this Statement of Requirement.

8.3 The Supplier shall:

HEALTH AND SAFETY, RISK MANAGEMENT AND FIRE RISK ASSESSMENTS IMPLEMENTATION SERVICES

8.4 by the time stated in Annex A, provide for Approval a draft "Health & Safety and Risk Management Detailed Solution" in line with Good Industry Practice that will detail the management of all health and safety issues and risks associated with the delivery of the Services. The Supplier shall reduce and minimise risks to As Low As Reasonably Possible (ALARP). The Authority requires that the Health & Safety and Risk Management Detailed Solution proposed by the Supplier is fully integrated with the existing overall Detailed Solutions as developed by the Supply Chain Integrator and all Authority Policies for Health and Safety & Risk Management which shall include but not be limited to:

a) Health and Safety & Risk Management Plan;
b) Fire and Evacuation Drill Solution;
c) Site Induction Process;
d) Fire Risk Assessment Plan; and
e) Dynamic Risk Assessments.

An indicative list of items to be included in this Health & Safety and Risk Management Detailed Solution is included in Annex A;

HEALTH AND SAFETY, RISK MANAGEMENT AND FIRE RISK ASSESSMENTS OPERATIONAL SERVICES

8.5 upon instruction by the Authority, execute, utilising Supplier Personnel, the approved "Health & Safety and Risk Management Detailed Solution" in line with the values and behaviours referred to in Paragraph 3;

8.6 for the avoidance of doubt, be required to adhere at all times to those overall health and safety & risk management detailed solutions developed by the Supply Chain Integrator and all Authority Policies; see schedule 2.6 (Authority Policies);

8.7 in the delivery of the Services as contained within this Statement of Requirements, ensure all the obligations of the Health and Safety at Work Act 1974, the Regulatory Reform (Fire Safety Order) 2005, Fire Precautions Act and other relevant Acts, Laws, Regulations and Good Industry Practice is fully delivered. This includes doing all that is reasonably practicable to ensure the health, safety and welfare at work of all Authority Personnel and those Authority Customers, Authority Visitors and other third parties who might be affected by the delivery of the Services as contained within this Statement of Requirements;

8.8 in the delivery of the Services as contained within this Statement of Requirements, ensure all Authority Personnel and Authority Customers are protected and feel at ease while on the Affected Properties. Supplier Personnel must at all times comply with the BS 18004:2008 guide to Occupational Health & Safety Management Systems or equivalent workplace health and safety practice;

8.9 in the delivery of the Services as contained within this Statement of Requirements, deliver in full the requirements of the Authority's Health and Safety policies and ad-hoc guidance on such matters. Escalate any issues accordingly in line with Authority Policies;

8.10 in the delivery of the Services as contained within this Statement of Requirements, ensure that the Authority Customers are also treated to the same duty of care as the Supplier and other Authority Supply Chain Members enjoy;

8.11 recognise that the Authority will retain overall accountability for the health and safety of its employees and Authority Customers but will rely on the Supplier's skill and experience in ensuring obligations are executed in the most effective and economic way. The Authority will retain responsibility for the Approval of all Detailed Solutions and Deliverables relating to health and safety and risk management and will retain ownership of all disaster recovery and business continuity plans;

8.12 use the Supply Chain Integrator System or an alternative system that has the required functionality and capability to interface effectively with the Supply Chain Integrator System to record details of accidents, Incidents, near misses and workplace ill-health issues;

8.13 support a co-ordinated and joined-up approach to all Health and Safety & Risk Management issues, including but not limited to Health and Safety incident management across the Authority, the Authority Supply Chain Members and other related third parties such as Emergency Services;

8.14 if required, provide a professional advice service on all matters relating to the Health and Safety at Work Act 1974 and any subsequent re-enactments relevant to the Services;

8.15 provide a Health and Safety expert who is either a member of the Institution of Occupational Safety and Health (IOAH) or holds an equivalent qualification that is issued by a recognised organisation for advice relating to the Services;

8.16 ensure all Environmental protection standards are met, followed up and adhered to, including but not limited to asbestos relevant to the Services;

8.17 provide First Aid training for all Security Officers which shall, as a minimum, require successful completion of a 1 day Emergency First Aid training course;

8.18 document and maintain accurate records of all First Aid training delivered to Supplier Personnel;

8.19 provide Supplier Personnel, as instructed by the Authority, for fire and bomb marshal training (including fire extinguisher training), which shall be delivered by the Supply Chain Integrator free of charge to the Supplier;

8.20 provide Supplier Personnel to complete the Affected Property Fire Risk Assessments;

8.21 on request, provide Fire Safety Consultants with a minimum qualification of Graduate Member of the Institution of Fire Engineers;

8.22 provide all Dynamic Risk Assessments including appropriate training;

8.23 throughout the Dynamic Risk Assessment process, communicate with all affected parties including but not limited to the Authority Representatives, Authority Personnel, Authority Customers and other Authority Supply Chain Members;

8.24 upon instruction from the Authority, provide the roles, responsibilities and duties of the Principle Contractor and Principle Designer under the Construction (Design and Management) Regulations 2015;

8.25 comply with the risk methodology as created by the Supply Chain Integrator;

8.26 upon identifying a risk, liaise with the Authority through the use of the Supply Chain Integrator System or an alternative system that has the required functionality and capability to interface effectively with the Supply Chain Integrator System, to record and give details of the risk; and

8.27 escalate the high-impact risks to the Authority and as appropriate the Authority will take a view on business-critical risks.

9 BUSINESS CONTINUITY AND DISASTER RECOVERY

9.1 The Authority requires the Supplier to undertake its duties in accordance with the Supply Chain Integrator’s policies and the Authority Policies and work with Authority Supply Chain

Members to execute contingency plans for the safety of the Affected Properties and all personnel at the relevant Sites.

9.2 The Supplier shall:

BUSINESS CONTINUITY AND DISASTER RECOVERY IMPLEMENTATION SERVICES

9.3 by the time stated in Annex A, the Supplier shall provide for Approval a draft "Business Continuity and Disaster Recovery Detailed Solution" in line with Good Industry Practice detailing the process to be executed in delivery of a professional business continuity and disaster recovery service. An indicative list of items to be included in Business Continuity and Disaster Recovery Detailed Solution is included in Annex A;

BUSINESS CONTINUITY AND DISASTER RECOVERY OPERATIONAL SERVICES

9.4 comply with the appropriate Authority policies concerned with business continuity including evacuation, disaster recovery and other emergency incidents;

9.5 in the event of an emergency, undertake all of its duties under the Business Continuity and Disaster Recovery Detailed Solution. Liaise with other Authority Supply Chain Members to execute this plan as required;

9.6 notify the Authority as soon as it becomes aware of an Emergency event or a likely emergency event through contacting the helpdesk in line with the Business Continuity and Disaster Recovery Detailed Solution;

9.7 be responsible for the immediate alerting and communication to all personnel at the relevant Site when an Emergency occurs. Make use of appropriate onsite equipment to inform of the situation and procedure; and

9.8 if required, ensure that Security Officers immediately alert Emergency Services. Liaise with the Authority to ensure communication is maintained in an Emergency event.

10 SECURITY THREAT AND RISK ASSESSMENT & SECURITY PLAN

SECURITY THREAT AND RISK ASSESSMENT

10.1 The Authority requires high-quality Security Threat and Risk Assessments to be completed and reviewed regularly, at a frequency agreed by the Authority but as a minimum on an annual basis and as per the Approved Security Threat and Risk Assessment Programme Plan to assess security risk, vulnerabilities and local threats across the Affected Property.

10.2 The Supplier shall:

SECURITY THREAT AND RISK ASSESSMENT TRANSFORMATION SERVICES

10.3 by the time stated in Annex A, provide for Approval a draft "Security Threat and Risk Assessment Detailed Solution" in line with Good Industry Practice. An indicative list of items to be included in this Security Threat and Risk Assessment Detailed Solution is included in Annex A;

10.4 upon instruction by the Authority, execute, utilising Supplier Personnel, the approved "Security Threat and Risk Assessment Detailed Solution" in line with the values and behaviours referred to in Paragraph 3;

10.5 as per the agreed programme, conduct Security Threat and Risk Assessments as per the approved Security Threat and Risk Assessment Detailed Solution;

10.6 conduct a Security Threat and Risk Assessment as per the agreed Security Threat and Risk Assessment Detailed Solution after the initial implementation of a Security Plan at each Affected Property to critically assess the impact of the first Security Plan implemented, the timescale will be agreed with the Authority. In the event that recommendations are made through the Security Threat and Risk Assessment, update the first Security Plan accordingly;

SECURITY THREAT AND RISK ASSESSMENT OPERATIONAL SERVICES

10.7 as directed by the Authority, complete and/or review existing Security Threat and Risk Assessments in response to a change in the relevant Affected Property's characteristics or risk profile, to include but not limited to:

a) Change in Authority Core Business;
b) Changes in Authority Customer / Visitor numbers;
c) Changes in the number of Authority Personnel, the Authority's teams or other site occupiers;
d) Changes in local demographics;
e) Changes in the UK Threat Level and/or changes in the Government Response Level; and
f) Acquisition of new property;

10.8 as per the approved Security Threat and Risk Assessment delivery Programme Plan (to be developed by the Supplier and submitted to the Authority for approval), execute, utilising Supplier Personnel, the approved "Security Threat and Risk Assessment Detailed Solution" in line with the values and behaviours referred to in Paragraph 3 and in order to provide, as a minimum, an annual Security Threat and Risk Assessment incorporating an annual local threat and risk assessment, for all Affected Properties throughout the Term; and

10.9 review the Security Threat and Risk Assessment Detailed Solution regularly, at a frequency agreed by the Authority but as a minimum on an annual basis, and provide a written report to the Authority that critically assesses the Approved Security Threat and Risk Assessment Detailed Solution and provides recommendations for improvement.

SECURITY PLAN

10.10 The Authority requires that detailed Security Plans are developed for each Affected Property, commensurate with the risk identified in the relevant Affected Property's Security Threat and Risk Assessment, which shall specify all the security measures which shall, once approved, form the Statement of Requirements for the Operational Services to be delivered at the relevant Affected Property.

10.11 The Supplier shall:

SECURITY PLAN IMPLEMENTATION SERVICES

10.12 during the Implementation Phase and before the Operational Service Commencement Date complete an Interim Security Plan for all Affected Properties, identifying the existing Security Officer hours deployed, correlating with the Transferred Former Supplier Employee Notional Data and the Transferring Former Supplier Employee Information (as applicable). This shall be provided by the Supplier in a format to be agreed with the Authority.

SECURITY PLAN TRANSFORMATIONAL SERVICES

10.13 by the time stated in Annex A, provide for Approval a draft "Security Plan Detailed Solution" in line with Good Industry Practice. An indicative list of items to be included in this Security Plan Detailed Solution is included in Annex A;

upon instruction by the Authority, execute, utilising Supplier Personnel, the Approved "Security Plan Detailed Solution" in line with the values and behaviours referred to in Paragraph 3;

SECURITY PLAN OPERATIONAL SERVICES

10.14 as directed by the Authority, update and/or review existing Security Plans in response to an update to the Security Threat and Risk Assessment for an Affected Property;

10.15 as per the approved Security Plan's programme plan (to be developed by the Supplier and submitted to the Authority for approval), execute, utilising Supplier Personnel, the approved "Security Plan Detailed Solution" in line with the values and behaviours referred to in Paragraph 3 and in order to provide, as a minimum, an annual assessment of the Security Plans for all Affected Property's throughout the Term; and

10.16 review the Security Plan Detailed Solution regularly, at a frequency agreed by the Authority but as a minimum on an annual basis, and provide a written report to the Authority that critically assesses the Approved Security Plan Detailed Solution and provides recommendations for improvement.

11 WORK ORDER MANAGEMENT

11.1 The Authority requires that the Supplier utilises the Work Order management system provided by the Supply Chain Integrator or provides an alternative system that has the required functionality and capability to interface effectively with the Supply Chain Integrator's Work Order management system to raise, track and signal completion of all Work Orders.

11.2 The Supplier shall:

WORK ORDER MANAGEMENT IMPLEMENTATION SERVICES

11.3 by the time stated in Annex A, provide for Approval a draft "Work Order Management Detailed Solution" in line with Good Industry Practice, detailing how the Supplier will utilise and/or interface with the Supply Chain Integrator's Work Order management system to raise, track and signal completion of all Work Orders. An indicative list of items to be included in this Work Order Management Detailed Solution is included in Annex A;

11.4 align the management of Work Orders with the processes and procedures dictated by the Authority and implemented by all Authority Supply Chain Members utilising the Supply Chain Integrator System or an alternative system that has the required functionality and capability to interface effectively with the Supply Chain Integrator Systems including but not limited to the Supply Chain Integrator's Work Order management system. For the avoidance of doubt, licenses to the Supply Chain Integrator's Work Order management system shall be provided to the Supplier free of charge.

WORK ORDER MANAGEMENT OPERATIONAL SERVICES

11.5 proactively update, as required by the Authority, all Work Orders to track progress through the Work Order management system, including performance tracking against the Performance Indicators;

11.6 fully cooperate with all complaints raised against the completion of own Work Orders as per the complaints process agreed with the Authority; and

11.7 fully cooperate with all on-site supervision for example of high-risk Work Orders by the Supply Chain Integrator or Authority.

11.8 For the avoidance of doubt, “proactively update” includes inserting a narrative description to provide an accurate audit trail, including:

a) for Work Orders completed within the required timeframes, details of any work undertaken outside of normal parameters, for example an explanation of why certain things were done; and

b) for Work Orders not completed or not likely to be completed within the required timeframes an update on why the work has not been completed and an estimated time of completion.

12 CONTROL AND MONITORING FACILITY

12.1 The Authority requires a central facility for receiving alarm notifications, monitoring CCTV images, radio and any other communication and controlling Responses to Emergencies or Incidents. This facility shall not be located on the Affected Properties but may be a shared facility. The Service will be delivered in accordance with the relevant Standards, legislation and Good Industry Practice.

12.2 The Authority requires the seamless transition of the existing alarm signalling services for Existing Systems, including managing the transition of the Services from any incumbent provider to the Supplier.

12.3 The Authority expects utilisation of the Control and Monitoring Facility for the monitoring of video and alarms to take place in a phased manner across the Authority Estate in line with required enabling works and the installation of Replacement Security Systems. The Authority does not guarantee that all Affected Properties shall be connected to the Control and Monitoring Facility during the Term.

12.4 The Supplier shall:

<u>CONTROL AND MONITORING FACILITY IMPLEMENTATION SERVICES</u>

12.5 by the time stated in Annex A, the Supplier shall provide for Approval a draft “Control and Monitoring Facility Detailed Solution” in line with Good Industry Practice, detailing how the Supplier will deliver the Service. An indicative list of items to be included in this Control and Monitoring Facility Detailed Solution is included in Annex A; and

12.6 liaise and develop procedures with the Aegis Existing AACS Supplier to ensure an integrated and seamless service delivery.

12.7 The Control and Monitoring Facility Detailed Solution shall also include details of how the Supplier will undertake the transition of services from the Aegis Existing AACS to the Supplier as the Replacement AACS and the replacement Intruder Detection Systems (as applicable

and subject to Approval of the relevant Affected Properties Security Plan) are installed across the Affected Properties.

12.8 The Control and Monitoring Facility Detailed Solution shall also include details of how the Supplier will undertake the transition of the Services from the Non-Aegis Existing AACS to the Replacement AACS and replacement Intruder Detection Systems (as applicable and subject to Approval of the relevant Affected Properties Security Plan) are installed across the Affected Properties.

12.9 The Supplier shall:

12.10 provide a dedicated telephone number and unique reference number (URN) at each Affected Property and from the Control and Monitoring Facility for the handling of all calls through to the Emergency Services as required from the Operational Service Commencement Date; and

12.11 identify Existing Systems which are remotely monitored and make the necessary arrangements to provide a similar monitoring service from the Operational Service Commencement Date. It should be assumed that the Authority will provide the relevant PSTN line (or similar).

CONTROL AND MONITORING FACILITY IMPLEMENTATION SERVICES OPERATIONAL SERVICES

12.12 Upon instruction by the Authority, execute, utilising Supplier Personnel, the approved "Control and Monitoring Facility Detailed Solution" in line with the values and behaviours referred to in Paragraph 3.

12.13 Provide the monitoring of Existing Systems as required until such time as the relevant Replacement Security Systems are installed.

13 SECURITY SYSTEMS

[REDACTED]

14 TRIALLING

14.1 The Authority requires that the Supplier's proposed solution, as contained in the set of Approved Detailed Solutions, shall be subject to statistically robust Trials to demonstrate the effectiveness of the proposed solution prior to wider adoption across the Affected Properties. Demonstrating that the proposed solution will achieve the strategic and transformation objectives will be fundamental to the Authority Personnel endorsing the transformation of the Services.

14.2 The Authority requires that the Supplier conducts two phased Trials of the Supplier's proposed solution beginning 4 weeks after the Operational Service Commencement Date. The Authority recognises the size and complexity of the overall proposed solution and intends to prioritise critical Services for transformation which shall form part of the first Trial. At the end of Trial 1 and subject to the Authority awarding Trial Success, the Supplier would be able to progress with wider adoption of those Services subject to Trial 1 through the transformation programme.

14.3 Each Trial shall test distinct aspects of the proposed solution and shall together demonstrate the effectiveness of the Supplier's overall proposed solution. A list of Detailed Solutions that shall be included in Trial 1 and Trial 2 is included in Part C of Annex A.

TRIAL 1

14.4 Upon instruction from the Authority and subject to an Approved Trialling Detailed Solution, Trial 1 shall commence on 1st May 2018.

14.5 The Authority expects that Trial 1 shall conclude on 30th June 2018.

TRIAL 2

14.6 Upon instruction from the Authority and subject to an Approved Trialling Detailed Solution, Trial 2 shall commence on 1st July 2018.

14.7 The Authority expects that Trial 2 shall conclude on 31st August 2018.

14.8 The Supplier shall:

TRIALLING IMPLEMENTATION SERVICES

14.9 by the time stated in Annex A, provide for Approval a draft "Trialling Detailed Solution" which shall include the Trialling Methodology (as required within the Trialling Detailed Solution and which shall be in line with Good Industry Practice and statistically robust) and a detailed Trialling Proposal (as required within the Trialling Detailed Solution), detailing the proposed security measures to be deployed at each Trial Site. An indicative list of items to be included in this Trialling Detailed Solution is included in Annex A;

14.10 work with the Supply Chain Integrator to identify up to a maximum of 10 Affected Properties which shall become the Trial Sites where the Trials shall be undertaken;

14.11 provide an Approved Security Threat and Risk Assessment and Approved Security Plan for each of the Trial Sites;

14.12 during the Implementation Phase by the time stated in Annex A, the Supplier shall conduct a separate Private Mobile Radio (PMR) Trial of their proposed PMR solution to demonstrate its operational effectiveness in line with the approved "Trialling Detailed Solution";

14.13 within 10 working days of completion of the PMR Trial, complete and submit a PMR Trial report to the Authority to assess the suitability of the rollout of the PMR solution to the Affected Property including identifying improvements to the Approved PMR Detailed Solution;

14.14 upon successful completion of the PMR Trial, deploy the Approved PMR Detailed Solution to Supplier Personnel ahead of the Operational Services Commencement Date in line with the values and behaviours referred to in Paragraph 3;

TRIALLING TRANSFORMATION SERVICES

14.15 during the Transformation Phase by the time stated in Annex A, utilising Supplier Personnel, implement the approved "Trialling Detailed Solution" at the Trial Sites in line with the values and behaviours referred to in Paragraph 3; and

14.16 upon successful completion of the Trial, review and critically assess the effectiveness of the Trialling Proposal by analysing, as a minimum:

a) Relative performance of the Services at the Trial Sites;
b) Review of any Incidents including response by Supplier Personnel; and
c) Satisfaction Surveys,

and provide a written Trial report to the Authority within 28 days of the end of the Trial.

14.17 The Trial report shall assess the suitability of the rollout of the Trialling Proposal to additional Affected Properties including identifying improvements to the Approved Detailed Solutions.

15 TESTING, COMMISSIONING AND HANDOVER REGIME

15.1 The Authority requires all Security Systems to undergo a rigorous testing, commissioning and handover regime.

15.2 The Supplier shall:

TESTING, COMMISSIONING AND HANDOVER REGIME IMPLEMENTATION SERVICES

15.3 by the time stated in Annex A, provide for Approval a draft "Testing, Commissioning and Handover Detailed Solution" which shall define and document approach to overall Testing, commissioning and handover in line with Good Industry Practice. An indicative list of items to be included in this Testing, Commissioning and Handover Detailed Solution is included in Annex A;

15.4 provide a documented Testing Strategy and Test Plan for each instance of Testing in compliance with the requirements of Schedule 6.2 (Testing). Testing will include:

a) Factory Acceptance Testing (FAT) to determine and document the equipment hardware and software operates according to its specification, covering the following key areas:
   i. functional;
   ii. performance;
   iii. fault management;
   iv. communications; and
   v. interface requirements;
b) Site Acceptance Testing (SAT) to determine and document the equipment hardware and software operates according to its specification following installation on site. The test outcome should give the test team confidence that the equipment behaves as expected under the full range of foreseeable conditions, including misuse and error. The test script and scope of each SAT shall be agreed with the Authority but it is anticipated that a SAT will be required following security equipment installation and configuration at each site;
c) Integrated Site Acceptance Testing (ISAT) to demonstrate sub-system integration including cause and effect testing. This will include load testing to confirm performance of the overall system under load conditions. The test should also demonstrate fault management by simulating errors (e.g. disconnecting power cables, communication cables and disabling software services). This will include failover testing to confirm the resilience of the security systems under load conditions, the failure mode and effects and the recovery; and
d) User Acceptance Testing (UAT) to demonstrate to the Authority that all Electronic Security Systems meet the requirements of the Security Plan. This will include any

remote functionality such as viewing of live images at the Control and Monitoring Facility;

15.5 document the FAT, SAT, ISAT and UAT and submit the results by way of Test Reports for Approval;

15.6 on successful completion of the SAT and UAT, commence the training of the relevant Authority Personnel. The Supplier shall also produce a user guide for the relevant Authority Personnel; and

TESTING, COMMISSIONING AND HANDOVER REGIME TRANSFORMATION AND OPERATIONAL SERVICES

15.7 once Approved by the Authority, execute, deliver and manage the Testing, Commissioning and Handover Detailed Solution in line with the values and behaviours referred to in Paragraph 3.

16 SUPPORT AND MAINTENANCE REQUIREMENTS

16.1 The Authority requires the Security Systems to be operational at all times. Any faults must be rectified efficiently, with minimal disruption to day to day operations and, in any event, within the specified Target Fix Times. Where the Supplier fails to rectify any faults within the relevant Target Fix Times or fails to provide the Services in accordance with the relevant Performance Indicators, the Authority shall have the right to specified remedies for such Performance Failures, including, but not limited to, Service Credits.

16.2 The Authority will make its IT network management tool available to the Supplier's maintenance and fault management team to allow them to undertake a Network Diagnostic Test as the first line support to establish if the Authority Network is the cause of any service interruption. The details of the access will be agreed between the Supplier and the Authority.

16.3 Where the Supplier believes (acting reasonably) that it will not be able to achieve the Target Fix Times in respect of certain Affected Properties due to circumstances outside of their control (including the remoteness of the Affected Property's location and/or transport links), the Supplier shall submit a Proposal to the Authority for Approval in accordance with Schedule 12 (Approval) prior to the Operational Readiness Completion Date detailing the name, address and the Supplier's proposed Target Fix Time for each relevant Affected Property. The Supplier shall provide full justification of why it proposes such Affected Properties should have Target Fix Times that are longer than those specified in the Target Performance Levels. Where the Authority Approves any Affected Property having an extended Target Fix time such Affected Property shall be inserted into Part C of Schedule 15 (Affected Properties, Aegis Existing AACS Properties and Extended Target Fix Time Properties) and shall become an Extended Target Fix Time Property.

SUPPORT AND MAINTENANCE OF EXISTING SYSTEMS

16.4 The Authority requires that the Existing Systems installed on each Affected Property continue to be operational from the Operational Service Commencement Date. Any faults must be rectified efficiently, with minimal disruption to day to day operations and, in any event, within the specified Target Fix Times. Where the Supplier fails to rectify any faults within the relevant Target Fix Times or fails to provide the Services in accordance with the relevant Performance Indicators, the Authority shall have the right to specified remedies for such Performance Failures, including, but not limited to, Service Credits.

16.5 As soon as reasonably possible, following the Approval of the Existing Security Systems Support and Maintenance Detailed Solution, the Authority requires that a comprehensive Asset Verification and Condition Survey is undertaken for all Security Systems and that the Supplier can assure the Authority of its capability to provide all required support and maintenance from the Operational Service Commencement Date.

16.6 The Supplier shall:

SUPPORT AND MAINTENANCE OF EXISTING SYSTEMS IMPLEMENTATION SERVICES

16.7 by the time stated in Annex A, provide for Approval a draft "Asset Verification and Condition Survey Plan" within the draft "Existing Systems Detailed Solution" in line with Good Industry Practice, detailing the process to be executed to undertake the Asset Verification and Condition Survey of Existing Systems to provide assurance to the Authority, by way of an Asset Verification and Condition Survey Report;

16.8 create an Asset Verification and Condition Survey Report and submit this to the Authority for Approval in accordance with Schedule 12 (Approval) as soon as reasonably possible and in any event at least four weeks prior to the Operational Service Commencement Date. The Asset Verification and Condition Survey Report shall detail (providing full justification and evidence) of the Supplier's capability to provide support and maintenance for Existing Systems. This shall specifically identify those Existing Systems that are closed protocol and detail their arrangements for providing required support and maintenance at all times ensuring continuity of service;

16.9 upon instruction by the Authority, execute, utilising Supplier Personnel, complete the approved Asset Verification and Condition Survey Plan by the Operational Service Commencement Date in line with the values and behaviours referred to in Paragraph 3;

16.10 if required, and following Approval of the Existing Systems Detailed Solution, create an Existing Systems Obsolescence/Unavailability Report and submit this to the Authority for Approval in accordance with Schedule 12 (Approval) as soon as reasonably possible and in any event at least four weeks prior to the Operational Service Commencement Date. The Existing Systems Obsolescence/Unavailability Report shall detail (providing full justification and evidence) all parts of the Existing Systems:

a) that are obsolete; and/or
b) for which replacement parts are unavailable nationally (providing that the Supplier has used all reasonable endeavours to source relevant replacement parts);

16.11 by the time stated in Annex A, provide for Approval a draft "Existing Systems Support and Maintenance Detailed Solution" in line with Good Industry Practice, detailing the process to be executed in delivery of a professional support and maintenance service. An indicative list of items to be included in this Existing System Support and Maintenance Detailed Solution is included in Annex A. The Authority requires that the Supplier provides reporting to enable the delivery of the Supply Chain Integrator' services and the Authority's Core Business which will include but not limited to the:

a) Annual Planned Preventative Maintenance Plan;
b) Life Cycle Plan;
c) Reactive Maintenance Plan;
d) Spares Holding Plan; and
e) Faults and Target Fix Times;

SUPPORT AND MAINTENANCE OF EXISTING SYSTEMS OPERATIONAL SERVICES

16.12 upon instruction by the Authority, execute, utilising Supplier Personnel, the approved Existing Systems Support and Maintenance Detailed Solution in line with the values and behaviours referred to in Paragraph 3;

16.13 provide a spares holding strategy within the Existing Systems Support and Maintenance Detailed Solution in order to meet the Target Fix Times;

16.14 provide the Existing System Maintenance Report as required by the Agreement;

16.15 provide appropriate engineering resource required to meet the Target Fix Times;

16.16 test all Panic Alarms monthly or at a frequency agreed in writing between the Authority and the Supplier, in line with approved Test Plan included in the Existing System Support and Maintenance Detailed Solution, industry standards and best practice to ensure full functionality can be relied upon in the event of an Incident or Emergency;

16.17 in the event of an Existing Systems Failure, complete a Network Diagnostic Test in accordance with the Approved Existing Security Systems Support and Maintenance Detailed Solution to assess the performance and availability of the Authority Network or Supplier Network as applicable and submit a report with findings to the Authority; and

16.18 provide and maintain, until such date as the Existing Systems are no longer present across the Authority Properties, the Excluded Existing Systems Parts Register as required by the Agreement.

SUPPORT AND MAINTENANCE OF REPLACEMENT SECURITY SYSTEMS

16.19 Following the Site Acceptance Test any Fix must be completed with minimal disruption to day to day operations and, in any event, within the Target Fix Times. Where the Supplier fails to fix any faults within the relevant Target Fix Times or fails to provide the Services in accordance with the relevant Performance Indicators, the Authority shall have the right to specified remedies for such Performance Failures, including, but not limited to, Service Credits.

16.20 For the avoidance of doubt, any Replacement Security System which incorporates Existing Systems components will be treated as a Replacement Security System for the purposes of the performance management scheme, Schedule 2.2 (Performance Levels) of the Agreement and the pricing of maintenance which shall utilise the Replacement Security Systems Maintenance rates as detailed in Schedule 7.7 (Financial Model) of the Agreement.

16.21 The Supplier shall:

SUPPORT AND MAINTENANCE OF REPLACEMENT SECURITY SYSTEMS TRANSFORMATION SERVICES

16.22 by the time stated in Annex A, provide for Approval a draft “Replacement Security Systems Support and Maintenance Detailed Solution” in line with Good Industry Practice, detailing the process to be executed in delivery of a high quality and professional support and maintenance service. An indicative list of items to be included in this Replacement Security Support and Maintenance Detailed Solution is included in Annex A. The Authority requires

that the Supplier provides reporting to enable the delivery of the Supply Chain Integrator's services and the Authority's Core Business which will include but not limited to the:

a) Annual Planned Preventative Maintenance Plan;
b) Life Cycle Plan;
c) Reactive Maintenance Plan; and
d) Spares Holding Plan;

SUPPORT AND MAINTENANCE OF REPLACEMENT SECURITY SYSTEMS OPERATIONAL SERVICES

16.23 upon successful completion of the Site Acceptance Test, execute the approved Replacement Security Systems Support and Maintenance Detailed Solution for any Replacement Security System in line with the values and behaviours referred to in Paragraph 3;

16.24 provide an updated spares holding strategy within the Replacement Security Support and Maintenance Detailed Solution in order to meet the Target Fix Times;

16.25 provide appropriate engineering resource required to meet the Target Fix Times;

16.26 design the Supplier Systems to enable the remote diagnosis of faults and should provide fault indications directly to the Supplier's helpdesk;

16.27 test all Panic Alarms monthly or at a frequency agreed in writing between the Authority and the Supplier, in line with approved Test Plan included in the Replacement Support and Maintenance Detailed Solution, industry standards and best practice to ensure full functionality can be relied upon in the event of an Incident or Emergency; and

16.28 in the event of a Replacement Systems Failure, complete a Network Diagnostic Test in accordance with the Approved Replacement Security Systems Support and Maintenance Detailed Solution to assess the performance and availability of the Authority Network or Supplier Network as applicable and submit a report with findings to the Authority.

17 SECURITY OFFICERS

17.1 The Authority requires that the Supplier provides Security Officers to undertake the duties as defined in this Statement of Requirement which are currently performed by Customer Care Officers (CCO) and Customer Service Officers (CSO) across the Affected Properties; see Job Descriptions included in the information provided to the Supplier by the Authority in the data room during the tender process for the Agreement. In addition, the Supplier shall provide Security Officers to perform all Services in line with Approved assignment instructions. The Service provided shall be professionally managed, high quality and in line with Good Industry Practice, specifically BS EN ISO 9001 or equivalent accreditation and compliant with all legislation governing the security industry.

FRONT OF HOUSE DUTIES TO BE PROVIDED BY THE AUTHORITY

17.2 The Authority shall use all reasonable endeavours to ensure that an appropriate member of Authority Personnel is present at each Affected Property during normal working hours to be the first point of contact with Authority Customers when they enter an Affected Property.

17.3 The Supplier shall:

SECURITY OFFICER DEPLOYMENT

SECURITY OFFICER DEPLOYMENT IMPLEMENTATION SERVICES

17.4 by the time stated in Annex A and as part of the overall draft Implementation Plan Detailed Solution, provide for Approval a draft "Existing Security Workforce Plan" in line with Good Industry Practice detailing the measures the Supplier shall take to execute the transfer of personnel in compliance with the Transfer of Undertakings for the Protection of Employment (TUPE) Regulations 2006; deploy Security Officers in line with the Baseline Security Officer Deployment Model as specified in the Approved Interim Security Plans detailing the deployment to be adhered to on the Operational Services Commencement Date at each Affected Property; the training requirements to be delivered as part of the training plan to be delivered and the development of all Security Officer assignment instructions during the Implementation Phase. An indicative list of items to be included in this Existing Security Workforce Plan is included in Annex A within the Implementation Plan Detailed Solution; and

17.5 upon instruction by the Authority, execute, utilising Supplier Personnel, the approved "Implementation Plan Detailed Solution" including the "Existing Security Workforce Plan" in line with the values and behaviours referred to in Paragraph 3.

17.6 Prior to the Operational Readiness Test, the Authority shall agree the uniform requirements to be worn by Supplier Personnel for each Affected Property and situation.

17.7 Prior to the Operational Service Commencement Date, the Supplier shall develop, in line with Good Industry Practice, a protocol the for the Response required following and attack or break-in at any Affected Property, as required by Paragraph 17.22 below (a **Response Protocol**) and submit such Response Protocol to the Authority for Approval.

SECURITY OFFICER DEPLOYMENT OPERATIONAL SERVICES

17.8 The Supplier shall:

17.9 increase and decrease deployment levels as may be required from time to time to effect required changes due to a change in the UK Threat Level and risk poses to the Affected Properties, Authority Personnel, Authority Visitors and contractors;

17.10 liaise with Emergency Services & Security Advisory bodies regarding the Detailed Solutions and all operational procedures and abide by all recommendations made;

17.11 develop, maintain and make available to the Authority for the purposes of audit an electronic Security Officer deployment system which includes time and attendance data. The time and attendance system will not be utilised by Authority Personnel and OGD Colleagues;

17.12 ensure that Supplier Personnel carry valid passes as approved by the Authority and challenge all personnel without a clearly displayed pass; and

17.13 ensure that all Supplier Personnel are suitably presented wearing all required uniforms and/or appropriate work wear at all times. Uniforms must cater for all seasons, e.g. winter patrols as agreed with the Authority. The purchase of uniforms for Supplier Personnel shall comply with the relevant standards as detailed in Schedule 2.3, specifically the relevant Government Buying Standards: http://sd.defra.gov.uk/advice/public/buying/products/textiles and Authority Policies.

17.14 All Security Officers deployed shall be First Aid trained. The Supplier should note that the existing roles of Customer Care Officers and Area Relief Officers (AROs) detailed in the Transferring Former Supplier Employee Notional Data provided in the Data Room have existing First Aid training. Suppliers should note that the existing Customer Support Officer role does not require First Aid training.

17.15 The Supplier shall:

17.16 develop a programme and operational policies for drugs and alcohol testing of Supplier Personnel in line with Good Industry Practice. Submit operational policies for approval by the Authority within 3 Months of the Operational Service Commencement Date;

17.17 randomly conduct a drugs and alcohol test for 20% of Supplier Personnel per annum in line with approved operational policies and take action as appropriate. All Supplier Personnel shall be tested over the Initial Term;

17.18 proactively conduct drugs and alcohol tests following suspected breaches of the Authority and/or Supplier drugs and alcohol policies by Supplier Personnel;

17.19 provide appropriate supervision of Security Officers including a visit to each Affected Property at least twice a month by a supervisor;

17.20 using the [REDACTED] where this can be provided by the Authority or Supplier and subject to Approval of the [REDACTED] Detailed Solution, provide the Security Officers with current [REDACTED and banned Authority Customers. For the avoidance of doubt, the current [REDACTED] does not include facial images;

17.21 utilise local intercom systems to answer calls from visitors and action in line with the approved Interim Visitor Management Detailed Solution or Replacement Visitor Management Detailed Solution as appropriate;

17.22 in the event of a break-in or attack on an Affected Property, provide a physical Response, utilising suitably trained Supplier Personnel, in accordance with the Approved Response Protocol and in line with the values and behaviours referred to in Paragraph 3, to secure and make the Affected Property safe in accordance with Good Industry Practice; and

17.23 in the case of an Emergency, provide assistance to Emergency Services to ensure the Affected Property is secure or given access and alarms reset. Following Emergency Services assistance at an Affected Property provide suitable Response.

OPERATION OF SECURITY SYSTEMS

OPERATION OF SECURITY SYSTEMS OPERATIONAL SERVICES

17.24 The Supplier shall:

17.25 provide Supplier Personnel to operate the following Security Systems:

a) CCTV;
b) Automated Access Control Systems (including the Aegis Existing AACS, the Non-Aegis Existing AACS and the Replacement AACS (as applicable);
c) Intruder Detection System and Panic Alarms; and
d) Fire Detection,

at each Affected Property where Supplier Systems are installed in accordance with the approved Supplier System operating procedures as defined within the approved Existing Systems Detailed Solution, Replacement Security Systems Detailed Solution or any other relevant Detailed Solutions (as applicable).

17.26 [**REDACTED]**

18 VISITOR MANAGEMENT

18.1 The Authority requires that the Supplier provides a professionally managed visitor management service for the efficient control, verification and receipt of Authority Visitors to each Affected Property; this shall not include the receipt of Authority Personnel.

VISITOR MANAGEMENT DUTIES TO BE PROVIDED BY THE AUTHORITY

18.2 The Authority will be responsible for visitor management for Affected Properties where it is agreed with the Supplier that the relevant Affected Property has low numbers of Authority Visitors and/or for another reason the Supplier is not required to provide Visitor Management Services at that Affected Property. For those Affected Properties where the Authority agrees to be responsible for visitor management, the Authority shall nominate a member of Authority Personnel who will be responsible for the recording of Authority Visitors in line with the Approved Interim Visitor Management Detailed Solution or Approved Replacement Visitor Management Detailed Solution as applicable.

18.3 The Supplier shall:

INTERIM VISITOR MANAGEMENT

INTERIM VISITOR MANAGEMENT IMPLEMENTATION SERVICES

18.4 by the time stated in Annex A, the Supplier shall provide for Approval a draft “Interim Visitor Management Detailed Solution” in line with Good Industry Practice detailing the measures the Supplier shall take to continue the current or similar arrangements for visitor management at all Affected Properties from the Operational Services Commencement Date. An indicative list of items to be included in this Interim Visitor Management Detailed Solution is included in Annex A.

INTERIM VISITOR MANAGEMENT OPERATIONAL SERVICES

18.5 upon instruction by the Authority, execute, utilising Supplier Personnel, the approved “Interim Visitor Management Detailed Solution” in line with the values and behaviours referred to in Paragraph 3.

18.6 provide an interim visitor management service on all Affected Properties with a permanent Security Officer presence during Authority Opening Hours from the Operational Service Commencement Date to cover:

a) all visits by Authority Personnel and OGD Colleagues;
b) all individuals with planned visits with Authority Personnel and OGD Colleagues;
c) all visits by contractor staff from Authority Supply Chain Members; and
d) all unplanned visits;

18.7 provide the means to record all Authority Visitors to Affected Properties, which shall include verification of each Authority Visitor's identity and shall also include but not be limited to recording of:

a) the Authority Visitor's full name;
b) the Authority Visitor's organisation;
c) the name of the person being visited;
d) time of arrival; and
e) time of departure; and

18.8 ensure that Supplier Personnel shall ensure that all visitors are made aware of the Authority's Emergency/Incident management procedures.

REPLACEMENT VISITOR MANAGEMENT

REPLACEMENT VISITOR MANAGEMENT IMPLEMENTATION SERVICES

18.9 The Supplier shall:

18.10 by the time stated in Annex A, the Supplier shall provide for Approval a draft "Replacement Visitor Management Detailed Solution" in line with Good Industry Practice, detailing the measures the Supplier shall take to provide a more efficient, technology based and paperless solution for visitor management. An indicative list of items to be included in this Replacement Visitor Management Detailed Solution is included in Annex A;

REPLACEMENT VISITOR MANAGEMENT OPERATIONAL SERVICES

18.11 upon instruction by the Authority execute, utilising Supplier Personnel, the approved "Replacement Visitor Management Detailed Solution" in line with the values and behaviours referred to in Paragraph 3;

18.12 provide a replacement visitor management service on all Affected Properties with a permanent Security Officer presence during Authority Opening Hours to cover:

a) all visits by Authority Personnel and OGD Colleagues;
b) all individuals with planned visits with Authority Personnel and OGD Colleagues;
c) all visits by contractor staff from Authority Supply Chain Members; and
d) all unplanned visits;

18.13 provide the means to record all visitors to Affected Property which shall include verification of visitor identity and shall also include but not be limited to recording of the following Visitor Data:

a) the Authority Visitor's full name;
b) the Authority Visitor's organisation;
c) the name of the person being visited;
d) time of arrival; and
e) time of departure;

18.14 provide a solution capable of providing a full list of all Authority Visitors for each Affected Property. Authority Visitor data should be stored centrally and be accessible from the Control and Monitoring Facility. Nominated Authority Personnel should be able to interrogate the Authority Visitor data with access provided through a secure portal; and

18.15 provide a visitor management system for pre-announcement of Authority Visitors by Authority Personnel. This shall include all hardware required to allow visitors to announce themselves and register on arrival, capture images of the Authority Visitor and print local ID badges (i.e. iPad and totem) and either a dedicated workstation and printer for use by reception staff or client software to operate on existing reception workstations. Provide a web portal that is accessible to Authority Personnel at any Affected Property. Provide licences for 2500 End Users to have access to the visitor management system. The quantity of hardware shall be subject to an assessment of local requirements by the Supplier and agreement with the Authority, this shall be matched to the local visitor numbers known for each Affected Property at peak hours.

18.16 For the avoidance of doubt, this shall include licenses to provide access for 2500 End Users to access an online visitor management software package, for which guidance, support and maintenance shall be included.

18.17 Supplier Personnel shall ensure that all Authority Visitors are made aware of the Authority's Emergency/Incident management procedures.

18.18 The Supplier shall provide all equipment, licences, training, support and maintenance and consumables required by nominated Authority Personnel providing the visitor management service on those Affected Properties agreed with the Authority.

19 INCIDENT MANAGEMENT

19.1 The Authority requires an Incident management service that is effective, consistent and mitigates the impact of Incidents upon Authority Personnel, Authority Visitors, Authority Customers and the Affected Property. On average **[REDACTED]** Incidents are reported across the Affected Properties each Month. The Authority has an existing fast track process for escalation of the most serious Incidents to senior managers. The Authority reported **[REDACTED]** fast track Incidents between April 2016 and April 2017.

19.2 The Supplier shall:

INCIDENT MANAGEMENT IMPLEMENTATION SERVICES

19.3 by the time stated in Annex A, the Supplier shall provide for Approval a draft "Incident Management Detailed Solution" in line with Good Industry Practice, detailing the process to be executed for each classification of Incident. An indicative list of items to be included in this Incident Management Detailed Solution is included in Annex A;

INCIDENT MANAGEMENT OPERATIONAL SERVICES

19.4 upon instruction by the Authority, execute, utilising Supplier Personnel, the approved "Incident Management Detailed Solution" in line with the values and behaviours referred to in Paragraph 3;

19.5 proactively identify improvements and lessons learnt to the Incident Management Detailed Solutions, proposing these for Approval. Upon Approval, the Supplier shall share all improvements and lessons learnt with all Supplier Personnel to successfully deliver improvements to the Authority throughout the Term; and

19.6 for those Incidents classified as “Serious Incidents”, follow all Serious Incident policies as developed, updated and owned by the Authority, organising, reporting to and convening any and all Serious Incident Review Groups making all Supplier Personnel available as required.

20 KEY MANAGEMENT

20.1 The Authority requires that the Supplier provides a professional key management service to control building access keys, internal access keys including restricted areas such as plant rooms, IT comms rooms and alarm system codes.

20.2 The Supplier shall:

KEY MANAGEMENT IMPLEMENTATION SERVICES

20.3 by the time stated in Annex A, provide for Approval a draft “Key Management Detailed Solution” in line with Good Industry Practice, detailing the process to be executed in delivery of a professional key management service. An indicative list of items to be included in this Key Management Detailed Solution is included in Annex A; and

KEY MANAGEMENT TRANSFORMATION SERVICES

KEY CABINET

20.4 subject to the requirements identified in the Approved Security Plan, provide a solution that allows key holding and distribution to be electronically managed that is integrated into the AACS for access permissions enabling cost effective and efficient management of keys, reducing losses as well as time trying to locate misplaced or lost keys. The solution shall be scalable to provide appropriate sized solutions for small, medium and large Affected Properties. The minimum functionality of the system shall be:

a) A quick and easy method of issuing and controlling keys;
b) Restrict access to individual keys;
c) Consist single or multiple electronic cabinets to suit the size of the site;
d) Be populated in modules of 10 receptor sockets allowing a minimum of 10 keys;
e) Expandable should the need arise;
f) [REDACTED]

KEY BARRELS

20.5 The minimum number of keys that can be held within the specified Key Cabinets required at the relevant Affected Properties shall be as follows:

a)	Small Affected Properties	30 keys
b)	Medium Affected Properties	120 keys
c)	Large Affected Properties	200 keys

The Supplier shall:

20.6 subject to the requirements identified in the Approved Security Plan, provide intelligent key barrels or offline controlled doors to be implemented to minimise the use of keys across the estate. The Authority intends to consider the use of electronic Key Barrels as a means of improving key management tasks and the overall security of the Affected Properties. The systems shall use the same HR Database interface for End User management and access

permissions. Ideally the solution shall be controlled using the relevant AACS management software. The solution shall support the following minimum functionality:

a) Time profiles shall be set so that entry can be free during normal hours with card presentation required out of hours for example;
b) Dynamic alteration of these settings shall be possible through a simple End User interaction at the door;
c) The off-line doors rely on data on card and would not require wireless receiver/transmitter operation;
d) Data transmitted and received by the off-line doors and the End Users cards shall be transmitted around the system carried by the card;
e) Transactions, blacklists and End User audit trails shall be written to the card from the escutcheons it is presented to. This information will be relayed back to the head end server when the card is presented to an on-line system reader;
f) Information to be delivered to each door shall be added to the cards as they are presented at a designated point to be identified by the Supplier;
g) Door escutcheons shall be battery powered using freely available lithium batteries. These shall facilitate a minimum of 30,000 transactions;
h) The Authority's preference is that each unit shall be IP46 compliant, although the Authority will accept products with a reduced ingress protection rating for liquids;
i) Locking mechanisms shall be fully compatible with European profile cylinders;
j) Locking modes shall accommodate the following as a minimum;
    i. Standard, valid card presentation required to open;
    ii. Open, free passage for all;
    iii. Timed, door changes from open to standard at a pre-defined time;
    iv. Scheduled opening, locks will release and re-lock at pre-defined times during the day; and
    v. Toggle, card presentation required to unlock and lock;

20.7 The approximate number of Key Barrels required at each Affected Property shall depend on the size of the relevant Affected Property as follows:

a)	Small Affected Properties	2 Key Barrels
b)	Medium Affected Properties	4 Key Barrels
c)	Large Affected Properties	10 Key Barrels

KEY MANAGEMENT OPERATIONAL SERVICES

The Supplier shall:

20.8 upon instruction by the Authority, execute, utilising Supplier Personnel, the approved "Key Management Detailed Solution" in line with the values and behaviours referred to in Paragraph 3;

20.9 provide a custodian service of building access keys and alarm system codes, ensuring compliance with the Security Industry Authority and its licensing requirements;

20.10 issue keys to authorised Authority Personnel for access across the Affected Properties as appropriate;

20.11 during the Authority Opening Hours, provide a key holding service on the Affected Properties for building keys and Automated Access Control Systems; and

20.12 provide a Key Holding Response to situations requiring a key holder on both a planned and unplanned basis, to attend the Affected Properties 24 hours a day, 7 days a week, 52 weeks a year.

20.13 These shall include but not be limited to provision of access for Authority Representatives, providing suitable Response to fire alarms, lift alarms and security alarms.

20.14 The Supplier shall log faults with keys and locks across the Affected Properties, including lost keys or damage. Report lock and key issues to the Helpdesk and assist the relevant FM Supplier for access to facilitate repair.

20.15 The Supplier shall provide repair and maintenance of all existing key boxes from the Operational Service Commencement Date. Any work required shall be instructed by the Authority via the Change Control Procedure.

21 CAR PARK MANAGEMENT

21.1 The Authority requires a Car Park management service that effectively controls access to Car Parks within the Affected Property whilst minimising disruption to Authorised Persons and Vehicles. The Authority requires that the Supplier provides continuity of the existing Car Park Management service in operation across the Affected Properties from the Operational Service Commencement Date. The Authority requires that the Supplier provides a Replacement Car Park Management service that delivers improved efficiency, integration and value for money.

21.2 The Supplier shall:

INTERIM CAR PARK MANAGEMENT

INTERIM CAR PARK MANAGEMENT IMPLEMENTATION SERVICES

21.3 by the time stated in Annex A, provide for Approval a draft “Interim Car Park Management Detailed Solution” in line with Good Industry Practice, detailing the measures the Supplier shall take to continue the current arrangement for Car Park management at all Affected Properties. An indicative list of items to be included in this Interim Car Park Management Detailed Solution is included in Annex A;

INTERIM CAR PARK MANAGEMENT OPERATIONAL SERVICES

21.4 upon instruction by the Authority, execute, utilising Supplier Personnel, the approved “Interim Car Park Management Detailed Solution” in line with the values and behaviours referred to in Paragraph 3; and

21.5 provide an Interim Car Park Management service on all Affected Properties with a Car Park.

21.6 The existing Car Parks contain a range of control mechanisms, including barriers, Security Officers and conventional manually openable gates. A number have interfaces with AACS to allow entry and a number reply on a Security Officer to operate the barrier locally.

21.7 The Supplier shall:

21.8 take all reasonable steps to protect against theft of vandalism of vehicles parked on the Affected Property and attacks on users of the Car Park;

21.9 as a minimum, record the following information for all vehicles that access the Car Parks:

a) Time of entry;
b) Time of exit;
c) Duration of visit;
d) Vehicle registration, make, model and colour; and
e) Driver Full name,

and which shall only be required from the Operational Service Commencement Date where there are Supplier Personnel able to collect this information (for example, where there is a guard house or permanent Customer Support Officer on the Affected Property; or where there is an automated car park system that can be utilised to provide the information defined at Paragraph 21.9 above); and

21.10 ensure that the barrier/gate operation complies with all current and relevant HSE guidance. The Supplier shall allow for any upgrade work required to meet the recommendations.

REPLACEMENT CAR PARK MANAGEMENT

REPLACEMENT CAR PARK MANAGEMENT IMPLEMENTATION SERVICES

21.11 By the time stated in Annex A, the Supplier shall provide for Approval a draft "Replacement Car Park Management Detailed Solution" in line with Good Industry Practice, detailing how the Supplier will control and protect Car Parks within the Affected Property. An indicative list of items to be included in this Car Park Management Detailed Solution is included in Annex A.

21.12 During the Implementation Phase, the Supplier shall conduct an assessment of the Car Park barriers and associated equipment, which shall include an assessment for compliance with HSE guidance.

REPLACEMENT CAR PARK MANAGEMENT OPERATIONAL SERVICES

21.13 Upon instruction by the Authority, the Supplier shall execute, utilising Supplier Personnel, the approved "Replacement Car Park Management Detailed Solution" in line with the values and behaviours referred to in Paragraph 3.

21.14 The Replacement Car Park Management Detailed Solution shall deliver the following minimum requirements subject to the requirements identified in the Approved Security Plan:

a) Replace all existing AACS interfaces such that the Replacement AACS cards can be used to gain entry to the Car Park;
b) Where electrically controlled gates exists without AACS interface the Supplier shall propose solutions to incorporate AACS control;
c) At all entry points with AACS, an intercom shall be provided that connects to the Affected Property security control room or other agreed location with the Authority. This facility shall be able to remotely open the barrier/gate;
d) An overview camera shall be provided to allow remote operation and monitoring to be achieved; and
e) An optional driver image camera shall be provided for record purposes.

21.15 The Supplier shall:

21.16 take all reasonable steps to protect against theft of vandalism of vehicles parked on the Affected Property and attacks on users of the Car Park.

21.17 as a minimum, record the following information for all vehicles that access the Car Parks:

a) Time of entry;
b) Time of exit;
c) Duration of visit;
d) Vehicle registration, make, model and colour; and
e) Driver Full name;

ensure that the barrier/gate operation complies with all current and relevant HSE guidance. The Supplier shall allow for any upgrade work required to meet the recommendations.

22 TEMPORARY ADDITIONAL SECURITY PROVISION

22.1 The Authority requires that the Supplier provides temporary additional security services as requested by the Authority to enable the delivery of the Authority's Core Business which will include but is not limited to:

a) security for extended opening hours;
b) security for events held on the Affected Property such as high-profile events and meetings;
c) security for events held outside of the Affected Property;
d) attendance when project works are being carried out;
e) attendance when out-of-hours maintenance is being undertaken;
f) compliance with Authority's Unacceptable Customer Behaviour Policy (set out in Schedule 2.6 (Authority Policies)) and approved Unacceptable Customer Behaviour Detailed Solution;
g) any temporary change (does not warrant a new Security Threat and Risk Assessment and updated Security Plan) in Affected Property Risk Profile that warrants additional security measures e.g. short notice protests or demonstrations; and
h) any request for Visitor Escort or Authority Personnel Escort,

and the provisions of Clauses 13.14 to 13.18 of the Agreement shall apply to any such additional security services. For the avoidance of doubt, where the Authority requires Authority Personnel Escorts, such Authority Personnel Escorts shall be delivered by appropriately trained Security Officers and those Security Officers shall be required to travel with the relevant Authority Employees.

22.2 The minimum number of additional Security Officer hours within any single Security Officer shift requested by the Authority shall be 4 hours.

22.3 The Supplier shall:

<u>TEMPORARY ADDITIONAL SECURITY PROVISION OPERATIONAL SERVICES</u>

22.4 provide a proactive response to meet all requests from the Authority for temporary additional security provision and this service should be available, on request, 24 hours a day, 7 days a week, 365 days a year;

22.5 for all requests from the Authority for temporary additional security provision, assess the requirement (including an appropriate Risk Assessment) and provide for Approval an "Additional Security Plan" detailing appropriate additional security services to be delivered to satisfy the requirement, commensurate with security risk and at all times maximising value for money for the Authority;

22.6 upon instruction by the Authority, execute the Additional Security Plan in line with the values and behaviours referred to in Paragraph 3; and

22.7 ensure that, at no point, Operational Services and requirements as detailed in Affected Property's Security Plans are compromised by the requirement to deliver temporary additional security provision.

23 REPORTING REQUIREMENTS

23.1 The Authority requires the Supplier to provide accurate and timely reporting (to include data, Performance Indicators and any other such information required). This data shall be provided in a standard, accessible format to be used for, but not limited to, performance management and progress towards efficiency and organisational targets. The Authority requires that the Supplier provides reporting to enable the delivery of the Supply Chain Integrator' services and the Authority's Core Business which will include but not limited to the:

a) Financial Management Solution;
b) Performance Reporting Process;
c) Compliance Reporting Regime; and
d) Satisfaction Surveys.

23.2 The Supplier shall:

<u>REPORTING REQUIREMENTS IMPLEMENTATION SERVICES</u>

23.3 by the time stated in Annex A, provide for Approval a draft "Reporting Detailed Solution" in line with Good Industry Practice, detailing the process to be executed in delivery of a reporting solution. An indicative list of items to be included in this Reporting Detailed Solution is included in Annex A; and

<u>REPORTING REQUIREMENTS OPERATIONAL SERVICES</u>

23.4 upon instruction by the Authority, execute, utilising Supplier Personnel, the approved "Reporting Detailed Solution" in line with the values and behaviours referred to in Paragraph 3.

24 SECURITY PROJECTS AND CAPITAL PROGRAMME

24.1 The Authority requires that the Supplier will act as the sub-contractor for all project works relating to the Supplier Systems. The Authority expects to appoint Authority Supply Chain Members who will be responsible for the delivery of large projects, as required. Small projects will be delivered by the relevant FM Supplier. The high-level process flow for the completion of project works to be followed by the Supplier is included in Schedule 2.6 (Authority Policies) – Part 10.

24.2 In relation to all project works, for the Supplier Systems, the Supplier shall:

24.3 provide detailed design services (agreed in accordance with the Change Control Procedure). For the avoidance of doubt, the Charges for any such project work shall be calculated in accordance with Schedule 7.1 (Charges and Invoicing) and Schedule 7.7 (Financial Model);

24.4 take instruction from the Supply Chain Integrator, the relevant FM Supplier and all Authority Supply Chain Members responsible for project delivery;

24.5 support the programming of all project works (to be led by the Supply Chain Integrator);

24.6 complete all project works as per the instruction provided by the Supply Chain Integrator, the relevant FM Supplier and all Authority Supply Chain Members responsible for project delivery, to the agreed programme and at all times compliant with Good Industry Practice;

24.7 complete all required Tests (including Site Acceptance Tests and User Acceptance Test) necessary to complete instructed project works;

24.8 provide updates as required on the completion of the project works and report the successful completion of the project works; and

24.9 create and store records of all project works in accordance with Schedule 8.4 (Records Provisions).

25 SUSTAINABILITY

25.1 The Authority requires the Supplier to comply with government policy on sustainability and works cooperatively with other Authority Supply Chain Members to identify and capitalise on improvements across the Affected Property.

25.2 The Supplier shall:

SUSTAINABILITY IMPLEMENTATION SERVICES

25.3 note that the Authority would like to maximise the re-use of the existing installations to minimise the carbon footprint of the Supplier System and the amount of infrastructure and assets that has to be disposed of; and

25.4 consider the use of the following solutions and adopt them where ever possible:

a) Existing camera coaxial cable for new cameras using Ethernet and power over coaxial;
b) Existing AACS door containment and cabling for the replacement solution; and/or
c) Use of LED IR technology for camera and lighting.

25.5 The Supplier is free to propose any other sustainable solutions that they feel would be of mutual benefit to them and the Authority.

SUSTAINABILITY OPERATIONAL SERVICES

25.6 The Supplier shall:

25.7 comply with the “Energy Management Solution” as set by the Supply Chain Integrator. Comply with the Authority Energy Management policy and any subsequent government policy;

25.8 in line with the values and behaviours as detailed in Paragraph 3, collaborate with other Authority Supply Chain Members to enact and comply with sustainability efforts, initiatives and property re-locations;

25.9 take account of and comply with the Authority’s targets and commitments under current government sustainability policy and any subsequent government policy;

25.10 work with the Authority to deliver building efficiency policy and targets as required, including liaising with Authority Supply Chain Members and informing the Authority's property strategy;

25.11 liaise with the Authority Supply Chain Members and utilise all other data sources to make investment recommendations to the Authority for asset additions, substitutions and or replacements that will, over time, reduce costs, reduce emissions or optimise asset efficiency; and

25.12 liaise with the Authority and other Authority Supply Chain Members in the event of property or site changes to minimise impact on business as usual and ensure a smooth transition in and out of properties.

25.13 The Authority will advise on investment criteria on a year by year basis. Any reduction in cost may form part of the Savings mechanism in Schedule 7.6 (Savings Payments).

26 RESPONSE TO HEIGHTENED THREAT

26.1 The Authority requires enhanced security services, developing and executing operational procedures for specific events that may occur at an Affected Property to maintain the security and operational integrity of moderate risk Affected Properties (as defined by the Authority and/or security services) including those Affected Properties located within the Westminster Government Secure Zone or other Affected Properties as determined by the Affected Property's risk profile, which is subject to change from time to time or as directed by the Authority.

26.2 The Supplier shall:

RESPONSE TO HEIGHTENED THREAT IMPLEMENTATION SERVICES

26.3 by the time stated in Annex A, work with Nominated Authority Contacts and all relevant Government Bodies to jointly develop for Approval a draft "Response to Heightened Threat Detailed Solution" in line with Good Industry Practice, containing the operational procedures to be executed in the event of heightened threat across the Affected Properties. An indicative list of items to be included in this Response to Heightened Threat Detailed Solution is included in Annex A.

RESPONSE TO HEIGHTENED THREAT OPERATIONAL SERVICES

26.4 upon instruction by the Authority, execute, utilising Supplier Personnel, the approved "Response to Heightened Threat Detailed" in line with the values and behaviours referred to in Paragraph 3.

26.5 Following the execution of the Response to heightened threat Detailed Solution, submit a report (which will additionally assess the effectiveness of the Detailed Solution) to the Authority within 5 Working Days of request.

26.6 during times of heightened security, provide further detailed security provision as required by the Authority. This may include, but shall not be limited to, searching of all Authority Visitors' bags, cancellation of all non-essential events and checking of vehicles entering onto the Affected Properties or in Car Park areas, for potential suspect devices.

27 [REDACTED]

28 CONTRACT IMPROVEMENT & DEVELOPMENT

28.1 The Authority requires that the Supplier provides a “Contract Improvement and Development Detailed Solution” including details of how the Supplier shall be subject to continuous improvement and development activity for Approval by the Authority.

28.2 The Supplier shall:

28.3 by the time stated in Annex A, provide for Approval a draft Contract Improvement and Development Detailed Solution in line with Good Industry Practice. An indicative list of items to be included can be found in Annex A.

29 EXIT

29.1 The Authority requires that the Supplier provides a draft “Exit Detailed Solution” detailing the activity to be completed by the Supplier at either the expiry of the Term or where terminated early, on termination. An indicative list of items to be included in this Exit Detailed Solution is included in Annex A.

29.2 The Supplier shall:

29.3 by the time stated in Annex A, provide for Approval a draft “Exit Detailed Solution” in line with Good Industry Practice. An indicative list of items to be included in the Exit Detailed Solution is included in Annex A;

29.4 provide all reasonable assistance to the Authority in the preparation and completion of tender document and processes for the procurement of the Services, including preparation of all information required;

29.5 ensure all data, (records, documents or other information), created or used in performance of this Agreement complies with the Authority Records Management Policy, at Schedule 2.6 of this Agreement; and

29.6 at a time to be agreed with the Authority, handover all data, records and information pertaining to the Services to either the Authority or a new supplier (to be notified by The Authority). The format of the data shall be determined by the Authority and notified to the Supplier not less than 3 Months' prior to the date on which the Authority requires the data to be provided by the Supplier.

END.

ANNEX A – DETAILED SOLUTIONS REQUIRED

PART A – DETAILED SOLUTION TIMETABLE

Below is a full list of the Detailed Solutions required pursuant to this Statement of Requirements.

Forecast Contract Award Date: 11.12.17

Operational Readiness Test Date: 28.02.2018

Operational Services Commencement Date: 01.04.2018

No.	Detailed Solution Title	Delivery Phase (Implementation/Transformation/Operational)	Draft Detailed Solution Submission Date (Working Days from the Effective Date)
1	Implementation Plan Detailed Solution	Implementation	0
2	Account Management Detailed Solution	Implementation	10
3	Human Resources Detailed Solution	Implementation	10
4	Quality Management Detailed Solution	Implementation	15
5	Document Management Detailed Solution	Implementation	20
6	Health and Safety and Risk Management Detailed Solution	Implementation	40
7	Business Continuity and Disaster Recovery Detailed Solution	Implementation	80
8	Security Threat and Risk Assessment Detailed Solution	Transformation	15
9	Security Plan Detailed Solution	Transformation	20
10	Work Order Management Detailed Solution	Implementation	25
11	Control and Monitoring Facility Detailed Solution	Implementation	30

12	Existing Security Systems Detailed Solution	Implementation	40
13	Replacement Security Systems Detailed Solutions	Transformation	50
14	PMR Detailed Solution	Implementation	1
15	Lone Worker Detailed Solution	Implementation	10
16	Security System Network Detailed Solution	Additional Operational Service	70
17	Body Worn Cameras Detailed Solution	Additional Operational Service	As requested after 01.04.2018
18	Trialling Detailed Solution	Implementation	45
19	Testing, Commissioning and Handover Detailed Solution	Implementation	35
20	Existing Security Systems Support and Maintenance Detailed Solution	Implementation	40
21	Replacement Security Systems Support and Maintenance Detailed Solution	Implementation	50
22	Interim Visitor Management Detailed Solution	Implementation	20
23	Replacement Visitor Management Detailed Solution	Transformation	25
24	Incident Management Detailed Solution	Implementation	25
25	Key Management Detailed Solution	Implementation	10
26	Interim Car Park Management Detailed Solution	Implementation	30
27	Replacement Car Park Management Detailed Solution	Transformation	60

28	Reporting Detailed Solution	Implementation	10
29	Response to Heightened Threat Detailed Solution	Implementation	70
30	Unacceptable Customer Behaviour Detailed Solution	Implementation	30
31	Unacceptable Customer Behaviour Database Detailed Solution	Additional Operational Service	As requested after 01.04.2018
32	Contract Improvement & Development Detailed Solution	Implementation	After 01.04.2018
33	Exit Detailed Solution	Operational	After 01.04.2018

PART B – DETAILED SOLUTION REQUIREMENTS

Each Detailed Solution shall include but not be limited to the proposed contents below. It is expected that the Supplier will augment these suggestions to include other relevant, appropriate and value adding content. For the avoidance of doubt, any and all changes shall be Approved by the Authority.

All Detailed Solutions must be reviewed annually (or when weaknesses/improvements are identified) in consultation with the Authority Representative and provide a written report to the Authority for approval that critically assesses the current Detailed Solutions and provides recommendations for improvement.

Update the Detailed Solutions to reflect recommendations within 2 weeks of Approval from the Authority and subsequently ensure that all Supplier Personnel are briefed to utilise and adhere to the updated Detailed Solutions.

1. Implementation Plan Detailed Solution

a) **Authority Role** – The role the Authority is expected to play in the development, and operation of the Implementation Plan Detailed Solution, including comment, critique and Approval. The information and support that shall be required from the Authority to enable successful delivery of the Implementation Plan Detailed Solution.
b) **Programme Plan** – Programme including all the activities to be completed during the Implementation Phase with schedule, duration, key milestones, identified milestones, dependencies, buffer periods, critical path, resources and Tests.
c) **Resource Plan** – Detailing the implementation team to be deployed including organisational structure, roles and responsibilities, job descriptions, identification of any Key Personnel & assignment to any Key Roles. Detailing the resources to be deployed to deliver the Implementation Services.
d) **Governance Plan** – Detailing the proposed governance and performance approach for managing and reporting progress in accordance with the Security Services Agreement more generally and, specifically, the Implementation Plan Detailed Solution.

e) **Communication Plan -** Detailing the supplier's communication strategy, identifying approach, type of communication, communication method and frequency of communication with all affected parties including but not limited to: the Integrator; Authority; OGD Colleagues and other stakeholders during the Implementation Phase. The Supplier shall provide and maintain a register to record contact details to include email and telephone numbers.

f) **Existing Security Workforce Plan** – Detailing the approach to engagement, consultation, TUPE, training and review of the existing security workforce to include, as a minimum, the following:

   i. **Skills Assessment** – Detailing how the supplier shall assess the skills, current training and security clearance of existing Security Workforce. The supplier shall assess the existing workforce to ensure that all qualifications are up to date ahead of the Operational Services Commencement Date;

   ii. **Workforce Review** – Detailing how the supplier shall review existing Job Descriptions; Baseline Security Officer Deployment and all related Assignment Instructions;

   iii. **TUPE Delivery Plan** – Detailed plan for the execution of required TUPE transfer of existing Security Workforce to ensure a smooth transfer, compliance with all legal requirements, maximum engagement and staff retention and all risks are proactively managed.

   iv. **Uniform Plan** – Detailing all uniforms to be worn by the Security Workforce from the Operational Services Commencement Date;

   v. **Equipment Plan** – Detailing all functional equipment and Personal Protective Equipment to be provided to the Security Workforce and procedures for management and maintenance from the Operational Services Commencement Date;

   vi. **FM / Security Existing Role Review** – How the supplier shall collaboratively conduct a detailed review with the Facilities Management Supplier and Integrator of existing roles and tasks relating to Customer Support Officer & Receptionist Services to ensure service alignment with this Schedule 2.1 - Statement of Requirements.
   The Supplier shall conduct a review of the existing Customer Support Officer to determine, in collaboration with the Facilities Management supplier where these roles best fit and enact the TUPE transfer accordingly.

g) **Training Plan** - Detailing all the training the supplier will deliver during the Implementation Phase including the roles that will be provided with the training listed. This shall include all Supplier and Authority training as required within the Statement of Requirements to be delivered during the Implementation Phase.

h) **Recruitment Plan** – Detailing your approach to any required recruitment that will be required during the Implementation Phase and in preparation for the Operational Services Commencement Date detailing all actions, associated timeline and Supplier Personnel utilised for the recruitment exercise.

i) **Operational Readiness Test Methodology** – Detailing how the supplier will demonstrate to the Authority its readiness to deliver the Operational Services to the required standards from the Operational Services Commencement Date. To include proposed draft Test Strategy, draft Test Plans and Acceptance Criteria as required by the Statement of Requirements, Annex A and the Security Services Agreement.

2. Account Management Plan Detailed Solution

a) **Authority Role** - The role the Authority is expected to play in the development, roll-out and operation of the Account Management Detailed Solution, including comment, critique and

Approval. The information and support that shall be required from the Authority to enable successful delivery of the Account Management Detailed Solution.

b) **Resource Plan** – Detailing the Account Management structure to be adopted for the management of the DWP account including organisational structure, roles and responsibilities, job descriptions, identification of any Key Personnel & assignment to any Key Roles throughout the term of the contract. The structure will clearly demonstrate how all the Service Elements will be managed.

c) **Stakeholder Management Plan** - Mapping of key relationships between the Supplier and:
   i. The Authority,
   ii. the Integrator,
   iii. the Authority Supply Chain Members, and
   iv. any other related third parties.

d) **Governance Plan** - Meeting structure / schedule and terms of reference (liaising with the Integrator).

e) **Customer Service Plan** – Detailing how the supplier will receive, process and respond to customer feedback and complaints management process including, but not limited to, how:
   i. feedback from Authority Employees, is sought / gained by the Supplier regarding the experience of the Operational Services provided by the Supplier.
   ii. feedback from other Authority Supply Chain Members is sought / gained regarding the experience of the delivery of the Operational Services provided by the Supplier;
   iii. feedback is analysed and classified in order to identify complaints;
   iv. negative feedback and/or complaints are managed; and
   v. negative feedback and/or complaints are dealt with and escalated by and/or within the Supplier and/or any Supplier Related Party and through to the Authority.

f) **Communication Plan** - Detailing the supplier's communication strategy, identifying approach, type of communication, communication method and frequency of communication with the Integrator, Authority and other stakeholders throughout the term of the contract. Suppliers should include appropriate reporting and monitoring mechanisms. The Supplier shall provide and maintain a register to record contact details to include email and telephone numbers.

g) **Document Management Plan** - Specification of appropriate document management systems and practices as required by the Integrator to be implemented throughout the term of the contract.

h) **TUPE Account Management Approach** – Detail your approach to the building of your proposed Account Management Team who shall be responsible for the delivery of your Account Management Detailed Solution, as identified in your completed Account Management Organisation Chart to meet the requirements as defined in the Statement of Requirements.

3. Human Resources Detailed Solution

a) **Authority Role** - The role the Authority is expected to play in the development, roll-out and operation of the Human Resources Detailed Solution, including comment, critique and Approval. The information and support that shall be required from the Authority to enable successful delivery of the Human Resources Detailed Solution.

b) **HR Systems and Management Plan** – Detailing the HR systems to be implemented by the supplier for the management of HR data. Detailing how the supplier will manage staff including: employment policies and procedures; complaints process, staff grievances and behaviour policies; approach to SIA licensing and compliance with SIA initiatives.

c) **Training Plan** – Detailing how the supplier, based on the Existing Security Workforce Training Plan delivered during the Implementation Phase, will provide training for staff

throughout the term of the contract. Describe your approach to the development of staff. Update to Document Management Detailed Solution specifying the process to document all training and ensure all qualifications e.g. SIA licensing remain up to date. How the supplier will provide specialist and value adding training e.g. Behavioural and Mental Health training as required throughout the life of the contract. How the supplier will collaborate with other Security Providers to support Collaborative Incident Management.

d) **Recruitment Plan** – Approach, actions and timeline for all planned recruitment and any recruitment requirements that may arise during the Transformation and Operational phases. Describe your approach to the provision of required security clearance and vetting.
e) **Staff Retention Plan** – Strategy to promote the retention of staff detailing specific measures to be implemented by the supplier including how these will be managed and reviewed.
f) **Reward and Recognition Plan** – How the supplier will implement policies for reward and recognition of staff, ensure that these are properly used and how this will contribute to improved workforce motivation and performance.
g) **Life Chances Plan** – Detailing how the Supplier will comply with Government policies: Life Chances through procurement and PPN "Procurement for Growth".

4. Quality Management Detailed Solution

a) **Authority Role** - The role the Authority is expected to play in the development, roll-out and operation of the Quality Management Detailed Solution, including comment, critique and Approval. The information and support that shall be required from the Authority to enable successful delivery of the Quality Management Detailed Solution.
b) **Quality Management System Specification** – Developed specification, to be aligned and agreed with the Integrator, for the Quality Management System to be utilised throughout the term of the contract. To cover:
    i. How the Supplier will demonstrate adherence to the appropriate British, European or International Standards that may be applicable.
    ii. How the Quality Management System links with and to all other Detailed Solutions referred to within this Statement of Requirements.

5. Documents Management Detailed Solution

a) **Authority Role** - The role the Authority is expected to play in the development, roll-out and operation of the Document Management Detailed Solution, including comment, critique and Approval. The information and support that shall be required from the Authority to enable successful delivery of the Document Management Detailed Solution.
b) **Operational Procedures** - How the Supplier will update and develop the Document Management Plan included within the Implementation Plan Detailed Solution used during the Implementation Phase to reflect all requirements under the Approved Detailed Solutions for use, once Approved, throughout the term of the contract.

6. Health and Safety & Risk Management Detailed Solution

a) **Authority Role** - The role the Authority is expected to play in the development, roll-out and operation of the Health & Safety and Risk Management Detailed Solution, including comment, critique and Approval. The information and support that shall be required from the Authority to enable successful delivery of the Health and Safety & Risk Management Detailed Solution.

b) **Resource Plan** – Detailing the Health and Safety & Risk Management resource to be deployed including organisational structure, roles and responsibilities, job descriptions, identification of any Key Personnel & assignment to any Key Roles.

c) **Training Plan** - Detailing all the training the supplier will deliver to those roles and individuals identified in the Health and Safety Detailed Solution including the roles that will be provided with the training listed. This shall include all Supplier and Authority training as required within the Statement of Requirements to be delivered during the Implementation Phase.

d) **Dynamic Risk Assessments** – The methodology the supplier will utilise for conducting Dynamic Risk Assessments (DRAs) as required by the Statement of Requirements. Tenderers shall address the process for conducting DRA, the Supplier Personnel who will conduct DRAs and their skills and qualifications.

e) **Compliance** - How the Supplier shall ensure compliance with and enable the Authority to respond to changing threats and risks as specified within the HMG Security Framework, details can be found at: www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework. How statutory and legal compliance will be assured for the Suppliers own health and safety systems (including the interfaces with the Integrator and Authority) ensuring that assurance can be provided by the Supplier on request to satisfy legal compliance such as the Health and Safety at work Act and Management of Health and Safety at work regulations.

f) **Risk Assessment** - A Risk Assessment methodology complying with the Integrator's requirements, detailing what risk assessments will be carried out throughout the Term, on what frequency and or basis, how risks are identified, how risk assessments are carried out, quantified and prioritised.

   a. How risks will be managed and by who in order to reduce the likelihood of occurrence and or the impact should the risk occur.
   b. Input to the Integrator's Master Risk Register for every site each and every property. The Register shall be updated at least quarterly.
   c. Reporting format and outcomes of the risk assessments:
   d. Detail the approach for ensuring all follow-up work required subsequent to a risk assessment has been completed.
   e. Accident reporting and near-miss reporting systems and processes.
   f. Lone working processes and protocols.
   g. Hostile working environment processes and protocols.
   h. A range of contingency plans based on various service failure scenarios (scope of these to be agreed with the Authority).

7. Business Continuity and Disaster Recovery Detailed Solution

a) **Authority Role** - The role the Authority is expected to play in the development, roll-out and operation of the Business Continuity and Disaster Recovery (BCDR) Detailed Solution, including comment, critique and Approval. The information and support that shall be required from the Authority to enable successful delivery of the Business Continuity and Disaster Recovery Detailed Solution.

b) **Interface Plan** – Alignment to the Business Continuity and Disaster Recovery (BCDR) Detailed Solution of the Integrator supplier to cover:

   i. The Supplier shall prepare and deliver to the Authority for Approval a plan, which shall detail the processes and arrangements that the Supplier shall follow to:
      - ensure continuity of the business processes and operations supported by the Services following any failure or disruption of any element of the Services; and

- the recovery of the Services in the event of a disaster.

ii. The BCDR Plan shall be divided into three parts:
    - Part A which shall set out general principles applicable to the BCDR Plan;
    - Part B which shall relate to business continuity (the “Business Continuity Plan”); and
    - Part C which shall relate to disaster recovery (the “Disaster Recovery Plan”).

iii. Provide details of how the invocation of any element of the BCDR Plan may impact upon the provision of the Services and any services provided to the Authority.

iv. Contain an obligation upon the Supplier to liaise with the Authority, the Integrator and the Authority’s Supply Chain with respect to issues concerning business continuity and disaster recovery where applicable;

v. Detail how the BCDR Plan links and interoperates with any overarching and/or connected disaster recovery or business continuity plan of the Authority, Integrator and the Authority Supply Chain,

vi. Contain a communication strategy including details of an incident and problem management service and advice and help desk facility which can be accessed via multi-channels.

vii. Contain a risk analysis, including:
    - failure or disruption scenarios and assessments and estimates of frequency of occurrence;
    - identification of any single points of failure within the provision of Services and processes for managing the risks arising therefrom;
    - identification of risks arising from the interaction of the provision of Services and with the services provided by the Authority Supply Chain; and
    - a business impact analysis (detailing the impact on business processes and operations) of different anticipated failures or disruptions;

i. Set out key contact details (including roles and responsibilities) for the Supplier (and any Sub-Contractors), the Authority and Integrator;

ii. Identify the procedures for reverting to “normal service”;

iii. Set out method(s) of recovering or updating data collected (or which ought to have been collected) during a failure or disruption to ensure that there is no more than the accepted amount of data loss and to preserve data integrity;

iv. identify the responsibilities (if any) that the Authority has agreed it will assume in the event of the invocation of the BCDR Plan; and

v. The BCDR Plan shall be designed so as to ensure that:
    - the Services are provided in accordance with the Contract at all times during and after the invocation of the BCDR Plan;
    - the adverse impact of any disaster, service failure, or disruption on the operations of the Authority is minimal as far as reasonably possible;
    - it complies with the relevant provisions of ISO 22301, ISO 22313 and ISO 27002 and all other industry standards from time to time in force; and
    - there is a process for the management of disaster recovery testing detailed in the BCDR Plan.

vi. The Supplier shall test the BCDR Plan on a regular basis (and in any event not less than once in every contract year).

vii. The Supplier shall, within twenty (20) Working Days of the conclusion of each test, provide to the Customer a report setting out:
    - the outcome of the test;
    - any failures in the BCDR Plan (including the BCDR Plan's procedures) revealed by the test; and

- the Supplier's proposals for remedying any such failures.

viii. Develop process flows / maps detailing who does what should the BCDR Plan be invoked.

ix. How a transition to a new location will be managed including relative timeframes.

x. How will the property subject to the incident, (i.e. the “down” site) be secured during the vacation to ensure assets left in situ cannot be stolen or compromised.

xi. How the Services and Authority Supply Chain Services will be maintained whilst in the disaster recovery site.

xii. How the Services and Authority Supply Chain Services will be restored to the effected / vacated site.

xiii. Contingency plans for potential Authority Supply Chain Services failure including unavailability of those services.

xiv. The Suppliers corporate Business Continuity Management System (BCMS) for its own properties / operations and that of its supply chain.

8. Security Threat and Risk Assessment Detailed Solution

a) **Authority Role** - The role the Authority is expected to play in the development, roll-out and operation of the Security Threat and Risk Assessment Detailed Solution, including comment, critique and Approval. The information and support that shall be required from the Authority to enable successful delivery of the Security Threat and Risk Assessment Detailed Solution.

b) **Security Threat and Risk Assessment Methodology** – For assessing the Threat and Risk profile of each Affected Property to address, as a minimum, the following:

i. How the Supplier will undertake a local threat and risk assessment.

ii. How Authority employees and other stakeholders will be engaged at the start of the process.

iii. How site specific information shall be used, e.g. footfall / usage / incidents.

iv. How the Supplier will consider the impact of neighbouring properties and their use.

v. How the Supplier will analyse incident data.

vi. Link with the UCB policy and specifically addresses / plans for visitor planning.

vii. Identify how the risk assessment process aligns with Good Industry Practice including the Centre for Protection of National Infrastructure guidance such as the operational requirements process.

viii. How the Security Threat and Risk Assessments will be scored.

c) **Resource Plan** - Detailing the resources to be deployed including organisational structure, roles and responsibilities, job descriptions, identification of any Key Personnel & assignment to any Key Roles throughout the term of the contract.

d) **Programme Plan** – Programme including all the activities to be completed to deliver the Security Threat and Risk Assessments with schedule, duration, key milestones, identified milestones, dependencies, buffer periods, critical path and resources. The supplier must provide this in Microsoft Project format. During the Implementation Phase, the supplier shall agree and co-ordinate this Programme Plan with the Integrator, including all the Security Threat and Risk Assessments to be completed throughout the life of the contract.

e) **Reassessment Criteria** - The methodology for triggering an update to a Security Threat and Risk Assessment and frequency for the ongoing programme of Security Threat and Risk Assessment to include re assessment following the implementation of measures previously identified. Reassessments will be required following security vulnerabilities identified by DWP security assurance staff.

9. Security Plan Detailed Solution

a) **Authority Role** - The role the Authority is expected to play in the development, roll-out and operation of the Security Plan Detailed Solution, including comment, critique and Approval. The information and support that shall be required from the Authority to enable successful delivery of the Security Plan Detailed Solution.
b) **Security Plan Methodology** – Detailing the methodology and template to be used to produce a Security Plan for each Affected Property to include, as a minimum, the following:
    i. Description of the property and the services delivered;
    ii. How the Security Plan will address and relate to the Security Risk Assessment;
    iii. Detail of current security services provision;
    iv. Recommended security officer deployment, their responsibilities and competencies;
    v. Recommended security systems investment referring to the Approved Replacement Security Systems Detailed Solution;
    vi. Rational for any change to the current security services provision vs. recommended security services delivery;
    vii. How the Supplier will provide integration with the Control and Monitoring facility;
    viii. How the Security Plan aligns with Good Industry Practice including the Centre for Protection of National Infrastructure guidance such as the operational requirements process.
    ix. The additional or reduced security measures to be introduced through an updated Security Plan should there be a change in the UK Threat Level.
    x. How the Supplier will implemented additional or reduced security measures in response to a change in the UK Threat Level including communicating to all Supplier Personnel within 2 hours as per the agreed UK Threat Level Communications Procedure.
c) **Resource Plan** - Detailing the resources to be deployed including organisational structure, roles and responsibilities, job descriptions, identification of any Key Personnel & assignment to any Key Roles throughout the term of the contract.
d) **Programme Plan** – Programme including all the activities to be completed during the Implementation Phase with schedule, duration, key milestones, identified milestones, dependencies, buffer periods, critical path and resources. The supplier must provide this in Microsoft Project format. During the Implementation Phase, the supplier shall agree and co-ordinate this Programme Plan with the Integrator, including all the Security Plans to be completed throughout the life of the contract.
e) **Update Replacement Security Systems Programme Plan** – Update to Replacement Security Systems Programme Plan, to be agreed and co-ordinated with the Integrator, for the delivery of measures identified in the Security Plan.
f) **Cost Analysis** - The price for the delivery of the measures identified in the Security Plan, including a cost benefit analysis.

10. Work Order Management Detailed Solution

a) **Authority Role** - The role the Authority is expected to play in the development, roll-out and operation of the Work Order Management Detailed Solution, including comment, critique and Approval. The information and support that shall be required from the Authority to enable successful delivery of the Work Order Management Detailed Solution.
b) **Interface Plan** – Detailing the interface and integration of the Suppliers processes with the Integrator's Work Order management system to include, as a minimum, the following:
    i. The work order management process flow agreed with the Integrator.
    ii. The process for generating work order for Failures identified by the Supplier.

iii. How the work order management system will be utilised by any sub-contractors.
iv. Detail how Purchase Orders, Work Orders and Invoices will be dealt with in particular how the Supplier intends to interface and interact with the Integrator.

11. Control and Monitoring Facility Detailed Solution

a) **Authority Role** – The role the Authority is expected to play in the development, and operation of the Control and Monitoring Facility Detailed Solution, including comment, critique and Approval. The information and support that shall be required from the Authority to enable successful delivery of the Control and Monitoring Facility Detailed Solution.
b) **Operational Procedures** – Develop the processes and procedures for the control and monitoring of the Service Elements and the operation of a control and monitoring facility in accordance with Good Industry Practice.
c) **Resource Strategy** - Describe your approach to the deployment of resources within your proposed Control and Monitoring Facility in the delivery of the Services throughout the term of the contract. To cover:
   i. How the supplier will provide an out of hours response.
   ii. How the supplier will ensure 24/7 365 cover; as required.
   iii. How the supplier will manage sick leave, annual leave and training requirements to ensure continuity of service at all times.
d) **Resource Plan** – Detailing the resources to be deployed within the Control and Monitoring Facility including organisational structure, roles and responsibilities, job descriptions, identification of any Key Personnel & assignment to any Key Roles.
e) **Training Plan** – Detailing how the supplier will provide and record training for staff throughout the Transformation and Operational Phases.
f) **Transition Plan** – Detailing how the supplier will transition services from the interim Automated Access Control System Supplier as replacement AACS and IDS are rolled out including increasing the capacity of the Control and Monitoring Facility in order to meet additional requirements as Replacement Security Systems are installed for Affected Properties.

12. Existing Security Systems Detailed Solution

[REDACTED]

13. Replacement Security Systems Detailed Solution

[REDACTED]

14. Private Mobile Radio (PMR) Detailed Solution

a) **Authority Role** – The role the Authority is expected to play in the development, roll-out and operation of the PMR Detailed Solution, including comment, critique and Approval. The information and support that shall be required from the Authority to enable successful delivery of the PMR Detailed Solution.
b) **Component List** – Detailing all components utilised in the PMR system solution including the device and all accessories.
c) **System Architecture** – Providing a comprehensive and technically sufficient system architecture diagram showing the push to talk devices and the communications infrastructure.
d) **System Requirements** – Detailing how the proposed PMR solution will fully satisfy the requirements of the Statement of Requirements including but not limited to:

a. How the PMR solution will allow Security Officers to communicate via the PMR system inside and outside Affected Properties maintaining seamless connectivity;
b. How the PMR solution will be activated at the start of the contract when no access will be available to Affected Properties for works, installation and testing before the Operational Services Commencement Date.
c. How the PMR solution can provide additional services through the device and how these add value to the Authority.

15. Lone Worker Detailed Solution

a) **Authority Role** - The role the Authority is expected to play in the development, roll-out and operation of the Lone Worker Detailed Solution, including comment, critique and Approval. The information and support that shall be required from the Authority to enable successful delivery of the Lone Worker Detailed Solution.
b) **Component List** – Detailing all components utilised in the Lone Worker solution.
c) **System Requirements** – Detailed design and specification for proposed Lone Worker service. To cover:
   i. Detail how the proposed Lone Worker solution will fully satisfy the requirements of the Statement of Requirements including but not limited to:
   ii. How the solution will comply with the controls set out in BS8484, ISO/IEC 27001 and 27002.
   iii. How the supplier shall provide a flexible service that will fully satisfy the varied needs of Authority users.
   iv. How the Lone Worker service will effectively integrate with the other elements of the overall Replacement Security Systems Detailed Solution.
   v. How alerts and communications generated by the Lone Worker service will be connected to and monitored by the Control and Monitoring Facility, as contained within the Control and Monitoring Facility Detailed Solution.
   vi. How the supplier will protect, secure and store Authority Employees data and Authority Customer data generated by the Lone Worker Detailed Solution.
   vii. How the supplier will provide any new equipment required for the Lone Worker service to additional Authority Users throughout the contract Term.
   viii. How all software and/or equipment upgrades and patches will be provided throughout the life of the contract.
b) **Operational Procedures** – For the management of Incidents utilising the Lone Worker service such as alerts from Authority Employees to potential customer violence.
c) **Resource Plan** – Detailing the resources to be deployed to deliver the proposed Lone Worker service including any nominated sub-contractors including organisational structure, roles and responsibilities, job descriptions, identification of any Key Personnel & assignment to any Key Roles during the Transformation Phase & Operational Phase. Update to the Control and Monitoring Facility Resource Plan to meet the requirements generated by the Lone Worker service to cover:
   i. How the supplier will provide an out of hours response.
   ii. How the supplier will ensure 24/7 365 cover; as required.
   iii. How the supplier will manage sick leave, annual leave and training requirements to ensure continuity of service at all times.
d) **Training Plan** – Detailing how the supplier will provide and record training for Supplier Personnel throughout the Transformation and Operational Phases. To cover:
   i. How the supplier will provide training to Control and Monitoring Centre Facility and Security Officer's involved in the delivery of the Lone Worker service.

ii. How the supplier will provide training to Authority users.

e) **Reporting Plan** – Detailing dashboards for the self-reporting of supplier performance including Incident Management outcomes and response times.

f) **Deployment Programme** – Programme including all the activities for the deployment of the proposed Lone Worker service to Authority users with schedule, duration, key milestones, identified milestones, dependencies, buffer periods, critical path and resources. The supplier must provide this in Microsoft Project format. During the Implementation Phase, the supplier shall agree and co-ordinate this Programme Plan with the Integrator.

g) **Testing / Acceptance Methodology** – Develop and implement a robust Testing Methodology for all Lone Worker service that will include but not be limited to:

   i. FAT
   ii. SAT
   iii. UAT (90 Day operational test)
   iv. NB: all testing must be fully documented and made available to the Authority

h) **Maintenance and Support Plan** – Detailing the on-going support and maintenance offered by the supplier throughout the life of the Lone Worker service.

i) **Update Business Continuity and Disaster Recovery Detailed Solution** – Arrangements for the Lone Worker service to be included within the overall Business Continuity and Disaster Recovery Detailed Solution.

16. Security System Network Detailed Solution

[REDACTED]

17. Body-Worn Camera Detailed Solution

a) **Authority Role** - The role the Authority is expected to play in the development, roll-out and operation of the Body-Worn Camera Detailed Solution, including comment, critique and Approval. The information and support that shall be required from the Authority to enable successful delivery of the Work Order Management Detailed Solution.

b) **System Requirements** – Detailed design and specification for proposed Body-Worn Cameras. To cover:

   i. How the Replacement Security Systems comply with the controls set out in ISO/IEC 27001 and 27002.
   ii. How the Supplier shall provide a flexible service that will meet the varied needs of Authority users.
   iii. How the Body-Worn Camera service will effectively integrate with the other elements of the overall Replacement Security Systems Detailed Solution.
   iv. How recording and content generated by the Body-Worn Cameras will be uploaded, stored and maintained to be accessible by the Authority and Integrator.
   v. How the Supplier will protect, secure and store recording and customer data generated by the Body-Worn Camera Detailed Solution.
   vi. How the Supplier will provide any new equipment required for the Body-Worn Camera service to additional Authority users throughout the contract life.
   vii. How all software and/or equipment upgrades and patches will be provided throughout the life of the contract.

a) **Operational Procedures** – For the management of Incidents utilising the Body-Worn Camera service such as to capture unacceptable customer behaviour.

b) **Resource Plan** – Detailing the resources to be deployed to deliver the proposed Body-Worn Cameras including any nominated sub-contractors including organisational structure, roles

and responsibilities, job descriptions, identification of any Key Personnel & assignment to any Key Roles during the Transformation Phase & Operational Phase. Update to the Control and Monitoring Facility Resource Plan to meet the requirements generated by the Body-Worn Cameras to cover:

iv. How the supplier will provide an out of hours response.
v. How the supplier will ensure 24/7 365 cover; as required.
vi. How the supplier will manage sick leave, annual leave and training requirements to ensure continuity of service at all times.

c) **Training Plan** – Detailing how the supplier will provide and record training for Supplier Personnel throughout the Transformation and Operational Phases. To cover:

iii. How the supplier will provide training to Control and Monitoring Centre Facility and Security Officer's involved in the delivery of the Body-Worn Camera service.
iv. How the supplier will provide training to Authority users.

d) **Deployment Programme** – Programme including all the activities for the deployment of the proposed Body-Worn Cameras with schedule, duration, key milestones, identified milestones, dependencies, buffer periods, critical path and resources. The supplier must provide this in Microsoft Project format. During the Implementation Phase, the supplier shall agree and co-ordinate this Programme Plan with the Integrator.

e) **Reporting Plan** – Detailing dashboards for the self-reporting of supplier performance including Incident Management outcomes and response times.

a) **Testing / Acceptance Methodology** – Develop and implement a robust Testing Methodology for all Body-Worn Camera deployment that will include but not be limited to:

i. FAT
ii. SAT
iii. UAT (90 Day operational test)
iv. NB: all testing must be fully documented and made available to the Authority

f) **Maintenance and Support Plan** – Detailing the on-going support and maintenance offered by the supplier throughout the life of the Body-Worn Camera service.

g) **Update Business Continuity and Disaster Recovery Detailed Solution** – Arrangements for the Body-Worn Camera service to be included within the overall Business Continuity and Disaster Recovery Detailed Solution.

18. Trialling Detailed Solution

a) **Authority Role** - The role the Authority is expected to play in the development, roll-out and operation of the Trialling Detailed Solution, including comment, critique and Approval. The information and support that shall be required from the Authority to enable successful delivery of the Work Order Management Detailed Solution.

b) **Trialling Methodology** – Detailing how the supplier will conduct a trial of their proposed solution for the Trial Sites to demonstrate to the Authority that this proposed solution will achieve the required transformation, meeting or exceeding the standards set out in this Statement of Requirements. The supplier shall detail how this trial shall assess the effectiveness of the overall solution proposed by the suppliers for example the link with the Replacement Security Systems Detailed Solution. The supplier shall also proposed Trialling Assessment Criteria to critically assess the effectiveness of the trial and enable statistically robust reporting on outcome of the trial such as increased service performance reporting at the trial sites during the trial period.

c) **Trialling Report** – Detailing how the supplier will report upon the progress implementing the proposed solution at the trial sites and subsequently reporting upon the outcomes of the trial

against the Approved Trialling Criteria. The supplier shall provide a Trialling Report Template and specify the reporting frequency.

d) **Resource Plan** – Detailing the transformation team to be deployed to conduct, manage and report upon the trial including organisational structure, roles and responsibilities, job descriptions, identification of any Key Personnel & assignment to any Key Roles.

e) **Programme Plan** – Programme including all the activities to be completed during the trial period with schedule, duration, key milestones, identified milestones, dependencies, buffer periods, critical path and resources. The supplier must provide this in Microsoft Project format. The supplier shall identify milestones based upon their proposed solution for the trial sites.

f) **Communications Plan** – Detailing the suppliers approach to communications, identifying approach and frequency of communication with the Integrator, Authority and other stakeholders throughout the trial period.

19. Testing, Commissioning and Handover Detailed Solution

a) **Authority Role** - The role the Authority is expected to play in the development, roll-out and operation of the Testing, Commissioning and Handover Detailed Solution, including comment, critique and Approval. The information and support that shall be required from the Authority to enable successful delivery of the Testing, Commissioning and Handover Detailed Solution.

b) **Testing / Acceptance Methodology** – Develop and implement a robust Testing Methodology for the Security Systems which should include:

   a. FAT
   b. SAT
   c. ISAT
   d. UAT (90 Day operational test)
   e. System Load Testing
   f. Testing of fault management
   g. Any training requirements
   h. Operational Readiness Testing
   i. Handover
   j. Documentation
   k. NB: all testing must be fully documented and made available to the Authority

20. Existing Security Systems Support and Maintenance Detailed Solution

a) **Authority Role** – The role the Authority is expected to play in the development, and operation of the Existing Security Systems Support and Maintenance Detailed Solution, including comment, critique and Approval. The information and support that shall be required from the Authority to enable successful delivery of the Existing Security Systems Support and Maintenance Detailed Solution.

b) **Resource Plan** – Detailing the resources to be deployed to deliver the required support and maintenance of Existing Security Systems including any nominated sub-contractors including organisational structure, roles and responsibilities, job descriptions, identification of any Key Personnel & assignment to any Key Roles.

c) **Training Plan** – Detailing how the supplier will provide and record training for staff to deliver the required support and maintenance of Existing Security Systems and comply with the Standards.

d) **PPM Strategy** – Overarching strategy document setting out approach to the delivery of Planned Preventative Maintenance of existing security systems.

e) **PPM Programme Plan** – An annual Programme, to be agreed and co-ordinated with the Integrator, for all Planned Preventative Maintenance to be completed for existing Security Systems with the frequency, schedule of tasks, input requirements and maintenance Standards to be applied and resource requirements. Monthly reports of planned PPM tasks v actuals will be provided. During the Implementation Phase, the supplier shall agree this Programme Plan with the Integrator.
f) **Reactive Strategy** – Overarching strategy document setting out approach to the delivery of Reactive Maintenance of existing security systems.
g) **Spares Holding Plan** – Detailing how the Supplier will hold and manage sufficient spares to be able to deliver the agreed rectification periods.
h) **Network Diagnostic Test Procedure** – Detailed procedure for conducting the Network Diagnostic Test to provide all required information for accurate assessment of network performance and availability.

21. Replacement Security Systems Support and Maintenance Detailed Solution

a) **Authority Role** – The role the Authority is expected to play in the development, and operation of the Replacement Security Systems Support and Maintenance Detailed Solution, including comment, critique and Approval. The information and support that shall be required from the Authority to enable successful delivery of the Replacement Security Systems Support and Maintenance Detailed Solution.
b) **Resource Plan** – Detailing the resources to be deployed to deliver the required support and maintenance of Replacement Security Systems including any nominated sub-contractors including organisational structure, roles and responsibilities, job descriptions, identification of any Key Personnel & assignment to any Key Roles.
c) **Training Plan** – Detailing how the supplier will provide and record training for staff to deliver the required support and maintenance of Replacement Security Systems and comply with the Standards.
d) **PPM Strategy** – Overarching strategy document setting out approach to the delivery of Planned Preventative Maintenance of existing security systems.
e) **PPM Programme Plan** – An annual Programme, to be agreed and co-ordinated with the Integrator, for all Planned Preventative Maintenance to be completed for existing Security Systems with the frequency, schedule of tasks, input requirements and maintenance Standards to be applied and resource requirements. Monthly reports of planned PPM tasks v actuals will be provided. During the Implementation Phase, the supplier shall agree this Programme Plan with the Integrator.
f) **Maintenance –** Specifically relating to notification periods, likely down time, constraints and on site presence.
g) **Fault Management** – Based on the use of the Authority Network, including but not limited to, the following:
    a. How the System will integrate with the Authority's IT system to report faults
    b. Identifying where elements of the system will not report a fault to the Control and Monitoring Facility;
    c. Identifying the historic report creation capability/methodology.
h) **Spares Holding Plan** – Detailing how the Supplier will hold and manage sufficient spares to be able to deliver the agreed rectification periods. Detailing the spares requirement.
i) **Network Diagnostic Test Procedure** – Detailed procedure for conducting the Network Diagnostic Test to provide all required information for accurate assessment of network performance and availability.

22. Interim Visitor Management Detailed Solution

a) **Authority Role** - The role the Authority is expected to play in the development, roll-out and operation of the Incident Management Detailed Solution, including comment, critique and Approval. The information and support that shall be required from the Authority to enable successful delivery of the Interim Visitor Management Detailed Solution.
b) **Equipment and consumables**: identify all equipment and consumables including any branding, approach to stock holding centrally and locally.
c) **Protocols and procedures**: develop and document the protocols and procedures to be implemented to ensure seamless service from Operational Services Commencement. How the interim solution manages any risk around data protection and fully complies with current DPA and future GDPR legislation.
d) **Training Plan**: document the approach to training Supplier Personnel and Authority Personnel required to deliver the Services. Develop any communications required to the Authority Personnel if required.
e) **Records**: how the proposed solution will ensure accurate records are maintained for all visitors to the Affected Properties.

23. Replacement Visitor Management Detailed Solution

a) **Authority Role** - The role the Authority is expected to play in the development, roll-out and operation of the Incident Management Detailed Solution, including comment, critique and Approval. The information and support that shall be required from the Authority to enable successful delivery of the Replacement Visitor Management Detailed Solution.
b) **Equipment, systems and consumables:** identify all equipment, systems and consumables including any branding and the approach to stock holding centrally and locally.
c) **Specification and functionality:** Provide a detailed specification and functionality including any relevant diagrams and images of the proposed equipment. Identify any network, power and any other interfaces.
d) **Support, maintenance, reliability, back up and continuity of service**: Document the approach to support and maintenance, response time to faults and how the Authority Personnel will receive the training and ongoing support to ensure the smooth running of the solution. How any data stored will be backed up, maintained in a secure manner and made available to the Authority. How the solution manages any risk around data protection and fully complies with current DPA and future GDPR legislation.
e) **Protocols and procedures**: develop and document the protocols and procedures to be implemented. Include a description of the procedures and system functionality for the enrolment of visitors.
f) **Training Plan**: document the approach to training the Supplier Personnel and Authority Personnel required to deliver the Services. Develop any communications required to the Authority Personnel if required.
g) **Records**: how the proposed solution will ensure accurate records are maintained for all visitors to the Affected Properties.

24. Incident Management Detailed Solution

a) **Authority Role** - The role the Authority is expected to play in the development, roll-out and operation of the Incident Management Detailed Solution, including comment, critique and

Approval. The information and support that shall be required from the Authority to enable successful delivery of the Incident Management Detailed Solution.

b) **Incident Classification** – A developed and approved Incident Classification to be applied to the classification of all security incidents across the Authority Estate.
c) **Operational Procedures** – To be executed for each Incident Classification including escalation procedures including an Incident response process and response times.
d) **Incident Report Template** – To be used to record all Incidents and to be inputted into the Incident Reporting Tool. In the reporting of all Incidents provide Root Cause Analysis and recommendations for process improvements to the Authority.

25. Key Management Detailed Solution

a) **Authority Role** - The role the Authority is expected to play in the development, roll-out and operation of the Key Management Detailed Solution, including comment, critique and Approval. The information and support that shall be required from the Authority to enable successful delivery of the Key Management Detailed Solution.
b) **Resource Plan** – Detailing the resources to be deployed to deliver the Key Management service including any nominated sub-contractors including organisational structure, roles and responsibilities, job descriptions, identification of any Key Personnel & assignment to any Key Roles during the Transformation Phase & Operational Phase.
c) **Operational Procedures** – For the management of the Key Management service to cover:
    i. How the Supplier will provide an effective and secure system to manage and control the onsite storage, issue and retrieval of keys.
    ii. How the Supplier will control access to keys on the Affected Property.
    iii. How the Supplier will provide secure storage of keys on the Affected Property.
    iv. How the Supplier will record the issue and receipt of keys to Authority staff.
    v. How the Supplier will co-ordinate with Authority Supply Chain Members to provide access to the Affected Property, for example in cases of repair or emergency maintenance.
    vi. How the Supplier will undertake replacement of keys and repair of physical locks on Affected Property.
    vii. How in the event of an emergency, the supplier shall co-ordinate with Authority Supply Chain Members, Emergency Services and the Authority to ensure access to the site.

26. Interim Car Park Management Detailed Solution

a) **Authority Role** - The role the Authority is expected to play in the development, roll-out and operation of the Interim Car Park Management Detailed Solution, including comment, critique and Approval. The information and support that shall be required from the Authority to enable successful delivery of the Interim Car Park Management Detailed Solution.
b) **Operational Procedures** – For the management of Authority car parks to include:
    i. How the supplier will control access to car parks
    ii. How the supplier will confirm and verify vehicle and driver identity
    iii. How the supplier will minimise the impact of operational procedures for car park management upon users of Authority car parks particularly at peak periods
    iv. How the supplier will take all reasonable steps to protect against theft of vandalism of vehicles parked on the Affected Property

v. How the supplier will operate any car park equipment such as barriers and control points
vi. How the supplier will develop proposals to utilise technology and innovation to improve service delivery

c) **Resource Plan** – Detailing the resources to be deployed to deliver the car park management service including organisational structure, roles and responsibilities, job descriptions, identification of any Key Personnel & assignment to any Key Roles during the Transformation Phase & Operational Phase.
d) **Training Plan** – Detailing how the supplier will provide and record training for staff in the delivery of the car park management service throughout the Transformation and Operational Phases.

27. Replacement Car Park Management Detailed Solution

a) **Authority Role** - The role the Authority is expected to play in the development, roll-out and operation of the Replacement Car Park Management Detailed Solution, including comment, critique and Approval. The information and support that shall be required from the Authority to enable successful delivery of the Replacement Car Park Management Detailed Solution.
b) **Solution Requirements** – Detail how the proposed Car Park Management solution will fully satisfy the requirements of the Statement of Requirements including but not limited to:
   a. How the AACS shall be interfaced for a range of different Affected Property types where electrically operated car park barriers are provided.
   b. How an intercom system shall be implemented where they do not exist.
   c. How the Security System Network will be extended to the required locations and the need for new power supply infrastructure minimised.
   d. How you will assess the existing installations for compliance with HSE guidelines and what recommendations may be made as a result.

28. Reporting Detailed Solution

a) **Authority Role** - The role the Authority is expected to play in the development, roll-out and operation of the Reporting Detailed Solution, including comment, critique and Approval. The information and support that shall be required from the Authority to enable successful delivery of the Reporting Management Detailed Solution.
b) **Interface Plan** – Alignment to the Reporting Detailed Solution of the Integrator supplier to detail how the supplier will manage a database to include the recording, collating, storage and analysis of data for source to include:
   xv. Security systems, including for existing and replacement systems (excluding existing arrangements for access control).
   xvi. Visitor management
   xvii. Access control
   xviii. Faults and issues with equipment and systems
   xix. Incident reports
   xx. Risks
   xxi. Key management
   xxii. Performance management indicators
   xxiii. Security Officer hours
   xxiv. Work orders
   xxv. Any other relevant measures required by the Authority

c) In what format the Supplier shall regularly report and present data to the Authority and Integrator as required.
d) How the Supplier shall manage its reporting system to ensure it is up to date, accurate and others.
e) How the Supplier shall make available to the Authority all requested data and analysis on a timely basis.
f) How the Supplier will prepare reporting for Integrator solutions and products as required.
g) How the Supplier shall comply with the Integrator's requirements for performance management including completing the Customer Satisfaction Survey.
h) How the Supplier's reporting database and processes shall interact with the System for accurate, timely and organised database management.
i) How the Supplier shall report incidents and alerts on the Affected Property, to comply with requirements set out in the Incident Management Detailed Solution.
j) Resourcing Plan for staff to deliver the reporting requirements for the Authority and Integrator.
k) How reporting will comply with Authority policy for records management.

29. Response to Heightened Security Threat Detailed Solution

a) **Authority Role** - The role the Authority is expected to play in the development, roll-out and operation of the Security Systems Network Detailed Solution, including comment, critique and Approval. The information and support that shall be required from the Authority to enable successful delivery of the Response to Heightened Security Threat Detailed Solution.
b) **Heightened Threat Strategy** – Identification of potential sources of Heightened Security Threat and the development of strategies including additional security measures and processes to be deployed to minimise risk and impact of the sources of Heightened Threat.

30. [REDACTED] Detailed Solution

31. [REDACTED] Detailed Solution

32. Contract Improvement & Development Detailed Solution

a) **Authority Role** - The role the Authority is expected to play in the development, roll-out and operation of the Contract Improvement & Development Detailed Solution, including comment, critique and Approval. The information and support that shall be required from the Authority to enable successful delivery of the Contract Improvement & Development Detailed Solution.
b) **Interface Plan** – Alignment to the Contract Improvement & Development Plan of the Integrator supplier to cover:
    i. Recommend changes to the estate, the way estates and FM is delivered and or; investment recommendations to save money longer term or improve service delivery.
    ii. Systematically address areas of un-Satisfactory performance through root-cause analysis and process (re)design.
    iii. Actively seeking improvement recommendations from the DWP Estates Supply Chain.
    iv. Utilise a range (to be agreed with DWP) of external benchmarking data-points and or sources to identify potential areas of improvement (or to flag good practice).
    v. Be used to demonstrate the on-going value for money of the Integrator Service and the wider DWP Estates Supply Chain.

vi. Quantify the cost / benefit of all improvement and development tasks.
vii. Record all value adding activity undertaken throughout the DWP Estates Supply Chain and enable performance management of these tasks.
viii. Be formally reviewed every 6 months at a time to be agreed with DWP.

33. Exit Detailed Solution

a) **Authority Role** - The role the Authority is expected to play in the development, roll-out and operation of the Exit Detailed Solution, including comment, critique and Approval. The information and support that shall be required from the Authority to enable successful delivery of the Exit Detailed Solution.
b) **Programme Plan** – Programme including all the activities within the Exit Detailed Solution with schedule, duration, key milestones, identified milestones, dependencies, buffer periods, critical path and resources required (to be updated within 20 working days upon either Party serving Termination Notice and or within 6 months from the date of Contract expiry). A timetable and critical issues for providing assistance during termination and any charges that would be payable.
c) **Demobilisation Plan** – Identify what tasks will be completed in order to effectively demobilise the Contract ensuring minimal disruption to the Authority Core Business.
d) **Resource Plan** – Identify what supplier resources will be deployed to execute the Exit Detailed Solution.
e) **Data Transfer Plan** – Detail how data used within the suppliers and Integrator's System (and other ways of working within the Suppliers operating model) will be transferred from and to the incoming / new systems. How the Exit Information is obtained, which includes but is not limited to the information provided by the Security Provider to the Integrator, for which the Security Provider is responsible:
    i. details of the Service(s);
    ii. a copy of the Registers, updated by the Supplier up to the date of delivery of such Registers;
    iii. an inventory of Authority Data in the Supplier's possession or control;
    iv. details of any key terms of any third party contracts and licences, particularly as regards charges, termination, assignment and novation;
    v. a list of on-going and/or threatened disputes in relation to the provision of the Services;
    vi. to the extent permitted by applicable Law, all information relating to Transferring Supplier Employees required to be provided by the Supplier under this Agreement;
    vii. such other material and information as the Authority shall reasonably require.
f) **TUPE Plan** – Detailed plan and programme for the execution of TUPE transfer of Security Workforce to new suppliers to ensure: all milestones are achieved, maximum engagement and staff retention and all risks are proactively managed.
g) **Final Account** – How the requirements relating to the final account (as referenced in the Contract) will be executed. How the requirements of the Contract and in particular Schedule 8.5 will be accommodated and facilitated by the Exit Detailed Solution.
h) **Management Structure** – to be employed during the Termination Assistance Period.
i) **Services Transfer** – How the Services will transfer to the Replacement Supplier and/or the Authority, including details of the processes, documentation, data transfer, systems migration, security and the segregation of the Authority's technology components from any technology components operated by the Supplier or its Sub-contractors (where applicable).
j) **Termination Services** – The scope of the Termination Services that may be required for the benefit of the Authority (including such of the services set out in Annex 1 as are applicable).

k) **Requests** – Procedures to deal with requests made by the Authority and/or a Replacement Supplier for Staffing Information.

PART C – DETAILED SOLUTION TRIALLING REQUIREMENTS

No.	Detailed Solution Title	Required for Operational Readiness Test (yes/no)	Trialling Requirement (yes/no and Trial number as applicable)
1	Implementation Plan Detailed Solution	Yes – delivery against Implementation Plan Detailed Solution during Implementation Phase	No
2	Account Management Detailed Solution	No	Yes
3	Human Resources Detailed Solution	No	Yes
4	Quality Management Detailed Solution	No	Yes
5	Document Management Detailed Solution	No	Yes
6	Health and Safety and Risk Management Detailed Solution	No	Yes
7	Business Continuity and Disaster Recovery Detailed Solution	No	No
8	Security Threat and Risk Assessment Detailed Solution	No	Yes
9	Security Plan Detailed Solution	No	Yes
10	Work Order Management Detailed Solution	No	Yes
11	Control and Monitoring Facility Detailed Solution	No	Yes
12	Existing Security Systems Detailed Solution	No	Yes
13	Replacement Security Systems Detailed Solutions	Yes – Trial 1	No

14	PMR Detailed Solution	Yes – PMR Trial	Yes
15	Lone Worker Detailed Solution	No	Yes
16	Security System Network Detailed Solution	No	Yes
17	Body Worn Cameras Detailed Solution	Yes – Trial 2 (if instructed by the Authority)	No
18	Trialling Detailed Solution	No	Yes
19	Testing, Commissioning and Handover Detailed Solution	No	Yes
20	Existing Security Systems Support and Maintenance Detailed Solution	No	Yes
21	Replacement Security Systems Support and Maintenance Detailed Solution	No	No
22	Interim Visitor Management Detailed Solution	No	Yes
23	Replacement Visitor Management Detailed Solution	Yes – Trial 2	No
24	Incident Management Detailed Solution	No	Yes
25	Key Management Detailed Solution	No	Yes
26	Interim Car Park Management Detailed Solution	No	Yes
27	Replacement Car Park Management Detailed Solution	Yes – Trial 2	No
28	Reporting Detailed Solution	No	Yes

29	Response to Heightened Threat Detailed Solution	No	No
30	Unacceptable Customer Behaviour Detailed Solution	No	No
31	Unacceptable Customer Behaviour Database Detailed Solution	Yes – Trial 2 (if instructed by the Authority)	No
32	Contract Improvement & Development Detailed Solution	No	No
33	Exit Detailed Solution	No	No