Department for Work & Pensions

SCHEDULE 2

STATEMENT OF REQUIREMENTS

Version 0.8

January 2017

CONTENTS

1. DEFINITIONS

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

"**Affected Property**" means	Sites and/or properties within the Authority's property portfolio (the current estate portfolio is included in Schedule _ which is subject to change prior to contract award) in scope for the relevant clause as detailed within this Statement of Requirements.
"Appropriate Vehicles" means	Vehicles provided by the Supplier to undertake the duties identified under the Service Elements.
"**Assignment Instructions**" means	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.
"**Automated Access Control System" (AACS)** means	The electronic system and associated equipment utilised to centrally control access and egress to the Affected Property.
"**Authorised Persons**" means	Persons authorised either by the Authority or other persons so authorised to be working on the Affected Property.
"**Authorised Vehicles**" means	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**" means	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**" means	Members of the public who may access the Authority's services or receive benefits.
"**Authority Employees**" means	Persons employed by the Authority which shall include permanent, temporary and contractor staff.
"**Authority Opening Hours**" means	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 Representatives**" means	Those named Authority Employees who are authorised to act on behalf of the Authority as notified to the Supplier from time to time.
"**Authority Supply Chain Members"** means	All other Suppliers contracted or delivering services on the Affected Property who collectively shall form part of the Authority estates services supply chain.

"**Baseline Staff Deployment**" means	The number of Supplier Personnel deployed and the number of hours incurred by each member of the Supplier Personnel directly in the delivery of the Services as defined by the Authority at the Commencement Date within Annex L – Baseline Security Officer Deployment to this Schedule 2.1 (Statement of Requirements).
"**CCTV**" means	Closed Circuit Television system used around the perimeter of Affected Properties; within Public Waiting Areas and at vulnerable/key points: (a) In the main, standard CCTV will be employed with all weather and light level capability; (b) CCTV will be monitored by the Supplier and could be linked to intruder detection systems (IDS) and other alarms.
"**Commencement Date**" means	Date for the Commencement of the service delivery; assumed 1st April 2018.
"**Contract Period**" means	The full term of the contract which shall be the date from contract award through to contract expiry or termination.
"**Contract Start Date**" means	The effective start date of the contract as signed and executed by both parties.
"**Control and Monitoring Facility"** means	A central control room to provide the monitoring, management and communication required to deliver the Service Elements.
"**Emergency**" means	A state of heightened security or business risk as a result of an Incident or the notification or alert generated by security systems.
"**Emergency Services**" means	Police, Fire Brigade or Ambulance Services.
"**Enrolment**" means	The procedures to be executed by the Supplier relating to the creation, addition and amendment of data utilised by the Automated Access Control System.
"**Existing Security Systems**" means	Those security systems including all hardware and equipment that form part of the individual security systems installed prior to the Commencement Date at each Affected Property.
"**Factory Acceptance Testing**" means	The test which shall be conducted to determine and document the equipment hardware and software operates according to its specification, covering the following key areas: (a) functional; (b) fault management; (c) communications; (d) interface requirements.

"**Furniture, Fixtures and Equipment**" or "**FFE**" means	Movable furniture, fixtures, or other equipment that have no permanent connection to the structure of a building or utilities.
"**Good Industry Practice**" means	In accordance with British Standards, SIA, BSIA guidance & ISO Standards and all recognised industry standards and other similar standards.
"**Government Response Level**" means	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**" means	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.
"**Implementation Services**" means	Services delivered during the Implementation Phase which is the period from Contract Start Date until the Operational Services Commencement Date.
"**Incident**" means	BS 7958:2015 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**" means	BS ISO/IEC 27001:2013 Information Security Management Part 2, Specification for Information Security Management Systems, or the equivalent DWP publication when available.
"Integrator" means	The supplier appointed by the Authority to monitor and manage the Authority's Supply Chain Members. For further information on the role of the Integrator, refer to Schedule __.
"Interim Automated Access Control System" means	The existing Automated Access Control System installed on the Affected Property as specified in Schedule _. For the avoidance of doubt, the Authority intends to contract with another supplier for the operation and maintenance of the existing automated access control system i.e. as currently installed at each Affected Property. The Existing Automated Access Control System Exclusions at point 13.4 shall apply,

	which includes: enrolling of new employees and maintaining appropriate records, monitoring of automated access control systems and intruder detection systems alarms, planned and reactive maintenance of the system (automated access control system only). The Authority intends this only as an interim arrangement whilst a new automated access control system is installed which shall be executed as per the Approved Replacement Security Systems Detailed Solution.
"**KPI**" means	Key Performance Indicator as set out in Schedule 2.2 (Performance Levels).
"**Milestone**" means	An event or task described in the Implementation Plan Detailed Solution which, if applicable, shall be completed by the relevant Milestone Date.
"**Milestone Date**" means	The target date set out against the relevant Milestone in the Implementation Plan Detailed Solution by which the Milestone must be achieved.
"**Milestone Payment**" means	A payment identified in Schedule 7.1 (Charges and Invoicing) to be made following the issue of a Milestone Achievement Certificate and Milestone Payments shall be construed accordingly.
"**Mobile Patrol**" means	BS 7499:2013 Assignment whereby a Security Officer performs various duties but is not solely assigned to one location or premises.
"**Month**" means	A calendar month and monthly shall be interpreted accordingly.
"**Operational Services**" means	Services delivered during the operational phase which is the period from the Commencement Date until expiry / contract termination.
"**Optional Services**" means	Services described as such in Schedule 2.1 (Statement of Requirements) which are to be provided by the Supplier if instructed by the Authority in accordance with _____ (Optional Services).
"**Other Government Departmental Colleagues**" (or "**OGD Colleagues**") means	The personnel of other Governmental Departments who may occupy or use the Affected Property.
"**Other Security Guarding Contractors**" means	Those contractors employed by other parties to secure their sites and associated areas e.g. at Authority co-location sites and neighbouring properties.
"**Patrols**" means	Internal and external patrols at each Affected Property.
"**Performance Management System**" means	a) the document set out in Annex 1 to Schedule 2.2 (Performance Levels); and/or b) the performance management system to be included in each Authority supply chain contract,

	as the context so requires.
"**Perimeter Patrols**" means	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. To be completed in accordance with Good Industry Practice.
"**Plan**" (and any term suffixed by "**plan**") means	Those Plans listed throughout Schedule 2.1 (Statement of Requirements) as specifically used in Annex A.
"**Process**" (and any term suffixed by "**process**") means	Those processes required to satisfactorily perform the Services listed throughout Schedule 2.1 (Statement of Requirements).
"**Prohibited Items**" means	Prohibited items include for example firearms, alcoholic beverages.
"**Project**" is defined as	a) having a minimum total spend of £5,000, (including VAT); b) 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; and c) being a project where less than 50% of the total costs relate to I.T. (otherwise it will be classed as an **IT Technology Project** and will be outside the scope of this Statement of Requirements). A Project does not include: d) Maintenance costs or provision of spares, or; e) Rent, rates, service charges, dilapidation costs and payments made to landlords to surrender building leases.
"**Public Waiting Areas**" means	The areas within Affected Property's that are open to the public, specifically Authority Customers from which the Authority delivers the Authority Core Business.
"**Radio System**" means	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.
"**Rectification Period**" means	The period of time in which the Supplier must successfully rectify any fault or issue with the Security Systems as detailed in Annex K.
"**Report**" (and any term pre or suffixed by "**report**") means	Those reports required by the Authority listed throughout Schedule 2.1 (Statement of Requirements).
"**Response Team**" means	Appropriate Supplier Personnel equipped and with Appropriate Vehicles.
"**Response Time**" means	Those timeframes referred to in the Schedule 2.2 (Performance Levels) and applied to all Work Orders.

"**Serious Incidents**" means	Incidents that have been classified as Serious Incidents in line with the Security Incident Classification that will be subject to the Serious Incident Escalation Process.
"**Security Incident Classification**" means	The agreed classification to be applied to categorisation of all Security 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 Escalation Process**" means	The process to be followed in the event of Serious Incident for escalation to and assessment by the Authority.
"**Serious Incident Review Group**" means	The escalation group for the review of all Serious Incidents with representatives from the Authority, Integrator, Supplier, trade unions and other Authority Supply Chain Members.
"**Security Officer**" means	BS 7499:2013 Trained person who performs duties at a static site or on a mobile patrol.
"**Security Officer Team Leader**" means	Those Security Officers responsible for the management and leadership of Security Officer teams.
"**Security Plan**" means	The site specific strategic document produced by the Supplier following the Security Threat and Risk Assessment. This defines for each Affected Property, the specific security measures deployed / to be deployed including security systems, fire systems and Security Officers.
"**Security Systems**" means	Those electronic and physical systems installed, maintained and operated on the Affected Property as detailed in Section 13: Security Systems of this Schedule 2.1 (Statement of Requirements).
"**Service Credits**" means	Credits payable by the Supplier to the Authority due to the occurrence of 1 or more performance failures.
"**Services**" means	(a) the Implementation Services; (b) the Transformation Services (c) the Operational Services; and (d) any other services as otherwise required by or reasonably to be inferred from this Agreement.
"**Service Element**" means	The individual services as identified in Schedule 2.1 (Statement of Requirements) which collectively form the Services.
"**SIA**" means	Security Industry Authority or any regulating authority which may replace it.
"**Site Acceptance Testing**"	The first phase of the testing process during which the

means	Authority and system 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; (e) interface requirements. The procedure shall be developed by the Supplier for Approval including pass / fail criteria.
"**SLA**" means	Service Level Agreement.
"**Supplier Personnel**" means	Those people employed by the Supplier and all sub-contractors for the purposes of performance of the Services.
"**System**" means	System to be provided by the 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.
"**Training**" means	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.
"**Transformation Services**" means	Services delivered during the transformation phase which the Authority expects to be the period two months from Contract Start Date until 18 months after the Commencement Date.
"**UK Threat Level**" means	The OFFICIAL current level of terrorism threat within the UK as determined by the UK Government, currently the Joint Terrorism Analysis Centre (JTAC) and available here https://www.mi5.gov.uk/threat-levels to be updated and changed from time to time.
"**Unacceptable Customer Behaviour**" means	Classification applied to certain high-risk Authority Customers by the Authority with a history of violence or aggressive behaviour who will be subject to the Unacceptable Customer Behaviour Policy as defined by the Authority in (Annexes F & G).
"**Unauthorised Persons**" means	Personnel who have failed to pass a screening or pre-screening process or who are otherwise not approved by the Authority and who are not to be permitted upon the Affected Property at any time.
"**Unauthorised Vehicles**" means	Vehicles that have failed to pass an authorisation process and which are not to be permitted upon the Affected Property at any time.
"**Updates**" means	In relation to any software and/or any Key Deliverable

	means a version of such item which has been produced primarily to overcome defects in, or to improve the operation of, that item.
"**Upgrades**" means	Any patch, new release or upgrade of software and/or a Key Deliverable, including standard upgrades, product enhancements, and any modifications, but excluding any Update which the Supplier or a third party software supplier (or any Affiliate of the Supplier or any third party) releases during the term.
"**User Acceptance Testing**" means	The last phase of the testing process during which the Authority and system 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.
"**User Group**" means	Has the meaning given in Annex B to Schedule 2.1 (Statement of Requirements).
"**Vehicle Record**" means	Record of Vehicles accessing and egressing from the Affected Property as set out in this Schedule 2.1 (Statement of Requirements).
"**Westminster Government Secure Zone**" means	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, Security Services and GCHQ.
"**Work Order**" means	A formal notification of activity required as issued by the 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 Contract Period.
"**Working Day**" means	Any day other than a Saturday, Sunday or public holiday in England and Wales.

2. INTRODUCTION

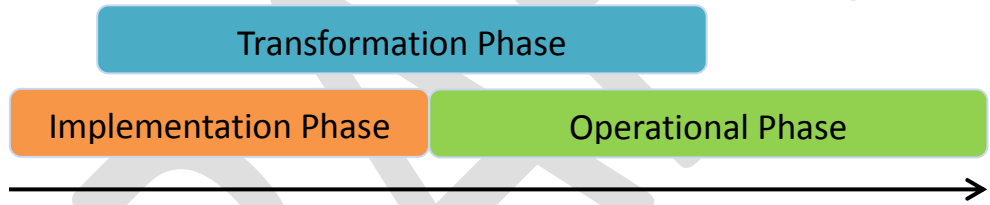
2.1 The Authority requires the Supplier, using the standard of care required by the Contract, to carry out all activities, operations and functions expressly stated in or reasonably to be inferred as required by this Schedule 2.1 (Statement of Requirements) in order to deliver the comprehensive security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



Definitions:

Implementation Services - Services delivered during the Implementation Phase which is the period from Contract Start Date until the Operational Services Commencement Date.

Transformation Services – Services delivered during the Transformation Phase which the Authority expects to be the period two months from Contract Start Date until 18 months after the Operational Services Commencement Date.

Operational Services – Services delivered during the Operational Phase which is the period from the Operational Services Commencement Date until expiry / contract termination.

2.5 The Services consist of all the individual Service Elements as listed in Section 8: Health and Safety & Risk Management through to Section 26: Unacceptable Customer Behaviour, inclusive and defined within this Statement of Requirements.

2.6 The Authority requires the Supplier to deliver the Services to further the following high level 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 Property making the optimal use of Security Systems 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's operating landscape, 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 Section 5.2) and continue to deliver value for money throughout the term of the Contract.
f) To enable a smooth transition and successful exit from the PRIME contract and a managed transition to the target operating model.
g) By working closely with operations, ensure customer service, performance and people engagement is protected, wherever possible, during Implementation.

2.7 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 template 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 Property;
d) Management of Incidents and Emergencies as they occur across the Affected Property;
e) provision and maintenance of a comprehensive range of Security Systems;
f) Security Systems capable of integrating and/or interfacing with other related systems including but not limited to those of the Authority and Authority Supply Chain Member(s);
g) Management of Work Orders associated with the Affected Property utilising the Authority's System as provided by the Integrator and reporting on the progress of completion of services required from such Works Orders.
h) deliver value for money throughout the Term;
i) management to enable the delivery of the "the Authority 2020 Vision", (including but not limited to extended operating hours, digital transformation and SMART Working);
j) 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;
k) compliance with all statutory, regulatory and any relevant policies, processes and standards;
l) 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.

SUPPLIER'S ROLE

2.8 The Supplier will provide the Services as set out in this Statement of Requirement and in accordance with the Contract.

THE AUTHORITY'S ROLE

2.9 The Authority shall:

a) act as a client and recipient of the Services and the Authority Supply Chain Services;

b) will utilise the Integrator to manage the Supplier on its behalf and as such from time to time audit the systems, processes, detailed solutions, plans and ways of working employed by the Supplier;
c) seek to be an exemplar organisation in relation to health and safety and require the highest level of health and safety legislation;
d) own and be accountable for health and safety policy;
e) provide policy in relation to the Affected Property, including security policy such as Unacceptable Customer Behaviour policy (ref); other Government / Authority security policies and occupier policy such as energy consumption targets and other sustainability related issues;
f) be responsible for financial planning, budgeting and internal recharging;
g) be responsible for stakeholder engagement, management and M.I. Reporting to these stakeholders, (based on M.I. reporting by provided by the Integrator to the Authority and supported by the Supplier);
h) provide human resources and operational excellence in respect of Authority Employees; and
i) payment of invoices and overall budget control.

INTEGRATOR'S ROLE

2.10 The Authority will appoint an independent third-party, the "Integrator" to act as the Authority's programme manager, project manager and contract administrator for the Security Services contract. It is intended that the Integrator will act as the Authority Representative and, where applicable, may act as the Authority's agent under the Contract.

2.11 The Integrator will monitor and manage the Authority's Supply Chain Members to ensure:

a) Compliance by Suppliers of their respective contractual obligations;
b) the Programme (as defined in the Contract) is 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 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 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's Customers, the Authority Employees 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's Employees can support, challenge and inspire the Authority's Customers to improve their lives and help each other to make a difference.
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 Employees, 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 values:

a) the health and safety of individuals is the Authority's primary concern. The Supplier shall deliver the Services and ensure each Authority Supply Chain Member delivers the Authority Supply Chain Services with due regard for 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) ensuring each member of the supply chain operates in a fair and consistent manner, respecting each party's right to make a fair and reasonable profit whilst aiming to reduce the overall cost of occupancy for the Authority and delivering all the required contractual obligations;

c) 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;

d) a full recognition that a successful supply chain will require high levels of cooperation between the Authority, Integrator, Supplier and Authority Supply Chain Members;

e) 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;

f) 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 with Authority policy 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 (ref.).

4 IMPLEMENTATION

IMPLEMENTATION SERVICES

4.1 Implementation Services shall be delivered during the Implementation Phase which is the period from Contract Start Date until the Operational Services Commencement Date. Implementation Services are identified within each relevant Service Element.

4.2 The Affected Property is currently serviced via a 20 year, Private Finance Initiative (PFI) the Expanded Private Resource Initiative for Management of the Estate (PRIME) 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 exit of this 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 across the Affected Property of the Operational Services.

4.4 By the time stated in Annex A, the Supplier shall provide for Approval an 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 Employees 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 execute, utilising Supplier Personnel the approved overall "Implementation Plan Detailed Solution" in line with the values and behaviours referred to in Section 3.

5 TRANSFORMATION

TRANSFORMATION SERVICES

5.1 Transformation Services shall be delivered during the Transformation Phase which the Authority expects to be the period two months from Contract Start Date until 18 months after the Operational Services Commencement Date. Transformation Services are identified 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 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 Security Systems including security equipment to reduce the Authority's requirement for Security Officer hours without negatively impacting the security and health and safety of Authority Employees and Authority Customers.
c) Redesign and significantly improve the quality of Security Risk Assessments and site specific Security Plans across the Affected Property.
d) Better protect Authority Staff, Authority Customers and the Affected Property by implementing the recommendations of the Security Plans.
e) To transition from Existing Security Systems 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 estate.
f) To support and assist the re-distribution of certain delivery tasks including receptionist duties within the Authority Supply Chain Members, for improved service delivery.
g) To deliver significant savings throughout the life of the contract.

6 OPERATION

OPERATIONAL SERVICES

6.1 Operational Services shall be delivered throughout the Operational Phase which is the period from the Operational Services Commencement Date through to Contract end date. Operational Services are described as such in Schedule 2.1 (Statement of Requirements) within each relevant Service Element.

7 GENERAL MANAGEMENT

ACCOUNT MANAGEMENT

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 Supplier Personnel shall have the skills and capability to liaise with and work alongside the 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:

IMPLEMENTATION SERVICES

7.3 By the time stated in Annex A, the Supplier shall provide for Approval an “Account Management Detailed Solution” in line 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 Section 3.

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 telephone numbers 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 sites 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;

7.7 Work collaboratively with the Authority, Integrator and Authority Supply Chain Members, integrating the delivery of Services with other Authority Supply Chain Members to maximise operational efficiencies and improve Value for Money for the Authority.

SUPPLIER'S PERSONNEL

7.8 The Authority requires that the Supplier provides highly competent and professional personnel to enable the delivery of the Services and the achievement of the Authority’s high level objectives and transformation objectives. The Supplier shall be a member of SIA Approved Contractor Scheme.

7.9 The Supplier shall:

IMPLEMENTATION SERVICES

7.10 By the time stated in Annex A, the Supplier shall provide for Approval a “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.

OPERATIONAL SERVICES

7.11 Upon instruction by the Authority execute, utilising Supplier Personnel the approved “Human Resources Detailed Solution” throughout the Contract Term in line with the values and behaviours referred to in Section 3.

7.12 The Supplier shall provide all personnel required to deliver the Services at all times and shall warrant 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 Contract.

7.13 The Supplier shall ensure, prior to commencing any work for the Authority, all personnel are subject to as a minimum HMG Baseline Personnel Security Standard security clearance. For certain properties to be advised by the Authority, further levels of personnel assessment may be required. 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.

7.14 The Supplier shall deploy personnel and other resources flexibly in order to ensure the Authority benefit from the scope and scale of the Supplier’s organisation.

COMMUNICATIONS

7.15 The Authority requires that the Supplier ensures regular communication between Supplier Personnel and Authority Employees across the Affected Property. 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 high level objectives and transformation objectives (reference).

7.16 The Supplier shall:

IMPLEMENTATION SERVICES

7.17 By the time stated in Annex A, the Supplier shall provide for Approval a “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 Contract Term. An indicative list of items to be included in the Account Management Detailed Solution is included in Annex A.

7.18 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 Section 3.

OPERATIONAL SERVICES

7.19 Ensure those individuals identified within the approved Account Management Detailed Solution make regular visits to all Affected Property and that contact is made with Authority Representatives specifically local managers to discuss contract performance and any issues.

7.20 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 contract.

QUALITY MANAGEMENT

7.21 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.

7.22 The Supplier shall:

IMPLEMENTATION SERVICES

7.23 By the time stated in Annex A, the Supplier shall provide for Approval a “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.

OPERATIONAL SERVICES

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

8 HEALTH AND SAFETY & RISK MANAGEMENT

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

8.2 The Supplier shall:

IMPLEMENTATION SERVICES

8.3 By the time stated in Annex A, the Supplier shall provide for Approval a “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, minimise and eradicate risks that may be identified. The Authority requires that this detailed solution proposed by the Supplier is fully integrated with the existing overall detailed solutions as developed by the 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 Solution.
b) Fire and Evacuation Drill Solution.
c) Site Induction Process.

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

OPERATIONAL SERVICES

8.4 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 Section 3.

8.5 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 Integrator and all Authority polices.

8.6 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 Employees and those customers, visitors and other third parties who might be affected by the delivery of the Services as contained within this Statement of Requirements.

8.7 In the delivery of the Services as contained within this Statement of Requirements, ensure all Authority Employees and Authority Customers are protected and feel at ease while on the Affected Property. Follow the BS 18004:2008 guide to Occupational Health & Safety Management Systems or equivalent workplace health and safety practice.

8.8 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 policy.

8.9 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.

8.10 Recognise that the Authority will retain overall accountability for the health and safety of its employees and 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 Key Deliverables relating to health and safety and risk management and will retain ownership of all disaster recovery and business continuity plans.

8.11 Use the System provided by the Integrator, to record details of accidents, incidents, near misses and workplace ill-health issues. Record this information on the System provided by the Integrator within [XX] of the issue occurring.

8.12 Work with fellow Authority Supply Chain Members to enact all Health and Safety policies and promote good practice across the Affected Property in line with the values detailed in Section 3.

8.13 Ensure 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 Member and other related third parties such as Emergency Services.

8.14 If required, provide services in relation to a professional advice service on all matters relating to the Health and Safety at Work Act 1974 and any subsequent re-enactments.

8.15 Provide a Health and Safety expert who is either a member of the Institution of Occupational Safety and Health (IOAH) or hold an equivalent qualification that is issued by a recognised organisation.

8.16 Ensure all Environmental protection standards are met, followed up and adhered to, including but not limited to Asbestos.

8.17 Provide Supplier Personnel for First Aid training as directed by the Integrator. Training will be provided by the Integrator.

8.18 Provide Supplier Personnel for fire and bomb marshall training.

RISK MANAGEMENT

8.19 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.

8.20 The Supplier shall:

IMPLEMENTATION SERVICES

8.21 By the time stated in Annex A, the Supplier shall provide for Approval a “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, minimise and eradicate risks that may be identified. The Authority requires that this detailed solution proposed by the Supplier is fully integrated with the existing overall detailed solutions as developed by the 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 Solution.
b) Fire and Evacuation Drill Solution.
c) Site Induction Process.

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

OPERATIONAL SERVICES

8.22 Upon instruction by the Authority execute, utilising Supplier Personnel, the approved “Health & Safety and Risk Management Detailed Solution”.

8.23 Comply with the risk methodology as created by the Integrator.

8.24 Upon identifying a risk, liaise with the Authority through the use of the System provided by the Integrator, to record and give details of the risk. Complete this within [XX] of risk identification. Both the Supplier and Authority shall use all reasonable effort to monitor, update and mitigate the risk.

8.25 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 under Integrator and Authority policy and work with Authority Supply Chain Members to execute contingency plans for the safety of the Affected Property and all site personnel.

9.2 The Supplier shall:

IMPLEMENTATION SERVICES

9.3 By the time stated in Annex A, the Supplier shall provide for Approval a “Security Disaster Recovery and Business Continuity 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 Security Disaster Recovery and Business Continuity Detailed Solution is included in Annex A.

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 Disaster Recovery and Business Continuity 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 Disaster Recovery and Business Continuity Detailed Solution.

9.7 Be responsible for the immediate alerting and communication to all personnel on site when an emergency occurs. Make use of appropriate onsite equipment to inform of the situation and procedure.

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

9.9 Notify the helpdesk of the issue within XX of the incident occurring. Use the Authority System to log and complete details of any accident within XX of the incident.

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 minimum of annually 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:

TRANSFORMATION SERVICES

10.3 By the time stated in Annex A, the Supplier shall provide for the Approval a “Security Threat and Risk Assessment Detailed Solution” in line with Good Industry Practice detailing the Security Threat and Risk Assessment methodology, Security Threat and Risk Assessment Template, Security Threat and Risk Assessment Tool and Security Threat and Risk Assessment Programme Plan. 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 Section 3.

10.5 As per the programme stated in Annex N – Security Milestone Plan conduct Security Threat and Risk Assessments as per the approved Security Threat and Risk Assessment Detailed Solution across the Affected Property ensuring completion of all Security Threat and Risk Assessments on, or before the Milestone date stated in Annex N – Security Milestone Plan.

10.6 Conduct a Security Threat and Risk Assessment as per the agreed Security Threat and Risk Assessment Detailed Solution after the implementation of a Security Plan at each Affected Property to critically assess the impact of the Security Plan. In the event that recommendations are made through the Security Threat and Risk Assessment, update the Security Plan accordingly.

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 Affected Property 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 Staff, Authority 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
f) Acquisition of new property

10.8 As per the approved Security Threat and Risk Assessment delivery programme (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 Section 3 to provide, at a minimum, an annual Security Threat and Risk Assessment incorporating an annual local threat and risk assessment, for all Security Risk Assessments throughout the Contract Term.

10.9 Review the Security Threat and Risk Assessment Detailed Solution regularly, at a frequency agreed by the Authority but minimum of annually, 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, commensurate with the risk identified in the Affected Property's Security 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 each Affected Property.

10.11 The Supplier shall:

TRANSFORMATIONAL SERVICES

10.12 By the time stated in Annex A, the Supplier shall provide for Approval a "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 Section 3.

OPERATIONAL SERVICES

10.13 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.

10.14 As per the approved Security Plan 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 Section 3 for all Security Plans throughout the Contract Term.

10.15 Review the Security Plan Detailed Solution every 6 months 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 utilise the Work Order management system provided by the Integrator or interface effectively with the Integrator's Work Order management to raise, track and signal completion of all Work Orders.

11.2 The Supplier shall:

IMPLEMENTATION SERVICES

11.3 By the time stated in Annex A, the Supplier shall provide for Approval a "Work Order Management Detailed Solution" in line with Good Industry Practice detailing how the Supplier will utilise and/or interface with the Integrators 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 members of the Authority Supply Chain utilising the Work Order management system provided by the Integrator.

OPERATIONAL SERVICES

11.5 Proactively update, as required by the Authority all Work Orders to track progress through the Work Order management system including tracking against SLAs/KPIs.

11.6 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 Response Times, details of any work undertaken outside of normal parameters, for example an explanation of why certain things were done;
b) for Work Orders not completed or not likely to be completed within the timeframes an update on why the work has not been completed and an estimated time of completion.

11.7 Fully cooperate with all complaints raised against the completion of own Work Orders as per the complaints process agreed with the Authority.

11.8 Fully cooperate with all on-site supervision for example of high-risk Work Orders by the Integrator or Authority.

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, controlling response to emergency incidents and providing a 24/7 helpdesk function. This facility shall not be located on the Affected Property and may be a shared facility. The service will be delivered in accordance with the Standards, legislation and Good Industry Practice

12.2 The Supplier shall:

IMPLEMENTATION SERVICES

12.3 By the time stated in Annex A, the Supplier shall provide for Approval a "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.

12.4 Liaise and develop procedures with the supplier of the Interim Automated Access Control System to ensure an integrated and seamless service delivery.

12.5 The Control and Monitoring Facility Detailed Solution shall also include for the transition of the services from the Interim Automated Access Control System to the Supplier as replacement AACS and Intruder Detection Systems are rolled out.

OPERATIONAL SERVICES

12.6 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 Section 3.

13 SECURITY SYSTEMS

13.1 This section sets out the Authorities requirements for the Security Systems. The Authority recognises the need to upgrade and replace the Existing Security Systems to fully comply with Good Industry Practice and achieve the transformation objectives. However, the scope of the deployment will be determined in the Security Plan for each Affected Property. Works to install Replacement Security Systems shall be aligned with the Approved Replacement Security System Detailed Solution.

GENERAL SECURITY SYSTEM REQUIREMENTS

13.2 The Supplier shall comply with the general requirements for all Security Systems:

a) Liaise with the Integrator and other Authority Supply Chain Members to agree and coordinate the programme for delivery.
b) Provide Security Systems that are:
   i. Integrated
   ii. Interoperable
   iii. Resilient
   iv. Flexible i.e. scalable and expandable
   v. Based on industry standard open architecture platforms
   vi. Utilising latest software versions, Upgrades and Patches
c) Be an NSI Gold approved company and comply at all times with the standards and practices for the installation of the security systems (including any subcontractors).
d) Deploy appropriate resource to satisfy all Security System requirements including the roll out programme.
e) Design development of Security Systems included within this document
f) Design Interface development with the Authority Supply Chain Members.
g) Supply of the Security System components
h) Provide all licences required by the Authority, Authority Supply Chain Members and any other users of the Security System
i) Provide on request Factory Acceptance Testing certification
j) Ensure Electro Magnetic Compatibility compliance
k) Ensure CE compliance of all components
l) Design and install components resistant to acts of vandalism

m) Undertake all Security System testing and validation on a simulated Data Network prior to installation
n) Install all the Security System components
o) Be responsible for the physical and logical connection and configuration of the Security System components
p) Be responsible for logical security of all Supplier devices, including:
   i. Anti virus software and anti virus signature updates
   ii. Software for the purposes of preventing malware and spyware being installed
q) Connect all Security Systems to power supplies (to be provided by another supplier)
r) Be responsible for the configuration of the Security Systems, including all Users.
s) Complete all required Site Acceptance Testing
t) Be responsible for the setting to work of the Security Systems
u) Interface Site Acceptance/Witness Testing and System Commissioning of the system
v) Complete all required Operational Readiness Testing of the Security Systems
w) Provide and manage all Security System documentation, including operational, equipment maintenance and training manuals as well as as-built drawings.
x) Provide all required Training of Security System Users
y) Provide 24/7 support and maintenance services (including maintenance tracking)
z) Provide support for the Security System to achieve the Rectification Periods as identified in Annex K.
aa) Comply with the principles of the Data Protection Act (DPA), the Regulation of Investigatory Powers Act 2000 (RIPA) the Data Retention and Investigatory Powers Act 2014 and the Investigatory Powers Act 2016.
bb) Comply with the requirements of ISO27001/2 and the Authority's Information Security Policy, and should be capable of implementing and enforcing appropriate security standards as specified by the Authority and subject to any information risk assessment undertaken pursuant to Part 12 (Enterprise Security Risk Management Strategy) to Schedule 2.6 (Authority Policies). The Supplier shall make design and controls information available to the Authority upon request.
cc) Ensure, as part of the HMG Security Policy Framework, the Security Systems comply with and shall have certified the HMG Cyber Essentials Scheme or Approved equivalent (further details available at: www.cyber-essentials –scheme.co.uk).
dd) Comply with all relevant aspects of the Government Digital Service Open Standards as included within the link below the System Detailed Solution shall detail how the System will comply, www.gov.uk/government/publications/open-standards-for-government;
ee) Ensure, no part of the Security Systems shall be hosted off-shore (i.e. outside mainland UK), without the approval of the Authority.
ff) Ensure the Security System has appropriate security controls in place to prevent unauthorised access to the Security System, including monitoring and auditing;
gg) Provide records of Security System use per user. Should user activity be deemed as inappropriate or representing a security risk, the user and activity shall be reported to the Authority immediately;
hh) Prepare risk assessments and method statements for approval prior to any works being undertaken.
ii) Comply with the Authority's Permit to Work system.
jj) Implement a quality assurance system to NSI or equivalent standards,
kk) Provide all Upgrades, Patches and latest versions of software.

GENERAL EXCLUSIONS (WORK BY OTHER AUTHORITY SUPPLY CHAIN MEMBERS)

13.3 The Supplier will be responsible for liaising with, specifying and confirming requirements with Authority Supply Chain Members but not for the delivery of the following services:

a) Building fabric e.g. coms rooms within the Affected Property.
b) Power supplies: power supplies will be provided by the Authority to a single location for each system.
c) Making good / decoration of building fabric following installation (the supplier must minimise damage to the building fabric).

EXISTING AUTOMATED ACCESS CONTROL SYSTEM EXCLUSIONS (WORK AUTHORITY INTENDS TO BE DELIVERED BY INTERIM AUTOMATED ACCESS CONTROL SUPPLIER)

13.4 The Authority intends that the Supplier will be responsible for instructing and liaising with an Interim Automated Access Control System supplier who will be contracted by the Authority for the continued administration, support and maintenance of an existing Automated Access Control System which is integrated with the existing Intruder Detection System. A list of sites where the existing Automated Access Control System is installed is included in Schedule _.

13.5 In summary, the Supplier will not be responsible for the delivery of the following services for the existing Automated Access Control System, which shall be delivered by the Interim Automated Access Control System supplier (see Schedule _ for full Statement of Requirements):

a) Planned Maintenance
b) Reactive Maintenance
c) Technology / System Support
d) Enrolment of New Users
e) Administration of User Records
f) Creation of Access Passes
g) Alarm notification and monitoring (including the IDS and Panic Alarms)
h) Asset verification and condition survey of the existing Automated Access Control System included in Schedule _.

13.6 The Authority intends to award a contract for the services defined in point 13.5 for the Interim Automated Access Control System Contract which will commence on 1st April 2018 and until a replacement AACS System has been installed and existing Intruder Detection System is repurposed or upgraded across the Affected Property.

13.7 The Supplier shall:

IMPLEMENTATION SERVICES

13.8 By the time stated in Annex A, the Supplier shall provide for Approval an “Existing Security Systems Detailed Solution” in line with Good Industry Practice detailing how the Supplier will ensure full and satisfactory delivery of the Existing Security Systems. An indicative list of items to be included in this Existing Security Systems Detailed Solution is included in Annex A.

TRANSFORMATION SERVICES

13.9 By the time stated in Annex A, the Supplier shall provide for Approval a "Replacement Security Systems Detailed Solution" in line with Good Industry Practice detailing how the Supplier will replace and/or upgrade the Existing Security Systems to ensure compliance with Good Industry Practice and the Authority's transformation objectives. An indicative list of items to be included in this Replacement Security Systems Detailed Solution is included in Annex A.

OPERATIONAL SERVICES

13.10 Upon instruction by the Authority execute, utilising Supplier Personnel the approved "Existing Security Systems Detailed Solution" and "Replacement Security Systems Detailed Solution" in line with the values and behaviours referred to in Section 3.

CCTV SYSTEM

13.11 The Authority requires the existing CCTV systems installed across the Affected Property to be maintained and operational in accordance with requirements specified within the Approved Security Plan for each Affected Property. The Security Plan will identify any replacement CCTV system requirement which shall be delivered by the Supplier.

13.12 The Supplier shall:

IMPLEMENTATION SERVICES

13.13 Within the Existing Security Systems Detailed Solution, address CCTV Systems to ensure full and satisfactory delivery of the existing CCTV system. An indicative list of items to be included in this Detailed Solution is included in Annex A.

TRANSFORMATION SERVICES

13.14 Within the Replacement Security Systems Detailed Solution, address CCTV Systems to ensure a replacement CCTV System will satisfy the General Requirements set out in paragraph 13.2 above and the following requirements:

a) record to a high resolution i.e. H264 standard or equivalent
b) record images in a digital format to a high resolution (H264 standard or equivalent) for 31 days with the provision to allow external agencies to remove images for use as evidence in possible prosecutions (compliance with BS 8495)
c) the ability to download recordings in "native" format to DVD with the associated software that enables replay on standard PC equipment
d) capable of remote monitoring
e) capable of integration with other systems and programmed to enable automatic "cause and effect" functions
f) confirming the activation of any Intruder Detection System (IDS)
g) capable of operating with or without security lighting
h) capable of local recording, playback and storage of images at a security control points e.g. where remote monitoring is not required

i) includes software which includes a mechanism to allow users to “protect” recordings i.e. prevent automatic over-writing
j) provide software that complies with the DPA requirement under Subject Access Request requirements (i.e. pixelate parts of an image)
k) be robust and capable of resisting acts of vandalism, e.g. external CCTV camera housings shall be vandal resistant to LPS1175 Rating 2
l) cabling concealed within the fabric of the building or secured in surface mounted ducts (subject to agreement with the Authority)
m) Uninterrupted Power Supplies (UPS) to power the CCTV system and communications devices for a minimum period of 6 hours
n) include all equipment racks, UPS power and distribution, cabling and cable management, installation of all hardware software and control equipment.

An indicative list of items to be included in the Replacement Security Systems Detailed Solution is included in Annex A.

AUTOMATED ACCESS CONTROL SYSTEM (AACS)

13.15 The Authority requires an AACS for the Affected Property ensuring only Authority Employees and Authority visitors with the necessary permission can gain access to and around the Affected Property.

13.16 The Authority intends to contract for an Interim Automated Access Control System Contract for the continued, administration, maintenance and support of the existing Automated Access Control System to be utilised by the Supplier in the delivery of an Access Control service on the Affected Property where the Existing Automated Access Control System is installed.

13.17 The Existing Automated Access Control System Exclusions at point 13.4 shall apply.

13.18 The Supplier shall:

IMPLEMENTATION SERVICES

13.19 The Existing Security Systems Detailed Solution shall detail how the Supplier shall ensure full and satisfactory delivery of the existing AACS system including how the Supplier shall interface with the Interim Automated Access Control System supplier. An indicative list of items to be included is included in Annex A.

TRANSFORMATION SERVICES

13.20 Within the Replacement Security Systems Detailed Solution the Supplier will address AACS Systems to ensure a replacement AACS System will satisfy the General Requirements set out in paragraph 13.2 above and the following requirements.

a) Control all external access points to Affected Property.
b) Control internal access points to ensure a separation between Public Waiting Areas and all other internal areas ensuring they are only accessible to Authority Employees and legitimate users of the site.
c) Prevent the entrance of unauthorised individuals to Affected Property at all times.

d) Produce all security passes for Authority Employees. The security pass should be the Common Civil Service Pass (CCSP) as included in Annex J.

e) Use Cards that must:
   i. In order of preference be based on one of the following technical options
   ii. NXP Mifare family (includes Classic, Desfire and Desfire EV1)
   iii. HID iClass family
   iv. Legic Avant family

f) Use Readers that must: must:
   i. Meet the ISO 7816, ISO 15693 and ISO 14443 standards and be fully interoperable across those standards

g) Utilise a Database that is vendor neutral (such as XML schema or JSON) with appropriate middleware where necessary to enable the importing and exporting of data from the Database

h) Work with any card and reader that meets ISO 15693 and ISO 14443 standards.

i) Integrate with other security systems such as Intruder Detection System, CCTV, Fire & Bomb and building systems as required by the Authority.

j) Support the estimated number of cardholders approximately 90,000 and all associated churn

k) Be inclusive and facilitate use by those with disabilities e.g. card readers to be installed at an accessible height.

l) Store and manage data in compliance with the Authority's Information Security requirements and data protection legislation.

m) The system shall backup the entire access control database off-network and off-site such that data is recoverable in the event of a catastrophic failure or event at the site. Back-ups shall be carried out automatically on a daily basis, or other interval agreed with the Authority.

n) Utilise a synchronised time signal accurately reflecting local time to within 1 second.

o) Provide a Voice Access Control System at user and goods entrances as detailed in the Affected Property Security Plan and at all public entrances.

p) All sites are to be fitted with a Grade 3 (Medium to High Risk) Automated Access Control System to BSEN 50133 to allow events to be accurately and timely tracked.

An indicative list of items to be included in the Replacement Security Systems Detailed Solution is included in Annex A.

FIRE DETECTION AND FIREFIGHTING SYSTEM

13.21 The Authority requires Fire Detection and Fighting Systems to be maintained and operational in accordance with the Fire Safety Regulations, Regulatory Reform (Fire Safety) Order 2005, other Standards, legislation and Good Industry Practice. The Security Plan will identify any replacement Fire Detection and Fighting Systems which shall be delivered by the Supplier.

13.22 The fire detection and fighting systems include:
   a) Heat and gas detection systems and associated alarms
   b) Voice alarm systems
   c) Public address systems
   d) Lift evacuation systems
   e) Bomb alarms

13.23 The Supplier shall:

IMPLEMENTATION SERVICES

13.24 Within the Existing Security Systems Detailed Solution, address Fire Detection and Fighting Systems to ensure full and satisfactory delivery of the existing Fire Detection and Fighting systems and detailing the management of all Fire Detection and Fighting systems issues and risks associated with the Affected Property that will aim to reduce, minimise and eradicate risks that may be identified. An indicative list of items to be included is included in Annex A.

TRANSFORMATION SERVICES

13.25 Within the Replacement Security Systems Detailed Solution the Supplier will address Fire Detection and Fighting Systems to ensure a replacement Fire Detection and Fighting System will satisfy the General Requirements and the indicative list of items to be included in the Replacement Security Systems Detailed Solution as included in Annex A.

INTRUDER DETECTION AND PANIC ALARM BUTTONS

13.26 The Authority requires the existing Intruder Detection Systems (IDS) and panic alarms to be maintained and operational in accordance with the Standards, legislation and Good Industry Practice. The Security Plan will identify any replacement IDS and Panic Alarms Systems which shall be delivered by the Supplier.

13.27 The Existing Automated Access Control System Exclusions at point 13.4 shall apply.

13.28 The Supplier shall:

IMPLEMENTATION SERVICES

13.29 Within the Existing Security Systems Detailed Solution, address Intruder Detection and Panic Alarm Buttons Systems to ensure full and satisfactory delivery of the existing address Intruder Detection and Panic Alarm Buttons system and will detail the management of all systems issues and risks associated with the Affected Property that will aim to reduce, minimise and eradicate risks that may be identified.. An indicative list of items to be included is included in Annex A.

TRANSFORMATION SERVICES

13.30 Within the Replacement Security Systems Detailed Solution the Supplier will address Intruder Detection and Panic Alarm Buttons Systems to ensure a replacement Intruder Detection and Panic Alarm Buttons System will satisfy the General Requirements. An indicative list of items to be included is included in Annex A.

PRIVATE MOBILE RADIO (PMR)

13.31 The Authority requires that the Supplier delivers the security Services with appropriate means of communicating to perform the duties identified in the Service Elements. The Supplier shall provide and operate an appropriate PMR including all hand held radio units (including personal attack buttons), vehicle and desk mounted terminal equipment and required control equipment and infrastructure.

13.32 The Supplier shall:

IMPLEMENTATION SERVICES

13.33 Within the Existing Security Systems Detailed Solution, address PMR Systems to ensure full and satisfactory delivery of the existing PMR system. An indicative list of items to be included is included in Annex A.

TRANSFORMATION SERVICES

13.34 Within the Replacement Security Systems Detailed Solution the Supplier will address PMR Systems to ensure a replacement PMR System will satisfy the General Requirements. An indicative list of items to be included in the Replacement Security Systems Detailed Solution is included in Annex A.

SECURITY SYSTEM NETWORK (additional operational service)

13.35 The Authority has existing infrastructure installed to allow Authorised Personnel using IP based devices to access the internet using wired networks or wireless access points in a controlled manner within the Affected Property that it may (at its absolute discretion) permit the Supplier to utilise for the purposes of providing the Approved Replacement Security Systems.

13.36 The Authority requires that the Supplier provides a proposal and option to plan, design, install, test, maintain and support a separate Security Systems network including all infrastructure required to provide all Replacement Security Systems network requirements based on distinct infrastructure to be installed on a defined needs basis on those Affected Property as required by the introduction of Replacement Security Systems (where this is not provided by the Authority for use by the Supplier).

13.37 The Supplier shall:

IMPLEMENTATION SERVICES

13.38 By the time stated in Annex A, the Supplier shall provide for Approval a proposed “Security System Network Detailed Solution” in line with Good Industry Practice to be introduced as an additional requirement that the Authority may wish to take further which will satisfy the General Requirements. This shall include a timeline for implementation across the Affected Property, to be developed in consultation with the Integrator. An indicative list of items to be included in the Security System Network Detailed Solution is included in Annex A.

13.39 Within the Security Systems Network Detailed Solution the Supplier will address a Security Systems Network that will satisfy the General Requirements set out in paragraph 13.2 above and the following requirements.

a) Ensure that wireless access points are based on the IEEE 802.11b/g/n wireless standard.
b) As a minimum provide non resilient Internet Access with unlimited download at each Affected Property using ADSL broadband.
c) Install and maintain a firewall at each Affected Property to deter security attacks on Supplier devices.

d) Support both static and dynamically configured IPv4 addressing and routing for each Supplier device.
e) Configure the network to not use a captive portal.
f) Only permit Supplier devices to connect to a specified set of Internet IPv4 addresses.

TRANSFORMATION SERVICES

13.40 Upon instruction by the Authority execute, utilising Supplier Personnel, the approved proposed “Security System Network Detailed Solution” in line with the values and behaviours referred to in Section 3.

BODY WORN CAMERAS (additional operational service)

13.41 The Authority requires that the Supplier provides a proposal and option to deploy Body Worn Cameras on a defined needs basis across the Affected Property.

13.42 The Supplier shall:

IMPLEMENTATION SERVICES

13.43 By the time stated in Annex A, the Supplier shall provide for Approval a proposed “Body Worn Camera Detailed Solution” in line with Good Industry Practice to be introduced as an additional requirement that the Authority may wish to take further which will satisfy the General Requirements. This shall include a timeline for implementation across the Affected Property. An indicative list of items to be included in the Body Worn Camera Detailed Solution is included in Annex A.

TRANSFORMATION SERVICES

13.44 Upon instruction by the Authority, undertake the preparation of, and deploy Body Worn Cameras to Security Officers to monitor and manage the safety across the Affected Property.

13.45 Use Body Worn Cameras to record both video and sound of Incidents to clearly define the identity, speech and actions of all participants of the recording.

13.46 Ensure the Body Worn Camera can be suitably attached to Supplier Personnel comfortable and conveniently for daily use across all environments of the Affected Property.

13.47 Ensure the Body Worn Camera can store at a minimum, [XX] hours of video recording and have a rechargeable battery life at a minimum meeting the maximum hours of recording time. The Detailed Solution should be practical and suited for daily use on the Affected Property.

BODY CAMERA STORAGE AND DATA PROTECTION

13.48 The Supplier shall propose a solution to:

13.49 Store the recordings of body worn cameras in a standard, non-proprietary format. This should be accessible by a number of common software programs.

13.50 Store on a platform which is accessible to the Authority at any time and practice good management of the recordings to ensure it is up to date and holds an accurate database.

Ensure recordings are uploaded to the platform on a regular, timely basis. The selected platform must be able to interface with the System.

13.51 Ensure the recordings cannot be edited nor deleted without the express permission of the Authority.

13.52 Ensure that the recordings and associated data are protected under the Data Protection Act and any other such data or information acts present or future.

13.53 Maintain and repair both the body-cameras and associated software as required.

TECHNICAL SPECIFICATIONS

13.54 The Supplier will propose the type, model and specification of Body Camera for use across the Affected Property. This will undergo a testing and approvals process by the Authority before any deployment.

LONE WORKER SOLUTION (additional operational service)

13.55 The Authority requires that the Supplier provides a proposal to provide a Lone Worker service for use by Authority Staff when conducting visits with Authority Customers, and when conducting investigations or as directed by the Authority. The Authority requires a proposal for a nationwide Lone Worker service that provides a discreet and instantaneous means of alert to Incidents raised by Authority users of the Lone Worker service including appropriate Emergency Response.

13.56 The Supplier shall:

IMPLEMENTATION SERVICES

13.57 By the time stated in Annex A, the Supplier shall provide for Approval a proposed “Lone Worker Detailed Solution” in line with Good Industry Practice to be introduced as an additional requirement that the Authority may wish to take further which will satisfy the General Requirements. This shall include a timeline for implementation across the Authority Estate. An indicative list of items to be included in the Lone Worker Detailed Solution is included in Annex A.

TRANSFORMATION SERVICES

13.58 Upon instruction by the Authority execute, utilising Supplier Personnel the approved proposed “Lone Worker Detailed Solution” in line with the values and behaviours referred to in Section 3.

14 TRIALLING, TESTING, COMMISSIONING AND HANDOVER REGIME

14.1 The Authority requires all Security Systems to undergo a rigorous trialling, testing, commissioning and handover regime. Fundamental to the Authority Employees endorsing the transformation of the security Services will be an initial trial phase which the Supplier shall develop.

14.2 The Supplier shall:

IMPLEMENTATION SERVICES

14.3 The Supplier shall develop a Trialling, Testing, Commissioning and Handover detailed solution that will include the list of items to be included in Annex A, the General Requirements and the following:

14.4 Provide a documented trialling methodology and trial plan for Approval at least two weeks prior to trial.

14.5 Provide a documented testing methodology and test plan for Approval at least two weeks prior to test and commissioning commencing. The testing will include:

- Site Acceptance Testing (SAT) to determine and document the equipment hardware and software operates according to its specification. 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 location of the SAT shall be agreed with the Authority.

- 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.

14.6 The Supplier shall document the trials, SAT and UAT and submit the results to the Authority for approval.

14.7 On successful completion of the SAT and UAT the Supplier shall commence the training of the Authorities Employees. The Supplier shall also produce a user guide for Authority Staff.

TRANSFORMATION AND OPERATIONAL SERVICES

14.8 Once Approved by the Authority, execute, deliver and manage the Trialling, Testing, Commissioning and Handover Regime detailed solution in line with the values and behaviours referred to in Section 3.

15 SUPPORT AND MAINTENANCE REQUIREMENTS

15.1 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 Rectification Periods. Where the Supplier fails to rectify any faults within the relevant Rectification Periods or fails to provide the Services in accordance with the KPIs, the Authority shall have the right to specified remedies for such performance failures, including, but not limited to, Service Credits.

SUPPORT AND MAINTENANCE OF EXISTING SECURITY SYSTEMS

15.2 The Authority requires that the existing security systems installed on each Affected Property continue to be operational from the Operational Services Commencement Date. Any faults must be rectified efficiently , with minimal disruption to day to day operations and, in any

event, within the specified Rectification Periods. Where the Supplier fails to rectify any faults within the relevant Rectification Periods or fails to provide the Services in accordance with the KPIs, the Authority shall have the right to specified remedies for such performance failures, including, but not limited to, Service Credits.

15.3 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 their capability to provide all required support and maintenance from the Operational Services Commencement Date.

15.4 The Existing Automated Access Control System Exclusions at point 13.4 shall apply.

15.5 The Supplier shall:

IMPLEMENTATION SERVICES

15.6 By the time stated in Annex A, the Supplier shall provide for Approval an “Asset Verification and Condition Survey Plan” within the “Implementation Plan Detailed Solution” in line with Good Industry Practice detailing the process to be executed to undertake the asset verification and condition survey of existing security systems to provide assurance to the Authority, by way of an Asset Verification and Condition Survey Report, of their capability to provide support and maintenance for existing security systems.

15.7 Upon instruction by the Authority execute, utilising Supplier Personnel the approved Asset Verification and Condition Survey Plan by the Operational Services Commencement Date in line with the values and behaviours referred to in Section 3.

15.8 By the time stated in Annex A, the Supplier shall provide for Approval a “Existing Security 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 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 Integrator and 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 Strategy

OPERATIONAL SERVICES

15.9 Upon instruction by the Authority execute, utilising Supplier Personnel the approved Existing Security Support and Maintenance Detailed Solution in line with the values and behaviours referred to in Section 3.

15.10 Provide a Spares Holding Strategy within the Existing Security Support and Maintenance Detailed Solution in order to meet the Rectification Periods identified in Annex K.

15.11 Provide appropriate engineering resource required to meet the Authorities Rectification Periods.

SUPPORT AND MAINTENANCE OF REPLACEMENT SECURITY SYSTEMS

15.12 The Authority requires that the replacement security systems installed on each Affected Property to be operational from date of installation. Any faults must be rectified efficiently, with minimal disruption to day to day operations and, in any event, within the specified Rectification Periods. Where the Supplier fails to rectify any faults within the relevant Rectification Periods or fails to provide the Services in accordance with the KPIs, the Authority shall have the right to specified remedies for such performance failures, including, but not limited to, Service Credits.

15.13 The Supplier shall:

TRANSFORMATION SERVICES

15.14 By the time stated in Annex A, the Supplier shall provide for Approval a "Replacement Security 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 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 Integrator and 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 Strategy

OPERATIONAL SERVICES

15.15 Upon instruction by the Authority execute, utilising Supplier Personnel the approved Replacement Security Support and Maintenance Detailed Solution for all installed security systems from Operational Services Commencement Date and for all security systems from (the end of the transformation phase) in line with the values and behaviours referred to in Section 3.

15.16 Provide an updated Spares Holding Strategy within the Replacement Security Support and Maintenance Detailed Solution in order to meet the Rectification Periods.

15.17 Provide appropriate engineering resource required to meet the Rectification Periods.

15.18 The systems will be designed to enable the remote diagnosis of faults and should provide fault indications directly to the Supplier's helpdesk.

16 SECURITY OFFICERS

16.1 The Authority requires that the Supplier provides Security Officers to undertake the duties currently performed by Customer Care Officers (CCO) and Customer Service Officers (CSO)

as described in the Job Descriptions included in (Annex H) across the Affected Property. In addition, the Supplier shall provide Security Officers to perform all security 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.

16.2 The Supplier shall:

SECURITY OFFICER DEPLOYMENT

IMPLEMENTATION SERVICES

16.3 By the time stated in Annex A, and as part of the overall Implementation Plan Detailed Solution, the Supplier shall provide for Approval an "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; deploy Security Officers in line with the Baseline Security Officer Deployment Model included in Annex I, which specifies 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.

16.4 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 Section 3.

OPERATIONAL SERVICES

16.5 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 Property, Authority Staff, Authority visitors and contractors.

16.6 Liaise with Emergency Services & Security Advisory bodies regarding the Detailed Solutions and all operational procedures and abide by all recommendations made.

16.7 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.

16.8 Ensure that Supplier Personnel carry valid passes as approved by the Authority and challenge all personnel without a clearly displayed pass.

16.9 Open and lockup of Affected Property including escort of cleaning personnel.

OPERATION OF SECURITY SYSTEMS

OPERATIONAL SERVICES

16.10 Provide Supplier Personnel to operate the following Security Systems;

a) CCTV
b) Automated Access Control System
c) Intruder Detection System and panic alarms
d) Fire Detection and Fighting Systems

at each Affected Property where Security Systems are installed in accordance with the approved Security System operating procedures as defined within the approved Existing Security Systems Detailed Solution and Replacement Security Systems Detailed Solution.

17 INCIDENT MANAGEMENT

17.1 The Authority requires an Incident Management service that is effective, consistent and mitigates the impact of Incidents upon Authority Employees, Authority Customers and the Affected Property.

17.2 The Supplier shall:

IMPLEMENTATION SERVICES

17.3 By the time stated in Annex A, the Supplier shall provide for Approval an "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.

OPERATIONAL SERVICES

17.4 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 Section 3.

17.5 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 contract term.

17.6 For those Incidents classified as "Serious Incidents" the Supplier shall follow the Serious Incident Review Process (see Annex O) as developed, updated and owned by the Authority, organising and convening any and all Serious Incident Review Groups making all Supplier Personnel available as required.

18 KEY MANAGEMENT

18.1 The Authority requires that the Supplier provides a professional key management service to control building access keys and alarm system codes. Provide a secure service to Authorised Users and Authorised Vehicles across the Affected Property to prevent unauthorised access and ensure compliance in line with Good Industry Practice and Authority policy.

18.2 The Supplier shall:

IMPLEMENTATION SERVICES

18.3 By the time stated in Annex A, the Supplier shall provide for Approval a "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.

OPERATIONAL SERVICES

18.4 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 Section 3.

18.5 Provide a custodian service of building access keys and alarm system codes, ensuring compliance with the Security Industry Authority and its licensing requirements.

18.6 Issue keys to Authorised Authority Employees for access across the site as appropriate.

18.7 During the Authority opening hours, provide a key holding service on the site premises for site keys and Automated Access Control Systems.

18.8 Respond to situations requiring a key holder on both a planned and unplanned basis, to attend the Affected Property 24 hours a day, 7 days a week, 52 weeks a Year. These shall include but not be limited to provision of access for Authority Representatives, responses to fire alarms, lift alarms and security alarms.

18.9 In the event of a break-in or attack on site, respond, secure and make safe in accordance with the Authority's requirements.

18.10 In the case of an emergency, provide assistance to emergency services to ensure the site is secure or given access and alarms reset.

18.11 Log faults with keys and locks across the building site, including lost keys or damage. Report lock and key issues to the Helpdesk and assist the Facilities Management Supplier for access to facilitate repair.

19 CAR PARK MANAGEMENT

19.1 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.

19.2 The Supplier shall:

IMPLEMENTATION SERVICES

19.3 By the time stated in Annex A, the Supplier shall provide for Approval a "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.

OPERATIONAL SERVICES

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

19.5 Take all reasonable steps to protect against theft of vandalism of vehicles parked on the Affected Property.

19.6 As a minimum, record the following information on all vehicles on access to Car Parks:

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

20 ADDITIONAL SECURITY PROVISION

20.1 The Authority requires that the Supplier provides Additional Security as requested by the Authority to enable the delivery of the Authority's Core Business which will include but 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 Unacceptable Customer Behaviour Policy (ref) and approved Unacceptable Customer Behaviour Detailed Solution
g) Any change in Affected Property Risk Profile that warrants additional security measures e.g. short notice protests or demonstrations

20.2 The Supplier shall:

OPERATIONAL SERVICES

20.3 Provide a proactive response to meet all requests from the Authority for Additional Security and this service should be available, on request, 24 hours a day, 7 days a week, 365 days a year.

20.4 For all requests from the Authority for Additional Security, assess the requirement including an appropriate Risk Assessment and provide for Approval an "Additional Security Plan" detailing appropriate Additional Security measures to satisfy the requirement commensurate with security risk and at all times maximising value for money for the Authority.

20.5 Upon instruction by the Authority execute the Additional Security Plan in line with the values and behaviours referred to in Section 3.

20.6 Ensure that at no point Operational Services and requirements as detailed in Affected Property's Security Plans are compromised by the requirement to deliver Additional Security Provision.

21 REPORTING REQUIREMENTS

21.1 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 Integrator and Authority's Core Business which will include but not limited to the:

a) Financial Management Solution.
b) Performance Reporting Process.
c) Compliance Reporting Regime.

21.2 The Supplier shall:

IMPLEMENTATION SERVICES

21.3 By the time stated in Annex A, provide for Approval a "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.

OPERATIONAL SERVICES

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

22 SECURITY PROJECTS AND CAPITAL PROGRAMME

22.1 The Authority requires that the Supplier will act as the sub-contractor for all Project works relating to Security Systems as defined within Section 13 of this Section 2.1 (Statement of Requirements). The Authority expects to appoint Authority Supply Chain Members who will be responsible for the delivery of large projects at each Affected Property. Small projects will be delivered by the Facilities Management Supplier. The high-level process flow for the completion of project works to be followed by the Supplier is included in Annex M.

22.2 In relation to all project works, for Security Systems requirements the Supplier shall:

22.3 Provide all design and consultancy works.

22.4 Take instruction from the Integrator, Facilities Management Supplier and all Authority Supply Chain Members responsible for project delivery.

22.5 Support the programming of all project works, to be led by the Integrator.

22.6 Complete all project works as per the instruction provided by the Integrator, Facilities Management Supplier all Authority Supply Chain Members responsible for project delivery to the agreed programme at all times compliant with Good Industry Standards.

22.7 Complete all required FAT, SAT and UAT testing necessary to complete instructed project works.

22.8 Provide updates as required on the completion of works and report the successful completion of works.

22.9 Create and store records of all project works at all times compliant with the Document Management policies and procedures set by the Authority and Integrator.

23 SUSTAINABILITY

23.1 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.

23.2 The Supplier shall:

OPERATIONAL SERVICES

23.3 Comply with the Energy Management Solution as set by the Integrator. Comply with the Authority Energy Management policy and any subsequent government policy.

23.4 In line with the values and behaviours as detailed in Section 3, collaborate with other Authority Supply Chain Members to enact and comply with sustainability efforts, initiatives and property re-locations.

23.5 Take account of and comply with the Authority's targets and commitments under current government sustainability policy and any subsequent government policy.

23.6 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.

23.7 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.

23.8 The Authority will advise on investment criteria on a year by year basis. Any reduction in cost may form part of the gain share mechanism.

23.9 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.

24 RESPONSE TO HEIGHTENED THREAT

24.1 The Authority requires enhanced security services, developing and executing operational procedures for specific Security Events. [Further detail to follow]

24.2 The Supplier shall:

IMPLEMENTATION SERVICES

24.3 By the time stated in Annex A, work with Authority Representatives and all relevant Government Bodies to jointly develop for Approval a "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 Property. An indicative list of items to be included in this Response to heightened threat Detailed Solution is included in Annex A.

OPERATIONAL SERVICES

24.4 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 Section 3.

24.5 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 days of request.

24.6 During times of heightened security, the Supplier shall provide further detailed security provision as required by the Authority. This may include but shall not be limited to searching of all visitor bags, cancellation of all non-essential events, checking of vehicles entering onto the Affected Property or in car park areas for potential suspect devices.

25 DOCUMENT MANAGEMENT

25.1 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 Property. This will interface with the System to be accessed by the Authority and Integrator for timely and robust document management.

25.2 The Supplier shall:

IMPLEMENTATION SERVICES

25.3 By the time stated in Annex A, the Supplier shall provide for Approval a "Document Management Plan" as part of the Account 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 Account Management Detailed Solution is included in Annex A.

OPERATIONAL SERVICES

25.4 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 Section 3.

26 UNACCEPTABLE CUSTOMER BEHAVIOUR (Incl. Database additional requirement)

26.1 The Authority requires that the Supplier provides a defined Unacceptable Customer Behaviour service for the risk assessment and mitigation of identified security risk posed by planned meetings and appointments by the Authority with those Authority Customers that the Authority deems to have demonstrated Unacceptable Customer Behaviour (UCB Customers).

26.2 The Supplier shall:

IMPLEMENTATION SERVICES

26.3 By the time stated in Annex A, provide for Approval a proposed "UCB Process Detailed Solution" in line with Good Industry Practice which will satisfy the General Requirements. An indicative list of items to be included in the UCB Process Detailed Solution is included in Annex A. Further illustration of a suggested process from the Authority, highlighting the key stages of the UCB process is included the UCB Process Flow; see Annex F.

OPERATIONAL SERVICES

26.4 Upon instruction by the Authority execute, utilising Supplier Personnel, the approved "UCB Process Detailed Solution" in response to all planned appointments with UCB customers and in line with the values and behaviours referred to in Section 3.

UCB DATABASE (additional requirement that the Authority may wish to take further)

26.5 The Authority additionally requires that the Supplier provides a proposal for the provision of a UCB Database application and associated management as the tool for the recording of UCB Incidents by Authority Staff and the storage of Authority data on UCB Customers for the purposes of effective risk assessment by the Supplier and appropriate identification by Supplier Staff.

26.6 The Supplier shall:

TRANSFORMATION SERVICES

26.7 By the time stated in Annex A, the Supplier shall provide for Approval a proposed "UCB Database Detailed Solution" in line with Good Industry Practice to be introduced as an additional requirement that the Authority may wish to take further which will satisfy the General Requirements. An indicative list of items to be included in the UCB Database Detailed Solution is included in Annex A.

26.8 At all times uphold the highest levels of professionalism and integrity in the management and storage of sensitive information held on UCB Customers and ensure compliance with all Authority IT and Data Management policies.

OPERATIONAL SERVICES

26.9 Upon instruction by the Authority execute, utilising Supplier Personnel the approved proposed "UCB Database Detailed Solution" in line with the values and behaviours referred to in Section 3.

END.