Home Office

AUTHORITY: The Secretary of State for the Home Department

SCHEDULE 4
SECURITY

Front End Services (FES) UK

CONTENTS

SCHEDULE 4

SECURITY

1. INTRODUCTION

1.1 This Schedule describes the Authority's security requirements that the Supplier is required to meet or exceed during the Contract Term in the fulfilment of the Service Requirements.

1.2 In this Schedule, unless the contrary intention appears, each capitalised term shall have the meaning set out in Schedule 1 (**Definitions**).

1.3 If and to the extent of any conflict or inconsistency between Annex 4-1 and/or Annex 4-2 and Paragraphs 1 to 16 of this Schedule 4 (**Security**), Paragraphs 1 to 16 shall prevail.

2. SECURITY POLICIES AND STANDARDS

2.1 The Supplier shall deliver the Services to the Authority in accordance with Her Majesty's Government's (HMG) Security Policy Framework and in accordance with Annex 4-1 (the Authority's Security Policy and Security Standards).

2.2 The Authority shall invite the Supplier to take part in the approval process which the Authority operates when making policy changes, but the Authority shall have the ultimate discretion in setting any new or changed Security Policy, Security Standard or Service Requirement.

2.3 Changes to the Supplier Solution and the Service Requirements which are necessary to meet changes occurring after the Effective Date to the Authority's Security Policy and Security Standards and/or the HMG's Security Policy shall be agreed through the Change Control Procedure.

2.4 Changes to the Supplier Solution required as a result of changes to HMG's Security Policy Framework or to reflect Good Industry Practice shall be agreed as an Operational Change through the Change Control Procedure.

2.5 The Supplier acknowledges that one of the key principles of the Authority's Security Policy and Security Standards set out in Annex 4-1 is to manage risks, rather than to prescribe fixed solutions. The Supplier shall therefore be required to apply judgement in discharging its responsibilities under this Agreement.

2.6 For the avoidance of doubt, it is solely the Supplier's, and not the Authority's, responsibility, to put in place the appropriate protection in relation to the security provisions described in this Schedule 4 (**Security**) and it shall also be

the Supplier's responsibility to manage the relevant risks relating to such security.

3. PRINCIPLES OF SECURITY

3.1 The Supplier acknowledges that the Authority places paramount importance on the confidentiality, integrity and availability of information, and on the Supplier's accreditation and compliance with the Authority's Security Policy and Security Standards (Annex 4-1).

3.2 The Authority continues to keep the Authority Security Policy and Security Standards under review. Changes may be made as a result of these reviews and any changes must be adhered to by the Supplier and agreed through the Change Control Procedure.

3.3 The Supplier shall ensure that there are efficient systems of identifying, reporting, recording and investigating breaches of security. All security breaches must be reported to the Authority in accordance with the agreed processes as set out in Schedule 14 **(Management Information and Reporting**).

3.4 It is solely the Supplier's responsibility to put in place the appropriate protection in relation to the security provisions described in this Schedule 4 (**Security**).

4. INFORMATION AND SECURITY MANAGEMENT SYSTEMS (ISMS) AND SECURITY MANAGEMENT PLAN

4.1 The Supplier shall develop, implement, operate, maintain and continuously improve (and ensure that all Supplier's Staff and Sub-Contractors implement and comply with) an ISMS which will be approved by the Authority, tested periodically, updated and audited in accordance with ISO/IEC 27001.

4.2 The Supplier shall develop and maintain a Security Management Plan in accordance with Paragraph 5 of this Schedule 4 (**Security**) to apply during the Contract Term.

4.3 The Supplier shall comply with its obligations set out in the Security Management Plan and any other provision of the Contract relevant to security.

4.4 Both the Information Security Management Systems (ISMS) and the Security Management Plan shall, unless otherwise specified by the Authority, aim to protect all aspects of the Services and all processes associated with the delivery of the Services, including but not exclusively; people, premises, property, location, the Supplier system and any IT, information and data (including the Authority classified information and the Authority Data) to the

extent used by the Authority or the Supplier in connection with this Contract against; attack, theft, disclosure, unauthorised access, corruption or non-availability, whether by deliberate or accidental means.

4.5 The Supplier is responsible for monitoring and ensuring that it is aware of any changes to the HMG Security Policy Framework. The Supplier shall keep the Security Management Plan up to date with the Security Policy Framework and any subsequent amendments.

4.6 The entire Service shall be covered by Accreditation in accordance with HMG Security Policy Framework to a specified level and scope to be agreed with the Authority.

4.7 The Supplier shall obtain Accreditation or Approval to Operate of the entire service by the Authority's Accreditor prior to live operation of the service as specified in Schedule 5 (**Implementation (Mobilisation and Transition)**). In obtaining this Accreditation, the Supplier shall fully consult the Accreditor and Authority representatives throughout the design, build and Accreditation process.

4.8 If the Authority Data is corrupted, lost or sufficiently degraded as a result of the Supplier's fault, so as to be unusable, the Authority requires the Supplier to:

4.8.1 restore or procure the restoration of the Authority Data (at the Supplier's expense) to the extent and in accordance with the Business Continuity and Disaster Recovery (BCDR) Plan as specified in Schedule 21 (**Business Continuity/Disaster Recovery**) and the Supplier shall do so as soon as practicable but in accordance with the time period notified by the Authority;

4.8.2 restore or procure the restoration of Authority Data, and where this is undertaken by the Authority any reasonable expenses incurred in doing so to the extent and in accordance with the requirements specified in the BCDR Plan shall be repaid by the Supplier; and,

4.8.3 if at any time the Supplier suspects or has reason to believe that the Authority Data has or may become corrupted, lost or sufficiently degraded in any way for any reason, then the Supplier shall notify the Authority immediately and inform the Authority of the remedial action the Supplier proposes to take for approval by the Authority.

5. DEVELOPMENT OF THE SECURITY MANAGEMENT PLAN

5.1 Within twenty (20) Working Days after the Commencement Date (or such other period specified in the Implementation Plan or as otherwise agreed by the Parties in writing) and in accordance with Paragraph 5.4 (amendment and

revision of the ISMS and Security Management Plan), the Supplier will prepare and deliver to the Authority for approval, a fully complete and up to date Security Management Plan in accordance with Paragraph 5.3, which will be based on the draft Security Management Plan.

5.2 If the Security Management Plan, or any subsequent revision to it in accordance with Paragraph 5.4 (amendment and revision of the ISMS and Security Management Plan), is approved by the Authority it will be adopted immediately and will replace the previous version of the Security Management Plan. If the Security Management Plan is not approved by the Authority the Supplier shall amend it within ten (10) Working Days or such other period as the Parties may agree in writing of a notice of non-approval from the Authority and re-submit to the Authority for approval. The parties will use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days (or such other period as the parties may agree in writing) from the date of its first submission to the Authority. If the Authority does not approve the Security Management Plan following its resubmission, the matter will be resolved in accordance with Schedule 25 (**Dispute Resolution Procedure**). No approval, to be provided by the Authority pursuant to this Paragraph 5.2, may be unreasonably withheld or delayed. However a refusal by the Authority to approve the Security Management Plan, on the grounds that it does not comply with the requirements set out in Paragraph 5.4, shall be deemed to be reasonable.

5.3 Content of the Security Management Plan:

5.3.1 The Security Management Plan will set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Services and all processes associated with the delivery of the Services and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the Services comply with the provisions of this Contract (including this Schedule, the principles set out in paragraph 5.4 and any other elements of this Contract relevant to security or any data protection guidance produced by the Authority).

5.3.2 The Security Management Plan (including the draft version) should also set out the plans for transiting all security arrangements and responsibilities from those in place at the Commencement Date to those incorporated in the Supplier's ISMS at the date set out in the Implementation Plan for the Supplier to meet the full obligations of the security requirements set out in this Agreement.

5.3.3 The Security Management Plan will be structured in accordance with ISO/IEC27001 and ISO/IEC27002, cross-referencing if necessary to other Schedules of this Contract which cover specific areas included within that standard.

5.3.4 The Security Management Plan shall be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Authority engaged in the Services and shall only reference documents which are in the possession of the Authority or whose location is otherwise specified in this Schedule.

5.4 Amendment and Revision of the ISMS and Security Management Plan

5.4.1 The ISMS and Security Management Plan will be fully reviewed and updated by the Supplier annually to reflect:

(a) emerging changes in Good Industry Practice;

(b) any change or proposed change to the Supplier System, the Services and/or associated processes;

(c) any new perceived or changed security threats;

(d) any reasonable request by the Authority.

5.4.2 The Supplier will provide the Authority with the results of such reviews as soon as reasonably practicable after their completion and amendment of the ISMS and Security Management Plan at no additional cost to the Authority. The results of the review should include, without limitation:

(a) suggested improvements to the effectiveness of the ISMS;

(b) updates to the risk assessments;

(c) proposed modifications to the procedures and controls that effect information security to respond to events that may impact on the ISMS; and

(d) suggested improvements in measuring the effectiveness of controls.

5.4.3 On receipt of the results of such reviews, the Authority will approve any amendments or revisions to the ISMS or Security Management Plan in accordance with the process set out at Paragraph 5.2.

5.4.4 Any change or amendment which the Supplier proposes to make to the ISMS or Security Management Plan (as a result of a Authority request or change to the requirement set out in this agreement shall be subject to a Change Control Notice and shall not be implemented until approved in writing by the Authority.

6. TESTING

6.1 The Supplier shall conduct tests of the ISMS ("Security Tests") on an annual basis or as otherwise agreed by the Parties. The date, timing, content and conduct of such Security Tests shall be agreed in advance with the Authority.

6.2 The Authority shall be entitled to send a representative to witness the conduct of the Security Tests. The Supplier shall provide the Authority with the results of such tests (in a form approved by the Authority in advance) as soon as practicable after completion of each Security Test.

6.3 Without prejudice to any other right of audit or access granted to the Authority pursuant to this Contract, the Authority and/or its authorised representatives shall be entitled, at any time and without giving notice to the Supplier, to carry out such tests (including penetration tests) as it may deem necessary in relation to the ISMS and the Supplier's compliance with the ISMS and the Security Management Plan. The Authority may notify the Supplier of the results of such tests after completion of each such test. Security Tests shall be designed and implemented so as to minimise the impact on the delivery of the Services. If such tests adversely affect the Supplier’s ability to deliver the Services to the agreed Schedule 7 Performance Levels (KPIs,) the Supplier shall be granted relief against any resultant under-performance for the period of the tests.

6.4 Where any Security Test carried out pursuant to Paragraphs 6.2 and 6.3 above reveals any actual or potential breach of security and/or security failure or weaknesses, the Supplier shall promptly notify the Authority in writing of any changes to the ISMS and to the Security Management Plan (and the implementation thereof) which the Supplier proposes to make in order to correct such failure or weakness. Subject to the Authority's approval in accordance with Paragraph 5.4, the Supplier shall implement such changes to the ISMS and the Security Management Plan in accordance with the timetable agreed with the Authority or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the ISMS or Security Management Plan to address a non-compliance with the Security Policy or security requirements (as set out in the Agreement), the change to the ISMS or Security Management Plan shall be at no cost to the Authority. For the purposes of this Paragraph 6.4, weaknesses means a vulnerability in security

and failure means a possible breach of the Security Management Plan or security requirements.

7. COMPLIANCE WITH ISO/IEC 27001

7.1 The Supplier shall be compliant with ISO/IEC 27001.

8. ACCREDITATION

8.1 Any technical solution provided by the Supplier, including biometric and digitisation (or any other digital interface provided by the Supplier), will be required to demonstrate that it is designed and developed to maintain the integrity of data captured and transferred from the supplier to the Authority's systems.

8.2 The Supplier will be required to demonstrate and evidence an adherence to the Home Office minimum security assumptions and HMG Security Policy Framework. This will need to be submitted to the Authority for approval in order to secure the appropriate Authority to Operate. The Supplier shall consult the Accreditor and Authority representatives throughout the design, build and implementation.

9. MANAGING SECURITY

9.1 The Supplier must nominate an individual to be accountable for the management of security and for assurance of the Authority's data, in relation to the Agreement (the "Supplier Security Manager"). The appointment of the Supplier Security Manager and any successor shall be subject to the approval of the Authority.

9.2 The responsibilities of the Supplier Security Manager shall include the following:

9.2.1 representing the Supplier at all meetings that address security concerns, events and issues, except where the Authority expressly requires otherwise;

9.2.2 ensuring that security is integrated into the Supplier and the Supplier Sub-contractors' day-to-day working with respect to the Service Requirements;

9.2.3 receiving service updates on a Monthly basis relating to security activities from each of the Supplier's nominated individuals responsible for each component of the Service Requirements. Such nominated individuals shall further report Security Incidents promptly

to the Supplier Security Manager, who shall be responsible for reporting all such incidents to the Security Incident Panel; and

9.2.4 attending at Security Incident Panels, when convened, to monitor Supplier's management of security; discuss and resolve security issues and share information.

9.3 The Security Incident Panel shall consist of the Authority's security staff and the Supplier Security Manager, and may include the Authority's operational representatives, other experts from HM Government, other Supplier security experts, one or more of Supplier Sub-Contractor's Security Manager and other relevant personnel, as appropriate; and

9.4 Giving assurance to the Authority as and when required that the Supplier Personnel, in operating the Service Points, are adhering to the requirements of this Schedule 4 (**Security**).and Schedule 11 (**Personnel and Key Representatives**).

9.5 The Supplier shall deliver assurance to the Authority, within a reasonable time of a request by the Authority for such assurance, that the Supplier Solution complies with HMG security policies, standards and guidance and, specifically, HMG Security Policy Framework and the Authority's Security Policy and Security Standards, or that an appropriate risk management decision (agreed in writing by duly authorised representatives of the Authority) enables the Supplier Solution to be delivered without complying with the Authority's Security Policy and Security Standards.

9.6 The Authority may, at any time, convene a meeting of a Security Incident Panel to monitor the Supplier's management of security; discuss and resolve security issues and share information.

10. SECURITY CLEARANCES

10.1 Please refer to Schedule 11 (**Representative and Key Personnel**).

11. PHYSICAL SECURITY

11.1 Please refer to Annex 4-1 of this Schedule 4 (**Security**) and Schedule 13 (**Facilities**).

12. DATA SECURITY

12.1 The Supplier shall develop an Information Security Management System (ISMS) reflecting the Security Policy which shall define the processes and procedures for delivering the Services to the Authority and shall specify the physical security requirements of the Supplier's and the Supplier Sub-

contractors' infrastructure and facilities. The ISMS shall be consistent with and integrate with the Security Policy.

12.2 The Supplier shall assess the risk of a compromise to the confidentiality, integrity and availability of information to the appropriate security classification using an appropriate risk assessment methodology presented in the National Cyber Security Centre (NCSC) Summary of Risk method and Frameworks (https://www.ncsc.gov.uk/guidance/summary-risk-methods-and-frameworks).

12.3 The Supplier shall manage the risk of compromise to the confidentiality, integrity and availability of information by implementing information assurance processes and follow the recommendations in the NCSC Risk Management Collection (https://www.ncsc.gov.uk/guidance/risk-management-collection).

12.4 The Supplier shall comply with the Authority's guidelines and instructions on the storage, security and privacy of Authority Data, which shall include guidelines on the type of, and the length of time that, data can be stored on the Supplier Systems.

12.5 The Supplier shall explain in a Risk Assessment Document how:

12.5.1 all information (stored electronically or otherwise) is securely stored and is resistant to non-authorised access; and

12.5.2 it will implement controls appropriate to the security classification of the information applied to maintain confidentiality, availability and integrity.

12.6 Paragraphs 12.5.1 and 12.5.2 above include information stored in both production and non-production environments, such as those used for testing and development, and environments used for the storage of information, such as IT system design documents.

12.7 The Supplier's Security Plan and policies must comply as a minimum with the requirements of the Data Protection Legislation. The Supplier, working together with the Authority's Accreditor, shall ensure that electronic personal data being transmitted outside secure boundaries is encrypted using appropriate cryptographic techniques.

12.8 The Supplier's Security Plan shall include how risks associated with loss of data confidentiality, integrity or availability of Customer Data will be mitigated appropriately whilst such data is in the control of the Supplier, which shall include whilst the Customer Data is in transit between the Service Points and the Authority.

12.9 The Supplier will notify the Authority immediately of any data loss whilst under it, or its Supplier Sub-contractors' control.

12.10 The Supplier's Security Plan shall also include a description of how:

12.10.1 risks associated with the obtaining of unauthorised access by anyone who does not require such access in order to carry out their obligations under this Agreement will be mitigated;

12.10.2 the Supplier will prevent unauthorised personnel from gaining access to Authority Data; and

12.10.3 the Supplier will maintain systems security measures to guard against the unauthorised, alteration or destruction of Authority Data.

12.11 The Supplier shall assist the Authority, and/or other bodies sanctioned by the Authority, in the investigation of any incident of unauthorised or attempted disclosure or tampering with the Authority's Data.

12.12 The Supplier Personnel and the Supplier Sub-contractors and their personnel shall not:

12.12.1 collect, stop, process or otherwise make use of Authority Data for any purpose other than that which is directly in relation to the supply of the Services;

12.12.2 purport to sell, let for hire, assign rights in or otherwise dispose of any of Authority Data;

12.12.3 make any of Authority Data available to any third party, other than to the extent necessary to enable that person to perform its part of the Services, and then only to that extent; or

12.12.4 commercially exploit Authority Data.

12.13 Without prejudice to the other rights of the Authority under this Agreement, if in the provision of the Services any Authority Data is lost through the fault or negligence of the Supplier Personnel, or the Supplier Sub-contractors or their personnel, or any breach by the Supplier of the terms of this Agreement, the Supplier shall regenerate such Authority Data to the most current back-up copy as required by the Agreement without additional expense to the Authority and, in doing so, shall use commercially reasonable efforts to ensure that the timings for the provision of the Services are not materially affected.

12.14 The Supplier may from time to time be required to respond to additional requests from the Authority for assurance regarding the handling of

information, to enable the Authority to assess the maturity of the Supplier's information handling policies and procedures.

12.15 The Supplier will continually review the Risk Assessment Document and will ensure that the relevant risks are taken into consideration when planning, selecting, designing and modifying its Facilities for delivering the Services.

13. BUSINESS CONTINUITY

13.1 Please refer to the Schedule 21 (**Business Continuity Disaster Recovery (BCDR) Plan**).

14. SECURITY INCIDENTS

14.1 The Supplier's Security Plan shall include a description of how all violations of the Security Policy will be reported to the Authority.

14.2 In addition to the Supplier's reporting obligation, and as outlined at Paragraph 14.1 above, if a Security Incident (as described in Annex 4-3) occurs, the Supplier shall carry out an immediate investigation (to start within twenty-four (24) hours) into the incident and initiate corrective actions and investigate the route cause to limit the likelihood of the incident occurring again. The Supplier shall also prepare and retain documentation of the investigation of the violation and provide a copy to the Authority.

14.3 The Authority shall have the right to investigate any or all security incidents, security concerns or unresolved security issues or refer incidents to others, as required. The Authority may also hold a Security Incident Panel as per Paragraph 9.4 above.

15. INSPECTION

15.1 The Authority shall have the right to inspect any and all security aspects of the Supplier's operations in order to verify compliance with the Security Policy, Security Standards and this Schedule, including attending the Service Points, to inspect the physical security and procedural security standards and measures in place.

16. SPECIFIC SECURITY REQUIREMENTS

16.1 Loss of Biometric Data

16.1.1 If the Supplier believes that biometric data has been or will be compromised, damaged or lost, or is aware of any unauthorised access, corruption or impostors, the Supplier shall immediately provide a detailed information report to the Supplier Security

Manager and the Authority's Contract Management Team in accordance with Schedule 14 (**Management Information and Reporting**).

16.1.2 In the event of an incident of the type described in Paragraph 16.1.1 above, the Authority is entitled to carry out an investigation into the incident and initiate corrective actions to minimise loss, damage and/or re-occurrence of the incident, including the right to cancel any Service Point, at the Authority's sole discretion, that such cancellation is necessary.

16.1.3 All Applications linked to biometric data affected by an incident of the type described in Paragraph 16.1.1 above shall be deemed void and, in this event and without prejudice to any of the Authority's other rights and remedies under the Agreement, the Supplier shall contact the Customers so affected and make arrangements for these individuals to re-apply and re-enrol for Biometric Capture, at no additional cost or charge to such individuals and at no cost or charge to the Authority save that the Authority shall be liable for the costs of such re-enrolment if Biometric Data is lost or damaged due to the Authority's systems, provided the Supplier has not caused such failure.

ANNEX 4-1 SERVICE POINTS AND BASELINE SECURITY REQUIREMENTS

The Authority's Security Policy and Security Standards

The Supplier's Security Plan must conform to HMG Security Policy Framework located at:

http://www.cabinetoffice.gov.uk/resource-library/security-policy-framework

Annex 4-1 sets out the security considerations that a Supplier must demonstrate due consideration of within Service Point proposals, both in terms of physical environment and Standard Operating Procedures (to be agreed alongside Supplier mobilisation plans).

The Authority has provided, at Annex 4-2, an indicative set of measures that should be addressed for each Service Point, when identifying and seeking Authority approval of Service Point locations.

The Supplier must also demonstrate that all Service Points conform to ISO 27001 in its:

- general security standards
- security Standard Operating Procedures used in the maintenance and operation of existing IT systems
- development and operation of all future IT systems; and
- day-to-day operations of Service Points.

While these requirements are the minimum acceptable to the Authority, the Supplier may propose within their own security design solutions any additional security features as controls.

Furthermore, the Supplier must demonstrate within their Security Plans consideration of, where applicable to relevant Service Point solutions, the following specific areas of Service Point security:

1. Perimeter of the Service Point
2. Building access points
3. Reception areas
4. Public areas
5. Staff and service areas

The Supplier's Security Plan shall include a security design solution that addresses Security Operating Procedures for the provision of overarching services at each Service Point with reference to each of the defined threats proportionately; alongside taking account of provision and ensuring the integrity of the following services:

1. Biometric equipment (including where applicable to storage and transportation);

2. Supplier personnel;
3. Authority Data;
4. Customer security; and
5. Business continuity.

The range of security measures used for protecting an individual Service Point will be commensurate with the United Kingdom security threat/risk level, as well as other identified threats, risks and vulnerabilities such as:

From terrorism	**From crime**
Vehicle borne improvised explosive devices (both moving and stationary)	Burglary or forced entry
Person borne IEDs (either inside or outside the building, including delivery by suicide attack/armed intruder assault)	Theft of cash or valuables or sensitive data or equipment; robbery, including from couriers
Suspicious items delivered by mail/post (both explosives and chemical and biological related devices)	Theft from customers or car parks and other petty crime in the neighbourhood of the Service Point
Physical attacks by skilled intruders who are equipped with tools to defeat security systems and insider threats	Kidnap of staff or arson
The risk that guard or response forces may be subject to bribery or coercion that could override or negate security measures or the security posture.	
Hostile incursion by an armed person(s) who intends causing harm to staff working within public caller buildings	
The risk from an insider threat such as fraud/integrity issues	

The controls and mitigations for potential threats listed above require the Supplier to implement physical security measures, and also include in its Security Plan procedural measures such as:

- Security awareness training to ensure staff are alert to threats and the forms they can take, including risks from vehicles, suspicious persons and delivered items
- Creation of a continuity plan and contingency actions in the event of security incidents, including establishment of clear responsibilities and a mechanism for handling incidents.

ANNEX 4-2 SUPPLIER SECURITY PLAN

1. The Supplier's Security Plan set out in this Annex 4-2 shall meet the minimum security requirements set out within Annex 4-1 above.

2. The Supplier shall develop and agree with the Authority the Security Plan by the relevant Service Point Commencement Date in accordance with the terms of this Schedule 4 (**Security**).

3. [Drafting Note: Placeholder for the Supplier's Security Plan
   The Security Plan shall include a summary and description of the policy and processes for the following areas:

   3.1. The Supplier's organisational risk assessment and treatment
   3.2. The Supplier's security policy
   3.3. The Supplier's information security policy and processes, including accreditation
   3.4. Asset management
   3.5. HR and personnel security
   3.6. Physical and environmental security
   3.7. Communications and operational management
   3.8. Access control procedures
   3.9. Information systems acquisition, development and maintenance
   3.10. Information security incident management
   3.11. Business continuity and disaster recovery
   3.12. Legal and regulatory compliance]

ANNEX 4-3 SECURITY INCIDENTS

Incident Category	Incident Description
Supplier Personnel (this includes sub-contractor staff)	Any allegation or conviction for corruption or other criminal activity involving Supplier Personnel
	Any immigration status breach, whether alleged or proved, involving Supplier Personnel
	Suspension or the termination of employment of any Supplier Personnel as a result of allegations of dishonesty or serious misconduct.
	Suspension or the termination of employment of any Supplier Personnel as a result of inefficiency or negligence in carrying out their duties.
	Any allegations by Customers of abusive behaviour by Supplier Personnel, including harassment, whether of a threatening, demeaning, racist, sexist or sexual nature
Physical Security	Intruder / Burglary at the Service Point, including attempted burglaries
	Physical assault on Supplier Personnel or Service Point Customer
	Any threatening communication of a violent nature
	Failure of Security Equipment that cannot be resolved immediately and which will impact on security controls at the Service Point.
	Failure by the Supplier to record Biometric Capture events or failure of the Biometric recording equipment (CCTV)
	Any bomb alerts at the Service Point or in the local vicinity
Data and IT Security	loss or theft of the Biometric Equipment
	Any loss or theft of Authority Data, including Biometric Data
	Loss or theft of a Customer's documents / data
	The Supplier shall report to the Authority – with at least an initial report on the day – any permanent or presumed temporary loss, theft or other unavailability of personal data, that comes to the Supplier's attention and regardless of whose personnel (e.g. Supplier's, Supplier Sub-contractor's) are considered to be responsible.
	Any breach by Supplier Personnel of the Data Protection Act or equivalent local legislation
	Failure of CCTV or other security equipment

Service Disruption	A Force Majeure event – e.g. natural disaster, terrorist activity or any other event that prevents supplier from delivering the services at a specific location(s)
	Excessive staff absence due to unforeseen events which impacts on service provided, e.g. mass staff sickness
	Failure of Supplier systems in excess of 1 hour
	Failure of Biometric Capture system (not individual pieces of equipment, but the whole system)
	Reports from Customers or Supplier Personnel that a Service hosted in the Central Infrastructure is hard down preventing a Customer applying or disrupting messaging between interconnecting IT systems.
	Damage to the Service Point or service disruptions that fall short of being a Force Majeure Event
Customer Service and Complaints	Significant issues with Service Point facilities, e.g. loss of water, heating or power or damage to the interior of the Service Point.
	Notification of any legal action or other claim for damages lodged by a Customer against the Supplier
	Claims from Customers that documents are missing or that they have been given the wrong documents.

ANNEX 4-4 ENHANCED CONTROLS TO SUPPORT BIOMETRIC CAPABILITIES

1. BACKGROUND

This section describes the Authority's additional security requirements relating to biometric capabilities that the Supplier is required to meet or exceed during the Contract Term in the fulfilment of the Services Requirements.

2. RISK MANAGEMENT AND ASSURANCE

i. The Supplier is responsible for flowing down security requirements and the Security Aspects letter to its Sub-contractors, and obtaining the relevant assurance on its sub-contractors' governance, technical solution, physical and personnel security to support the assurance of the overall system. The Supplier shall on reasonable request provide evidence of such assurance to the Authority.

ii. The Supplier shall ensure that all systems adhere to NCSC security standards and guidance, and achieve formal approval by the Home Office Biometrics Accreditor before entry into service and renewed on an annual basis.

iii. The Supplier shall produce and accurately maintain, either directly or if agreed by cooperating with the Authority's representatives, the Risk Management Artefacts to the satisfaction of the Authority's Accreditor. This is to include as a minimum: the Solution Security Design, (which will detail how the solution implements the Project Security Architecture), and SyOPs to cover procedural security of the solution. It will also include the IT Security Health Check scope, and Remedial Action Plan.

iv. The Supplier shall describe details of its approach to assuring the security and integrity of the supply chain for all hardware and software components used in the delivery of the Services, including ensuring that components do not contain hidden or undocumented features that could be exploited to compromise the confidentiality, integrity or availability of the enrolment data set or other information. The Supplier shall provide evidence of the assurance activities upon reasonable request by the authority.

v. The Supplier must highlight risks and vulnerabilities associated with the service at the earliest possible opportunity to the Authority, in a form agreed with the Authority.

vi. The Supplier shall use reasonable endeavours to proactively monitor relevant briefings and alerts for information pertaining to emerging threats and/or vulnerabilities associated with software and hardware used by the Supplier in

the provision of the Services to the Authority and shall propose appropriate corrective measures to the Authority.

3. SECURE DESIGN AND DEVELOPMENT

The supplier shall demonstrate that all development personnel working on the project shall follow secure coding practices, including the OWASP Top Ten and NCSC guidance (SafeCode) and industry standards.

4. MESSAGING FORMATS & STANDARDS

i. The Supplier shall apply the standards provided by the OASIS Web Services Security Standards - SOAP Message Security 1.1 for Authority Data transmitted from the Supplier Solution to the Authority system.

ii. The Supplier shall apply the message format standards defined within the HONE-1 interface control documents for Authority Biometric Data transmitted from the Supplier Solution to the Authority system.

iii. Notwithstanding the message security specifications provided by the OASIS Web Services Security Standards - SOAP Message Security 1.1, the Supplier shall apply the recommended digital signing standards specified in the extant W3C XML Information Set for Signature Syntax and Processing.

5. SECURE CONFIGURATION

i. Solution components, including servers, workstations and supporting ICT infrastructure, must be configured into a known and secure state using the appropriate CIS Level 1 Benchmarks that relate to the solution component.

ii. The Authority requires that any Authority Data transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile User Device must be encrypted using a product or system component which has been formally assured through a certification process such as Commercial Product Assurance (CPA) by CESG.

iii. The Supplier shall only connect Supplier approved, owned and managed devices to the Solution.

iv. Solution end user devices must be configured in accordance with the extant and relevant NCSC end user device specifications.

6. OPERATIONAL SECURITY

i. The Supplier shall perform monthly host vulnerability scans to monitor and assess the supplier solution infrastructure using CVE vulnerability scoring metrics.

ii. The Supplier shall ensure that any exploitable vulnerability is managed following a defined policy and supporting process to identify vulnerabilities, prioritise and mitigate those vulnerabilities.

iii. The Supplier shall ensure that Supplier Solution components are maintained in an up-to-date and vendor supportable state by applying vendor updates This will be of the order of: Critical vulnerabilities patched within fourteen (14) days, important vulnerabilities patched within thirty (30) days and all others patched within sixty (60) days.

iv. The manufacture and assembly of components shall occur in a country and a secure environment that is acceptable to the Authority.

v. The Supplier Solution components shall be time synchronised to a known, trusted and accurate time service.

vi. The Supplier Solution shall be subject to real-time performance and availability monitoring such that excessive message volumes and sizes can be detected.

vii. The Supplier Solution administrators and end users must be accountable for their actions by using uniquely identifiable user IDs. The use of shared user accounts is forbidden.

7. CRYPTOGRAPHY

i. The Supplier shall use cryptographic algorithms that are included within the NSA Commercial National Security Algorithm (CNSA) Suite.

ii. The Supplier shall protect any Authority Data transmitted over any public network using TLS transport-level or IPSec encryption.

iii. The cryptographic protocol for the TLS connection (outside of the message layer) is TLS 1.2 only. Allowable TLS1.2 cipher-suites for your BSG application server are:

- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

iv. The cryptographic configuration for an IPSec connection must adhere to NCSC guidance “using IPSec to protect data” using the PRIME cryptographic profile.

v. The Supplier shall use a trusted Certificate Authority for the supply of trusted x509 certificates and shall comply with the subscriber obligations in the Certificate Authority's Certificate Practice Statement.

vi. The Supplier shall use the RSA-SHA256 or RSA-SHA384 message signing algorithm for signing operations carried out within the supplier solution.

8. AUTHENTICATION AND AUTHORISATION

i. The Supplier shall have auditable processes and controls in place for provisioning users, that limit access to ICT systems and estates used in providing the Services, such that access is only granted when absolutely necessary and only to authorised staff (whether Supplier or Sub-contractor) who have appropriate Security Clearances.

ii. The Supplier shall implement Role Based Access Control (RBAC) for all users of the System, including system administrators. The RBAC shall be able to provide different access levels to systems and data. Roles may be based on job profiles, management grades and team responsibilities. The principle of Least Privilege must be adhered to for all accounts.

iii. The Supplier shall implement x509v3 digital certificate-based mutual authentication between the supplier solution and the Authority system.

iv. The Supplier shall implement two-factor authentication for user access to biometric capture workstations.

9. LOGGING AND MONITORING

i. The Supplier shall ensure solution user and administrator accountability by maintaining a log of solution transaction activity containing a minimum of the following data items:

- Network (IP address) of the solution component that originates the event
- Username of the person or system account originating the event
- Timestamp (date and time that the event was originated)
- Solution transaction function carried out

ii. The Supplier shall ensure that a transaction together with the log of such cannot be tampered with once it is closed. The integrity of records of individual transactions must be maintained.

10. BIOMETRIC CAPTURE DEVICES

i. The Supplier shall-own and manage all Biometric Capture Devices used by the solution.

ii. The Supplier shall ensure that Biometric Capture Devices meet functional and capture quality requirements specified by the Home Office Biometric Capture Device standards.

iii. The Supplier shall provide evidence that its application software and associated fingerprint capture hardware (scanner) model have successfully passed testing and quality assurance processes to confirm that the HOB Biometric Standards are met.