Agreement

relating to the service and maintenance of fixed and mobile RN detection equipment

Schedule 2.4 (Security Management)

SCHEDULE 2.4
SECURITY MANAGEMENT

1 INTRODUCTION

1.1 The Parties acknowledge that the purpose of the ISMS and Security Management Plan are to ensure a robust organisational approach to security under which the specific requirements of this Agreement will be met.

1.2 The Parties shall each appoint a member of personnel to be responsible for security (each a **"Security Representative"**). The initial member of personnel appointed by the Supplier for such purpose shall be the person identified as the Supplier Security Representative in Schedule 9.2 (Key Personnel) and the provisions of Clause 20 (Supplier's Personnel and Key Personnel) shall apply in relation to such person.

1.3 The Authority shall clearly articulate its high-level security requirements so that the Supplier can ensure that the ISMS, security related activities and any mitigations are driven by these fundamental needs.

1.4 Both Parties shall provide a reasonable level of access to any members of their personnel for the purposes of designing, implementing and managing security.

1.5 The Supplier shall use as a minimum Good Industry Practice in the day to day operation of any system holding, transferring or processing Authority Data and any system that could directly or indirectly have an impact on that information, and shall ensure that Authority Data remains under the effective control of the Supplier at all times.

1.6 The Supplier shall ensure the up-to-date maintenance of a security policy relating to the operation of its own organisation and systems and on request shall supply this document as soon as practicable to the Authority.

1.7 The Authority and the Supplier acknowledge that information security risks are shared between the Parties and that a compromise of either the Supplier's or the Authority's security provisions represents an unacceptable risk to the Authority requiring immediate communication and co-operation between Parties.

1.8 The Supplier will participate in periodic service data reviews to identify trends, aggravating factors and weaknesses to identify service improvement opportunities, as required and agreed between the Parties.

2 ISMS

2.1 By the date specified in the Implementation Plan the Supplier shall develop and submit to the Authority for the Authority's approval in accordance with Paragraph 4.4 of this Schedule 2.4 (Security Management) an information security management system for the purposes of this Agreement, which:

(a) shall have been tested in accordance with Schedule 6.2 (Testing); and

(b) shall comply with the requirements of paragraphs 2.3 to 2.5 of this Schedule 2.4 (Security Management).

2.2 The Supplier acknowledges that the Authority places great emphasis on the reliability of the Services and confidentiality, integrity and availability of information and consequently on the security provided by the ISMS and that the Supplier shall be responsible for the effective performance of the ISMS.

2.3 The ISMS shall:

(a) unless otherwise specified by the Authority in writing, be developed to protect all aspects of the Services and all processes associated with the delivery of the Services, including the Authority Premises, the Supplier System, the Authority System (to the extent that it is under the control of the Supplier) and any ICT, information and data (including the Authority Confidential Information and the Authority Data) to the extent used by the Authority or the Supplier in connection with this Agreement;

(b) meet the relevant standards in ISO/IEC 27001 and ISO/IEC 27002 in accordance with paragraph 6 of the Schedule 2.4 (Security Management); and

(c) at all times provide a level of security which:

(i) is in accordance with Law and this Agreement;

(ii) as a minimum demonstrates Good Industry Practice, compliant with HMG standards (GOV.UK Government Standards including SPF), National Cyber Security Centre (NCSC) guidance and security policies as instructed by the Authority;

(iii) complies with the Baseline Security Requirements;

(iv) complies with the information handling requirements stated in the Security Aspects Letter;

(v) addresses issues of incompatibility with the Supplier's own organisational security policies;

(vi) meets any specific security threats of immediate relevance to the Services and/or Authority Data; and

(vii) complies with the security requirements as set out in Schedule 2.1 (Services Description).

(d) document the security incident management processes and incident response plans;

(e) document the vulnerability management policy including processes for identification and mitigation of system vulnerabilities;

(f) document the content and frequency of security related reporting; and

(g) be certified by (or by a person with the direct delegated authority of) a Supplier's main board representative, being the Chief Security Officer, Chief Information Officer, Chief Technical Officer or Chief Financial Officer (or equivalent as agreed in writing by the Authority in advance of issue of the relevant Security Management Plan).

2.4 The references to standards, guidance and policies set out in paragraph 2.3 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Supplier from time to time.

2.5 In the event that the Supplier becomes aware of any inconsistency in the provisions of the standards, guidance and policies set out in paragraph 2.3, the Supplier shall immediately notify the relevant Authority Security Representative of such inconsistency and the Authority Security Representative shall, as soon as practicable, notify the Supplier which provision the Supplier shall comply with.

2.6 If the ISMS submitted to the Authority pursuant to paragraph 2.1 is approved by the Authority, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule 2.4 (Security Management). If the ISMS is not approved by the Authority, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Authority and re-submit it to the Authority for approval. The Parties shall 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 ISMS following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No approval to be given by the Authority pursuant to this paragraph 2 may be unreasonably withheld or delayed. However, any failure to approve the ISMS on the grounds that it does not comply with any of the requirements set out in paragraphs 2.3 to 2.5 shall be deemed to be reasonable.

2.7 Approval by the Authority of the ISMS pursuant to paragraph 2.6 of this Schedule 2.1 (Security Management) or of any change to the ISMS shall not relieve the Supplier of its obligations under this Schedule 2.4 (Security Management).

3 SECURITY MANAGEMENT PLAN

3.1 Within thirty (30) Working Days of the Effective Date, the Supplier shall prepare and submit to the Authority for approval in accordance with Clause 4.3 a fully developed, complete and up-to-date Security Management Plan which shall.:

(a) comply with the Baseline Security Requirements;

(b) detail the process for managing any security risks from Sub-contractors and third parties authorised by the Authority with access to the Services, processes associated with the delivery of the Services, the Authority Premises, the Supplier System, the Authority System (to extent that it is under the control of the Supplier) and any ICT, information and data (including the Authority Confidential Information and the Authority Data) and any system that could directly or indirectly have an impact on that information, data and/or the Services;

(c) unless otherwise specified by the Authority in writing, be developed to protect all aspects of the Services and all processes associated with the delivery of the Services, including the Authority Premises, the Supplier System, the Authority System (to the extent that it is under the control of the Supplier) and any ICT, information and data (including the Authority Confidential Information and the Authority Data) to the extent used by the Authority or the Supplier in connection with this Agreement or in connection with any system that could directly or indirectly have an impact on that information, data and/or the Services;

(d) set out the plans for transiting all security arrangements and responsibilities from those in place at the Effective Date to those incorporated in the ISMS at the date set out in Schedule 6.1 (Implementation Plan) for the Supplier to meet the full obligations of the security requirements set out in Schedule 2.1 (Services Description) and this Schedule 2.4 (Security Management);

(e) set out the scope of the parts of Authority System that are under the control of the Supplier;

(f) be structured in accordance with ISO/IEC 27001 and ISO/IEC 27002, cross-referencing if necessary to other Schedules which cover specific areas included within those standards; and

(g) be written in plain English in language which is readily comprehensible to the Supplier's Personnel and the Authority engaged in the Services and shall reference only documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule 2.4 (Security Management).

3.2 If the Security Management Plan submitted to the Authority pursuant to paragraph 3.1 is approved by the Authority, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule 2.4 (Security Management). If the Security Management Plan is not approved by the Authority, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Authority and re-submit it to the Authority for approval. The Parties shall use all reasonable endeavours to ensure that the approval process takes as little time as possible. If the Authority does not approve the Security Management Plan following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No approval to be given by the Authority pursuant to this paragraph 3.2 may be unreasonably withheld or delayed. However, any failure to approve the Security Management Plan on the grounds that it does not comply with the requirements set out in paragraph 3.1 shall be deemed to be reasonable.

3.3 Approval by the Authority of the Security Management Plan pursuant to paragraph 3.2 or of any change or amendment to the Security Management Plan shall not relieve the Supplier of its obligations under this Schedule.

4 AMENDMENT AND REVISION OF THE ISMS AND SECURITY MANAGEMENT PLAN

4.1 The ISMS and Security Management Plan shall be fully reviewed and updated by the Supplier at least annually to reflect:

(a) emerging changes in Standards, Good Industry Practice and HMG practices;

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

(c) any new perceived or changed security threats; and

(d) any reasonable change in requirement requested by the Authority.

4.2 The Supplier shall provide the Authority with the results of such reviews as soon as reasonably practicable after their completion and amend the ISMS and Security Management Plan at no additional cost to the Authority.

4.3 Subject to paragraph 4.4, any change which the Supplier proposes to make to the ISMS or Security Management Plan (as a result of a review carried out pursuant to Clause 4.1, an Authority request, a change to Schedule 2.1 (Services Description) or otherwise) shall be subject to the Variation Procedure and shall not be implemented until approved in writing by the Authority.

4.4 The Authority may, where it is reasonable to do so, approve and require changes or amendments to the ISMS or Security Management Plan to be implemented on timescales faster than set out in the Variation Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Variation Procedure for the purposes of formalising and documenting the relevant change or amendment for the purposes of this Agreement.

5 SECURITY TESTING

5.1 The Supplier shall conduct relevant Security Tests from time to time (and at least annually across the scope of the ISMS) and additionally after significant architectural changes to the ICT Environment or after any change or amendment to the ISMS, (including security incident management processes and incident response plans) or the Security Management Plan. Security Tests shall be designed and implemented by the Supplier (and where deemed necessary, through the services of independent certified companies) so as to minimise the impact on the delivery of the Services and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Authority.

5.2 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.

5.3 Without prejudice to any other right of audit or access granted to the Authority pursuant to this Agreement, the Authority and/or its authorised representatives shall be entitled, at any time upon giving reasonable 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 (**"Authority Tests"**). The Authority may notify the Supplier of the results of Authority Tests after completion of each Authority Test. If any Authority Test adversely affects the Supplier's ability to meet the Service Levels Targets, the Supplier shall be granted relief against any resultant under-performance for the period of the Authority Test.

5.4 Where any Security Test carried out pursuant to paragraph 5.2 or 5.3 of this Schedule 2.4 (Security Management) reveals any actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the Supplier shall promptly notify the Authority 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 prior written approval, the Supplier shall implement such changes to the ISMS and the Security Management Plan and repeat the relevant Security Tests 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 is to address a non-compliance with the Baseline Security Requirements or security requirements (as set out in Schedule 2.1 (Services Description)) or the requirements of this Schedule 2.4 (Security Management), the change to the ISMS or Security Management Plan shall be at no cost to the Authority.

5.5 If any repeat Security Test carried out pursuant to paragraph 5.4 of this Schedule 2.4 (Security Management) reveals an actual or potential Breach of Security exploiting the same root cause failure, such circumstances shall constitute a material Default. At the Authority's discretion, the Authority shall agree such actions as required with the Supplier to prevent further potential Breach of Security from occurring. All actions shall be at the Supplier's expense.

6 ISMS COMPLIANCE

6.1 The Authority shall be entitled to carry out such security audits as it may reasonably deem necessary in order to ensure that the ISMS maintains compliance with the principles and practices of ISO 27001, the specific security requirements set out in Schedule 2.1 (Services Description) and the Baseline Security Requirements (**"Security Audits"**).

6.2 If, on the basis of evidence provided by Security Audits, it is the Authority's reasonable opinion that compliance with the principles and practices of ISO/IEC 27001, the specific security requirements set out in Schedule 2.1 (Services Description) and/or the Baseline Security Requirements is not being achieved by the Supplier (a **"Security Non-Compliance"**), then the Authority shall notify the Supplier of the Security Non-Compliance and give the Supplier a reasonable time (having regard to the extent and criticality of any non-compliance and any other relevant circumstances) to implement any necessary remedy. If the Supplier does not remedy the Security Non-Compliance within the required time then the Authority shall have the right to obtain an independent audit against these standards in whole or in part (an **"Independent Security Audit"**).

6.3 If, as a result of any Independent Security Audit, the Supplier is found to be non-compliant with the principles and practices of ISO/IEC 27001, the specific security requirements set out in Schedule 2.1 (Services Description) and/or the Baseline Security Requirements then the Supplier shall, at its own expense, undertake those actions required in order to achieve the necessary compliance and shall reimburse in full the costs incurred by the Authority in obtaining such audit.

7 BREACH OF SECURITY

7.1 Either Party shall notify the other in accordance with the agreed security incident management process as defined by the ISMS upon becoming aware of any Breach of Security or attempted Breach of Security.

7.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in paragraph 7.1, the Supplier shall immediately take all reasonable steps (which shall include any action or changes reasonably required by the Authority) necessary to:

(a) minimise the extent of actual or potential harm caused by any Breach of Security;

(b) remedy such Breach of Security to the extent possible and protect the integrity of the ICT Environment to the extent within its control against any such Breach of Security or attempted Breach of Security;

(c) apply a tested mitigation against any such Breach of Security or attempted Breach of Security and, provided that reasonable testing has been undertaken by the Supplier, if the mitigation adversely affects the Supplier's ability to deliver the Services so as to meet the Service Level Targets, the Supplier shall be granted relief against any resultant under-performance for such period as the relevant Authority, acting reasonably, may specify by written notice to the Supplier;

(d) prevent a further Breach of Security or attempted Breach of Security in the future exploiting the same root cause failure; and

(e) supply any requested data to the Authority or the Computer Emergency Response Team for UK Government ("NCSC Incident Management Team") on the Authority's request within 2 Working Days and without charge (where such requests are reasonably related to a possible incident or compromise). Any fines issued to the Authority resulting from failure to comply that is reasonably determined to be caused by the Supplier's inactivity or actions shall be reimbursed by the Supplier; and

(f) as soon as reasonably practicable provide to the Authority full details (using the reporting mechanism defined by the ISMS) of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Authority.

7.3 In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the ISMS with the Baseline Security Requirements or security requirements (as set out in Schedule 2.1 (Services Description)) or the requirements of this Schedule, then any required change to the ISMS shall be at no cost to the Authority.

8 VULNERABILITES AND CORRECTIVE ACTION

8.1 The Authority and the Supplier acknowledge that from time to time vulnerabilities in the ICT Environment will be discovered which unless mitigated will present an unacceptable risk to the Authority's information.

8.2 The severity of threat vulnerabilities for Supplier COTS Software and Third Party COTS Software shall be categorised by the Supplier as 'Critical', 'Important' and 'Other' by aligning these categories to the vulnerability scoring according to the agreed method in the ISMS and using the appropriate vulnerability scoring systems including:

(a) the 'National Vulnerability Database' 'Vulnerability Severity Ratings': 'High', 'Medium' and 'Low' respectively (these in turn are aligned to CVSS scores as set out by NIST http://nvd.nist.gov/cvss.cfm); and

(b) Microsoft's 'Security Bulletin Severity Rating System' ratings 'Critical', 'Important', and the two remaining levels ('Moderate' and 'Low') respectively.

8.3 The Supplier shall procure the application of security patches to vulnerabilities within a maximum period from the public release of such patches with those vulnerabilities categorised as 'Critical' within two (2) days of release, 'Important' within ten (10) days of release and all 'Other' within thirty (30) days of release, except where:

(a) the Supplier can demonstrate that a vulnerability is not exploitable within the context of any Service (e.g. because it resides in a software component which is not running in the service) provided vulnerabilities which the Supplier asserts cannot be exploited within the context of a Service must be remedied by the Supplier within the above timescales if the vulnerability becomes exploitable within the context of the Service;

(b) the application of a 'Critical' or 'Important' security patch adversely affects the Supplier's ability to deliver the Services in which case the Supplier shall be granted an extension to such timescales of 5 days, provided the Supplier had followed and continues to follow the security patch test plan agreed with the Authority; or

(c) the Authority agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the ISMS.

8.4 The Supplier Solution and Implementation Plan shall include provisions for major version upgrades of all Supplier COTS Software and Third Party COTS Software to be upgraded within 6 months of the release of the latest version, such that it is no more than one major version level below the latest release (normally codified as running software no older than the 'n-1 version') throughout the Term unless:

(a) where upgrading such Supplier COTS Software and Third Party COTS Software reduces the level of mitigations for known threats, vulnerabilities or exploitation techniques, provided always that such upgrade is made within 12 months of release of the latest version; or

(b) it is otherwise agreed with the Authority in writing.

8.5 The Supplier shall:

(a) implement a mechanism for receiving, analysing and acting upon threat information supplied by NCSC Cyber Information Sharing Partnership (CiSP), or any other competent Central Government Body;

(b) ensure that the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;

(c) ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the ICT Environment by actively monitoring the threat landscape during the Term;

(d) pro-actively scan the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) for vulnerable components and address discovered vulnerabilities through the processes described in the ISMS as developed under paragraph 2.3(e) of this Schedule 2.4 (Security Management);

(e) from the date specified, and at the agreed frequency specified in the Security Management Plan provide reports to the Authority covering both patched and outstanding vulnerabilities in the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier).

(f) propose interim mitigation measures to vulnerabilities in the ICT Environment known to be exploitable where a security patch is not immediately available;

(g) remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of the Supplier Solution and ICT Environment); and

(h) inform the Authority when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the security of the ICT Environment and provide initial indications of possible mitigations.

8.6 If the Supplier is unlikely to be able to mitigate the vulnerability within the timescales under paragraph 8 of this Schedule 2.4 (Security Management), the Supplier shall immediately notify the Authority.

8.7 A failure to comply with paragraph 8.5 of this Schedule 2.4 (Security Management) shall constitute a Default.

ANNEX 1- Baseline Security Requirements

1 Higher Classifications

The Supplier shall not handle Authority information classified SECRET or TOP SECRET except if there is a specific requirement and in this case prior to receipt of such information the Supplier shall seek additional specific guidance from the Authority.

2 End User Devices

2.1 When Authority Data resides on a mobile, removable or physically uncontrolled device it must be stored encrypted using a product or system component which has been formally assured through a recognised certification process of the UK National Cyber Security Centre (NCSC) to at least Foundation Grade, for example, under the CESG Commercial Product Assurance scheme ("CPA").

2.2 Devices used to access or manage Authority Data and services must be under the management authority of relevant Authority or Supplier and have a minimum set of security policy configuration enforced. These devices must be placed into a 'known good' state prior to being provisioned into the management authority of the Authority. Unless otherwise agreed with the relevant Authority in writing, all Supplier devices are expected to meet the set of security requirements set out in the NCSC End User Devices Platform Security Guidance (https://www.ncsc.gov.uk/guidance/end-user-device-security). Where the guidance highlights shortcomings in a particular platform the Supplier may wish to use, then these should be discussed with the Authority and a joint decision shall be taken on whether the residual risks are acceptable. Where the Supplier wishes to deviate from the NCSC guidance, then this should be agreed in writing on a case by case basis with the Authority.

3 Security Architectures

3.1 The Supplier shall apply the 'principles of least privilege and need-to-know' (the practice of limiting systems, processes, information and user access to the minimum possible level) to the design and configuration of IT systems which will process or store Authority Information.

3.2 When designing and configuring the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) the Supplier shall follow Good Industry Practice and seek guidance from recognised security professionals with the appropriate skills and/or industry wide recognised professional certification for all bespoke or complex components of the Supplier Solution.

3.3 The Supplier shall:

(a) consider the use of cryptography to ensure effective controls to protect the confidentiality, authenticity and integrity of information assets;

(b) use encryption of information to protect data at rest and in transit;

(c) use cryptography to verify the authenticity and integrity of stored or transmitted information; and

(d) use cryptographic techniques to authenticate users and other systems requesting access to system entities and resources.

3.4 Where cryptography is used, a devised policy must be in place which describes the use, protection and lifecycle (i.e. generation of keys, storage, retrieval and distribution process and cryptographic destruction).

4 Supplier's Personnel Security

4.1 Supplier Personnel shall be subject to pre-employment checks that include, as a minimum: identity HMG Baseline Personnel Security Standard (BPSS), unspent criminal convictions and right to work.

4.2 The Supplier shall agree on a case by case basis Supplier's Personnel roles which require specific government National Security Vetting (NSV) clearances (such as 'SC') including system administrators with privileged access to IT systems which store or process Authority Data.

4.3 Where applicable, all Supplier Personnel that require access to police premises or handle live policing information must obtain Non Police Personnel Vetting (NPPV) clearances as detailed in the National Police Chiefs Council (NPCC) IS Community Security Policy. The Supplier shall agree with the Authority where it is necessary to access such premises or information on a case by case basis Supplier Personnel roles which require specific NPPV clearances (such as NPPV level 3 clearance required for national systems contractors).

4.4 The Supplier shall prevent Supplier Personnel who are unable to obtain the required Authority confirmed NSV security clearances from accessing Authority's information assets and systems which store, process, or are used to manage Authority Data except where agreed with the Authority in writing.

4.5 All Supplier's Personnel that have the ability to access Authority Data or systems holding Authority Data shall undergo regular training on secure information management principles. Unless otherwise agreed with the relevant Authority in writing, this training must be undertaken annually.

4.6 Where the Supplier or Sub-contractors grants increased IT privileges or access rights to Supplier Personnel, those Supplier Personnel shall be granted only those permissions necessary for them to carry out their duties. When Supplier Personnel no longer need elevated privileges or leave the organisation, their access rights shall be revoked within one (1) Working Day.

5 Identity, Authentication and Access Control

The Supplier shall operate an access control regime to ensure all users and administrators of the Supplier Solution are uniquely identified and authenticated when accessing or administering the Services. Access to information and application system functions should be restricted in accordance to "least privilege and need-to-know" principles, users and administrators shall be allowed access only to those parts of the Supplier Solution and information they require. The Supplier shall retain an audit record of accesses.

6 System and Application Access Control

6.1 Restriction to access must be based on individual business duties; the following should be implemented to support access restrictions:

(a) controls of what data can be accessed;

(b) control of access rights of users, e.g. read, write, delete and execution of specific programmes and applications;

(c) limiting information to necessity;

(d) provisions of physical and logical access controls (to isolate applications and systems); and

(e) secure log-on procedures and password management processes and procedures and:

(i) enforce users to use individual user IDs and passwords to maintain accountability;

(ii) maintain a record of previously used passwords to prevent re-use;

(iii) store and transmit passwords in protected form;

(iv) store passwords securely;

(v) prioritise administrators and remote user accounts, ensure that robust measures are in place to protect administrators and remote user accounts;

(vi) use account lockouts / account throttling and protective monitoring; and

(vii) password blacklisting (i.e. to prevent dictionary attacks).

7 Audit and Monitoring

7.1 The Supplier shall collect audit records which relate to security events in the systems or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Supplier audit records should (as a minimum) include:

(a) logs to facilitate the identification of the specific asset which makes every outbound request external to the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier). To the extent the design of the Supplier Solution and Services allows such logs shall include those from DHCP servers, HTTP/HTTPS proxy servers, firewalls and routers; and

(b) security events generated in the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) and shall include: privileged account logon and logoff events, session activities, the start and termination of remote access sessions, security alerts from desktops and server operating systems and security alerts from third party security software.

7.2 The Supplier and the Authority shall work together to establish any additional audit and monitoring requirements for the ICT Environment.

7.3 The Supplier shall retain audit, security and other non-application logs or records for a period of at least 12 months. These include but not limited to:

(a) user IDs;

(b) date and time of log on and log off, and other key events;

(c) terminal identity;

(d) successful and failed attempts to access systems, data or applications;

(e) files and networks accessed;

(f) changes to system configurations;

(g) use of system utilities;

(h) exceptions and other security-related events, such as alarms triggered;

(i) activation of protection systems, such as intrusion detection systems; and

(j) antimalware.

8 Secure Sanitisation and Destruction of Storage Media

8.1 All items of equipment used to sore Authority's information assets must be risk assessed to determine whether such items may be re-used or physically destroyed.

8.2 Sanitisation is the process of treating data held on storage media to reduce the likelihood of retrieval and reconstruction to an acceptable level. Sanitisation allows for the re-use of equipment; the National Cyber Security Centre (NCSC) provides a range of guidance relating to overwriting / sanitisation services and tools

8.3 Once there is no longer a need for the information or asset it must be destroyed. The destruction of sensitive items should be undertaken via a secure process in accordance with Centre for the Protection of National Infrastructure (CPNI) guidance.

ANNEX 2 - Security Aspects Letter

Border Force

Home Office Border Force
Critical System and Services
2 Marsham St,
Westminster,
London
SW1P 4DF

Monday, 17 September 2018

Dear Sir / Madam,

SECURITY ASPECTS LETTER relating to: Home Office Border Force Cyclamen System

Introduction

This letter establishes the security provisions with which the **Supplier** shall comply in providing Service and Maintenance of Fixed and Mobile RN Detection Equipment services (the **Services**) the Home Office (the **Authority**). The instructions in this letter must be followed by all personnel involved in Cyclamen including the **Supplier's** Programme Team, Delivery Partners and commercial suppliers, where there is doubt in their application; advice must be sought from **Authority's** Departmental Security Unit in the first instance.

The **Authority** requires the **Supplier**, as appropriate, to comply with guidance contained in the latest versions of Cabinet Office Security Policy Framework (SPF), current CESG Information Standards, current CESG Good Practices and current CESG Cryptographic Standards.

Where there is no guidance or specific **Authority** policy in place, then the current industry best business practice should be employed. The emphasis should always be for the Supplier to seek guidance from the Authority where clarity is required.

The **Services** shall be provided under a services contract between the **Authority** and the Supplier (as defined under the main **Contract**), and will involve the **Supplier** holding material that has been assigned a classification under the Government Security Classifications (GSC)[1] and also legacy material marked under the Government Protective Marking System (GPMS).

It is a condition of the Contract that:

1. Access to sensitive information must ONLY be granted on the basis of a genuine "need to know" and to personnel's with appropriate security control (i.e. clearance / vetting)
2. Classified material under either the GSC or GPMS must be protected i accordance to the HMG Security Policy Framework (SPF). Any system used to handle the **Authority's** classified material will have to provide appropriate assurance in accordance with the **Authority's** policy, Cabinet Office policy and CESG guidance.

It is a condition of the Contract that classified material under either the GSC or GPMS must be protected according to HMG Security Policy Framework (SPF) and any further Data Handling Procedures as defined by **Authority**.

The **Authority** may notify the **Supplier**, from time to time of additional protective measures, such

[1] Government Security Classifications April 2014, Version 1.0, dated October 2013 issued by the Cabinet Office

measures may be subject to formal change control.

The permission to release sensitive information outside of the **Contract** framework must be made in writing and formally approved by Information Asset Owner (IAO).

The **Supplier** shall undertake the Contract within the United Kingdom at pre-designated sites (to be agreed by the **Authority** and the **Supplier**) and shall not transfer any caveated or classified material obtained through this Contract to any other site without the prior written consent of the **Authority's** Corporate Security Unit

Any system used to handle the **Authority's** classified material will have to provide appropriate assurance in accordance with the **Authority's** policy, Cabinet Office policy and CESG guidance.

Government Protective Marking System (GPMS)

Cyclamen's legacy information will continue to be protectively marked under the old scheme. Existing documentation may retain its classification provided no changes are made to the document and the document continues to be used for internal, departmental purposes only.

Government Security Classifications (GSC)

GSC is a 3 Tier classification system comprising OFFICIAL, SECRET and TOP SECRET.

All information created on or after 02 April 2014 should be classified under the new three tiers, or as and when agreed (i.e. from date of transition to the new classification).

Material generated prior of the agreed date of transition to GSC and classified according to the legacy GPMS is to retain its marking and not be re-classified according to GSC unless both of the following are true:

- The document is revised and/or re-issued.
- The originator of the document or, after reasonable endeavours to locate the originator have failed, the IAOs have approved its remarking.
- It is being shared or exchanged with other Government Departments, external partners or communicated outside the UK after 01 April 2014.

Material that is classified OFFICIAL may not be marked. Material that is classified OFFICIAL but has the caveat SENSITIVE applied to it will be marked OFFICIAL-SENSITIVE (i.e., markings must be in CAPITALS at the top and bottom of each page on the document). The standard of protection required, as a minimum, to protect classified material is described as an annex of this letter.

OFFICIAL-SENSITIVE is not another classification. It is a handling caveat within the OFFICIAL Classification. OFFICIAL-SENSITIVE should be used for OFFICIAL information where there is a clear and justifiable requirement to reinforce the 'need to know' for information judged to be more sensitive (by application of additional handling controls). Handling instructions need to be included for all OFFICIAL-SENSITIVE documentation by writing at the top of an email or the front page of documentation, e.g. "This is for your eyes only – it remains highly contentious and should not be copied any further." Other instructions should include:

1. Who is allowed access to the information?
2. How the information or data is allowed to be circulated or forwarded
3. How that information is to be stored.
4. Time sensitive information, where information can be distributed more widely or re-classified after a particular date or event has passed.
5. National caveat to restrict the dissemination outside of UK and to UK nationals only.

Handling and management of OFFICIAL-SENSITIVE must be followed with instructions as provided by the author of the data asset.

Material that is classified as SECRET is VERY sensitive information; justifying heightened protective measures and restrictive handling due to the nature or source of its content. For the storage and control of assets marked SECRET, do everything possible to:

1. avoid making accidental compromises or damages during storage, handling, use, processing, transmission or transport.
2. limit knowledge of planned movement of physical assets.
3. offer resistance to professionals or violent attacks deliberately compromises and detection to actual or attempted compromises and help identify those responsible.
4. dispose of or destroy in a manner to make retrieval or reconstruction highly unlikely and prevent identification of constituent parts.

All information in this security domain should be clearly and conspicuously marked 'SECRET'. Information that requires more restrictive handling due to the nature or source of its content may merit special handling instructions as detailed below.

The Cabinet Office maintains the following list of core descriptors to ensure a consistent approach is adopted across all departments. There are 3 descriptors: COMMERCIAL, LOCSEN and PERSONAL.

LOCSEN refers to sensitive information not to be accessed by overseas personnel.

COMMERCIAL: Indicates commercial or market sensitive information, including that subject to statutory or regulatory obligations that may damage the **Authority** or commercial partners if improperly accessed. For example, information relating to contract negotiations, external communications and procurement tender exercises.

PERSONAL: Indicates particularly sensitive information relating to an identifiable individual, where inappropriate access could have damaging consequences. For example, where relating to investigations, vulnerable people or individuals, poor performance reviews, grievances, disciplinary action, personal medical records or details of sensitive appointments.

Specific markings may be used either to indicate the provenance of sensitive information, or as a means to control dissemination. National Caveats may be used to designate assets of particular sensitivity to the UK

or where dissemination must be restricted to individuals from specific foreign nations. Unless explicitly named, information bearing a national caveat must not be sent to foreign governments, overseas contractors, international organisations or released to any foreign nationals (either overseas or in the UK) without the **Authority**'s consent.

As a general rule all information marked RESTRICTED, PROTECT and UNCLASSIFIED under GPMS are provided sufficient protection when stored in an OFFICIAL environment and no additional security controls other than that specified in the SPF are required.

All GPMS documents are to be handled as follows:

GPMS	GSC
Not Protectively Marked PROTECT RESTRICTED	OFFICIAL (with caveats applied as appropriate)
SECRET	SECRET

Table of Security Aspects

Aspect	Description	Security Classification	Comments
General			
Description and system name	General purpose of the Cyclamen System	OFFICIAL	Public knowledge
Existence of the system	Existence of Cyclamen Systems	OFFICIAL	Public knowledge
Delivery Partners	Names of Delivery Partners	OFFICIAL	
Suppliers	Names of Commercial Suppliers	OFFICIAL	
Project Management Office			
Cyclamen Port Codes (numbers)		OFFICIAL	
Cyclamen Port Names		OFFICIAL-SENSITIVE	
'Customers' / Stakeholders	Names of 'customers' / stakeholders (such as OGD's etc.)	OFFICIAL	
Business Requirements	Individual or collated business requirements	OFFICIAL for HIGH level business requirements. OFFICIAL-SENSITIVE for LOW Level, detailed requirement document sets.	
Business requirements, non-functional requirements.		OFFICIAL for most reports, however depending on content, reports could be up to OFFICIAL-SENSITIVE (e.g. Document sets which includes Security Requirements and user stories containing security enforcing functions)	
Project plans, dependencies and prioritised backlogs		OFFICIAL-SENSITIVE	
Delivery metrics and detailed MI reports		OFFICIAL-SENSITIVE	

Aspect	Description	Security Classification	Comments
Incident reports		OFFICIAL for most reports (identified by Port Code), however depending on content, sensitive reports should be classified at OFFICIAL-SENSITIVE	
Risks, issues, assumptions and actions		OFFICIAL-SENSITIVE	
Change requests		OFFICIAL for most reports, however depending on content, sensitive reports should be classified at OFFICIAL-SENSITIVE	
Programme Documentation	Programme documentation which includes: Detailed Systems and Architectural Designs, Data Model Detailed Installation guides, Identification or Configuration of the system, network and Assets and documentation which describes the operational capabilities and practices, Audits. Documentation WITH ANY of the following: IP addresses, Server Names, Identification and Naming of programme specific Assets and Stakeholders, Naming Conventions or detailed information about operational capabilities and security-enforcing functions.	OFFICIAL-SENSITIVE	Strict handling instructions required. Transmission of information restricted to secure, trusted government networks only. UK National caveat (exception to rule must be made in writing to Border Force / Home Office OSCT)

Aspect	Description	Security Classification	Comments
Programme Documentation (HIGH level)	High level programme documentation (e.g. plans and progress reports) without reference to specific capabilities	OFFICIAL	
Detailed Description of current capability (fixed and mobile) covering ALL Cyclamen locations. Reporting against: capability gaps, location of equipment, etc.	Documents which indicate where, when and what specific capabilities or infrastructure will be deployed, design parameters, e.g. architecture A complete set of information covering **ALL** aspects such as How (The complete Cyclamen process from end to end), Where (location), What (actions, processes and tasks), When (times and dates), Frequency (timings and how often), etc.	SECRET Subset of Information: OFFICIAL-SENSITIVE	UK National caveat (exception to rule must be made in writing to Border Force / Home Office OSCT)
Policy / legislation formulation or proposals regarding non-sensitive subject matter		OFFICIAL	
Sensitive or contentious policies		OFFICIAL-SENSITIVE	
Sensitive internal / operational policy and guidance documents		OFFICIAL-SENSITIVE	
Management documentation & plans WITHOUT financial information		OFFICIAL	

Aspect	Description	Security Classification	Comments
Management documentation & plans WITH financial information		OFFICIAL for: Internal communications relating to contracts; Internal information relating to procurement exercises. OFFICIAL-SENSITIVE for key commercial information: contract negotiations, external communications and procurement tender exercises	
Delivery Partners Contract	Details of the contract that can be released under an FOI request	OFFICIAL	The aspects of the contract that can be released under FOI should be confirmed with UKBF before release.
Cyclamen Dosimeter (management) reports		OFFICIAL	
Operating Mandate Guidance		OFFICIAL	
Technical Design, Development and Architecture			
Architecture of the system / network **WITH** IP Addresses		OFFICIAL-SENSITIVE	
Audit and Accounting Data	Audit and accounting data	OFFICIAL	OFFICIAL-SENSITIVE where data is requested for investigative purposes.
Authentication Credentials	User passwords	OFFICIAL-SENSITIVE	Transmission of password must be secure and via a trusted government network (i.e. GSi, PSN, CJSM, etc).
AWE issued configuration instructions to Delivery Partners and Subcontractors of the Delivery Partners for other devices	Calibrations instructions as provided by AWE for dissemination.	OFFICIAL-SENSITIVE	

Aspect	Description	Security Classification	Comments
Data Centre Names		OFFICIAL	
Data Centre Locations (including Security Operations Centre)	Identification of physical location(s) at which central equipment and service facilities reside (primary and secondary data centres).	OFFICIAL-SENSITIVE	
Data Model	Requirements pertaining to the Data Model, including policies and requirements	OFFICIAL-SENSITIVE	
Details of IP Addresses	Applies to "Live" production systems only. Other systems (e.g. Test systems) with DIFFERENT IP addresses are to be treated as OFFICIAL.	OFFICIAL-SENSITIVE	Strict handling instructions required. Transmission of information restricted to secure, trusted government networks only. UK National caveat, (exception to rule may be provided to Delivery Partner, upon written request to Border Force / Home Office OSCT)
Server Names		OFFICIAL	
System passwords		OFFICIAL-SENSITIVE	Strict handling instructions required. Transmission of information restricted to secure, trusted networks only. UK National caveat, (exception to rule may be provided to Non-UK Delivery Partner(s), upon written request to Border Force / Home Office OSCT)
Test Data: Anonymised / Fictitious Data	Fictitious data generated for test purposes only	OFFICIAL	

Aspect	Description	Security Classification	Comments
System Configuration Data	System configuration data, e.g. network configuration and IP addresses	OFFICIAL-SENSITIVE	UK National caveat, (exception to rule may be provided to Non-UK Delivery Partner(s), upon written request to Border Force / Home Office OSCT)
Pre-Production Systems	Pre-Production systems	OFFICIAL for HIGH level development designs which excludes locations and IP addresses. OFFICIAL-SENSITIVE for LOW Level, detailed development document sets.	
Qualification / System Acceptance Test data & reports	Fictitious data generated for test purposes only	N/A	
Redacted Detailed Designs	Redacted Architecture designs detailing the Configuration of the system/network. WITHOUT: IP addresses, Server Names, System Identification or Naming Conventions, or detailed information about security-enforcing functions.	OFFICIAL	
Business Support and Administration			
Authority issued staff lists and org charts,		OFFICIAL	
Commercial documentation including MACs, DACs, time sheets, resource forecasts, contracts, tender information, purchase orders, invoices.		OFFICIAL	
Supplier's Personnel contact details (both Authority and Supplier side)		OFFICIAL	

Aspect	Description	Security Classification	Comments
Security Agency Correspondence		OFFICIAL-SENSITIVE	
Ministerial reports and submissions		OFFICIAL-SENSITIVE	
Security and Technical			
Security Documentation	IT Health Check (ITHC) reports Risk Management, Risk Treatment Plans (RTP) and Accreditation Document Sets (RMADS)	OFFICIAL-SENSITIVE	UK National caveat Exception to rule authorised through Border Force / Home Office OSCT.
Known vulnerabilities relevant to the system, compliance and patch deficits		Are to be classified at the highest classification of the data contained in the system to which it relates. Where the vulnerability only applies to OFFICIAL information the caveat SENSITIVE is to be applied.	
Security Working Group Minutes		OFFICIAL-SENSITIVE	
Requirements / designs /security enforcing functions relating to OFFICIAL SENSITIVE data		OFFICIAL-SENSITIVE	
Incident reports		OFFICIAL for most reports, however depending on the content, sensitive reports should be classified at OFFICIAL-SENSITIVE	

Aspect	Description	Security Classification	Comments
Configuration details, and specifically amendment of common or best practice, of software or hardware used in the development or operational environment		OFFICIAL-SENSITIVE	Strict handling instruction required. Transmission of information restricted to secure, trusted network only. UK National caveat (exception to rule must be made in writing to the Authority's Departmental Security Unit).
Cryptographic Keys / "Key Material"		Are to be classified at the highest classification of the data contained in the system to which it relates and for OFFICIAL information the caveat SENSITIVE is to be applied (plus Crypto caveats such as ACCSEC in accordance with CESG Information Assurance Standard Number 4)	

Personnel Security Requirements

The Security Policy Framework (SPF) provides guidance on the general requirements for National Security Vetting (NSV) and clearance requirements in relation to the Protective Marked assets.

The Supplier shall report immediately to the Home Office Corporate Security Directorate (HO CSD), via the UKBF BSP Security team, any incident or information that raises doubts as to the suitability of an individual's continued security clearance.

Employees / contractors / individuals (who provide a service to Home Office Border Force Cyclamen) with access to classified material must be warned against divulging it to any unauthorised person and must be informed that the Official Secrets Acts 1911-1989 apply to them. The Supplier must ensure Home Office Corporate Security Directorate have the full particulars of all individuals who at any time are concerned with protectively marked matters, in order that appropriate security clearances can be confirmed or undertaken.
NSV/clearance may be undertaken by suppliers where they have the facilities and organisation to do so, in which event a 'Confirmation of Clearance' form must be submitted to UKBF prior to work being undertaken by the individual concerned. Where the organisation does not have the ability to undertake clearance/vetting, the process will be undertaken by the Home Office Departmental Security Unit. Sufficient time must be allowed for this process to complete before the individual may undertake any work on Cyclamen Programme.
The clearance requirements detailed in this section apply to all personnel within UKBF, Delivery Partners and suppliers who are involved in the Cyclamen Programme.

As a general rule, 'equivalent' levels of vetting/clearance granted outside the UK are not automatically accepted as an equivalent to UK vetting. If in doubt, please refer to the Home Office CSD for further guidance.

The table below provides details of the clearance/vetting requirements that apply to individuals involved in the Cyclamen Programme. For reference, the minimum standard of Security Check for Home Office Programmes is Baseline Personnel Security Standard (BPSS) followed by one of the following UK NSV levels, in ascending order: Counter-Terrorist Check (CTC); Security Check (SC); and Developed Vetting (DV).

Vetting Requirements:	
Minimum Requirement for all work associated with the main Cyclamen **Programme and without access to: core IT architecture,** Security Enforcing Functions information and Low Level **Technical Design Documentation.**	**Home Office CSD confirmed Counter-Terrorist Check (CTC)**
Access to Cyclamen Server Room	**Home Office CSD confirmed Security Check (SC).**
Individuals with any access to material bearing the UK EYES ONLY caveat	**Minimum Requirement; and** **UK National**
Individuals with the ability to influence any aspect of the design or implementation of Security Enforcing Functions	**Home Office CSD confirmed Security Check (SC).**
Individuals with sign-off authority on any aspect of the business or technical design for any aspect of the Programme	**Home Office CSD confirmed Security Check (SC).**
All others	**As agreed and documented with UKBF**

Roles and Requirements	
Security Manager (responsible for day-to-day security functions)	**Home Office CSD confirmed Security Check (SC).**
Crypto Custodian (may have additional special requirements for clearance)	**Home Office CSD confirmed Security Check (SC).**
System Management & System Administrator staff with **authorised access to sensitive classified data**	**Home Office CSD confirmed Security Check (SC).**
Design, development and other Supplier's Personnel with authorised access to data **classified at OFFICIAL_SENSITIVE or above**	**Home Office CSD confirmed Security Check (SC).**
Technical/Maintenance staff (other than System Administrators) with unescorted access to live systems or data	**Home Office CSD confirmed Security Check (SC).**
Escorted Technical / **Maintenance staff with limited access to system details to the live systems or data**	**None**
Service Engineers for Mobile Detection Vehicles (provided vehicle is absent of personal data and AWE Cyclamen calibration information)	**Home Office CSD confirmed Counter-Terrorist Check (CTC)**

By signing and dating this letter, below, the **Supplier** acknowledges receipt of this letter and confirms that the levels of classification associated with the requirements listed above have been brought to the attention of the individuals directly responsible for the provision of the **Services** associated with the Contract. Additionally, the **Supplier** confirms that it has fully understood this letter and that the required security controls can and will be taken to safeguard the material concerned.

Signed [signature] Dated 2/7/19

Name LEAH MARSH Position SECURITY ADMINISTRATOR

For and on behalf of (Supplier Name)

Security Department - Leonardo MW Ltd. Sigma House - Christopher Martin Rd - Basildon - SS14 3EL 2/7/19

	OFFICIAL (GSC Tier 1)	OFFICIAL-SENSITIVE (GSC Tier 1)	SECRET (GSC Tier 2)
Clear desk policy	All information and/or assets must be locked away in appropriate security containers when not in use or when away from your workstation for pro-longed periods of time. Computer screens must lock when Supplier's Personnel are away from their workstation.		
Document storage		Protected by one **Authority** approved barrier, e.g. a locked container in secure building.	**Supplier** must meet the criterion for List X status. Class 2/Class 3 cabinet
Electronic storage	May be stored on corporate networks known to be controlled and secured in line with best industry practice and standards. OFFICIAL-SENSITIVE may be securely transferred and stored on a secure Delivery Partner's internal system ("system") provided: 1. The system must be technological and physically secured / compartmentalised to protect and prevent unapproved access from internal and external threats (i.e. 'need to know' principle must be maintained throughout). I. The system must be appropriately assured; II. The system must protect and secure data at rest; III. The system or components of this system when no longer used for day to day operations (e.g. due to faults, etc) must be sanitised in accordance with HMG guidance; IV. When store on this system, all handling rules as described within the document remains. 2. The original handling caveat of the document does not detail the prevention or prohibits the removal of the 'document' to a non-government system.		be stored on an appropriately accredited **SECRET** Network.

(paper)	destruction standard. Particles should be no larger than 4 x 15 mm.	sacks. Keep sacks secure until contents can be burnt (in accordance with CPNI standards)
Disposal (digital storage)	Securely destroy; in accordance with NCSC and CPNI instructions. CESG HMG Information Standard 5: Secure Sanitisation is still applicable.	

Classification – Transmission - The following table defines the transmission methods for Service related data.

	OFFICIAL (GSC Tier 1)	OFFICIAL-SENSITIVE (GSC Tier 1)	SECRET (GSC Tier 2)
	By post or courier, in a Single, sealed envelope with a return address and no classification marking. Use first or second class post.	By post or courier, double enveloped, both fully addressed. Classification shown on inner envelope only. Return address on outer envelope.	Seek permission from Head of Unit. Register movement. Use approved registered mail services in a tamper evident envelope with a 'track and trace.' If local, consider transporting the information by hand with two escorts at SC in a sealed tamper-evident container.
GSI/CJSM or any other Secure Government Network	May be used.	May be used.	Not to be used. Only via an approved system with defined users. Mark the email 'SECRET'. Use specific handling instructions. See separate
Telephone	May be used		Brent to Brent / Russett to Russett in secure area
	May be used. Ensure Conversations cannot be		

Corporate network	May be used Personal data cannot be sent outside the secure boundary - government secure intranet (GSI) or Criminal Justice Secure eMail (CJSM) unless encrypted.	May be used only with permission of the IAO and information is protected with approved encryption controls.	Not to be used
Internet*	May be used		Not to be used
Wireless network*	Acceptable provided material is protected in transit across the wireless network by an approved and encrypted Virtual Private Network (VPN).		Not to be used
SMS Messages	Ensure you have the correct contact number for your recipient and that there is a business requirement to share that information with them. Information to be kept at a minimum. Devices must be company issued / not personally owned. Delete messages when no longer required. Try not to retain messages for longer than a month. Devices must at minimum be PIN or password protected.	Not to be used	Not to be used
Fax	Check recipient is on hand to receive then transmit.	Check recipient is on hand to receive. Send cover sheet first, wait for confirmation before	Not to be used, unless secure, encrypted fax service appropriate to the classification of the data

Appendix 1 – Classification definitions

The **Authority** will advise the **Supplier** on the classification definitions from time to time and the current classifications are described below. (The legacy definition for CONFIDENTIAL is described for completeness and is to be applied where appropriate.) At the date of issue of this Security Aspects Letter, the definitions given in the HMG Security Policy framework are as follows:

Criteria for assessing SECRET assets: Directly threaten an individual's life, liberty or safety (from highly capable threat actors); cause serious damage to the operational effectiveness or security of UK or allied forces in the delivery of the Military tasks such that current or future capability would be rendered unusable, lives would be lost or damage would be caused to installations rendering them unusable; cause serious damage to the operational effectiveness of highly valuable security or intelligence operations; cause serious damage to relations with friendly governments or damage international relations resulting in formal protest or sanction; cause serious damage to the safety, security or prosperity of the UK or friendly nations by affecting their commercial, economic and financial interests; cause serious damage to the security and resilience of Critical National Infrastructure (CNI) assets; cause major impairment to the ability to investigate or prosecute serious organised crime.

Criteria for assessing OFFICIAL assets: All routine **Authority's**, operations and services should be treated as OFFICIAL and this includes a wide range of information, of differing value and sensitivity, which needs to be defended against the OFFICIAL threat profile and to comply with legal, regulatory and international obligations. This includes: The day to day business of the **Authority**, service delivery and public finances and routine international relations and diplomatic activities; public safety, criminal justice and enforcement activities; many aspects of defence, security and resilience; commercial interests, including information provided in confidence and intellectual property; personal information that is required to be protected under the Data Protection Act (1998) or other legislation (e.g. health records).

Within the classification OFFICAL there is a limited subset of information that could have more damaging consequences (for individuals, or the **Authority)** if it were lost, stolen or published in the media. This subset of information is to be managed ***within*** the 'OFFICIAL' classification tier, but may attract additional measures (generally procedural or personnel) to reinforce the 'need to know', especially where it is being released outside the **Authority's** control. In such cases where there is a clear and justifiable requirement to reinforce the 'need to know' within the Tier or when being passed to a third party, assets are to be conspicuously marked: 'OFFICIAL–SENSITIVE'.

Appendix 2 – Declaration

I have read and understood the contents of the SAL, having had the opportunity to clarify any points with the **Authority's** Departmental Security Unit, and will implement the requirements of the SAL to protect the **Authority's** data and information.

I understand that failure to implement the contents of the SAL may result in a report being raised and incur breach points that may lead to further action depending on the seriousness of the breach.

I also understand that I am to report any suspected breach to the **Authority's** Departmental Security Unit as soon as possible after becoming aware of the breach.

Name:	LEAH MARSH
Post/Department:	SECURITY ADMINISTRATOR
Date:	2/7/19