Department of Energy & Climate Change

Smart Meters Programme
Schedule 2.5

(Security Management Plan) (CSP Central version)

Schedule 2.5 (Security Management Plan) (CSP Central version)

Amendment History			
Version	**Date**	**Author**	**Status**
v.1	Signature Date	DECC	Execution Copy

SCHEDULE 2.5
SECURITY MANAGEMENT PLAN

PURPOSE

This Schedule 2.5 (Security Management Plan) addresses the following issues:

(a) the principles of security to be applied in relation to the Contractor Solution (including in relation to the management, implementation and operation of all Sub-contractors);

(c) the development, implementation, operation, maintenance and continual improvement of:

(i) the Contractor Security Policy;

(ii) an "Information Security Management System" (as defined by ISO/IEC 27001 and as further described in Part B of this Schedule 2.5) (the "**ISMS**"); and

(iii) the Security Management Plan,

(together, the "**Contractor Security Documents**");

(d) compliance with the Security Requirements;

(e) compliance with standards relating to security issues (as further described in Schedule 2.3 (Standards)) (the "**Security Standards**"); and

(f) obligations in the event of actual, potential or attempted breaches of security.

Without limiting the DCC's other rights and remedies under this Agreement or otherwise, the parties acknowledge that the DCC shall be entitled to exercise its rights under Schedule 8.10 (Enhanced Scrutiny and Step-in) in response to a breach or material breach (as applicable) by the Contractor in relation to its obligations under this Schedule 2.5.

This Schedule 2.5 comprises the following parts:

Part	Scope
Part A	Principles of security
Part B	Contractor Security Documents
Part C	Testing
Part D	ISO/IEC 27001 certification
Part E	Security audits
Part F	Breach of Security
Appendix 1	Security Management Requirements

Appendix 2	Contractor Security Policy
Appendix 3	Outline Security Management Plan

PART A – PRINCIPLES OF SECURITY

1. IMPORTANCE OF SECURITY ISSUES

1.1 The Contractor acknowledges that the DCC places great emphasis on the confidentiality, integrity and availability of the DCC Data, and consequently on the security of:

(a) the Contractor Solution;

(b) the DCC Environment; and

(c) the DCC Services.

The Contractor also acknowledges the critical and confidential nature of the DCC Data.

2. OVERVIEW OF CONTRACTOR OBLIGATIONS

2.1 The Contractor shall be responsible for:

(a) the security of the Contractor Solution;

(b) the security of the Sites;

(c) the security of Contractor Personnel (including compliance with paragraph 3.3(b));

(d) the security of all Sub-contractors (including their systems, solutions and services) in respect of their involvement in the provision of the Services; and

(e) the implementation and on-going management of, and compliance with, the Contractor Security Documents.

2.2 The Contractor shall comply at all times with the DCC Security Architecture and Contractor Security Architecture.

3. CONTRACTOR'S SECURITY OBLIGATIONS

3.1 The Contractor shall, at all times during the Service Period, ensure that the Contractor Solution provides and ensures a level of security which:

(a) is in accordance with Good Industry Practice including any applicable Guidance;

(b) complies with all applicable Laws and the requirements of this Agreement;

(c) subject to paragraph 4 of this Part A, complies with the DCC Security Policy;

(d) appropriately manages security threats to the Contractor Solution;

(e) appropriately manages security threats to the DCC Environment and/or the DCC Services (as such threats emerge or change from time

to time), to the extent that such security threats are due to a failure by (i) the Contractor, (ii) the Contractor Solution or (iii) any of the Contractor Security Documents to comply with the requirements of this Agreement;

(f) complies with the Security Standards; and

(g) complies with the Security Requirements.

3.2 If there is any inconsistency between any of the requirements, standards, guidance and policies referred to in paragraph 3.1, the Contractor shall notify the DCC of such inconsistency promptly upon becoming aware of the same, and the DCC shall, as soon as reasonably practicable, advise the Contractor which of the applicable requirements, standards, guidance and policies the Contractor shall be required to comply with in the relevant circumstances.

3.3 Without limiting paragraph 3.1, the Contractor shall:

(a) at all times ensure that the level of security employed in relation to the Contractor Solution is appropriate and adequate to ensure that the risk of any Breach of Security occurring is maintained in accordance with the applicable risk level specified in the relevant Contractor Security Document(s) (and is otherwise consistent with the Contractor's obligations under this Agreement);

(b) comply with the requirements of Clauses 41.5 to 41.7 (Staffing Security) (inclusive) regarding all Contractor Personnel employed or engaged in the provision of the Services; and

(c) implement and maintain physical security controls which are intended to prevent any unauthorised access to any of the Sites (and taking into account any Sites which are identified as being critical in the BCDR Plan).

4. DCC SECURITY POLICY

4.1 The Contractor acknowledges that the DCC Security Policy will not be finalised until after the Signature Date. Accordingly, the DCC shall:

(a) before finalising the DCC Security Policy, provide the Contractor with a reasonable opportunity to review and comment on the draft DCC Security Policy;

(b) take reasonable account of any comments from the Contractor (and other relevant DCC Service Providers) in finalising the DCC Security Policy; and

(c) provide the Contractor with a copy of the finalised DCC Security Policy as soon as reasonably practicable.

4.2 The finalised DCC Security Policy (as provided to the Contractor under paragraph 4.1(c)) is not intended to increase the scope of the Contractor's obligations under this Agreement. However, to the extent that compliance with the finalised DCC Security Policy would require:

(a) a change in relation to any of the Contractor's obligations under this Agreement; and/or

(b) the Contractor to incur any material additional costs (being costs which it would not have otherwise incurred under this Agreement),

then the Contractor shall notify the DCC accordingly and the parties (acting reasonably) shall agree any necessary Change to this Agreement in accordance with the Change Control Procedure.

4.3 Paragraph 4.2 is without prejudice to the parties' respective rights and obligations under paragraph 6 of Part B of this Schedule 2.5 in relation to subsequent changes to the DCC Security Policy.

PART B – CONTRACTOR SECURITY DOCUMENTS

1. OVERVIEW

1.1 The Contractor's security policy relating to the Contractor Solution ("**Contractor Security Policy**") is set out in Appendix 2. Without limiting the Contractor's obligations under paragraph 6, the Contractor shall ensure that, at all times, the Contractor Security Policy complies with:

(a) subject to paragraph 4 of Part A of this Schedule 2.5, the DCC Security Policy;

(b) the requirements set out in this Schedule 2.5; and

(c) any other applicable requirements of this Agreement.

1.2 The Contractor shall develop, implement, operate, maintain and continuously improve an ISMS and the Security Management Plan which shall, without prejudice to the requirements of Part A of this Schedule 2.5, be subject to the approval of the DCC in accordance with paragraph 4 of this Part B.

2. OUTLINE SECURITY MANAGEMENT PLAN

An outline security management plan ("**Outline Security Management Plan**") has been agreed between the DCC and the Contractor and is set out in Appendix 3. The Outline Security Management Plan shall be binding upon the Contractor from the Effective Date until the full Security Management Plan is agreed between the parties in accordance with paragraph 4 of this Part B.

3. COMPLIANCE WITH CONTRACTOR SECURITY DOCUMENTS

Without limiting paragraph 2 of this Part B, once agreed in accordance with paragraph 4 of this Part B, the Contractor shall comply with its obligations set out in the Contractor Security Documents at all times during the Service Period.

4. DEVELOPMENT OF THE ISMS AND SECURITY MANAGEMENT PLAN

4.1 By no later than twenty (20) Working Days after the Effective Date (and, where applicable, in accordance with paragraph 6), the Contractor shall deliver to the DCC:

(a) a draft of the ISMS which:

(i) complies with the requirements set out in ISO/IEC 27001;

(ii) is consistent with the Contractor Security Policy and the draft Security Management Plan;

(iii) sets out retention periods assigned to all the categories of data;

(iv) details the approach to performing monitoring, security information and event correlation; and

(v) otherwise complies with the requirements set out in this Schedule 2.5, including paragraph 5 below;

(b) a draft of the Security Management Plan which:

(i) is based on the Outline Security Management Plan;

(ii) is consistent with the Contractor Security Policy and the draft ISMS; and

(iii) otherwise complies with the requirements set out in this Schedule 2.5, including paragraph 5 below.

In order to demonstrate the commitment of the Contractor's management to implementing and maintaining the security measures referred to in this Schedule 2.5, the Contractor shall ensure that each version of the ISMS and the Security Management Plan is approved by a member of the Contractor's senior management team (being at board level and as agreed with the DCC in writing), who shall also have overall responsibility for the implementation and maintenance of such security measures by the Contractor and any relevant Contractor Person.

4.2 Within forty (40) days after receipt of the draft ISMS and Security Management Plan from the Contractor, the DCC shall notify the Contractor if it (acting reasonably) considers that either draft:

(a) is insufficiently detailed to be properly evaluated; and/or

(b) does not comply with the requirements set out in this Schedule 2.5, including paragraph 5 below,

(each, for the purposes of this paragraph 4, a "**non-conformity**"). The DCC shall provide reasonable details regarding the nature of, and the rationale for, any non-conformities notified to the Contractor under this paragraph 4.2.

4.3 By no later than twenty (20) days after receipt of a notice from the DCC under paragraph 4.2 or 4.4, the Contractor shall:

(a) make any amendments to the ISMS and/or the Security Management Plan (as applicable) that are necessary to address the non-conformities notified by the DCC under paragraph 4.2 or 4.4; and

(b) re-submit the revised ISMS and/or Security Management Plan (as applicable) to the DCC for approval.

4.4 Within thirty (30) days after receipt of the revised ISMS and/or Security Management Plan (as applicable) from the Contractor, the DCC shall notify the Contractor of:

(a) any outstanding non-conformities from the previous version of the ISMS and/or Security Management Plan (as applicable); and/or

(b) any new non-conformities appearing in the revised ISMS and/or Security Management Plan (as applicable).

The DCC shall provide reasonable details regarding the nature of, and the rationale for, any non-conformities notified to the Contractor under this paragraph 4.4.

4.5 The process in paragraphs 4.3 and 4.4 will then be repeated until the DCC notifies the Contractor that both the ISMS and the Security Management Plan are approved (except that the timescales in paragraphs 4.3 and 4.4 may be adjusted in relation to any repetition of the process in such paragraphs by the DCC, acting reasonably and taking appropriate account of the extent of any amendments to be made to the ISMS and/or the Security Management Plan by the Contractor). Any dispute relating to the existence of non-conformities in the ISMS and/or Security Management Plan (as applicable) shall be referred to the Dispute Resolution Procedure.

4.6 The DCC shall provide any information or assistance reasonably requested by the Contractor in relation to the preparation of the ISMS and/or the Security Management Plan under this paragraph 4 (or any updates under paragraph 6).

4.7 Once the ISMS and the Security Management Plan, or any subsequent revision to either of them in accordance with paragraph 6 below, are approved by the DCC in accordance with this paragraph 4, they will be adopted immediately and will replace the previous version of the ISMS or Security Management Plan (if applicable).

5. CONTENT OF THE ISMS AND THE SECURITY MANAGEMENT PLAN

The ISMS and the Security Management Plan shall:

(a) set out the security measures to be implemented and maintained by the Contractor in relation to all aspects of the Contractor Solution (including all processes associated with the delivery of the Services);

(b) specify the security tests to be conducted by the Contractor in accordance with Part C of this Schedule 2.5 (which shall be sufficient to determine the extent to which the Contractor Solution and the security measures set out in the Contractor Security Documents are sufficient to enable the Contractor to comply with its obligations under this Schedule 2.5);

(c) at all times comply with, and specify security measures and procedures which are sufficient to ensure that the Contractor Solution complies with, the provisions of this Schedule 2.5 (including the principles set out in Part A of this Schedule 2.5);

(d) be structured in accordance with ISO/IEC 27001 and ISO/IEC 27002, cross-referencing if necessary to other Schedules of this Agreement which cover specific areas included within that standard;

(e) be written in plain English in language which is readily comprehensible to the Contractor Personnel and any DCC personnel engaged in relation to the Services; and

(f) only reference documents which have been provided to the DCC by the Contractor (or which are attached to the ISMS and/or the Security Management Plan, as applicable).

6. REVIEW OF THE CONTRACTOR SECURITY DOCUMENTS

6.1 The Contractor shall fully review and update the Contractor Security Documents in accordance with this paragraph 6:

(a) on an annual basis by no later than each anniversary of the Effective Date;

(b) within ten (10) Working Days after the implementation of (i) any material Change to this Agreement or (ii) any Project;

(c) within five (5) Working Days after the occurrence of any actual, potential or attempted Breach of Security;

(d) within ten (10) Working Days after any material change to the DCC Security Policy, the DCC Environment and/or the DCC Services (as notified to the Contractor by the DCC from time to time); and

(e) at such other times as may be necessary to ensure that the Contractor complies with the requirements of this paragraph 6.

6.2 The purpose of reviews of, and updates to, the Contractor Security Documents under this paragraph 6 shall be to ensure that they accurately and properly reflect:

(a) emerging changes in Good Industry Practice and applicable Mandatory Requirements;

(b) any change to the Contractor Solution;

(c) any change to the DCC Security Policy, the DCC Environment and/or the DCC Services (as notified to the Contractor by the DCC from time to time);

(d) any change to the organisational structure or operating procedures of any Contractor Person which could have an impact on any security related issues;

(e) any change in the services and/or systems provided by the DCC Service Providers (as notified to the Contractor by the DCC from time to time);

(f) any new perceived or changed security threats that the Contractor becomes aware of (having made reasonable enquiries and analysis), including those identified by the DCC or third parties, including Government intelligence authorities; and

(g) the recommendation of internal security audits,

and that they otherwise continue to comply with the requirements of this Schedule 2.5.

6.3 Subject to paragraph 6.4, the parties shall comply with the procedure set out in paragraph 4 of this Part B in relation to the approval by the DCC of any updated versions of the ISMS and/or the Security Management Plan under this paragraph 6 from time to time. Any updated version of the Contractor Security Policy under this paragraph 6 shall be subject to the prior written approval of the DCC.

6.4 Any change or amendment to the Contractor Security Documents resulting from:

(a) the circumstances referred to in paragraph 6.2(c) or 6.2(e); or

(b) any other circumstances not contemplated by paragraph 6.2,

shall be subject to the Change Control Procedure and shall not be implemented until approved in writing by the DCC.

6.5 Any changes to any of the Contractor Security Documents, whether under paragraph 6.3 or 6.4 of this Part B or paragraph 5 of Part C, shall be approved by the relevant member of the Contractor's senior management team, as further described in paragraph 4.1 of this Part B.

PART C – TESTING

1. SECURITY TESTS BY THE CONTRACTOR

1.1 The Contractor shall conduct security tests in relation to the Contractor Solution and the operation of the security measures set out in the Contractor Security Documents (as further described in paragraph 5(a) of Part B of this Schedule 2.5) in accordance with the testing arrangements set out in the Contractor Security Documents ("**Security Tests**"). The Security Tests shall be conducted:

(a) on an annual basis by no later than each anniversary of the Effective Date;

(b) within thirty (30) days after the implementation of (i) any material Change to this Agreement or (ii) any Project;

(c) within ten (10) Working Days after the implementation of any steps under this Part C which are intended to address any Security Weakness;

(d) within ten (10) Working Days after the implementation of any steps under Part F of this Schedule 2.5 which are intended to address the occurrence of any actual, potential or attempted Breach of Security;

(e) within thirty (30) days after any material change to the DCC Environment and/or the DCC Services (as notified to the Contractor by the DCC from time to time); and

(f) at such other times as may be necessary to ensure that the Contractor complies with the requirements of this Schedule 2.5.

1.2 The date, timing and conduct of the Security Tests shall be agreed in advance with the DCC. Unless otherwise agreed with the DCC, all Security Tests shall be designed and implemented so as to minimise the impact on the delivery of the Services to the extent reasonably possible.

1.3 The DCC shall be entitled to send representative(s) to witness the conduct of all or any of the Security Tests.

1.4 The Contractor shall provide the DCC with the results of all Security Tests (in a form approved by the DCC in advance) as soon as practicable (but, in any event, within ten (10) Working Days) after completion of each Security Test.

2. DCC SECURITY TESTS

2.1 The DCC and/or its authorised representatives shall be entitled to carry out such additional security tests (including penetration tests) in relation to the Contractor Solution and the operation of the security measures set out in the Contractor Security Documents as it may deem necessary in order to assess:

(a) the adequacy of the Contractor Security Documents;

(b) the Contractor's compliance with this Schedule 2.5;

(c) the Contractor's compliance with the Security Requirements; and/or

(d) the Contractor's compliance with the Contractor Security Documents,

(the "**DCC Security Tests**"). Subject to paragraph 2.2, the DCC shall provide the Contractor with at least five (5) Working Days' notice of any DCC Security Tests. The DCC shall notify the Contractor of the results of the DCC Security Tests as soon as reasonably practicable after their completion.

2.2 Where the DCC (acting reasonably) considers that the conduct of the DCC Security Tests will have a material adverse effect on the Contractor's ability to deliver the Services in accordance with this Agreement (including compliance with the Performance Measures):

(a) the DCC shall provide the Contractor with reasonable advance notice (but, in any event, at least twenty (20) Working Days' notice) of the DCC Security Tests;

(b) the Contractor shall, as soon as reasonably practicable (but, in any event, within ten (10) Working Days) after receipt of such notice from the DCC, advise the DCC:

(i) whether the conduct of the DCC Security Tests will, in its reasonable opinion, have a material adverse effect on the Contractor's ability to deliver the Services in accordance with this Agreement (including compliance with the Performance Measures); and

(ii) if so, any activities that the Contractor may reasonably be able to undertake to mitigate such effect on the Services;

(c) the DCC shall, within ten (10) Working Days after receipt of such notice from the Contractor, confirm in writing to the Contractor the extent of any relief to be granted to the Contractor in the event of any actual non-performance by the Contractor of its obligations under this Agreement (including any under-performance against the Performance Measures) as a result of the conduct of the DCC Security Tests (and taking account of any mitigation activities notified by the Contractor under paragraph 2.2(b)(ii));

(d) if there is any Dispute between the parties in relation to the matters contemplated by this paragraph 2.2, including:

(i) the extent to which the conduct of the DCC Security Tests will have a material adverse effect on the Contractor's ability to deliver the Services in accordance with this Agreement (including compliance with the Performance Measures);

(ii) the Contractor's ability to mitigate such effect on the Services; and/or

(iii) the relief against any actual non-performance by the Contractor of its obligations under this Agreement (including any under-performance against the Performance Measures),

either party may refer the Dispute to the Dispute Resolution Procedure. For the avoidance of doubt, and unless otherwise agreed by the DCC in writing, the existence of any such Dispute (or its referral to

the Dispute Resolution Procedure) shall not prevent or delay the conduct of the DCC Security Tests by the DCC and/or its authorised representatives in accordance with paragraph 2.1.

3. SECURITY ASSURANCE BY THE CONTRACTOR

3.1 The Contractor shall at all times:

(a) demonstrate to the DCC, by regular reporting to the Service Delivery and Change OMB (or the PMB or EMB, if escalated) and otherwise in accordance with the governance arrangements set out in Schedule 8.1 (Governance), that it is performing security assurance of the Contractor Solution in accordance with the Security Requirements; and

(b) perform security assurance activities (as further described in the Security Requirements).

4. SECURITY ACCREDITATION

4.1 The Contractor shall provide such information and assistance as may be reasonably requested by the DCC (or any relevant independent entity) from time to time in relation to conducting any accreditation of the End-to-end Smart Metering System against SMETS and/or associated security standards.

4.2 If any accreditation referred to in paragraph 4.1 of this Part C is not obtained due to a failure by the Contractor to comply with its obligations under this Agreement (including this Schedule 2.5), the Contractor shall immediately take all steps necessary to rectify such failure and notify the DCC as soon as the failure has been rectified.

4.3 If any failure by the Contractor referred to in paragraph 4.2 of this Part C amounts to a material breach for the purposes of any provision of Clause 60.2.1, the DCC may require the Contractor to comply with the Remedial Plan Process in respect of such breach.

5. SECURITY WEAKNESSES

5.1 Where:

(a) any Security Tests;

(b) any DCC Security Tests;

(c) any security assurance activities carried out pursuant to paragraph 3 of this Part C; and/or

(d) any security accreditation carried out pursuant to paragraph 4 of this Part C,

reveal any (i) actual or potential Breach of Security, (ii) any other failure or weakness in the Contractor Solution and/or any of the Contractor Security Documents, or (iii) any failure by the Contractor to comply with any of the Security Requirements (each a "**Security Weakness**"), then, subject to paragraph 5.2, the Contractor shall notify the DCC of any changes to Contractor Solution and/or the relevant Contractor Security Document(s),

and any other steps, which the Contractor (acting reasonably) proposes to implement in order to address the relevant Security Weakness (and a proposed timetable for the implementation of such matters).

5.2 Where any Security Weakness relates to an actual or potential Breach of Security that is not due to a failure by (i) the Contractor, (ii) the Contractor Solution or (iii) any of the Contractor Security Documents to comply with the requirements of this Agreement, then the Contractor shall notify the DCC of:

(a) any steps which the Contractor could itself implement in order to address the relevant Security Weakness (and a proposed timetable, and estimated costs, regarding the implementation of such steps); and/or

(b) where known to the Contractor (having given the matter reasonable consideration), any steps which may need to be implemented by the DCC and/or the relevant DCC Service Provider(s) in order to address the Security Weakness.

5.3 The Contractor's notice under paragraph 5.1 or 5.2 (as applicable) shall be provided to the DCC as soon as possible and, in any event, within:

(a) five (5) Working Days after completion of the relevant Security Tests;

(b) two (2) Working Days after notification by the DCC of the results of the DCC Security Tests under paragraph 2.1;

(c) five (5) Working Days after any security assurance activities carried out pursuant to paragraph 3 of this Part C reveal the relevant Security Weakness; and/or

(d) five (5) Working Days after notification by the DCC of any Security Weakness revealed by any security accreditation carried out pursuant to paragraph 4 of this Part C,

or such other period agreed by the parties in writing.

5.4 Within ten (10) Working Days (or such other period agreed in writing by the parties) after receipt of the Contractor's proposal under paragraph 5.1, the DCC shall notify the Contractor as to whether the proposal is approved. The DCC's approval shall not be unreasonably withheld, provided that the DCC shall be entitled to reject the Contractor's proposal if (in the reasonable opinion of the DCC):

(a) the proposal (including the proposed timetable) would be inappropriate or insufficient to address the relevant Security Weakness;

(b) any proposed changes to the relevant Contractor Security Document(s) would result in those documents failing to comply with the requirements set out in this Schedule 2.5, including paragraph 5 of Part B, in any respect; and/or

(c) any other proposed steps would be inconsistent with the requirements of this Schedule 2.5.

5.5 If there is any Dispute between the parties in relation to the matters contemplated by paragraph 5.4, either party may refer the Dispute to the Dispute Resolution Procedure. Until such time as the Dispute is resolved in accordance with the Dispute Resolution Procedure, the Contractor shall comply with any additional or alternative security measures notified by the DCC which are (in the reasonable opinion of the DCC) necessary to address relevant Security Weakness.

5.6 Subject to the approval of the DCC under paragraph 5.4, the Contractor shall implement any proposed changes to the relevant Contractor Security Document(s) and/or take any other proposed steps to address the relevant Security Weakness in accordance with the approved timetable.

5.7 Within ten (10) Working Days (or such other period agreed in writing by the parties) after receipt of the Contractor's proposal under paragraph 5.2(a), the DCC shall notify the Contractor whether the proposal is approved in principle, in which case, the proposal shall be fully agreed and implemented by the parties in accordance with the Change Control Procedure.

5.8 In relation to any proposal of the Contractor under paragraph 5.2(b), the DCC shall discuss such matters further with the relevant DCC Service Provider(s) and use reasonable endeavours to address the relevant Security Weakness as soon as reasonably practicable.

PART D – ISO/IEC 27001 CERTIFICATION

1. The Contractor shall obtain independent certification of the ISMS with the requirements of ISO/IEC 27001, using an appropriate organisation which is certified by the UK Accreditation Service (the "**UKAS Entity**"), within twelve (12) months after the Effective Date and shall maintain such certification at all times during the Service Period, including by complying with any on-going audit and testing requirements of the relevant UKAS Entity.

2. If certain parts of the ISMS do not conform to the requirements of ISO/IEC 27001 and/or Good Industry Practice, and/or the controls as described in ISO/IEC 27002 are not consistent with the DCC Security Policy, and, as a result, the Contractor reasonably believes that it is not compliant with ISO/IEC 27001, the Contractor shall promptly notify the DCC of this.

3. If the Contractor notifies the DCC under paragraph 2 that:

   (a) any part of the ISMS does not comply with the requirements of ISO/IEC 27001 and/or does not conform to Good Industry Practice, the Contractor shall (at its own expense) take such steps as may be necessary to rectify such non-compliance and are approved by the DCC (acting reasonably), including, where necessary, re-obtaining ISO/IEC 27001 certification in accordance with paragraph 1; or

   (b) the controls as described in ISO/IEC 27002 are not consistent with the DCC Security Policy, the Contractor shall comply with any direction notified by the DCC in response to such request (which may involve the amendment of the DCC Security Policy to be consistent with the relevant ISO/IEC 27002 controls).

PART E – SECURITY AUDITS

1. SCOPE OF DCC SECURITY AUDITS

1.1 The DCC may conduct a security audit under this Part E (each, a "**DCC Security Audit**") for the following purposes:

(a) to verify the Contractor's compliance with its obligations under:

(i) this Schedule 2.5;

(ii) any of the Contractor Security Documents; and/or

(iii) the Security Requirements;

(b) to review the confidentiality, integrity and availability of any DCC Data that is processed, stored or transmitted by any Contractor Person under this Agreement (including by examining the systems, processes and procedures used in relation to such processing, storage and transmission activities); and

(c) to ensure that the ISMS maintains compliance with the principles and practices of ISO/IEC 27001.

SOC2 audits for SEC Panel and/or Secretary of State

1.2 As part of the DCC Security Audit process set out in this Part E, the DCC shall provide independent assurance to the SEC Panel and the Secretary of State that the DCC, the Contractor and the DCC Service Providers have fully complied with the DCC Security Architecture and implemented the Security Requirements. This assurance is to be annually provided by the DCC through the provision of a completed SOC2 audit report with the first report due within twelve (12) months after the date on which the Commencement of Market Entry Milestone has been Achieved. The parties shall comply with their respective obligations, and may exercise their respective rights, in respect of any DCC Security Audit relating to this paragraph 1.2.

2. OBLIGATIONS OF THE CONTRACTOR

The Contractor shall comply with its obligations under paragraph 2 of Part A of Schedule 8.4 (Records and Audit Provisions) in respect of any DCC Security Audit conducted under this Part E. For the avoidance of doubt, any reference to a "DCC Audit" in paragraph 2 of Part A of Schedule 8.4 shall, for the purposes of this Part E, be deemed to be a reference to the relevant DCC Security Audit.

3. FREQUENCY OF DCC SECURITY AUDITS

3.1 Subject to the limitations set out in paragraph 3.2, the DCC may conduct DCC Security Audits at any time during the Service Period and for up to twenty-four (24) months after the Termination Date. Any audit after the Termination Date shall be limited to a review of the records and other materials retained by the Contractor in accordance with the requirements of this Agreement or otherwise.

3.2 Except as set out in paragraph 3.3:

(a) the DCC shall provide at least five (5) Working Days' written notice of its intention to conduct a DCC Security Audit, specifying in reasonable detail the purpose and scope of the DCC Security Audit and the estimated duration;

(b) the DCC may not conduct a DCC Security Audit more than twice in any Contract Year during the Service Period;

(c) the DCC may not conduct a DCC Security Audit more than once in any twenty-four (24) month period after the Termination Date; and

(d) the DCC shall use reasonable endeavours to conduct each DCC Security Audit at such times as to minimise disruption to the Contractor Solution.

3.3 The limitations set out in paragraph 3.2 shall not apply where a DCC Security Audit is to be conducted by the DCC in connection with any actual or suspected material breach by the Contractor or any other Contractor Person of any of the Contractor's obligations under:

(a) this Schedule 2.5;

(b) any of the Contractor Security Documents; and/or

(c) the Security Requirements.

4. DCC OBLIGATIONS

4.1 The DCC shall use reasonable endeavours to ensure that the conduct of any DCC Security Audit does not unreasonably delay or disrupt the provision of the Services or unreasonably disrupt the operations of the Contractor generally and shall, in undertaking any DCC Security Audit, comply with such reasonable policies (as notified by the Contractor in advance and in writing) as are generally applicable in respect of access to the relevant Sites.

4.2 The DCC shall ensure that any third party conducting a DCC Security Audit on behalf of the DCC shall, prior to commencing the DCC Security Audit, be subject to confidentiality obligations in favour of the DCC on terms which provide substantially equivalent protection in relation to the Contractor's Confidential Information as the provisions of Clause 50 of this Agreement.

5. COST OF DCC SECURITY AUDITS

5.1 The parties shall bear their own costs and expenses in respect of any DCC Security Audit under this Part E, unless any DCC Security Audit identifies any material breach by the Contractor or any other Contractor Person of any of the Contractor's obligations under:

(a) this Schedule 2.5;

(b) any of the Contractor Security Documents; and/or

(c) the Security Requirements,

in which case the Contractor shall reimburse the DCC for the reasonable costs incurred by it in relation to the relevant DCC Security Audit.

6. OUTCOME OF DCC SECURITY AUDITS

6.1 If any DCC Security Audit identifies any material breach by the Contractor or any other Contractor Person of any of the Contractor's obligations under:

(a) this Schedule 2.5;

(b) any of the Contractor Security Documents; and/or

(c) the Security Requirements,

the DCC shall be entitled to exercise its applicable rights and remedies under this Agreement (including, where applicable, requiring the Contractor to comply with Clause 61 (Remedial Plan Process)).

6.2 If any DCC Security Audit identifies that the ISMS is not compliant with the principles and practices of ISO/IEC 27001, then the DCC shall notify the Contractor accordingly and the Contractor shall immediately (and at its own cost) undertake such actions as are necessary to ensure that the ISMS becomes compliant with the principles and practices of ISO/IEC 27001.

6.3 Where the DCC (in its sole discretion) considers that it would be useful for the Contractor to review and comment on the draft findings of a DCC Security Audit, the Contractor shall provide such comments within a reasonable period as requested by the DCC.

7. INDEPENDENT SECURITY REVIEW

DCC's obligations

7.1 The Contractor acknowledges that:

(a) the DCC is required to provide assurance to the SEC Panel and the Secretary of State that the DCC, the Contractor and the DCC Service Providers have fully complied with the DCC Security Architecture and fully implemented the Security Requirements; and

(b) in order to comply with paragraph 7.1(a), the DCC and/or the SEC Panel may appoint a "Competent Independent Organisation" (the "**CIO**") to perform the activities referred to in paragraph 7.3.

7.2 The CIO must:

(a) be fully independent of the DCC;

(b) be recognised as being appropriately qualified to conduct information security audits by virtue of:

(i) employing one or more persons who are members of the CESG Listed Adviser Scheme ("**CLAS**") (or any successor to that scheme);

(ii) being accredited under the CESG CHECK (IT Health Check Service) Scheme (or any successor to that scheme);

(iii) being approved as a provider of CTAS (CESG Tailored Assurance Service) assessments (or any successor to those assessments); or

(iv) any other membership, accreditation, approval, or similar form of validation that is substantially equivalent in its status and effect to one or more of the arrangements referred to in paragraphs 7.2(b)(i) to 7.2(b)(iii); and

(c) have engaged, as its lead auditor, an individual who is a member of CLAS or of any successor to, or equivalent of, that scheme.

7.3 The tasks and duties of the CIO may include:

(a) working with the DCC, the Contractor and/or the DCC Service Providers during the design and implementation of the DCC Services (including the design and implementation of the Contractor Solution under this Agreement) to review the security aspects of the DCC Services (including the Contractor Solution);

(b) preparing, when requested by the DCC and/or the SEC Panel from time to time, an up-to-date and independent assessment of the compliance by the DCC, the Contractor and the DCC Service Providers with the DCC Security Architecture and the Security Requirements (together with an analysis of the approach taken by such entities to risk assessment and risk treatment);

(c) if necessary, providing recommendations to the DCC in relation to specific actions to be taken by the DCC, the Contractor and/or the DCC Service Providers to ensure full compliance with the DCC Security Architecture and the Security Requirements; and

(d) providing a copy of its assessment under paragraph 7.3(b), together with any recommendations under paragraph 7.3(c), to the SEC Panel and/or the Secretary of State on request.

Contractor's obligations

7.4 Without limiting the Contractor's other obligations under this Agreement, the Contractor shall:

(a) promptly provide the CIO with reasonable access to any Sites (or other premises) and other resources (including the Contractor System and other Assets) used by any Contractor Person (whether exclusively or non-exclusively) in relation to the performance of the Services;

(b) promptly provide any co-operation, documentation, data, information or other assistance reasonably requested by the DCC and/or the CIO from time to time in relation to the performance of the CIO's tasks and duties (as set out in paragraph 7.3);

(c) ensure that appropriate representatives of the Contractor (or, where applicable, any Contractor Person), including any representatives

specifically identified by the DCC or the CIO, attend any meetings with the DCC and/or the CIO that are reasonably requested by the DCC from time to time in relation to the performance of the CIO's tasks and duties (as set out in paragraph 7.3); and

(d) where any of the CIO's recommendations under paragraph 7.3(c) relate to a failure by the Contractor to comply with its obligations under this Agreement, immediately rectify such failure. Where any CIO's recommendations under paragraph 7.3(c) do not relate to a failure by the Contractor to comply with its obligations under this Agreement, such recommendations shall be implemented (if requested by the DCC) in accordance with the Change Control Procedure.

8. NO IMPACT ON OTHER AUDIT RIGHTS

8.1 The parties' rights and obligations under this Part E are without prejudice to:

(a) the parties' rights and obligations under Schedule 8.4; and

(b) any other audit, inspection or access rights of the DCC under this Agreement.

PART F – BREACH OF SECURITY

1. NOTIFICATION

1.1 Each party shall notify the other:

(a) immediately upon becoming aware of any actual, potential or attempted Breach of Security (regardless of the cause of such Breach of Security); or

(b) promptly after becoming aware of any actual, potential or attempted breach of security (which is equivalent to a Breach of Security) in relation to the DCC, any DCC Service Provider or any DCC Service User that may also affect the Contractor Solution (each, a "**Third Party Breach of Security**"),

such notification shall, where applicable, be made in accordance with the agreed security incident management process set out in the ISMS.

1.2 The Contractor acknowledges and agrees that:

(a) the DCC is entitled to notify the relevant DCC Service Providers and/or DCC Service Users of any actual, potential or attempted Breach of Security that may also affect the Systems of such persons; and

(b) unless otherwise agreed by the parties in writing, the DCC shall be solely responsible for liaising with:

(i) the relevant DCC Service Providers and/or DCC Service Users regarding their respective response to any actual, potential or attempted Breach of Security under paragraph 1.2(a); and

(ii) the relevant Regulatory Bodies regarding any actual, potential or attempted Breach of Security under paragraph 1.2(a) (provided that this paragraph 1.2(b)(ii) shall not prevent the Contractor liaising with any relevant Regulatory Bodies to the extent that the actual, potential or attempted Breach of Security also affects any services provided by the Contractor other than the Services).

1.3 As soon as reasonably practicable (but, in any event, within one (1) hour of the occurrence of the actual, potential or attempted Breach of Security), the Contractor shall provide to the DCC a further report setting out all details of the actual, potential or attempted Breach of Security that are then available to the Contractor (having made all enquiries and analysis that are reasonably practicable within the timescales referred to in this paragraph 1.3).

2. RECTIFICATION

General

2.1 Subject to paragraph 2.2, upon becoming aware of any actual, potential or attempted Breach of Security under paragraph 1.1(a) of this Part F, the Contractor shall immediately take all reasonable steps necessary to:

(a) remedy any actual Breach of Security or protect the integrity of the Contractor Solution against any potential or attempted Breach of Security; and

(b) prevent an equivalent Breach of Security in the future.

Such steps shall include any action or changes reasonably required by the DCC.

Breach of Security not due to Contractor default

2.2 Where an actual, potential or attempted Breach of Security under paragraph 1.1(a) of this Part F is not due to a failure by (i) the Contractor, (ii) the Contractor Solution or (iii) any of the Contractor Security Documents to comply with the requirements of this Agreement, then the Contractor shall notify the DCC of:

(a) any steps which the Contractor could itself implement in order to address the Breach of Security (and a proposed timetable, and estimated costs, regarding the implementation of such steps); and/or

(b) where known to the Contractor (having given the matter reasonable consideration), any steps which may need to be implemented by the DCC and/or the relevant DCC Service Provider(s) in order to address the Breach of Security.

2.3 The Contractor's notice under paragraph 2.2 shall be provided to the DCC as soon as possible and, in any event, within five (5) Working Days after the occurrence of the relevant Breach of Security (or such other period agreed by the parties in writing).

2.4 Within ten (10) Working Days (or such other period agreed in writing by the parties) after receipt of the Contractor's proposal under paragraph 2.2(a), the DCC shall notify the Contractor whether the proposal is approved in principle, in which case, the proposal shall be fully agreed and implemented by the parties in accordance with the Change Control Procedure.

2.5 In relation to any proposal of the Contractor under paragraph 2.2(b), the DCC shall discuss such matters further with the relevant DCC Service Provider(s) and use reasonable endeavours to address the circumstances giving rise to the relevant Breach of Security as soon as reasonably practicable.

Other breaches of security

2.6 Subject to paragraph 2.9, in relation to any actual, potential or attempted Third Party Breach of Security, the Contractor shall notify the DCC of any steps which the Contractor could itself implement in order to address the Third Party Breach of Security (and a proposed timetable, and estimated costs, regarding the implementation of such steps).

2.7 The Contractor's notice under paragraph 2.6 shall be provided to the DCC as soon as possible and, in any event, within five (5) Working Days (or such other period agreed by the parties in writing) after the earlier of:

(a) the date on which the Contractor became aware of the occurrence of the relevant Third Party Breach of Security; and

(b) the date of receipt of the DCC's notification regarding the relevant Third Party Breach of Security.

2.8 Within ten (10) Working Days (or such other period agreed in writing by the parties) after receipt of the Contractor's proposal under paragraph 2.6, the DCC shall notify the Contractor whether the proposal is approved in principle, in which case, the proposal shall be fully agreed and implemented by the parties in accordance with the Change Control Procedure.

2.9 To the extent that the relevant Third Party Breach of Security is due to a failure by (i) the Contractor, (ii) the Contractor Solution or (iii) any of the Contractor Security Documents to comply with the requirements of this Agreement, the Contractor shall immediately take all steps necessary to rectify such failure and notify the DCC as soon as the failure has been rectified.

2.10 Paragraph 2.9 is without prejudice to any other rights or remedies of the DCC in relation to the relevant failure by (i) the Contractor, (ii) the Contractor Solution or (iii) any of the Contractor Security Documents to comply with the requirements of this Agreement.

Appendix 1 – Security Management Requirements

Appendix 2 – Contractor Security Policy

Appendix 3 – Outline Security Management Plan