Schedule 2.4 - Lot 3

Security Management

Version 4.0

This document is based on Schedule 2.4 of the Crown Commercial Service Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright

CHANGE HISTORY

Version No.	Date	Details of Changes included in Update	Author(s)	Document Number
4.0	12.11.15	Execution copy	ESMCP	35090828.23

This document is based on Schedule 2.4 of the Crown Commercial Service Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright

Contents

1	Definitions	4
2	Introduction	4
3	Information Security Management System (ISMS)	4
4	Security Management Plan	6
5	Amendment And Revision Of The ISMS And Security Management Plan	8
6	Security Testing	9
7	Compliance Of The ISMS with ISO/IEC 27001	10
8	Breach Of Security	11
ANNEX 1: Baseline Security Requirements		13
ANNEX 2: Security Management Plan		16
Emergency Services Mobile Communications Programme		17
Schedule 2.4		17
Security Management		17
Outline Security Plan		17
1.	Overview	23
2.	Information Security Management System	27
3.	Detailed Draft Security Management Plan	30
4.	Amendment and Revision of the ISMS and Security Management Plan	46
5.	Security Audit, Testing and Vulnerability Management	46
6.	Breach of Security Activities	49
7.	Conclusion	51

This document is based on Schedule 2.4 of the Crown Commercial Service Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright

1 Definitions

1.1 In construing this Schedule 2.4 (Security Management), unless otherwise expressly specified in this Schedule terms defined and used in Schedule 1 (Definitions) will have the same meaning in this Schedule.

2 Introduction

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

2.2 The Parties shall each appoint a member of the Programme Board to be responsible for security. The initial member of the Programme Board appointed by the Supplier for such purpose shall be the person named as such in Schedule 9.2 (Key Personnel) and the provisions of Clauses 14.5 and 14.6 (Key Personnel) shall apply in relation to such person.

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

2.4 The Supplier shall use as a minimum Good Industry Practice in the day to day operation of any system storing, 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.

2.5 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.

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

3 Information Security Management System (ISMS)

3.1 Within twenty one (21) months after the Effective Date, the Supplier shall develop and submit to the Authority for the Authority's approval in accordance with Paragraph 4.3 an ISMS for the purposes of this Agreement, which:

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

(b) shall comply with the requirements of Paragraphs 3.3 to 3.5.

This document is based on Schedule 2.4 of the Crown Commercial Service Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright

3.2 The Supplier acknowledges that the Authority places great emphasis on the reliability of the services for confidentiality, integrity, availability, and authenticity of information and consequently on the security, non-repudiation and accountability provided by the ISMS and that it shall be responsible for the effective performance of the ISMS;

3.3 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 any IT, 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 7;

(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;

(iii) complies with the Baseline Security Requirements;

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

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

(vi) complies with at least the minimum set of security measures and standards set out in the Security Policy Framework (Tiers 1-4);

(vii) complies with the security requirements as set out in Schedule 2.1 (Service Description);

(d) document the security incident management processes and incident response plans in sufficient detail to the extent to which planned activities are realised and planned results achieved to ensure it is fit for purpose and enables the recovery of services to be achieved with minimum resources, effort and costs;

(e) document the vulnerability management policy and assessment of the potential impact on the Services of any new threat, vulnerability or exploitation technique of which the Supplier becomes aware; and

(f) 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).

This document is based on Schedule 2.4 of the Crown Commercial Service Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright

3.4 Subject to Clause 20.11 (Authority Data and Security Requirements) the references to standards, guidance and policies set out in Paragraph 3.3 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.

3.5 In the event that the Supplier becomes aware of any inconsistency in the provisions of the standards, guidance and policies set out in Paragraph 3.3, the Supplier shall immediately notify the Authority Representative of such inconsistency and the Authority Representative shall, as soon as practicable, notify the Supplier which provision the Supplier shall comply with.

3.6 If the ISMS 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. 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 3 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 3.3 to 3.5 shall be deemed to be reasonable.

3.7 Approval by the Authority of the ISMS pursuant to Paragraph 3.6 or of any change or amendment to the ISMS shall not relieve the Supplier of its obligations under this Schedule.

4 Security Management Plan

4.1 Within thirty (30) Working Days after the Effective Date, the Supplier shall prepare and submit to the Authority for approval in accordance with Paragraph 4.3 a fully developed, complete and up-to-date Security Management Plan which shall comply with the requirements of Paragraph 4.2.

4.2 The Security Management Plan shall:

(a) be based on the Security Management Plan set out in Annex 2 and as submitted as part of the Supplier's ITSB response;

(b) comply with the Baseline Security Requirements;

(c) identify the necessary delegated organisational roles defined for those responsible for ensuring this Schedule is complied with by the Supplier;

(d) detail the process for managing any security risks from Sub-contractors (including ensuring the provision of a Security Aspects Letter and, where relevant, regarding the inclusion or exclusion of relevant terms in the Sub-contract, as identified in Schedule 4.3 (Notified Key Sub-contractors)) and third parties authorised by the Authority with access to the Services, processes associated with the delivery of the Services, the

This document is based on Schedule 2.4 of the Crown Commercial Service Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright

Authority Premises, the Sites, the Supplier System, the Authority System (to extent that it is under the control of the Supplier) and any IT, 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;

(e) 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 Sites, the Supplier System, the Authority System (to the extent that it is under the control of the Supplier) and any IT, 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;

(f) set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Services and all processes associated with the delivery of the Services and at all times comply with and specify security measures and procedures which are sufficient to ensure that the Services comply with the provisions of this Schedule (including the requirements set out in Paragraph 3.3);

(g) demonstrate that the Supplier Solution has minimised the Authority and Supplier effort required to comply with this Schedule through consideration of available, appropriate and practicable pan-government accredited services (for example, 'platform as a service' offerings from the G-Cloud catalogue);

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

(i) set out the scope of the Authority System that is under the control of the Supplier;

(j) be structured in accordance with ISO/IEC27001 and ISO/IEC27002, cross referencing if necessary to other Schedules which cover specific areas included within those standards;

(k) be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Authority engaged in the Services and shall reference only documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule; and

(l) be Protectively Marked in accordance with the Cabinet Office Government Security Classification Policy and the Security Policy Framework.

4.3 If the Security Management Plan submitted to the Authority pursuant to Paragraph 4.1 is approved by the Authority, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not approved by the Authority, the Supplier shall amend it within ten (10) Working Days of a

This document is based on Schedule 2.4 of the Crown Commercial Service Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright

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 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 4.3 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 4.2 shall be deemed to be reasonable.

4.4 Approval by the Authority of the Security Management Plan pursuant to Paragraph 4.3 or of any change or amendment to the Security Management Plan shall not relieve the Supplier of its obligations under this Schedule.

5 Amendment And Revision Of The ISMS And Security Management Plan

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

(a) emerging changes in Good Industry Practice;

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

(c) any new perceived or changed security threats;

(d) any change or proposed change to the Security Policy Framework;

(e) any change or proposed change to the CESG IA Policy Portfolio; and

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

5.2 The Supplier shall provide the Authority with the results of each review of the Security Management Plan as soon as reasonably practicable after their completion and amend the ISMS and Security Management Plan at no additional cost to the Authority. The results of the Security Management Plan review shall include, without limitation:

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

(b) updates to the risk assessments;

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

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

5.3 Subject to Paragraph 5.4, any change or amendment which the Supplier proposes to make to the ISMS or Security Management Plan (as a result of a review carried out pursuant to Paragraph 5.1, an Authority request, change to Schedule 2.1 (Services Description) or

This document is based on Schedule 2.4 of the Crown Commercial Service Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright

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

5.4 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 Change Control Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Change Control Procedure for the purposes of formalising and documenting the relevant change or amendment for the purposes of this Agreement.

6 Security Testing

6.1 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 IT Environment or after any change or amendment to the ISMS, (including security incident management processes and incident response plans) or the Security Management Plan. The implementation of Security Tests shall be designed by the Supplier so as to minimise the impact on the delivery of the Services. Subject to Paragraph 6.2, the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Authority. Subject to compliance by the Supplier with the foregoing requirements, if any Security Tests adversely affect the Supplier's ability to deliver the Services so as to meet the Minimum Service Thresholds, the Supplier shall be granted relief against any resultant under-performance for the period of the Security Tests. The output of such tests should be recorded in a format agreed by the Authority.

6.2 The Supplier agrees that the Authority is able to request Security Tests without prior notice.

6.3 Security Tests should comply with the recommendations set out in the Security Policy Framework and CESG IA Policy Portfolio.

6.4 Within thirty (30) Working Days after the Effective Date the Supplier shall prepare and submit to the Authority for approval in accordance with Paragraph 6.1 (Implementation Plan), a template to be used for reporting Security Test results (the "**Security Test Results Template**").

6.5 If the Security Test Results Template submitted to the Authority pursuant to Paragraph 6.4 is approved by the Authority, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the Security Test Results Template 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 Security Test Results Template 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 6.5 may be unreasonably withheld or delayed. However any failure to approve the

This document is based on Schedule 2.4 of the Crown Commercial Service Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright

Security Test Results Template on the grounds that it does not comply with the requirements set out in Paragraph 6.1 shall be deemed to be reasonable.

6.6 The Supplier shall submit to the Authority the output of all Security Tests carried out in accordance with Paragraph 6.1 (Implementation Plan), using the Security Test Results Template approved by the Authority within no more than fifteen (15) Working Days (or such other period as the Parties may agree in writing) from the date of completion of the relevant Security Test**.**

6.7 The Authority shall be entitled to send representation to witness the conduct of Security Tests.

6.8 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 and 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. The Authority may notify the Supplier of the results of such tests after completion of each such test. If any such Authority test adversely affects the Supplier's ability to deliver the Services so as to meet the Minimum Service Thresholds, the Supplier shall be granted relief against any resultant under-performance for the period of the Authority test.

6.9 Where any Security Test carried out pursuant to Paragraphs 6.1 or 6.8 reveals any actual or potential Breach of Security or weaknesses (included 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. 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, the change to the ISMS or Security Management Plan shall be at no cost to the Authority.

6.10 If any repeat Security Test carried out pursuant to Paragraph 6.9 reveals an actual or potential Breach of Security exploiting the same root cause failure, such circumstance shall constitute a material Default for the purposes of Clause 27.1(c) (Rectification Plan Process).

7 Compliance Of The ISMS with ISO/IEC 27001

7.1 Where Authority Data is stored, processed or transmitted, and under the management and/or control of the Supplier, the Supplier shall achieve and maintain ISO/IEC 27001 certification of compliance for those services, systems, processes and procedures throughout the term of this contract.

7.2 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

This document is based on Schedule 2.4 of the Crown Commercial Service Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright

practices of ISO 27001, the specific security requirements set out in Schedule 2.1 (Services Description) and the Baseline Security Requirements.

7.3 If, on the basis of evidence provided by such 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, then the Authority shall notify the Supplier of the same 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 become compliant within the required time then the Authority shall have the right to obtain an independent audit against these standards in whole or in part.

7.4 If, as a result of any such independent audit as described in Paragraph 7.3 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.

8 Breach Of Security

8.1 If a Breach of Security or attempted Breach of Security is discovered by either Party, that Party shall notify the other Party using the security incident management processes and procedures expressed and agreed in the ISMS.

8.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 8.1, the Supplier shall:

(a) immediately take all reasonable steps (which shall include any action or changes reasonably required by the Authority) necessary to:

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

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

(iii) 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 Minimum Service Thresholds, the Supplier shall be granted relief against any resultant under-performance for such period as the Authority, acting reasonably, may specify by written notice to the Supplier; and

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

This document is based on Schedule 2.4 of the Crown Commercial Service Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright

(b) 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.

8.3 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.

This document is based on Schedule 2.4 of the Crown Commercial Service Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright

ANNEX 1: Baseline Security Requirements

Valuation and Classifications of Assets

1 The Supplier shall evaluate and classify Authority assets using industry good practice, ensuring that access to Authority Data and other assets is correctly managed and that the physical, procedural, personnel and technical areas of the assets are safeguarded to an agreed and proportionate level throughout their lifecycle, including creating, processing, storage, transmission and destruction. The Supplier shall ensure that:

(a) the system is designed to support HMG business, and meet the requirements of relevant legislation, international standards, international agreements, and contractual obligations;

(b) the system is designed to protect information (and other assets) from accidental or deliberate compromise, which may lead to damage and/or criminal offence;

(c) operational data and information assets remain the property of the rightful User Organisation irrespective of any proprietary or open standard technique used to format or package the data;

(d) the Authority Data is only accessible to those verified with a need to know and that the location of where data is stored is transparent to the Authority and available upon request; and

(e) formal approval is sought from the Authority prior to sharing any data generated from User activity, User Device data or User identity data with any third party.

Data Processing, Storage, Management and Destruction

2 The Supplier and Authority recognise the need for the Authority Personal Data to be safeguarded under the Data Protection Act 1998 and/or EU Directive 95/46/EU. To that end, the Supplier must be able to state to the Authority the physical locations in which the Authority Data/Information may be stored, processed and managed from, and what legal and regulatory frameworks Authority Data/Information will be subject to at all times.

3 The Supplier shall agree any change in location of data storage, processing and administration with the Authority in advance where the proposed location is outside the UK. Such approval shall not be unreasonably withheld or delayed provided that any proposed change is in accordance with the Security Policy Framework and CESG IA Policy Portfolio.

4 Where the Supplier stores Authority Data (that is under the management and control of the Supplier, the Supplier shall:

(a) provide the Authority within twenty (20) working days of a request, a data sample of sufficient quantity to ascertain potential risks from compromise, loss or theft. The data shall be sent by the Supplier to the Authority in a secure format to be prescribed by the Authority, at no additional cost to the Authority;

This document is based on Schedule 2.4 of the Crown Commercial Service Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright

(b) have documented processes to guarantee availability of Authority Data in the event of the Supplier ceasing to trade;

(c) securely destroy all media that has held Authority Data at the end of life of that media in line with Good Industry Practice, the Security Policy Framework and CESG IA Policy Portfolio;

(d) securely erase any or all Authority Data held by the Supplier when requested to do so by the Authority in line with Security Policy Framework and CESG IA Policy Portfolio; and

(e) the Supplier shall ensure that any Personal Data that is no longer required is securely erased in accordance with HMG IA Standard No. 5.

Networking

5 The Supplier shall ensure that the network control function (the means and mechanisms used to configure network components (routers, switches, firewalls)) remains within the physical boundaries of the UK. This shall be done in accordance with Security Policy Framework and CESG IA Policy Portfolio.

6 The Supplier shall ensure that the network and service function provided is accessible and controllable from within the physical boundaries of the UK.

Personnel Security

7 Supplier Personnel shall be subject to pre-employment checks that are compliant with ISO/IEC 27001 and ISO/IEC 27002 and HMG Personnel Security Controls and shall include the verification of, as a minimum: identity, unspent criminal convictions and right to work.

8 At a time agreed between the Supplier and Authority, but in any event within ninety (90) days after the Effective Date, the Supplier in collaboration with the Authority shall conduct a Personnel Security Risk Assessment for each role within their organisation where that role will have direct access to Authority information or assets. The Supplier may choose the method of assessment, but it must conform to Good Industry Practice or CPNI 'Personnel Security Risk Assessment' available at: http://www.cpni.gov.uk/documents/publications/2010/2010037-risk_assment_ed3.pdf?epslanguage=en-gb

9 The Supplier shall agree with the Authority on a case by case basis those Supplier Personnel roles that require National Security Clearance such as Counter Terrorist Check (CTC), Security Check (SC) or possibly Developed Vetting (DV). These roles include, but are not limited to:

(a) the Supplier employees, contractors or Sub-contractors system administrators; and

(b) individuals with elevated privileges that can access IT systems which store or process Authority Data.

10 The Supplier shall obtain the necessary clearance for each of its staff before services or systems are made operational whereby Authority data is stored, processed or transmitted on

This document is based on Schedule 2.4 of the Crown Commercial Service Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright

or over Supplier infrastructure and in any event within 21 months after the Effective Date. Any costs associated with obtaining the necessary staff clearances shall be borne by the Supplier

11 The Supplier shall prevent Supplier Personnel who are unable to obtain the required security clearances from accessing systems which store, process, or are used to manage Authority Data except where agreed with the Authority in writing.

12 All Supplier 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 Authority in writing, this training must be undertaken annually.

13 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 staff no longer need elevated privileges or leave the organisation, their access rights shall be revoked within one (1) Working Day.

Business Continuity and Disaster Recovery

14 The Supplier shall produce a Business Continuity Management System in accordance with BS ISO 22301

This document is based on Schedule 2.4 of the Crown Commercial Service Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright

ANNEX 2: Security Management Plan

Emergency Services Mobile Communications Programme

Home Office

Schedule 2.4

Security Management

Outline Security Plan

Version	<<enter the version number of the document>>
Date Issued	<<enter the date as: >> YYYY-MM-DD
Purpose of Issue	For Review | For ITT | For Approval | For Record
Approval Status	Draft | In Review | Approved
Author	<<enter lead author name>>
Security Classification	OFFICIAL | OFFICIAL – SENSITIVE

Document Control

METADATA	
Document Identifier	<<enter File Name or EDRM ID, e.g.>> Lot 3 - Schedule 2 4 Security Management 4 0(35090828_23) (2)_final_050516.doc
Document Abstract	<<enter short description of content and purpose of document>>
Creation Date	<<enter date document was initiated: >> YYYY-MM-DD
Title	<<enter title of the report>>
Online Location	<<enter file path>> http://share/projects/ProjectSoteria/Shared Documents/Contract redaction/Fully_Redacted_Schedules/Lot 3 - Schedule 2 4 Security Management 4 0(35090828_23) (2)_final_050516.docx
Contributing Author(s)	<<enter names responsible for contributing to document's creation
Originating Unit	<<enter name of work stream responsible for document>>

REVISION HISTORY			
Version	**Revision Date**	**Revised By**	**Change Description**
x.x	YYYY-MM-DD	Name	Brief Summary of Key Changes

DISTRIBUTION LIST				
Date Issued	**Version Issued**	**Name**	**Job Title**	**Role**
YYYY-MM-DD	x.x	Name	Title Name	R / I / A

R = Reviewer; I = For information Only; A = Approver

APPROVALS				
Name	**Job Title**	**Version Approved**	**Date Approved**	**e-Signature**

REFERENCES	
#	<<include date, author, title, version/edition, hyperlink also>>

Table of Contents

1 Definitions 4

1.1 In construing this Schedule 2.4 (Security Management), unless otherwise expressly specified in this Schedule terms defined and used in Schedule 1 (Definitions) will have the same meaning in this Schedule. 4

2 Introduction 4

2.1 The Parties acknowledge that the purpose of the ISMS and Security Management Plan are to ensure a good organisational approach to security under which the specific requirements of this Agreement will be met. 4

2.2 The Parties shall each appoint a member of the Programme Board to be responsible for security. The initial member of the Programme Board appointed by the Supplier for such purpose shall be the person named as such in Schedule 9.2 (Key Personnel) and the provisions of Clauses 14.5 and 14.6 (Key Personnel) shall apply in relation to such person. 4

2.3 Both Parties shall provide a reasonable level of access to any members of their personnel for the purposes of designing, implementing and managing security. 4

2.4 The Supplier shall use as a minimum Good Industry Practice in the day to day operation of any system storing, 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. 4

2.5 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. 4

2.6 The Authority and the Supplier acknowledge that information security risks are shared between the Parties and that a compromise of either the Supplier or the Authority's security provisions represents an unacceptable risk to the Authority requiring immediate communication and co-operation between the Parties. 4

3 Information Security Management System (ISMS) 4

3.1 Within twenty one (21) months after the Effective Date, the Supplier shall develop and submit to the Authority for the Authority's approval in accordance with Paragraph 4.3 an ISMS for the purposes of this Agreement, which: 4

3.2 The Supplier acknowledges that the Authority places great emphasis on the reliability of the services for confidentiality, integrity, availability, and authenticity of information and consequently on the security, non-repudiation and accountability provided by the ISMS and that it shall be responsible for the effective performance of the ISMS; 5

3.3 The ISMS shall: 5

3.4 Subject to Clause 20.11 (Authority Data and Security Requirements) the references to standards, guidance and policies set out in Paragraph 3.3 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. 6

3.5 In the event that the Supplier becomes aware of any inconsistency in the provisions of the standards, guidance and policies set out in Paragraph 3.3, the Supplier shall immediately notify the Authority Representative of such inconsistency and the Authority Representative shall, as soon as practicable, notify the Supplier which provision the Supplier shall comply with. 6

3.6 If the ISMS 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. 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 3 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 3.3 to 3.5 shall be deemed to be reasonable. 6

3.7 Approval by the Authority of the ISMS pursuant to Paragraph 3.6 or of any change or amendment to the ISMS shall not relieve the Supplier of its obligations under this Schedule. 6

4 Security Management Plan 6

4.1 Within thirty (30) Working Days after the Effective Date, the Supplier shall prepare and submit to the Authority for approval in accordance with Paragraph 4.3 a fully developed, complete and up-to-date Security Management Plan which shall comply with the requirements of Paragraph 4.2. 6

4.2 The Security Management Plan shall: 6

4.3 If the Security Management Plan submitted to the Authority pursuant to Paragraph 4.1 is approved by the Authority, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. 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 and in any event no longer than fifteen (15) Working Days (or such other period as the Parties may agree in writing) from the date of its first submission to the Authority. If the Authority does not approve the Security Management Plan following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No approval to be given by the Authority pursuant to this Paragraph 4.3 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 4.2 shall be deemed to be reasonable. 7

4.4 Approval by the Authority of the Security Management Plan pursuant to Paragraph 4.3 or of any change or amendment to the Security Management Plan shall not relieve the Supplier of its obligations under this Schedule. 8

5 Amendment And Revision Of The ISMS And Security Management Plan 8

5.1 The ISMS and Security Management Plan shall be fully reviewed and updated by the Supplier from time to time and at least annually to reflect: 8

5.2 The Supplier shall provide the Authority with the results of each review of the Security Management Plan as soon as reasonably practicable after their completion and amend the ISMS and Security Management Plan at no additional cost to the Authority. The results of the Security Management Plan review shall include, without limitation: 8

5.3 Subject to Paragraph 5.4, any change or amendment which the Supplier proposes to make to the ISMS or Security Management Plan (as a result of a review carried out pursuant to Paragraph 5.1, an Authority request, change to Schedule 2.1 (Services Description) or otherwise) shall be subject to the Change Control Procedure and shall not be implemented until approved in writing by the Authority. 8

5.4 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 Change Control Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Change Control Procedure for the purposes of formalising and documenting the relevant change or amendment for the purposes of this Agreement. 9

6 Security Testing 9

6.1 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 IT Environment or after any change or amendment to the ISMS, (including security incident management processes and incident response plans) or the Security Management Plan. The implementation of Security Tests shall be designed by the Supplier so as to minimise the impact on the delivery of the Services. Subject to Paragraph 6.2, the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Authority. Subject to compliance by the Supplier with the foregoing requirements, if any Security Tests adversely affect the Supplier's ability to deliver the Services so as to meet the Minimum Service Thresholds, the Supplier shall be granted relief against any resultant under-performance for the period of the Security Tests. The output of such tests should be recorded in a format agreed by the Authority. 9

6.2 The Supplier agrees that the Authority is able to request Security Tests without prior notice. 9

6.3 Security Tests should comply with the recommendations set out in the Security Policy Framework and CESG IA Policy Portfolio. 9

6.4 Within thirty (30) Working Days after the Effective Date the Supplier shall prepare and submit to the Authority for approval in accordance with Paragraph 6.1 (Implementation Plan), a template to be used for reporting Security Test results (the "**Security Test Results Template**"). 9

6.5 If the Security Test Results Template submitted to the Authority pursuant to Paragraph 6.4 is approved by the Authority, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the Security Test Results Template 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 Security Test Results Template 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 6.5 may be unreasonably withheld or delayed. However any failure to approve the Security Test Results Template on the grounds that it does not comply with the requirements set out in Paragraph 6.1 shall be deemed to be reasonable. 9

6.6 The Supplier shall submit to the Authority the output of all Security Tests carried out in accordance with Paragraph 6.1 (Implementation Plan), using the Security Test Results Template approved by the Authority within no more than fifteen (15) Working Days (or such other period as the Parties may agree in writing) from the date of completion of the relevant Security Test**.** 10

6.7 The Authority shall be entitled to send representation to witness the conduct of Security Tests.10

6.8 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 and 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. The Authority may notify the Supplier of the results of such tests after completion of each such test. If any such Authority test adversely affects the Supplier's ability to deliver the Services so as to meet the Minimum Service Thresholds, the Supplier shall be granted relief against any resultant under-performance for the period of the Authority test. 10

6.9 Where any Security Test carried out pursuant to Paragraphs 6.1 or 6.8 reveals any actual or potential Breach of Security or weaknesses (included 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. 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, the change to the ISMS or Security Management Plan shall be at no cost to the Authority. 10

6.10 If any repeat Security Test carried out pursuant to Paragraph 6.9 reveals an actual or potential Breach of Security exploiting the same root cause failure, such circumstance shall constitute a material Default for the purposes of Clause 27.1(c) (Rectification Plan Process). 10

7 Compliance Of The ISMS with ISO/IEC 27001 10

7.1 Where Authority Data is stored, processed or transmitted, and under the management and/or control of the Supplier, the Supplier shall achieve and maintain ISO/IEC 27001 certification of compliance for those services, systems, processes and procedures throughout the term of this contract. 10

7.2 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. 10

7.3 If, on the basis of evidence provided by such 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, then the Authority shall notify the Supplier of the same 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 become compliant within the required time then the Authority shall have the right to obtain an independent audit against these standards in whole or in part. 11

7.4 If, as a result of any such independent audit as described in Paragraph 7.3 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. 11

8 Breach Of Security 11

8.1 If a Breach of Security or attempted Breach of Security is discovered by either Party, that Party shall notify the other Party using the security incident management processes and procedures expressed and agreed in the ISMS. 11

8.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 8.1, the Supplier shall: 11

8.3 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. 12

ANNEX 1: Baseline Security Requirements 13

ANNEX 2: Security Management Plan 16

Emergency Services Mobile Communications Programme 17

Schedule 2.4 17

Security Management 17

Outline Security Plan 17

Document Control 18

METADATA 18

REVISION HISTORY 18
DISTRIBUTION LIST 18
APPROVALS 19
REFERENCES 20
Table of Contents 21

1. Overview 27

2. Information Security Management System 31

2.1 Existing ISMS and ISO Certification 31
2.2 Use of standards, guidance and policies 32
2.3 ISMS Audit 32
2.4 ISMS Review and Finalisation for ESN 33
2.5 ISMS Approval Procedure 33

3. Detailed Draft Security Management Plan 34

3.1 Introduction 34
3.1.1 Review and Finalisation of Security Management Plan ... 35
3.1.2 Security Management Plan Approval Procedure ... 35
3.2 Personnel Security 36
3.2.1 Employment Screening ... 36
3.2.2 Personnel Security Risk Assessment and Elevated Security Clearance ... 37
3.2.3 Terms and Conditions of Employment ... 37
3.2.4 Mandatory training and regular security awareness ... 37
3.2.5 Role Based Access Control ... 38
3.2.6 Controls for change or termination of employment ... 38
3.3 Physical Security 39
3.3.1 Supplier's Company-wide Controls ... 39
3.3.2 Technical Sites ... 39
3.3.3 Cell Sites ... 39
3.4 Procedural Security Controls 39
3.4.1 Governance, leadership and responsibilities ... 39
3.4.2 Valuation and Classification of Assets ... 41
3.4.3 Data Processing, Storage, Management, Disposal and Destruction ... 42
3.4.4 Risk Management ... 44
3.4.5 Access to Secure Areas ... 45
3.4.6 Security in Supplier Relationships ... 45
3.5 Business Continuity and Disaster Recovery 46
3.6 Technical Security Controls 46
3.6.1 Networking ... 46
3.6.2 System development and maintenance ... 47
3.6.3 Operational management ... 47
3.6.4 Encryption and authentication ... 47
3.6.5 Security architecture ... 47
3.6.6 Supplier's Mobile Data Services Security Architecture ... 48
3.6.7 Protection against Distributed Denial of Service (DDoS) attacks ... 48
3.6.8 Identity and Access Management ... 48
3.6.9 Security Incident Event Monitoring ... 49
3.6.10 Vulnerability Scanning ... 49
3.6.11 Password Control ... 49
3.6.12 Monitoring ... 49

4.	**Amendment and Revision of the ISMS and Security Management Plan**	**50**
5.	**Security Audit, Testing and Vulnerability Management**	**50**
5.1	Audit and Testing	50
5.2	Vulnerability management	52
5.3	Security Test Results Template	53
6.	**Breach of Security Activities**	**53**
6.1	Security Incident Management	53
7.	**Conclusion**	**55**
A1.	Annex 1	56
A2.	Annex 2	57
A3.	Annex 3	58

1. Overview

Security Management has always been a core discipline for the Supplier with executive management sponsorship and a dedicated security department. The security framework is signed off by the Supplier's Chief Executive Officer and cross functional business sponsors provide oversight through governance boards.

The Supplier has always recognised that we have had to protect customers, systems and services, especially in relation to operating part of the Telecommunications Critical National Infrastructure of the UK. In the context of operating a key part of the ESN we especially recognise the importance of security management, the enhanced need to fully protect the services from both cyber and physical security threats, and the implications that inadequate security management could have for the Emergency Services, the national security of the country, and the safety of the population. Therefore the Supplier understands the importance of ensuring maintained security for the ESN and mitigating the risk posed by security threats as much as possible. The Services will provide the critical communications for the UK's Emergency Services, and any loss of Service due to a Security incident would severely impact the ability of the Emergency Services to function at the level the UK requires in order to:

- Keep the Emergency Services personnel safe
- Communicate in the event of an emergency; and
- Save human life and property.

The Supplier understands the need for strict security controls to counter any cyber or physical threats that may affect the service. The Supplier already demonstrates a high level of commitment to protecting existing commercial services from attacks such as Denial of Service, un-authorised access to systems and sites and protecting information such as geo-location data (e.g. in the context of the ESN, protecting against unauthorised identification of the locations of Emergency Services vehicles at any time – any breach which could severely hamper the ability of the ESN to function). Although, in this case such an attack would be highly technical and complicated to carry out, the Supplier is confident that the security controls and monitoring it will have in place for the service would mitigate the risk down to a negligible level and it will maintain this security stance for all aspects of the ESN service the Supplier would be responsible for.

Secure by design is a key feature of the Supplier's technology architecture, build and operate methodologies. The Supplier's architecture deploys a segregated, defence in depth model and security requirements are fed into projects at an early stage of the project lifecycle. Development quality is checked for security adherence using automated and human techniques and the ongoing security of the technologies is monitored by an operational security team.

In accordance with the requirements of Schedule 2.4 paragraph 2.4 the security framework deployed by the Supplier is based around industry best practice. Upon the formation of the company the Supplier immediately obtained certification to ISO27001.

The scope of applicability for the Supplier's ISO27001 certification has been designed to ensure that it maintains the confidentiality, integrity and availability of its network to ensure that its customers can confidently make use of the first and largest LTE network in the UK. The scope of applicability is extremely pertinent for the Emergency Services Network as it is a direct map for the services we would provide. Since the Supplier's overall solution for the ESN is based on the services for which it already has ISO27001 certification, there is strong alignment between the Supplier's Security Management

approach, and its overall Solution. The Supplier has just successfully completed the transition from ISO27001:2005 to ISO27001:2013 in March 2015.
The Supplier has also been assessed and found to be compliant for the ND1643 standard of which the Supplier was one of the founder supporters. This helps protect the Supplier's Interconnects with other Telecommunication providers.
The security controls the Supplier operates are of a high standard and are based on best practices.
The Supplier recognises that in the context of the ESN, security plays an ever more important role, due to the potential implications for national security and for the continuity of the safe operation of the Emergency Services Network. For this reason along with the importance of Security Management to its day to day business, the Supplier recognises that there is a need for continuous improvement and therefore undertakes regular reviews and tests to ensure that it is not only mitigating the current security threats, but is also striving to identify future threats. The Supplier identifies these threats through its strong understanding of its operating environment, by working closely within the industry, with its suppliers and with the UK government and security services. For ESN specific services the Supplier will undertake extra diligence if required to ensure that the appropriate security coverage is in place and will ensure the Supplier maintains ISO27001:2013 certification.
A good example of this would be in the launch of LTE. Prior to launch the Supplier worked with the CPNI to test its pilot for LTE (in 2012). The tests carried out identified a potential weakness in the backhaul of LTE, for which the mitigation was the implementation of IPSEC on all the Supplier's backhaul links. Combine this with working closely with the Supplier's major RAN providers to improve their security (the Supplier was the first company to use the Huawei Cyber Security Evaluation Centre in Banbury) and the Supplier can demonstrate that not only was it the first adopter of LTE in the UK, but it also undertook security testing from pilot to full deployment and this practice continues today.
The Supplier has included a detailed list of the relevant security policies and procedures for the ESN Service in the Appendices of this document.
The Supplier has shown in the table below the detail of why its response meets the Authority's evaluation criteria for scoring 100%.

Table 1: Table demonstrating why Supplier response scores 100%

Scoring guidance criteria for 100%	How we meet these criteria	Method Statement Reference
Detailed draft Security Management plan giving high level of confidence in the information assurance and security of the services	The Supplier has provided a detailed draft Security Management Plan to meet the requirements listed in Schedule 2.4. This is to be finalised following the Effective Date and submitted to the Authority for approval within 30 Working Days	
BS ISO/IEC 27001 (or equivalent) certification to include personnel, physical, procedural and technical aspects	The Supplier holds BS ISO 27001:2013 – the scope of applicability of the Supplier's certification covers the personnel, physical, procedural and technical aspects of its service for business customers. This covers the entire scope of the service to be delivered to the Authority for the ESN.	
Recognition of broader ESN context	The Supplier recognises the broader ESN	

and its implications	context throughout its Security Management plan. The risk of Security breach in the ESN context could have implications for national security, and the effectiveness of the Emergency Services Network. Therefore the Supplier's approach in this plan is to base its approach on its ISO 27001, ND1643 and other best practice standards, and to set out in its Method Statement its approach to confirming whether there are any gaps in its approach and closing them.	
Strong alignment to the Bidder's solution	The Supplier's Security Management systems currently manage the security of the Supplier's operations. There is strong alignment to the Bidder's solution since the solution is based on the Supplier's existing network and systems, which the Supplier's ISO 27001 certification already covers. The Supplier's ESN solution also incorporates some segregated core elements with enhanced management of security.	
Accompanying Method Statement demonstrating finalisation of Plan, implementation and accreditation	The accompanying Method Statement details a plan for the activities which the Supplier will undertake with the Authority and Other ESN Suppliers to finalise the Plan. It also details the activities the Supplier will undertake to implement the Plan and ensure accreditation is ensured.	

The requirements listed by the Authority in Schedule 2.4 are met in the following sections of the Plan:

Schedule 2.4 requirement	**Section of detailed draft Security Management Plan where this is addressed**
2.1	Section 2.1
2.2	Section 3.4.1
2.3	Section 3.1
2.4	Section 3.4.1
2.5	Section 2.3
2.6	Section 3.4.4
3.1	Section 2.4
3.2	Section 2.1
3.3 a)	Section 2.4
3.3 b)	Section 2.1
3.3 c)	Section 2.1
3.3 d)	Section 6.1
3.3 e)	Section 5.2

Schedule 2.4 requirement	Section of detailed draft Security Management Plan where this is addressed
3.3 f)	Section 2.1
3.4	Section 2.2
3.5	Section 2.2, 2.4, 2.5
3.6	Section 2.5
3.7	Section 2.5
4.1	Section 3.1.1
4.2 a)	Section 3.1.1
4.2 b)	Section 2.1
4.2 c)	Section 3.4.1
4.2 d)	Section 3.1, 3.4.4, 3.4.6
4.2 e)	Section 3.1
4.2 f)	Section 3.1
4.2 g)	Section 3.1
4.2 h)	Section 3.1.1
4.2 i)	Section 3.1
4.2 j)	Section 3.1
4.2 k)	Addressed throughout the Plan
4.2 l)	Section 3.1.1
4.3	Section 3.1.1, 3.1.2
4.4	Section 3.1.2
5.1	Section 4
5.2	Section 4
5.3	Section 4
5.4	Section 4
6.1	Section 5.1, 5.2
6.2	Section 5.1
6.3	Section 5.1
6.4	Section 5.3
6.5	Section 5.3
6.6	Section 5.1
6.7	Section 5.1
6.8	Section 2.3
6.9	Section 5.2
6.10	Section 5.2
7.1	Section 2.1
7.2	Section 2.3
7.3	Section 2.2
7.4	Section 2.3
8.1	Section 6.1
8.2 a)	Section 6.1
8.2 b)	Section 6.1
8.3	Section 6.1

Schedule 2.4 requirement	Section of detailed draft Security Management Plan where this is addressed
Annex 1: 1	Section 3.2.5, 3.3.1, 3.4.2
Annex 1: 2	Section 3.4.3
Annex 1: 3	Section 3.4.3
Annex 1: 4	Section 3.4.3
Annex 1: 5	Section 3.4.3
Annex 1: 6	Section 3.6.1
Annex 1: 7	Section 3.2.1
Annex 1: 8	Section 3.2.2
Annex 1: 9	Section 3.2.2
Annex 1: 10	Section 3.2.2
Annex 1: 11	Section 3.2.2
Annex 1: 12	Section 3.2.4
Annex 1: 13	Section 3.2.5
Annex 1: 14	Section 3.5

2. Information Security Management System

2.1 Existing ISMS and ISO Certification

In accordance with Schedule 2.4 paragraph 4.2(e) the Supplier holds ISO 27001:2013, certificate number IS 610421. The scope is the "Provision, operation and support of EE mobile, broadband and integrated products and services for business customers" in accordance with the Statement of Applicability (SOA) Version 7, dated 17th October 2014 which covers the locations, systems, processes and procedures in scope of the ESN service. Therefore it is the intention of the Supplier to submit our current independently approved ISO27001:2013 ISMS to enable the Authority to confirm it is fit for purpose for the Supplier to provide the ESN service to the Authority.

The ISMS ensures the Supplier has a good organisational approach to security to ensure the specific requirements of the Authority can be met, meeting the requirements of Schedule 2.4 paragraph 2.1.

The Supplier acknowledges that the Authority places great emphasis on the reliability of services for confidentiality, integrity, availability, and authenticity of information and consequently on the security, non-repudiation and accountability provided by the ISMS. The Supplier acknowledges that it shall be responsible for the effective performance of the ISMS (meeting the requirements of Schedule 2.4 paragraph 3.2).

The Supplier's Information Security Management System (ISMS) complies with the requirements of ISO27001 and ISO27002 and meets the requirements of all relevant legislation (meeting the requirement in Schedule 2.4 paragraph 3.3 (b)). All ISO27001 Annex A controls have been implemented as applicable to the Supplier's business and to the ESN as demonstrated by the inclusion of Annex 5 ISO 27001 Statement of Applicability (redacted customer version).

This provides the comprehensive framework for security solutions that protect the Authority Service and information against internal and external threats; and at all times provides a level of security which is in accordance with Law and this Agreement, demonstrates Good Industry Practice at a minimum and complies with the Baseline Security Requirements (meeting the requirements in Schedule 2.4 paragraph 4.2 (b))., addresses issues of incompatibility with the Supplier's own organisational security policies, meets any specific security threats of immediate relevance to the Services or Authority Data, complies with the security measures and standards set out in the Security Policy Framework (Tiers 1-

4), and complies with the security requirements as set out in Schedule 2.1 (meeting the requirements in Schedule 2.4 paragraph 3.3 (c)). The Supplier. The Supplier recognises that there is additional work to do in this area (see section 4 of the Security Management Method Statement)

The Supplier confirms that where Authority Data is stored, processed or transmitted, and under the management and/or control of the Supplier. The Supplier shall maintain its existing ISO 27001 certification of compliance for those services, systems, processes and procedures pertaining to the ESN service throughout the term of this Agreement (meeting the requirement in Schedule 2.4 paragraph 7.1)

Overall ISO 27001 controls allow the Supplier to maintain the confidentiality, integrity and availability of Authority information and the security of the ESN service. The ISMS will be certified by the Supplier's Chief Technical Officer in accordance with the requirements of Schedule 2.4 paragraph 3.3 (f). The Supplier. The Supplier will notify the Authority of any changes to the ISMS pertinent to the ESN service in accordance with the requirements of Schedule 2.4 paragraph 5.3.

In addition to the requirements of Schedule 2.4 and to provide the Authority with additional confidence in the Supplier's approach to, and expertise in Security Management, the Supplier is compliant with ND1643, the NICC minimum standards required to protect the UK National Infrastructure applicable to telecommunications interconnection.

2.2 Use of standards, guidance and policies

The Supplier accepts the requirement in Schedule 2.4 paragraph 3.4 – subject to Clause 20.11 in the ESMCP Framework Terms and Conditions – Lot 3 (regarding Change Control for the Baseline Security Requirements), the Supplier agrees that references to standards, guidance and policies contained within the Authority's ISMS requirements (Schedule 2.4 paragraph 3.3) shall be deemed to be references to future updates and replacements to these standards, guidance and policies (meeting the requirement in Schedule 2.4 paragraph 3.4).

In the event that the Supplier becomes aware of any inconsistency in the provision of these standards, it shall notify the Authority Representative. The Authority Representative shall then inform the Supplier which provision to comply with (meeting the requirement in Schedule 2.4 paragraph 3.5).

2.3 ISMS Audit

The ISMS is subject to regular independent audit by the Supplier's external certification body (currently BSI) and is subject to a programme of internal audit to ensure the Supplier continues to comply with the requirements of ISO 27001:2013. Any non-conformities identified during the course of audit will be rectified through appropriate corrective action management plans. In accordance with the requirements of Schedule 2.4 paragraph 2.5, the Supplier's security policies, standards processes and procedures are aligned with ISO27002 and are reviewed at least annually to ensure they continue to meet Industry Best Practice, continue to protect against emerging or changed security threats and continue to meet the demands of emerging technologies. The Authority is welcome to review the Supplier's ISO27001 document set at the Supplier's premises due to the classification of the documents which means they must stay within the Supplier. Please refer to Annex 1 – Technology Security Document Framework which provides a complete list of the Supplier's security document set. Redacted versions of the Suppliers Information Security Management System, Information Security Policy and ISO 27001 Statement of Applicability are provided in Annex 3, 4 and 5 respectively.

In accordance with the requirements of Schedule 2.4 paragraph 6.8 the Supplier recognises the Authorities' right to audit, at any time and with reasonable written notice, to carry out such tests

(including penetration tests) deemed necessary in relation to the ISMS, the Supplier's compliance with the ISMS and the Security Management Plan.
In accordance with the requirements of Schedule 2.4 paragraph 7.2 the Authority shall be entitled to carry out such security audits as it deems reasonably necessary to ensure the ISMS maintains compliance with the principals and practices of ISO 27001, the specific security requirements set out in Schedule 2.1 and the baseline security requirements.
In accordance with the requirements of Schedule 2.4 paragraph 7.4 if, as a result of independent audit, described in Schedule 2.4 paragraph 7.3, the Supplier is found to be non-compliant with the principals and practices of ISO 27001, the specific security requirements set out in Schedule 2.1 and the /or the baseline security requirements, then the Supplier will undertake the actions required to achieve necessary compliance at its own expense.
All audit requirements will be in alignment with Schedule 7.5 of the Agreement.
If on the basis of evidence provided by such audits, the Authority believes the Supplier is not achieving compliance with the principles and practices of ISO 27001, the security requirements in Schedule 2.1 or the Baseline Security Requirements, the Authority shall notify the Supplier of this and give the Supplier a reasonable time to implement any necessary remedy. If the Supplier does not become compliant within the required time then the Authority shall have the right to obtain an independent audit against these standards in whole or in part (meeting the requirement in Schedule 2.4 paragraph 7.3). If, as a result of this independent audit, the Supplier is found to be non-compliant, the Supplier will implement a corrective action plan to achieve necessary compliance and shall reimburse the Authority for the full costs of an audit commissioned by the Authority in line with the requirements of Schedule 2.4 paragraph 7.4.

2.4 ISMS Review and Finalisation for ESN

The Supplier's existing ISMS covers all aspects of the Services and all processes associated with the delivery of the Services, including any IT, information and data; unless otherwise specified by the Authority in writing, any development to the ISMS will continue to cover these elements, meeting the requirement in Schedule 2.4 paragraph 3.3 (a) the Supplier recognises that amendments may be required to the Supplier's documentation depending on the outcome of the gap analysis described throughout the Security Management Method Statement. The Supplier will put in place any required amendments such that it can submit its ISMS, that will have been tested and comply with the Authority's requirements in Schedule 2.4 paragraphs 3.3-3.5, for the Authority's approval within 17 months after the Effective Date (meeting the requirement detailed in Schedule 2.4 paragraph 3.1)

2.5 ISMS Approval Procedure

Upon submission of the ISMS to the Authority the following process shall take place:

- If the ISMS is approved by the Authority, it shall be adopted immediately and maintained as detailed in this section of the Plan
- If the ISMS is not approved, the Supplier shall amend it within 10 Working Days of a notice of non-approval and resubmit to the Authority for approval
- If the Authority does not approve the ISMS following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure

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 15 Working Days (or such other period as the Parties may

agree in writing) from the date of its first submission to the Authority. The Authority must provide timely approval if appropriate, however the Supplier acknowledges that lack of approval on the basis of not meeting the requirements set out in Schedule 2.4 paragraphs 3.3-3.5 is acceptable (meeting the requirement listed in Schedule 2.4 paragraph 3.6).
In accordance with the requirements set out in Schedule 2.4 paragraph 3.7 the Supplier confirms it will continue to meet the obligations set out under Schedule 2.4 regardless of Authority approval of the ISMS or any amendment to the ISMS.

3. Detailed Draft Security Management Plan

3.1 Introduction

The following detailed draft plan is based on an enhanced version of the existing mature Security Management Plan that the Supplier already has in place which the Supplier believes will be fit for purpose for the provision of the ESN service. The plan is designed around Security best practice and allows the Supplier to maintain its ISO27001:2013 certification. The plan is divided into key areas of security best practice which combine to ensure ongoing compliance with the requirements of ISO 27001:2013: –

- Personnel Security (Section 3.2)
- Physical Security (Section 3.3)
- Procedural Security Controls (Section 3.4)
- Technical Security Controls (Section 3.6)
- Security Audit & Testing (Section 5)
- Security Incident Management (Section 6.1)

In accordance with Schedule 4.2 paragraph 4.2 (d) the Security Management plan details the process for managing security risks from Sub-contractors and third parties authorised by the Authority with access to the Services (Section 3.4.4), processes associated with the delivery of the Services (Section 3.4), the Authority Premises, the Sites (Section 3.3), the Supplier System, the Authority System (to the extent that it is under the control of the Supplier) and any IT, Information and data (including 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 (Section 3.6)
As the Security Management Plan is aligned to the Supplier's ISO 27001:2013 certification which covers the scope of services required by the Authority, the Security Management Plan protects all aspects of the Services detailed above (meeting the requirement in Schedule 2.4 paragraph 4.2 (e)).
The Security Management Plan sets out the security measures that will be implemented and maintained by the Supplier in relation to the aspects of the ESN service the Supplier is responsible for, and will at all times comply with and specify security measures and procedures which are sufficient to ensure that the Services comply with the provisions of Schedule 2.4 (meeting the requirement in Schedule 2.4 paragraph 4.2 (f))
In accordance with the requirements of Schedule 2.4 paragraph 4.2 (g) the Supplier believes the overall Supplier Solution minimises Authority and Supplier effort required to comply with Schedule 2.4 – the Supplier will continue to consider any applicable pan-government accredited services to help deliver the Security Management Plan.
In accordance with the requirements of Schedule 2.4 paragraph 4.2 (i) the response sets out the security measures that protect all aspects of the Service including premises, systems, processes, information and data contained within Lot 3. The Supplier's current understanding is that it will not

have any of the Authority System under its control as the Supplier's submission is restricted to the provision of Lot 3 services which doesn't include a requirement to manage the Authority System.
The Supplier will confirm this assumption through the actions set out in the Method Statement Section 4.
As shown above, the Security Management Plan is structured in accordance with ISO 27001:2013 and ISO 27002 where relevant. [The Plan cross references to Schedules 7.4 , 7.5, 8.6 and 9.2 where they cover testing procedures, financial reports and audit reports, business continuity and disaster recovery, and key personnel] (meeting the requirement in Schedule 2.4 paragraph 4.2 (j))
Where applicable, the Supplier will provide a reasonable level of access to any members of the Authority for the purposes of designing, implementing and managing security which meets the requirements of Schedule 2.4 paragraph 2.3.

3.1.1 Review and Finalisation of Security Management Plan

In accordance with the requirements of Schedule 2.4 paragraph 4.1, this plan will be finalised following the Effective Date and submitted to the Authority for approval within 30 days and in accordance with the requirements. This detailed draft security management plan represents the Supplier's submission to meet the requirements of Schedule 2.4 Annex 2 (meeting the requirements of Schedule 2.4 paragraphs 4.2 (a))
In accordance with the requirements of Schedule 2.4 paragraph 4.2 (h) the Supplier will also undertake to ensure that if any gaps are identified between its operation of ISO27001:2013 (which the Supplier believes is ready to be used as the ISMS for the ESN) and the Security Policy Framework and CESG IA Policy Portfolio. This will ensure it adopts the most applicable and most relevant best practice and will submit an amended Plan for approval by the Authority within the timescales set out in schedule 2.4 paragraph 4.3. Details for how the Supplier will complete this transition are contained in section 4 Finalisation of the Security Management Plan of the Security Management Method Statement set out in the sections listed below: -

- Personnel Security – Section 4.1
- Security Training – Section 4.2
- Access Control – Section 4.3
- Physical Security – Section 4.4
- Governance, risk and incident management – Section 4.5
- Valuation and classification of assets – Section 4.6
- Data disposal and destruction – Section 4.7
- 3rd party suppliers – Section 4.8
- Vulnerability Management – Section 4.9
- Audit, testing and monitoring – Section 4.10

Once developed, the Security Management Plan will be Protectively Marked in accordance with the Cabinet Office Government Security Classification Policy and the Security Policy Framework (meeting the requirement in Schedule 2.4 paragraph 4.2 (l))

3.1.2 Security Management Plan Approval Procedure

Once finalised, the Security Management Plan will be submitted to the Authority and the following process will take place:

- If the Security Management Plan is approved by the Authority, it shall be adopted immediately and maintained as detailed in this draft Plan
- If the Security Management Plan is not approved, the Supplier shall amend it within 10 Working Days of a notice of non-approval and resubmit to the Authority for approval
- 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

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 15 Working Days (or such other period as the Parties may agree in writing) from the date of its first submission to the Authority. The Authority must provide timely approval if appropriate, however the Supplier acknowledges that lack of approval on the basis of not meeting the requirements set out in Schedule 2.4 paragraph 4.2 is acceptable (meeting the requirement listed in Schedule 2.4 paragraph 4.3).
In accordance with the requirements set out in Schedule 2.4 paragraph 4.4 the Supplier confirms it will continue to meet the obligations set out under Schedule 2.4 regardless of Authority approval of the Security Management Plan or approval of any changes to the Security Management Plan.

3.2 Personnel Security

The Supplier understands the risk the insider threat poses to the security of the Authority information and Service and therefore personnel security is actively managed prior to on boarding and throughout the term of employment. The controls set out below are what the Supplier already operates and will meet the criteria set out for the operation of the ESN in Schedule 2.4 Annex 1 paragraphs 7 - 13. They will be updated as required based on the outcome of the Security Management Method Statement, section 4.1.
This is achieved by: -

- employment screening (Section 3.2.1)
- terms and conditions of employment (Section 3.2.3)
- mandatory training and regular security awareness (Section 3.2.4)
- strict role based access control (Section 3.2.5)
- controls for change or termination of employment. (Section 3.2.6)

An overview of the Supplier's existing approach to Personnel Security is described in Annex 3, Information Security Management System Section 8 Personnel Security and Section 11 Access Control and evidence of the ISO 27001 controls adopted by the Supplier in support of Personnel Security can be viewed within Annex 5 Statement of Applicability.
This multi layered approach to personnel security recognises that in the context of the ESN, personnel security controls play an important role, due to the potential implications for national security, the need to maintain the safety of Emergency Services personnel and for the continuity of the safe operation of the ESN to ensure the Emergency Services can continue to communicate in the event of an emergency and save human life and property. Therefore the controls implemented reduce the risk of unauthorised access to or loss of the ESN service.

3.2.1 Employment Screening

All the Supplier's employees, including contractor and temporary agency employees, are required to undergo the Supplier's employee vetting process prior to commencing employment. The process is

compliant with ISO27001:2013 and ISO27002:2013 and HMG Personnel Security Controls and is run on the Supplier's behalf by a specialist 3rd party vetting company and meets the requirements set out in Schedule 2.4 Annex 1 paragraph 7.

Before an employee is hired the following information is validated :-

- Proof of identify
- Proof of their Right to Work (RTW)
- Proof of address.
- Mother's maiden name
- 5 years' worth of addresses and 2 years' worth of work and/or education history.
- Basic Disclosure Check which identifies unspent criminal convictions

In addition to the requirements set out in Schedule 2.4 Annex 1 – Personnel Security, depending on the role applied for financial probity checks are conducted and/or evidence of Professional qualifications must be provided. In addition candidates are checked against the TIED (Telecom Industry Employee database) prior to interview.

Candidates failing employee screening are not employed by the Supplier.

3.2.2 Personnel Security Risk Assessment and Elevated Security Clearance

In accordance with Schedule 2.4 Annex 1 paragraph 8, 9 & 10 the Supplier understands additional screening checks and/or elevated security clearance will be required for roles with access to Authority information. Roles will be identified and assessed as described in the Security Management Method Statement Section 4.1

Further to the details in the Security Management Method Statement, where required the Supplier shall agree Supplier personnel roles that require National Security Clearance, including Supplier employees, contractors or Sub-Suppliers system administrators, and individuals with elevated privileges that can access IT systems which store or process Authority Data (meeting the requirement in Schedule 2.4 Annex 1 paragraph 9).

As detailed in the Security Management Method Statement, the Supplier shall obtain the necessary clearance for each of its staff. Any costs associated with obtaining the necessary staff clearances shall be borne by the Supplier meeting the requirement in Schedule 2.4 Annex 1 paragraph 10).

In accordance with Schedule 2.4 Annex 1 paragraph 11 personnel unable to obtain required security clearance will be prevented from accessing systems which store, process or manage Authority Data since evidence of security clearance must be provided before access is granted for in scope roles.

3.2.3 Terms and Conditions of Employment

In addition to the requirements set out in Schedule 2.4 Annex 1 – Personnel Security, all the Supplier's employees are required to sign confidentiality agreements and agree to meet the requirements of the Supplier's security policies and standards in the terms and conditions of their employment. Failure to comply with security policy and standards will result in disciplinary action and may result in dismissal for gross misconduct.

The Supplier understands any employee identified as working on the ESN must sign the Official Secrets Act (Security Management Method Statement Section 4.1.1).

3.2.4 Mandatory training and regular security awareness

In accordance with Schedule 2.4 Annex 1 paragraph 12, all of the Supplier's employees (including those who have the ability to access Authority Data) must complete mandatory Security and Data Protection training during induction and annually. The training includes, but is not limited to, information

on safe use of email and internet, secure password management and handling personal and sensitive information. All 3rd Party suppliers are mandated through contract to provide Security and Data Protection training to employees. The Supplier understands additional role specific security training will be required for roles with access to Authority information. Roles will be identified and training provided as described in the Security Management Method Statement. – Section 4.2.
Security awareness is achieved via a number of delivery mechanisms, including internal social media pages, visual media and onsite roadshows. The Supplier has recently launched a SAFE (Security Awareness for Everyone) campaign in our contact centres which has been very well received and will be extended to our retail stores shortly.

3.2.5 Role Based Access Control

In accordance with Schedule 2.4 Annex 1 paragraph 13 access controls are in place to prevent unauthorised access to ESN information and the Service infrastructure. These will be updated as required based on the actions outlined in the Security Management Method Statement Section 4.3.
Roles are assigned specific privileges granting only those permissions necessary for them to carry out their duties. The required users are then assigned to a role. When staff no longer need elevated privileges or leave the organisation (see section 3.2.6), the Supplier will revoke their access […..✂…..]
In accordance with Schedule 2.4 Annex 1 paragraph 1 (d) access is restricted to the level of access required to perform the employee's role so that access is on a need to know basis; the principle of least privilege is applied. This means that Authority Data is only accessible to those verified with a need to know. The location of where data is stored will be transparent to the Authority and available on request.
Rules are in place to prevent unauthorised access to Authority information and services as follows: -

- Access requests are managed through a User Access Management System.
- Access is not permitted without line management approval
- Access is not permitted without a valid SAP HR ID
- Access requires an individual User ID and password.
- A review of access will be undertaken on a quarterly basis
- Allocation of passwords is controlled by a managed process.
- Password rules are in place (described in detail within Section 3.6.11).
- Logging and system monitoring are in place (described in detail within Section 3.6.12)

An additional layer of control is in place for employees and 3rd Party suppliers who require external access to the Supplier's network (i.e. they are not physically connected to a LAN network port).
Formal approval will be sought from the Authority prior to sharing any data generated from Authority User activity, Authority User Device data or Authority User identity data with any third party (meeting the requirement in Schedule 2.4 Annex 1 paragraph 1 (e)).
The Supplier understands more stringent access controls may be required for roles with access to Authority information. The controls that will be required will be assessed as described in the Security Management Method Statement Section 4.4

3.2.6 Controls for change or termination of employment

In addition to the requirements set out in Schedule 2.4 Annex 1 – Personnel Security: Changes or termination of employment triggers output to the User Access Management System which results in a change or revocation of access rights.
All equipment and access cards must be returned to the Line Manager on the employee's last day of service.

The Supplier understands more stringent controls for leavers with roles with access to Authority information may be required. Roles will be identified and assessed as described in the Security Management Method Statement – Section 4.3.2.

3.3 Physical Security

The Supplier understands the critical importance of physical security controls (e.g the solution includes some elements of a segregated core with enhanced security management) in preventing unauthorised access to its assets and services and therefore to the Authority assets and Service; this is an integral part of our security controls. Physical security and access controls procedures are operational at all the Supplier's sites and extends to all office premises, switch sites, data centres, call centres and retail stores. Physical security perimeters have been created to protect processing facilities such as switch sites from unauthorised access, damage and interference. Evidence of the ISO 27001 controls adopted by the Supplier in support of Physical Security can be viewed within Annex 5 Statement of Applicability.

The Supplier's physical security controls will be in line with the Baseline Security Requirements (Schedule 2.4 Annex 1 paragraph 1) after any updates identified through the activities outlined in the Security Management Method Statement, section 4.4.

The Supplier's multi layered approach to physical security, documented below, together with the procedural controls set out in section 3.4.5, recognise that in the context of the ESN, maintaining the safety of Emergency Services personnel by protecting the confidentiality and integrity of information; and maintaining continuity of service to ensure the Emergency Services can continue to communicate in the event of an emergency and save human life and property, is of paramount importance. Therefore physical security plays an integral role in maintaining the confidentiality, integrity and availability of data and the ESN service. and the controls implemented reduce the risk of unauthorised access to Authority data or loss of the ESN service.

3.3.1 Supplier's Company-wide Controls

[…..✂…..]

3.3.2 Technical Sites

Technical sites where Authority services are located are designated as Secure sites and are therefore subject to more stringent control. As well as security perimeters and entry controls, access is further restricted by procedural security controls set out in Section 3.4 of this document.

3.3.3 Cell Sites

[…..✂…..]

3.4 Procedural Security Controls

Procedural security controls underpin the Supplier's security framework and therefore the protection of the Authority information and the ESN service. The Supplier has industry leading governance and procedures implemented as follows.

3.4.1 Governance, leadership and responsibilities

The Supplier has a fully implemented and defined Security Governance model responsible for development, implementation, management and continual improvement of information security within the Supplier which will meet the requirements of Schedule 2.4 Paragraph 4.2 (c) after any required changes detailed as part of the Security Management Method Statement section 4.5 are made.

The governance model is graphically represented in Figure 1. The intention of this diagram is to describe the way in which the governance model can be expressed in terms of Plan/Do/Check/Act process model (Figure 1 – Plan/Do/Check/Act Process Model).
The security organisation defined within the governance model develops, implements, manages and continually improves the information security of the Supplier in line with business requirements. This organisation will:

- Define the scope and policy in line with business strategy taking the needs of internal and external interested parties such as legal, regulatory requirements and contractual security obligations into account
- Approve information security policies, assign roles and co-ordinate information security across the organisation
- Undertake reviews of the effectiveness of the ISMS taking into account results of security audits, automated reporting, incidents and feedback from the business
- Record actions and events that could impact on the effectiveness of the ISMS including internal and external issues to the business
- Review the Supplier's risk appetite to determine acceptable levels of risk, taking into account changes to the business, business objectives, the needs of internal and external interested parties, technology and internal or external issues e.g. changes to legal or contractual obligations

A multi-disciplined approach to information security exists which involves input not only from Technology Security & Risk Management but also from representatives across the business as represented by the Information Security Steering Board (ISSB) and Information Security Working Group (ISWG).
Security responsibilities are defined across the Supplier's business but ultimately everyone working for the Supplier is responsible for demonstrating their commitment to the ISMS by ensuring that the Supplier's environment is secure and that relevant policies, standards, processes and procedures are adhered to, to safeguard our customer data and EEs own corporate assets.
The Supplier's existing approach to Security Governance, leadership and responsibilities is described in Annex 3, Information Security Management System Section 4.1 Security Governance and Section 5 Organisational Security – Leadership and responsibility.

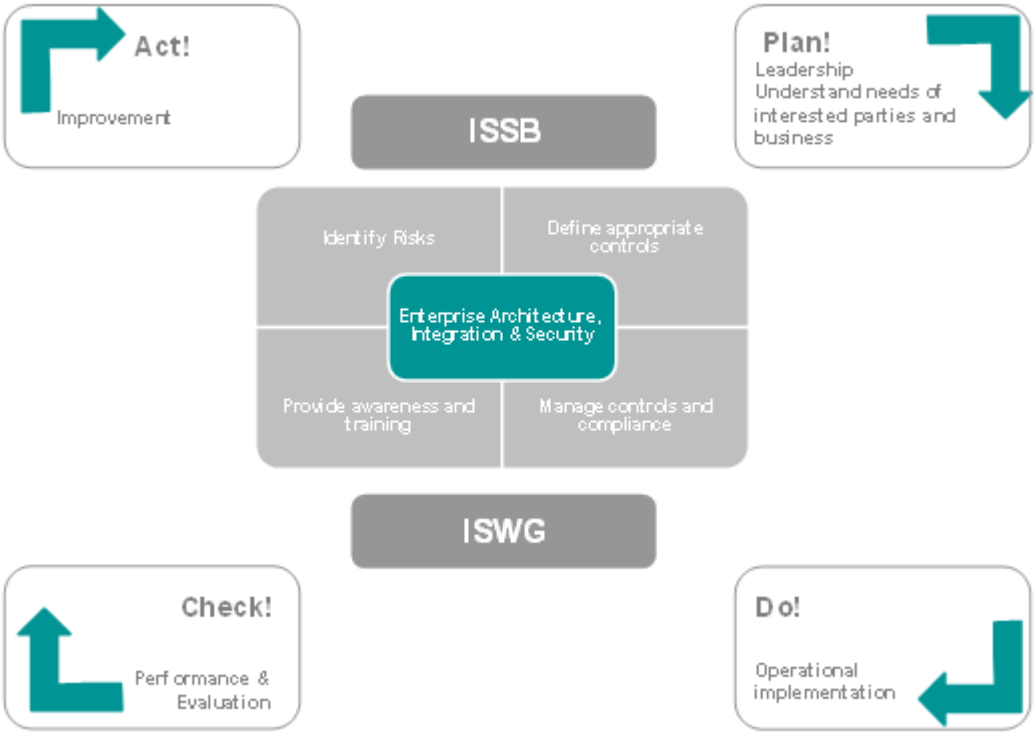

Figure 1 – Plan/Do/Check/Act Process Model

Overall leadership lies with the Supplier's CEO. Management is devolved further through the ISSB whose members are senior business leaders and the ISWG for day to day working. The key Supplier Operational Personnel listed below, who are responsible for compliance with Schedule 2.4, are members of the ISSB and their delegates attend the ISWG:

- Chief Technology Officer – […..✂…..]
- Director of Security and Integration –[…..✂…..]
- Head of Technology Security - […..✂…..]

As detailed above, the Supplier has appointed a member of the Programme Board to be responsible for security. This initial member is the person named as such in Schedule 9.2 (Key Personnel) as the Security Representative and the provisions of Clauses 14.5 and 14.6 (Key Personnel) apply to them (meeting the requirement listed in Schedule 2.4 paragraph 2.2). As the Security Representative Martin Pickford will be responsible for ensuring that this Schedule is complied with by the Supplier
The Supplier recognises additional security governance will be required for the Authority service and other providers of the service. The Supplier will take an active part in the structure and participation of these Governance forums which will be formed. These are described in the Security Management Method Statement Section 3.5.

3.4.2 Valuation and Classification of Assets

In accordance with Schedule 2.4 Annex 1 Section 1 (a) the Supplier has facilities to handle Authority assets classified up to "TOP SECRET" and has applied to upgrade this to a List X facility.

In accordance with Schedule 2.4 Annex 1 paragraph 1 the Supplier will classify Authority assets using industry good practice, ensuring that access to Authority Data and other assets is correctly managed and that the physical, procedural, personnel and technical areas of the assets are safeguarded throughout their lifecycle as documented throughout this Plan and in accordance with the Supplier's ISO 27001 certification. Any updates required to the Supplier's processes will be identified and implemented as part of the Security Management Method Statement, Section 4.6.

Authority assets will be classified into categories using industry best practice via an existing classification scheme designed to protect information and other assets from accidental or deliberate compromise and meets the requirements set out in Schedule 2.4 Annex 1 Section 1 (b). The scheme consists of 4 classification categories: -

- Public
- Internal
- Confidential
- Highly Confidential

However, the Supplier understands that Government classification will need to be followed. For the purposes of ESN, a minimum classification of Confidential will be applied to Authority information.

In accordance with Schedule 2.4 Annex 1 paragraph 1 (a), the evaluation and classification system is designed to support HMG business, and meet the requirements of relevant legislation, international standards, international agreements, and contractual obligations. Clear rules are defined for classification, labelling, handling/processing, retention and disposal, and are designed to ensure compliance with legal and regulatory requirements including, but not limited to, the Data Protection Act 1998.

In accordance with the requirements of Schedule 2.4 Annex 1 paragraph 1 (c) operational data and information assets will remain the property of the rightful User Organisation irrespective of any proprietary or open standard technique used to format or package the data.

Government Protective Marking Scheme arrangements will be confirmed as part of the Security Management Method Statement Section 6.1

The Supplier recognises additional handling requirements (such as the secure storage and transmission of ESN classified information) will be required for information relating to the Authority service and will be assessed, to ensure it follows the rules set out in the Government classification scheme as described in the Security Management Method Statement Section 6.1 – 6.3

3.4.3 Data Processing, Storage, Management, Disposal and Destruction

The Supplier recognises the need for Authority Personal Data to be safeguarded. The Supplier implements safeguards for all customer information and this will be extended to the Authority to ensure and meet the requirement to safeguard Authority information. Data will be processed in line with the requirements of Data Protection Act 1998 and ESN requirements and retained only for the timescales to be agreed between the Supplier and the Authority.

The Supplier uses as a minimum Good Industry Practice, which formally represents tested and proven technical and procedural techniques that minimise the risk to the confidentiality, integrity and availability of data and services, in the day to day operation of any system storing, 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, meeting the requirement in Schedule 2.4 paragraph 2.4. Any updates that are required will be identified and implemented through the Security Management Method Statement Section 4.7.

The technical and procedural controls implemented by the Supplier to maintain the confidentiality of the ESN data throughout its complete lifecycle, creation to destruction effectively support recognise the importance of maintaining the safety of Emergency Services personnel by protecting the confidentiality and integrity of information.

If required, the Supplier will state to the Authority the physical locations in which the Authority Data/Information may be stored, processed and managed from and what legal and regulatory frameworks it will be subject to (meeting the requirement in Schedule 2.4 Annex 1 paragraph 2). As below, Authority Data will be physically located in UK Data Centres.

In line with the requirement listed in Schedule 2.4 Annex 1 paragraph 4 (b) and the requirements in Schedule 7.4, the Supplier agrees that where it stores Authority Data it shall have documented the processes necessary to guarantee the availability of Authority Data in the event of the Supplier ceasing to trade.

The Supplier will not share Authority Data with any 3rd party or move the location of data processing without prior approval from the Authority. Authority data will be physically located in UK Data Centres and managed within the physical boundaries of the UK by a UK based network control function. (meeting the requirement in Schedule 2.4 Annex 1 paragraph 5)

Should there be a change in location and the proposed location for the Supplier's data storage, processing and administration is outside the UK, the Supplier will gain the Authority's approval for this change in advance. The Authority shall not unreasonably withhold or delay approval provided that any proposed change is in accordance with the Security Policy framework and CESG IA Policy Portfolio (meeting the requirement in Schedule 2.4 Annex 1 paragraph 3).

In response to question ESNNEG022 raised separately by the Authority, the Supplier's confirmation of the MNO infrastructure where information is generated and/or stored; 3rd parties with whom data is shared, including the type of data and purpose of sharing; and, all users (by appointment/role/title) that are able to view this information is included in Annex 2 of this document.

Where the Supplier stores Authority Data, it will securely destroy all media that has held Authority data at the end of life of the media in line with Good Industry Practice, the Security Policy Framework and CESG IA Policy Portfolio (meeting the requirement in Schedule 2.4 Annex 1 paragraph 4 (c)). The Supplier will also securely erase any or all Authority Data held by the Supplier when requested to by the Authority in line with the Security Policy Framework and CESG IA Portfolio (meeting the requirement in Schedule 2.4 Annex 1 paragraph 4 (d)), and the Supplier will ensure that any Personal Data that is no longer required is securely erased in accordance with HMG Standard No. 5 (meeting the requirement in Schedule 2.4 Annex 1 paragraph 4 (e)).

To provide further detail on the processes used, (to the extent commercially and technically feasible), Authority information will be deleted or disposed of in such a way that recovery of any information is impossible from: -

- media or equipment that will be re-used
- media or equipment which leaves the control of the Supplier, including, but not limited to, faulty disks, tapes, and other media types, including defective parts

Equipment containing Authority information that will be re-used will be securely overwritten (to the extent commercially and technically feasible) in such a way that the recovery of any information is impossible. This will comprise of 3 separate overwrites in line with CESG requirements utilising a CESG approved product.

Equipment that will not be re-used will be physically destroyed (to the extent commercially and technically feasible) in such a way that recovery of any information is impossible to current Supplier standards: -

- disk drives - Destruction will be to a standard equivalent to the European Association of Data Media Security's 2008 Standard for Physical hard disk drive destruction Security Level B (EA DMS 2008). (Disk is destroyed in particles of 30 mm).
- backup tapes - Backup tapes at 'end of life' will be physically destroyed by degaussing or shredding using a cross cut shredder.

The Supplier will conduct a review to confirm processes comply with requirements taking into account HMG standards for data disposal as described in the Security Management Method Statement Section 7.1 – 7.3.

In line with the requirements of Schedule 2.4 Annex 1 paragraph 4 (a), where the Supplier stores Authority Data, the Supplier will share a sample of sufficient quantity to enable the Authority to assess the risk likely to occur from compromise, loss or theft. The Supplier will provide the data to the Authority within 20 working days of a request, in an agreed format as prescribed by the Authority and at no additional cost to the Authority.

3.4.4 Risk Management

The Supplier acknowledges that any information security risks are shared between the Parties and that a compromise of either the Supplier or the Authority's security provisions represents an unacceptable risk to the Authority requiring immediate communication and co-operation between the Parties, as required in Schedule 2.4 paragraph 2.6.

The Supplier's approach to risk management recognises that in the context of the ESN, the effective management of risk plays an important role in reducing levels of risk to a level acceptable to the Authority. This will maintain the confidentiality and integrity of information; and ensure continuity of service to allow continuity of critical communication and the safety of Emergency Services personnel.

The Supplier's approach to risk management includes the use of preventative actions to reduce the occurrence of risks. This approach includes, but is not limited to, the use of perimeter security controls, the use of secure design patterns when deploying or updating the ESN service infrastructure, embedding security considerations within the development lifecycle, application security testing and the risk assessment of 3rd party suppliers.

An overview of the Supplier's existing approach to Risk Management is described in Annex 3, Information Security Management System Section 7 Asset Identification and Risk Management and evidence of the ISO 27001 controls adopted by the Supplier in support of Asset Identification and Risk Management can be viewed within Annex 5 Statement of Applicability.

In accordance with Schedule 2.4 paragraph 4.2 (d) the Supplier sites and the availability of Authority Service will be assessed and managed using the established Technology Security Risk Management Framework which is aligned to CRAMM (CCTA Risk Analysis and Management Method). The Supplier's approach to risk assessment is a continual process. It is a process by which risks are reduced and by which residual risks are effectively managed by undertaking a methodical approach to enable the effective management of risks. Risk assessment takes into account internal and external issues that could prevent the Supplier from achieving business objectives and meeting business, legal, regulatory and contractual requirements. Identification of assets enables the Supplier to identify, prioritise and manage key risks associated with Authority information and the ESN Service.

As part of the standard project process, a risk assessment is undertaken for each project which takes into account the nature of the project deliverable, the information that will be processed, the involvement of 3rd party suppliers and the impact a potential data breach would have on the Supplier. This enables appropriate security and testing requirements, including but not limited to security testing, to be specified and ensures any residual risk is managed.

All 3rd party suppliers, utilised by the Supplier, who access the Supplier's systems, premises or data (including but not limited to personal information or payment card information); or develop software or applications for the Supplier or its customers are risk assessed prior to on boarding and throughout their tenure as a supplier to ensure they continue to meet their contractual security requirements and to ensure any residual risk is managed effectively.

Non-conformances and observations raised as a result of external ISO27001:2013 certification audits, other external audits and internal audits audit also trigger a formal risk assessment to ensure corrective actions and/or any residual risk is managed effectively.

The Supplier recognises alignment will be required for the management of risk relating to the ESN service and this will be reviewed as described in the Security Management Method Statement Sections 4.5 and 4.8

3.4.5 Access to Secure Areas

In addition to the physical security controls set out in section 3.3 Physical Security and in accordance with Schedule 2.4 Annex 1 paragraph 13 a register of individuals with approved permanent access to one or more secure areas is maintained and reviewed on a quarterly basis to ensure physical access is restricted to authorised personnel who are in possession of appropriate identification and authentication at point of entry.

In accordance with Schedule 2.4 Annex 1 paragraph 13 access to secure areas for individuals not listed on the Approved Access List is strictly controlled and only permitted with an approved 'Access to Work' request that fully meets the criteria stipulated. Individuals are only permitted access to secure areas within the timeframe documented on the 'Access to Work' request and after confirming their identity matches that listed on the form. Technical changes also require an approved change request which must include start and finish times of the change. 'Access to work' requests linked to technical work that do not have an associated change request are rejected.

3.4.6 Security in Supplier Relationships

In accordance with Schedule 2.4 paragraph 4.2 (d) the Supplier conducts security assurance reviews (Suppliers are required to answer a third party security questionnaire, if necessary site visits are also conducted) prior to on boarding and at least annually for all 3rd party suppliers supporting the ESN service and/or with access to Authority information. Potential suppliers who fail to meet the Supplier's security standards will not be accepted. In accordance with Schedule 2.4 paragraph 4.2 (d) contracts with Suppliers supporting the Authority Service and/or with access to Authority information include a security schedule containing requirements appropriate for the service provided (to ensure 3rd Party suppliers are contractually obligated to implement and maintain security controls no less restrictive than that of the Supplier) and a Data Processing Schedule where applicable (to ensure 3rd Party Suppliers are contractually obligated to process data in line with the requirements of the Data Protection Act 1998).

The Supplier's approach to 3rd Party security recognises that in the context of the ESN, 3rd Party security plays an important role, due to the potential implications for national security and for the continuity of the safe operation of the ESN therefore the controls implemented reduce the risk of unauthorised access to or loss of the ESN service.

An overview of the Supplier's existing approach to Security in Supplier Relationships is described in Annex 3, Information Security Management System Section 7 Asset Identification and Risk Management and evidence of the ISO 27001 controls adopted by the Supplier in support of Security in Supplier Relationships can be viewed within Annex 5 Statement of Applicability.
The Supplier understands additional contractual controls will be required for 3rd Party Suppliers with access to Authority information and/or who support the ESN Service. Contracts will be updated dependant on the outcome of the gap analysis described throughout the Security Management Method Statement. Amendments will be put in place in order to have a completed ISMS within the timescales set out by the Authority.
The Supplier understands the need for additional audits of 3rd Party Suppliers with access to Authority information or who support the Authority Service. Audit requirements will be updated dependant on the on the outcome of the gap analysis described in the Security Management Method Statement Sections 4.8. Any additional audits and remediation actions arising from them will be completed by 21 months after the Effective Date in time for the required delivery date of the ISMS.

3.5 Business Continuity and Disaster Recovery

In accordance with the requirements of Schedule 2.4 Annex 1 Section 14, the Supplier will produce a detailed business continuity management system. In accordance with the requirements of BS ISO 22301, the system has been designed to incorporate a high degree of resilience based on co-location and back-ups across multiple geographically diverse locations; with failover and DR plans tested regularly the Supplier can ensure pre-defined recovery point objectives can be met. A detailed preliminary Business Continuity and Disaster Recovery plan is included in schedule 8.6. (meeting the requirement in Schedule 2.4 Annex 1 paragraph 14)

3.6 Technical Security Controls

The Supplier understands the importance of technical security controls in the protection of our customers and therefore the Authority information and services. The Authority should also refer to Schedule 4.1 for additional Technical information. The Supplier deploys a defence in depth and segregated architectural design. The Supplier utilises best of breed security tools and best practices. […..✂…..] The controls contribute to ensuring the Emergency Services can continue to communicate in the event of an emergency and save human life and property and the ensure the safety of Emergency Services personnel by reducing the risk of unauthorised access to Authority data or loss of the ESN service.
An overview of the Supplier's existing approach to Technical Security controls is described in Annex 3, Information Security Management System Section 10 Communications and operations management and Section 12 Security architecture and evidence of the ISO 27001 technical controls adopted by the Supplier can be viewed within Annex 5 Statement of Applicability.

3.6.1 Networking

In accordance with Schedule 2.4 Annex 1 paragraphs 5 and 6, the network control function for the Authority service will be within the physical boundaries of the UK and the network and service function provided will be accessible and controllable from within the physical boundaries of the UK in accordance with the Security Policy Framework and CESG IA Policy Portfolio) (meeting the requirement in Schedule 2.4 Annex 1 paragraph 6)

3.6.2 System development and maintenance

Security requirements are built into the Authority Service and are applicable to the infrastructure and applications used to support the Authority Service and are defined as follows: -.

- operating system configuration are hardened and documented;
- services, applications not used will be disabled where practical;
- the most recent security patches and hot fixes will be installed on the system as soon as practical following testing and within documented timescales
- trust relationships between servers will be avoided
- use of “least privilege” to perform a function is implemented
- default passwords are changed prior to services going live
- measures are in place to handle Denial of Service attacks
- all default passwords will be changed before the infrastructure element goes live.

Testing is conducted throughout the development lifecycle including preliminary acceptance testing (PAT), acceptance testing (OAT) and Integration testing (IT) to ensure that the Authority Service is tested to detect and eliminate security vulnerabilities.

3.6.3 Operational management

Controls are in place to ensure the secure operations of the Authority Service.

- Development and test environments are separated from operational environments.
- Changes to the Authority Service are subject to a strict technical change control process which includes impact assessment, a formal approval process and a procedure for communication . Anti-malware solutions and content-filtering software are in place to protect the Authority Service against malicious software.
- Regular Vulnerability scans are run against the whole of the Core Network which would include those dedicated ESN elements. The Supplier will work with the US to review vulnerability testing approach for the shared interfaces.
- Information back-up for the Authority Service is done daily and restore operations are tested to ensure the integrity of the backed-up data (see BCDR Plan Schedule 8.6 for more detail).

3.6.4 Encryption and authentication

Handset traffic is protected wherever it exists outside of a secure data […..✂…..]

3.6.5 Security architecture

The Security architecture is designed to protect the Authority information and Service and includes: -

- Perimeter routers
- Multiple best of breed firewall types
- Content and URL filtering software, multiple network zones including perimeter zones (see figure 3), management zones, customer zones and demilitarized DMZ zones (DMZ which is sometimes referred to as a perimeter network is a physical or logical sub network that contains and exposes an

organization's external-facing services to an untrusted network which adds an additional layer of security.

- Use of encryption and certificate based authentication (IPSEC and PKI on backhaul links) (see figure 2)
- Anti DDoS protection
- Security monitoring (SIEM)
- Anti-Malware protection
- Intrusion Detection/Protection systems
- Vulnerability Scanning

3.6.6 Supplier's Mobile Data Services Security Architecture

The Supplier's mobile data network is designed and implemented according to a zoning and segregation architecture known as the Standard Server Architecture (SSA). The architecture provides the following features:-

- Segregation between services and vendors.
- Segregation between publicly available servers and servers storing confidential data.
- Enforcement of security policies embedded into the design.
- A "defence in depth" strategy requiring that no single software bug or misconfiguration should result in data breach of confidential information.

[…..✂…..]

[…..✂…..]
[…..✂…..]

3.6.7 Protection against Distributed Denial of Service (DDoS) attacks

[…..✂…..]

3.6.8 Identity and Access Management

the Supplier is rolling out a centralised Identity and Access Management (IAM) platform to provide the following benefits:-

- Centralised password management so that password policies such as complexity and expiration will be enforced across the whole of the Supplier's network.
- Centralised authentication so that users will only have one password for the systems that they maintain.
- Centralised authorisation so that users will only have access to systems to which it is necessary for their role. The IAM platform will automate migration of users from one role to another and will also link to the Supplier's leavers' process so when employees leave the business their accounts are automatically disabled.

- Auditing and reporting features which allow service owners to review who has access to their systems and who approved access for individual users.

3.6.9 Security Incident Event Monitoring

The Supplier utilises an industry leading Security Incident Event Monitoring (SIEM) platform […..✂…..]
It has the ability to analyse information in near real-time to detect security events and produce alerts, and to correlate security incidents across multiple discreet events. It also provides the ability for the Supplier to store historical logs and review raw log information as situations require it.
[…..✂…..]
The coverage of the systems are reviewed and maintained by a dedicated security engineering and research team.
These security monitoring systems are monitored by a dedicated security operations team for security events. The team also interlink with our Technology Operations Centre (TOC) to ensure that any security monitoring that will effect availability of any monitored systems will be flagged to the TOC for escalation via the TOC incident management system. For further details please refer to the Supplier's Service Management response (Schedules 8.1-8.11)
[…..✂…..]

3.6.10 Vulnerability Scanning

[…..✂…..]
The vulnerability scanning infrastructure is designed to find poorly patched, hardened or configured systems within the network so that such systems can be identified and remediated. Scan reports are regularly generated and fed into the Supplier's Vulnerability Management process.
The scanning consists of a mixture of specially built scanning firewalls and scanning through existing OAM firewalls.
The Supplier is working towards increasing the number of systems which are scanned using authenticated scans in order to reduce the number of false positives. Authenticated scans are performed only using public/private key SSH connections.

3.6.11 Password Control

Password rules are in place to ensure the use of strong passwords to protect the Authority information and ESN Service: -

- […..✂…..]
- […..✂…..]
- […..✂…..]
- […..✂…..]

3.6.12 Monitoring

Security monitoring is covered in detail in Section 3.6.10. The Supplier also operates a Technology Operations Centre that monitors system availability. […..✂…..]
the Supplier's multi layered approach to technical security controls, documented above, recognise that in the context of the ESN, technical security plays an important role, due to the potential implications for national security and for the continuity of the safe operation of the ESN therefore the controls implemented reduce the risk of unauthorised access to Authority data or loss of the ESN service.

4. Amendment and Revision of the ISMS and Security Management Plan

The ISMS and Security Management Plan detailed in sections 2 and 3 of this document will be fully reviewed and updated by the Supplier on a regular basis depending on the changes set out below and as a minimum at least annually to reflect the following which meet the requirements of Schedule 2.4 paragraph 5.1:

- emerging changes to Good Industry Practice in Security Management;
- any change or proposed change to the IT Environment of the ESN or the Supplier (;
- any change to the Services or associated processes;
- any new perceived or changed security threats;
- any change or proposed change to the Security Policy Framework;
- any change or proposed change to the CESG IA Policy Portfolio;
- any reasonable change in requirement requested by the Authority.

The results of the Supplier's reviews of its Security Management plan shall be provided to the Authority as soon as reasonably practicable after their completion, and shall include:

- suggested improvements to the effectiveness of the ISMS
- updates to risk assessments
- proposed modifications to the procedures and controls that effect information security to respond to events that may impact on the ISMS
- suggested improvements in measuring the effectiveness of controls

This review process is in line with the Supplier's current approach of continuous improvement as outlined in Section 1 of this document, and the Supplier's position as a leader in security management developments in the telecommunications industry in the United Kingdom (as evidenced by its adoption of ISO 27001 on its formation, its leading the move to use IPSec on backhaul)
Any changes the Supplier proposes to make to the ISMS or Security Management Plan as a result of these reviews, an Authority request, a change to the Services (detailed in Schedule 2.1) or otherwise, shall be subject to the Change Control Procedure and shall not be implemented until approved in writing by the Authority. Should the Authority require changes to the ISMS or Security Management Plan to be implemented on timescales faster than set out in the Change Control Procedure the Supplier will agree and adopt them as required. The Supplier acknowledges that any changes which bypass the Change Control Procedure due to their urgency will thereafter be subject to the Change Control Procedure so that they are formalised and documented for the purposes of this Agreement (meeting the requirements in Schedule 2.4 paragraph 5.2, 5.3 and 5.4).

5. Security Audit, Testing and Vulnerability Management

5.1 Audit and Testing

All controls described in Sections 2 and 3 are audited regularly as part of the Suppliers ISO 27001 internal audit programme and by the Suppliers ISO 27001 external certification body. In order for the Supplier to maintain its ISO 27001 certification, testing takes place across the scope of the Supplier's ISMS on an annual basis. Any updates to the Audit and Testing requirements for the ISMS will be identified and implemented as part of the Security Management Method Statement, Section 4.10.

the Supplier's multi layered approach to security audit and testing, documented below, recognises that in the context of the ESN, security audit and testing play an important role in monitoring the efficacy of implemented security controls and reducing the risk of vulnerabilities in the ESN service which is essential, due to the potential implications for national security and for the continuity of the safe operation of the ESN.

- A minimum of 4 technical sites are audited annually by the Suppliers external ISO 27001 certification body
- In accordance with Schedule 2.4 paragraph 6.1, any change to the ISMS (including security incident management processes and incident response plans) or Security Plan is tested before introduction utilising use case scenarios to ensure the continued efficacy of the controls in place.
- In accordance with Schedule 2.4 paragraph 6.1, any significant architectural change to the IT Environment is tested
- In accordance with Schedule 2.4 paragraph 6.1, vulnerability assessments are carried out regularly by internal employees and external auditors to identify threats and vulnerabilities and the impact of these vulnerabilities being exploited. Remedial procedures are in place to mitigate these threats. The remedial processes include monitoring and managing of assets. The process is described in more detail in Section 5.2
- In accordance with Schedule 2.4 paragraph 6.1, penetration testing is conducted prior to network changes going live and at least on an annual basis
- Security Tests comply with the recommendations set out in the Security Policy Framework and CESG IA Policy Portfolio (meeting the requirement in Schedule 2.4 paragraph 6.3)

The availability and quality of the Supplier's mobile network is critical to the continued success of the Supplier's business; therefore tthe Supplier currently designs the implementation of its Security Tests to minimise the impact on the delivery of its operations, and will continue to do so for the Authority so as to minimise the impact on the delivery of the Services. The date, timing, content and conduct of the Supplier's Security Tests on systems, processes and procedures related to the delivery of the Services will be agreed in advance with the Authority through the governance structures agreed in the Security Management Method Statement and taking these points into account, if any Security Tests adversely affect the Supplier's ability to deliver the services so as to meet the Target Performance Levels, the Supplier shall be granted relief against any resultant under-performance, for example loss of service or degradation in the quality of service for the period of the Security Tests (meeting the requirements listed in Schedule 2.4 paragraph 6.1).

The Supplier understands additional audit and testing requirements are necessary for the Authority Service. Audit and testing requirements will be updated dependant on the outcome of the gap analysis described in Management Method Sections 10.1 – 10.3. Amendments will be put in place according to the timescales set out by, and in a format agreed with the Authority

In accordance with Schedule 2.4 paragraphs 6.6 and 6.7, the Authority will be entitled to send representation to witness the conduct of Security Tests and the Supplier will submit to the Authority the outcome of all security tests using the Security Test Results Template explained below, within no more than 15 Working Days (or such other period as the Parties may agree in writing) from the data of the completion of the relevant Security Test.

The Supplier agrees that the Authority is able to request Security Tests without prior notice (meeting the requirements of Schedule 2.4 paragraph 6.2)

5.2 Vulnerability management

In accordance with Schedule 2.4 paragraphs 6.1 and 6.9 the Supplier has a sophisticated set of controls to manage vulnerabilities identified as affecting the Authority service. These are undertaken as part of the Supplier's normal business and will also form part of Security Tests. Any updates to these controls required to meet the Authority's requirements will be identified and implemented as part of the Security Management Method Statement, Section 4.9. The Supplier has documented these in line with the requirements of Schedule 2.4 paragraph 3.3 (e) as follows: -

- Vulnerability standards such as the Common Vulnerability Scoring System v2 (CVSSv2), and databases such as Common Vulnerabilities and Exposures (CVE), and the National Vulnerability Database (NVD) are referenced to determine the impact level on the Services and remediation priority of any new threat, vulnerability or exploitation technique of which the Supplier becomes aware (meeting the requirement in Schedule 2.4 paragraph 3.3 (e))
- To ensure it is up to date, the Supplier also subscribes to services to discover new vulnerabilities when published by vendors and/or industry wide alerting systems.
- Security Operations manage the scheduling of production environment vulnerability scanning
- All systems that accept network connections are vulnerability scanned regularly
- Externally accessible Supplier assets are mapped weekly to capture any new externally facing systems
- Scanning tools use a known and current standard to classify vulnerabilities and takes into account vulnerability factors as priority, exploitability and impact.

Vulnerability scanning is designed to be non-intrusive as to not impact service availability.
Where any Security Test or vulnerability scan carried out reveals any actual or potential Breach of Security or weakness (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 which the Supplier proposes to make in order to correct such failure or weakness. Subject to the Authority's prior written approval, the Supplier will implement these changes to the ISMS and the Security Management Plan and repeat the relevant Security Tests in accordance with the timetable agreed with the Authority. The Supplier acknowledges that where the change to the ISMS or Security Management Plan is to address a non-compliance with the Baseline Security Requirements, security requirements set out in Schedule 2.1, or the requirements of Schedule 2.4, these changes shall be at no cost to the Authority (meeting the requirement in Schedule 2.4 paragraph 6.9). The Supplier acknowledges that any repeat Security Test which reveals an actual or potential Breach of Security exploiting the same root cause failure, such circumstance shall constitute a material Default for the purposes of Clause 27.1 (c) (Rectification Plan Process) (meeting the requirement in Schedule 2.4 paragraph 6.10).
The Supplier undertakes this process of scanning and improvement as part of its day to day business and proposes the following remediation timescales by severity for vulnerability incidents:

- Critical - Within 24 hours;
- High -Within 1 month;

- Moderate - Next available window of opportunity or scheduled patch cycle - must be done within 4 months;
- Low Next available window of opportunity or scheduled patch cycle – must be done within 1 year.
- In accordance with the requirements of Schedule 2.4 paragraph 6.1, any remediation action employed to fix a discovered vulnerability must follow established change control procedures for all system and software configuration changes.

The Supplier understands the importance of managing vulnerabilities within the Service infrastructure, therefore vulnerability management requirements will be updated if necessary dependant on the outcome of the review described in the Security Management Method Statement Section 4.9
In accordance with Schedule 2.4 paragraph 6.1, the Supplier conducts specific Security (penetration) tests. Where appropriate new systems are tested using specialist third party penetration testing companies prior to going live. Applicable systems will also be security tested annually. Any remediation will follow our standard process as per vulnerability management.

5.3 Security Test Results Template

The Supplier will work with the Authority as detailed in the Security Management Method Statement to agree the format of the output for Security Tests (meeting the requirement in Schedule 2.4 paragraph 6.1). Within 30 Working days after the Effective Date the Supplier will finalise this Security Test Results Template and submit to the Authority, as detailed in the Security Management Method Statement (meeting the requirement in Schedule 2.4 paragraph 6.4)
The process for approving the Security Test Results Template will be as follows:

- If the Security Test Results Template is approved by the Authority, it shall be adopted immediately and maintained as detailed in this draft Plan
- If the Security Test Results Template is not approved, the Supplier shall amend it within 10 Working Days of a notice of non-approval and resubmit to the Authority for approval
- If the Authority does not approve the Security Test Results Template following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure

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 15 Working Days (or such other period as the Parties may agree in writing) from the date of its first submission to the Authority. The Authority must provide timely approval if appropriate, however the Supplier acknowledges that lack of approval on the basis of not meeting the requirements set out in Schedule 2.4 paragraph 6.1 is acceptable (meeting the requirement listed in Schedule 2.4 paragraph 6.5).

6. Breach of Security Activities

6.1 Security Incident Management

The Supplier has a documented and fully tested security incident management process and incident response plans that will be used for reporting and managing incidents relating to the Authority service. the Supplier recognises alignment will be required for the management of incidents relating to the ESN service, to ensure compliance with Schedule 2.4 paragraph 8.1 so that if a Breach of Security or attempted Breach of Security is discovered by either Party, that Party shall notify the other Party using

the security incident management processes and procedures expressed and agreed in the ISMS. This will be reviewed as described in the Security Management Method Statement section 4.5.
The objective of the Security Incident Management Process is to restore normal state service operations as quickly as possible to minimise the adverse impact on the ESN service so that ESN service quality is maintained and incidents are resolved within established ESN service targets.
The Supplier's process includes categorisation, prioritisation, handling, escalation and notification procedures. For clarity, if a Breach of Security is discovered by either Party, the Supplier's existing processes will allow the Supplier to:

- Minimise the harm (actual or potential) caused to the ESN service by a Breach of Security
- Remedy the Breach of Security to the extent possible and protect the integrity of the IT Environment to the extent within the Supplier's control against any such Breach of Security or attempted Breach of Security
- Apply a tested mitigation against any such Breach of Security or attempted Breach of Security. Provided 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 Target Performance Levels, the Supplier shall be granted relief against any resultant under-performance for such period as the Authority, acting reasonable, may specify by written notice to the Supplier
- Prevent a further Breach of Security or any potential or attempted Breach of Security in the future exploiting the same root cause failure (meeting the requirement in Schedule 2.4 paragraph 8.2 (a))

Using the reporting mechanism defined by the ISMS, the Supplier will provide the Authority with full details of the Breach of Security or attempted Breach of Security (including a root cause analysis where required) (meeting the requirement in Schedule 2.4 paragraph 8.2 (b))
the Supplier acknowledges that in the event 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 in Schedule 2.1 or Schedule 2.4, any change to the ISMS shall be at no cost to the Authority (meeting the requirement in Schedule 2.4 paragraph 8.3)
The security incident management process and plans track the extent to which planned activities are realised and planned results are achieved, providing assurance on the fact that they are fit for purpose and that they allow recovery of services with minimum resources, effort and costs, meeting the requirement in Schedule 2.4 paragraph 3.3 (d).
The following flow chart represents the process followed by the Supplier when dealing with a Security Incident. The process allows for a re-evaluation of the incident once the Incident Response Team have been involved

[…..✂…..]

7. Conclusion

Security is a core discipline that is well embedded and proven within the Supplier. The framework which underpins Security for the Supplier is signed by the Chief Executive Officer, governed by Senior Leaders of the Supplier and managed by cross business teams. Dedicated security departments ensure industry best practice techniques are deployed across all areas of the business, not just within Technology.

Industry standards such as the Supplier's ISO27001: 2013 certification provide external verification, demonstrating the Suppliers competence in this field.

the Supplier is confident that they will provide security of all the relevant areas for the ESN, will ensure that the Confidentiality, Integrity and Availability of the ESN will always be maintained and constantly monitored and adapted to meet current and future threats.

The Supplier welcomes the opportunity to work with the other ESN providers to ensure that the security of the ESN is completely end to end.

A1. Annex 1

Technology Security Document Framework
Information Security Management System (ISMS) – redacted version supplied – Annex 3
ISO 27001 Statement of Applicability – redacted version supplied – Annex 5
ISO27001 Corrective Action Management Process
Legal & Regulatory Requirements ISO27001
Third Party Supplier Assurance Process
Technology Risk Management Framework
Technology Security Document Governance Process
Acceptable Use Policy
Access Control Policy
Antivirus Policy
Audit Logging Policy
Business Continuity Management Policy
Cryptographic Controls Policy
Data Protection Policy
Data Retention & Disposal Policy
Firewall Security Policy
Information Security Policy – redacted version supplied – Annex 4
Patch Management Policy
Secure Development Policy
Vulnerability Management Policy
Vulnerability Scanning Policy
Wireless Security Policy
Access Control Standard
Business Continuity Management Standard
Cryptographic Controls Standard
Information Classification & Data Handling Standard
Security Operations Standard
Secure Development Standard
Mobile Device Usage Standard
RAN Security Standard
Infrastructure & Comms Standard
Crisis Management Plan
Security Incident Handling Process
Security Incident Handling Procedure
Technology Security Solutions Process
Application Security Requirements
Data Release Approval Form
Customer Data Retention Schedule
Finance Data Retention Schedule
HR Data Retention Schedule
Legal & Regulatory Data Retention Schedule
ISSB TOR
ISWG TOR
BCMWG TOR

A2. Annex 2

Location	Users within the Qualified bidders organisation that are able to access the information
[…..✂…..]	[…..✂…..]
[…..✂…..]	[…..✂…..]
[…..✂…..]	[…..✂…..]
[…..✂…..]	[…..✂…..]
[…..✂…..]	[…..✂…..]
[…..✂…..]	[…..✂…..]
[…..✂…..]	[…..✂…..]
[…..✂…..]	[…..✂…..]
[…..✂…..]	[…..✂…..]
[…..✂…..]	[…..✂…..]
[…..✂…..]	[…..✂…..]
[…..✂…..]	[…..✂…..]

A3. Annex 3

[…..✂…..]

……

[…..✂…..]