CONNECTIVITY CONSOLIDATED CONTRACT SCHEDULE

CONSOLIDATED SCHEDULE 7

SECURITY REQUIREMENTS

for Contract Number DCNS/080

Table of Contents

Contents **Page**

CONSOLIDATED SCHEDULE 7
SECURITY REQUIREMENTS

This Consolidated Schedule provides a consolidated version of the requirements of Schedule 2.2 (*Security Requirements and Plan*) to the Call-Off Terms, Appendix 6 to the Call-Off Form and the Customer Authority's special terms relating to the Security Requirements.

Capitalised terms used but not defined in this Consolidated Schedule are defined in Consolidated Schedule 1 (*Definitions*).

1 INTRODUCTION

1.1 This Consolidated Schedule sets out:

1.1.1 the overview of Security Requirements that support the delivery of the Services, including the secure sustainment of the legacy aspects of the Services (as more particularly described at Paragraph 2 below);

1.1.2 the Information Assurance requirements at the enterprise level (as more particularly described at Paragraph 3 below), including the requirements for an ISMS, IMP, PCP and RMADS;

1.1.3 the content required to be included in the IMP and related requirements (as more particularly described at Paragraph 4 below);

1.1.4 the process for amending and revising the IMP and RMADS (as more particularly described at Paragraph 5 below);

1.1.5 the audit and testing of the IMP and compliance with the Security Requirements described in this Consolidated Schedule (as more particularly described at Paragraphs 6 and 7 below);

1.1.6 the Contractor's obligations in the event of actual, potential or attempted Breach of Security (as more particularly described at Paragraph 8 below); and

1.1.7 the Contractor's obligations in relation to Malware (as more particularly described at Paragraph 9 below).

2 OVERVIEW OF SECURITY REQUIREMENTS

2.1 Within five (5) Working Days from receipt of written notice from the Customer Authority, the Contractor shall initiate discussions with the Customer Authority in relation to:

2.1.1 the scope of the Certification for each Service; and

2.1.2 a list of residual risks that have been identified by the Contractor and agreed with the Customer Authority in writing from time to time as potentially affecting that Service,

(the "**Agreed Risk Envelope**").

2.2 In addition to the obligations set out in Paragraph 2.1 above, the Contractor shall meet with the Customer Authority (including at designated security working group ("**Security Working Group**" or "**SWG**") meetings) as reasonably requested by the Customer Authority from time to time and provide all information and submit all documentation requested by the Customer Authority in order for the Customer Authority to Approve (at its sole discretion) a Certification scope and Agreed Risk Envelope for each of the Services.

2.3 The Contractor shall provide and be responsible for the effective performance of a PSN Encryption Overlay Service and shall at all times provide a level of security which:

2.3.1 meets any specific Threats to Security and Breach of Security;

2.3.2 permits effective risk management and ensures that the level of risk to the Customer Authority does not exceed the Agreed Risk Envelope for each of the Services; and

2.3.3 meets the specific security controls set out in a Service Code of Connection.

2.4 Without limiting Paragraph 2.3 above, the Contractor shall at all times ensure that the level of security that it employs in the provision of each of the Services is appropriate to maintain the Agreed Risk Envelope for that Service, including in relation to the following risks:

2.4.1 loss of integrity and confidentiality of Customer Authority Data, including Classified Information;

2.4.2 unauthorised access to, use or disclosure of, or interference with Customer Authority Data, including Classified Information, by any person or organisation;

2.4.3 unauthorised access to network elements, buildings, the Customer Authority Premises, the Sites and tools (including equipment) used by the Contractor and any Sub-contractors in the provision of the Services;

2.4.4 use of the Contractor System or Services by any third party in order to gain unauthorised access to any computer resource or Customer Authority Data; and

2.4.5 loss of availability of Customer Authority Data, including Classified Information, due to any failure or compromise of the Services.

2.5 The Contractor shall ensure that all Contractor Personnel:

2.5.1 receive training in the Threat to Security, as well as specific security training relevant to their role and operations requirements for the Customer Authority Premises on which such Contractor Personnel will be located; and

2.5.2 have security clearance appropriate for the relevant Customer Authority Premises and level of access required in accordance with JSP 440.

2.6 The Contractor shall put in place, and shall ensure that all Contractor Personnel comply with, policies and procedures for the control, storage, use, transport and destruction of removable media in accordance with JSP 440 and HMG IA Standard No. 5 – *Secure Sanitisation of Protectively Marked or Secretive Information*.

2.7 For TOP SECRET Services, the Contractor shall put in place, and shall ensure that all Contractor Personnel comply with, measures limiting the opportunities for remote working including requiring Contractor Personnel to formally request permission from the Contractor in order to work remotely.

2.8 The Contractor shall ensure that products relevant to the security of the Services or integral to the security design have been Approved, in order to manage product diversity across the Services.

2.9 The Contractor shall only use appropriate commercial Off the Shelf and product assurance components sourced from Approved vendors.

2.10 The Contractor shall notify the Customer Authority if the Contractor is under any obligation to a Sub-contractor to allow that Sub-contractor access to data channels or networking devices. On receipt of such notification, the Customer Authority may, at its sole discretion, Approve or reject any such access.

2.11 The Contractor shall ensure that any manufacturer password values on networking components and applications are changed from the default password or value settings prior to any such components or applications being used in connection with the Services, or to deliver the Services.

2.12 The Contractor shall notify the Customer Authority if any aspect of their Service provision is to be provided from a country other than the United Kingdom ("**off-shored**"), such notification to be given in accordance with the CESG Good Practice Guide (GPG) – 6, version 2.1, date 09/2010). On receipt of such notification, the Customer Authority may, at its sole discretion, Approve or reject any such off-shoring and the Contractor shall not commence such off-shoring unless the Customer Authority has Approved it in accordance with this Paragraph 2.12.

2.13 The Contractor shall be responsible for ensuring that it has appropriate representation at the SWGs throughout the Term (and during any Exit Period) including:

2.13.1 both:

(i) a CESG certified professional ("**CCP**") scheme security information risk advisor (SIRA); and

(ii) a CCP technical security architect,

who is capable of making decisions that are compliant with the Standards on behalf of, and to support, the Contractor; and

2.13.2 a representative of the Contractor who has the authority to make commercial decisions on behalf of the Contractor, including authorisation of design changes during any SWG.

2.14 Subject to Clauses 10.5 and 23.3 of this Consolidated Contract, where the Customer Authority determines, acting reasonably, that certain equipment supplied by the Contractor in the delivery of the Services (including any New Exclusive Equipment) is inadequate to maintain the level of risk to the Customer Authority within the Agreed Risk Envelope for any of the Services, the Customer Authority may require the Contractor (at the Contractor's own cost) to replace such equipment with equipment which is adequate to maintain the level of risk to the Customer Authority within the Agreed Risk Envelope.

2.15 Within five (5) Working Days' of written notice from the Customer Authority, the Contractor shall grant the Customer Authority full access to the Contractor Systems, Sub-contractors' systems and the Services and permit the Customer Authority to inspect, audit and test the Contractor Systems, and the Services from time to time.

2.16 For any of the Services which are routed through shared or multi-tenanted ICT hosting environments, the Contractor shall provide documented evidence of assured electronic separation of Customer Authority Data. The Contractor shall also provide documented evidence that Contractor Personnel are always accompanied by at least one (1) other member of Contractor Personnel in network equipment rooms and data centre halls that host critical data processing functions, whether located on a Customer Authority Premise or Contractor Site.

2.17 The Contractor shall ensure that each of the Services that support the transmission of Customer Authority Data use cryptographic devices that are compliant with the Network Technical Authority's cryptographic management plan and the Customer Authority's cryptographic management plan, and that have been approved by CESG and certified for use at the required Security Classification and are compliant with JSP 490 and rule 22 in JSP 604.

2.18 The Contractor shall ensure that all Contractor Systems and Customer Authority Systems that are connected to the Customer Authority's networks at different Security Classifications are connected by the Boundary Protection Service provided by the Contractor in accordance with Consolidated Schedule 3 (*Service Requirements and Contractor Service Descriptions)* and assured by CESG tailored assurance service (CTAS) in accordance with the Standards.

3 INFORMATION ASSURANCE AT THE ENTERPRISE LEVEL

Development of the Information Security Management System

3.1 The Contractor shall provide documented evidence of the Contractor's Information Assurance processes, including an ISMS in accordance with Paragraph 3.2 below.

3.2 The Contractor shall maintain, continuously improve and comply with, and ensure that all Contractor Personnel and Sub-contractors comply with, the ISMS throughout the Term (and during any Exit Period).

3.3 The ISMS shall, without prejudice to Paragraph 2.2 above and Paragraph 4.1 below, be at all times in accordance with the Standards and Approved in accordance with this Consolidated Schedule.

Development of the Information Security Management Plan and the Project Cryptographic Management Plan

3.4 The Contractor shall, for each of the Services, provide documented evidence of the Contractor's implementation and operation of Information Assurance processes, including in accordance with Paragraph 3.5 below.

3.5 The Contractor shall (in accordance with the provisions of this Consolidated Schedule and the Standards) develop, implement, comply with (and ensure that all Contractor Personnel and Sub-contractors comply with) maintain, and continuously improve throughout the Term (and during any Exit Period):

3.5.1 an IMP for the Services; and

3.5.2 a PCP where required in respect of any of the Services,

and, within thirty (30) Working Days from the Effective Date (or as otherwise agreed by the Parties in writing) submit to the Customer Authority for Approval a complete and up-to-date copy of the same.

3.6 The IMP shall, unless otherwise specified in writing by the Customer Authority:

3.6.1 protect all aspects of the Services and all processes associated with the delivery of the Services, including the Customer Authority Premises, the Contractor System and any ICT, information and data including the Customer Authority Confidential Information, including Classified Information to the extent used by the Customer Authority or the Contractor in connection with this Consolidated Contract; and

3.6.2 have the specific content as set out in Paragraph 4 of this Consolidated Schedule.

3.7 If the IMP or PCP (or both), or any subsequent revision to either of the IMP or PCP (or both) in accordance with Paragraph 5 below, is (or are, as the case may be) not Approved in accordance with Paragraph 3.5 above, the Contractor shall submit a revised version of each such document, taking into account any Customer Authority comments, to the Customer Authority if required by the Customer Authority's defence security and assurance services body (or any successor to it) for Approval.

3.8 Once any IMP or PCP (or both), or any subsequent revision to either of the IMP or PCP (or both) in accordance with Paragraph 5 below, is (or are, as the case may be) Approved by the Customer Authority, the Contractor shall (and shall ensure that all Contractor Personnel and Sub-contractors) adopt and comply with such IMP or PCP (or both).

3.9 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 thirty (30) Working Days or such other period as the Parties agree in writing from the date of first submission of the IMP or PCP (as applicable) in accordance with Paragraph 3.5 above.

3.10 Any delay caused by a failure to achieve an approval milestone within the IMP, as defined in the Standards, shall not relieve the Contractor of its obligation to follow and comply with the Implementation Plan and shall not result in any changes to the Milestone Date(s). The Contractor shall escalate any delay in achieving any approval milestone set out in the IMP or the PCP to the SWG for a risk management decision.

Development of the Risk Management Accreditation Document Set ("RMADS")

3.11 The Contractor shall submit to the Customer Authority's defence security and assurance services body (or any successor to it) a RMADS to support its application for Certification of each of the Services in accordance with the HMG IA Standard No. 2 set out in the Standards. The Contractor shall ensure that all aspects of each of the IMPs are incorporated into the relevant sections of the RMADS for each of the Services.

3.12 The Contractor shall maintain, and make available to the Customer Authority on request from time to time, the RMADS documenting that Certification has been achieved during the Term (and during any Exit Period).

4 CONTENT OF THE IMP

4.1 The IMP shall set out the security measures to be implemented and maintained by the Contractor in relation to all aspects of the Services and all processes associated with the delivery of the Services throughout the Term (and during any Exit Period). Furthermore, the IMP shall at all times comply with, and specify, security measures and procedures which are sufficient to ensure that the Services comply with this Consolidated Schedule (including the requirements set out in Paragraph 2 above) and the other provisions of this Consolidated Contract relevant to security requirements (including the Service Requirements).

4.2 The IMP (including the draft version) shall also set out the plans for transitioning all security arrangements and responsibilities from the Outgoing Service Provider to the Contractor in accordance with Consolidated Schedule 2 (*Implementation Plan*), including for the Contractor to meet its security obligations set out in the Service Requirements and other provisions of this Consolidated Contract.

4.3 The IMP shall be structured in accordance with the Standards, cross-referencing if necessary to other Consolidated Schedules of this Consolidated Contract which cover specific areas included within those Standards.

4.4 The IMP shall be written in plain English and in a manner which is readily comprehensible to Contractor Personnel and the Customer Authority's staff who are engaged in the Services and shall not reference any other documents which cannot be provided, or otherwise made available, to the Customer Authority by the Contractor.

4.5 The Contractor shall provide the following IA Artefacts in support of the IMP, and to support any subsequent Certification of the Service, as to the extent such IA Artefacts may be applicable to each of the Services:

4.5.1 ISMS;

4.5.2 Security Policy Delivery Statement;

4.5.3 RMADS;

4.5.4 Security Requirements Document (SRD);

4.5.5 Project Cryptographic Management Plan (PCP);

4.5.6 Infosec Architecture Model;

4.5.7 Migration Plans;

4.5.8 Architecture Definition Document (ADD);

4.5.9 ADD Compliance Matrix;

4.5.10 Information Assurance risk assessment;

4.5.11 Risk Register;

4.5.12 Security Impact Statement;

4.5.13 any assessment, Security Audit and Test Reports; and

4.5.14 Service Code of Connection / Code of Practice Policy.

5 AMENDMENT AND REVISION OF THE IMP AND RMADS

5.1 In addition to its obligations under Paragraphs 3 and 4 above and subject to Clauses 10.5 and 23.3 of this Consolidated Contract, the Contractor shall review and update the IMP or RMADS annually or such other period as agreed by the Parties in writing to reflect:

5.1.1 emerging changes in the Standards which may include changes to the CESG Good Practice Guides and any associated processes described in the Standards;

5.1.2 any change or proposed change to the IMP, RMADS, and the Services;

5.1.3 any new, perceived or changed Threat to Security; and

5.1.4 any reasonable requests by the Customer Authority, including requests made in accordance with Clause 34.11 of this Consolidated Contract.

5.2 The Contractor shall provide the Customer Authority with a short report of the reviews described at Paragraph 5.1 above within twenty (20) Working Days after their completion

and amend the IMP or RMADS at no additional cost to the Customer Authority. The report shall include:

5.2.1 suggested improvements to the effectiveness of the IMP or RMADS;

5.2.2 updates to the HMG IA Standard No. 1 risk assessments set out in the Standards;

5.2.3 proposed modifications to the procedures and controls that affect information security to respond to events that may impact on the IMP or RMADS; and

5.2.4 suggested improvements in measuring the effectiveness of controls.

5.3 On receipt of the results of the report described in Paragraph 5.2 above, the Customer Authority may determine whether it shall Approve any amendments or revisions to the IMP, or RMADS in accordance with the process set out at Paragraph 3.5 above.

5.4 Any versions of the IMP or PCP that are revised in accordance with this Paragraph 5, shall replace any previous version of either document respectively.

6 SECURITY TESTING AND VALIDATION

6.1 The Contractor shall, in accordance with this Paragraph 6, conduct security audits and tests of the Services ("**Security Tests**") on an annual basis or as otherwise agreed in writing by the Parties. The date, timing, content and conduct of such Security Tests shall be appropriate to the Security Classification of the relevant Service and shall be Approved by the Customer Authority.

6.2 The Customer Authority may send a representative to witness the Security Tests or any parts thereof. The Contractor shall provide to the Customer Authority the results of such Security Tests in an Approved form as soon as practicable after completion of each Security Test and in any event within ten (10) Working Days from completion of such Security Test.

6.3 Without prejudice to any other right of audit or access granted to the Customer Authority pursuant to this Consolidated Contract and subject to Clauses 10.5 and 23.3 of this Consolidated Contract, the Customer Authority may and its authorised representatives may, at any time and on reasonable notice to the Contractor, carry out such Security Tests including penetration tests, web application security assessments, and forensic analysis as it may deem necessary in relation to the IMP or RMADS and the Contractor's compliance with and implementation of the IMP or RMADS. The Customer Authority may notify the Contractor in writing of the results of such Security Tests after completion of each Security Test. The Contractor shall cooperate with the Customer Authority to ensure that such Security Tests are designed and implemented so as to minimise any disruption to the delivery of the Services.

6.4 Where any Security Test carried out pursuant to Paragraph 6.2 or 6.3 above, reveals any actual or potential Breach of Security or security failure or weaknesses, the Contractor shall determine what changes to the IMP or RMADS are required to remedy such Breach of Security or security failure or weakness. The Contractor shall promptly notify the Customer Authority in writing of any such proposed changes. Subject to the Customer Authority's Approval, the Contractor shall implement such changes to the IMP or RMADS in accordance with the timetable agreed in writing with the Customer Authority or, otherwise, as soon as reasonably possible. Where the change to the IMP or RMADS addresses non-compliance on the part of the Contractor with the Standards or this

Consolidated Schedule, the Contractor shall implement the change at no additional cost to the Customer Authority.

7 COMPLIANCE AND AUDIT

7.1 The Contractor shall obtain Certification of the Services in accordance with the Standards within twelve (12) months of the relevant Operational Service Commencement Date (or such other period specified in the Implementation Plan or as otherwise agreed by the Parties in writing). If certain parts of the RMADS do not conform to the Standards, or if the controls described in the RMADS are not consistent with the Standards and, as a result the Contractor reasonably believes that it is not compliant with the Standards, the Contractor shall promptly notify the Customer Authority in writing of this and the Customer Authority in its absolute discretion may waive the requirement for Certification in respect of the relevant parts of the RMADS, providing effective risk mitigation has been put in place by the Contractor, and there is appropriate justification to do so.

7.2 If, on the basis of evidence provided by any of the Security Audits that the Customer Authority may carry out in accordance with Clause 22.1 of this Consolidated Contract, it is the Customer Authority's reasonable opinion that compliance with the Standards is not being achieved by the Contractor, then the Customer Authority shall notify the Contractor in writing of the same and give the Contractor a reasonable period of time (having regard to the extent and criticality of any non-compliance and any other relevant circumstances) to become compliant with the principles and practices set out in the Standards. If the Contractor does not become compliant within the required time then the Customer Authority has the right to obtain an independent audit against the Standards in whole or in part.

7.3 If, as a result of any such independent audit as described in Paragraph 7.2 above, the Contractor is found to be non-compliant with the Standards then the Contractor 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 Customer Authority in obtaining such independent audit.

7.4 The Contractor shall conduct regular internal security audits in order to maintain delivery of the Services in compliance with the Standards.

7.5 The Contractor shall promptly provide to the Customer Authority any associated internal security audit reports and shall notify the Customer Authority promptly in writing the results of such internal security audits.

8 BREACH OF SECURITY

8.1 The Contractor shall, where appropriate, integrate with the Customer Authority’s alerting and escalation mechanisms as defined in the Standards.

8.2 Either Party shall notify the other (in each case notification must go to the individual(s) designated in the IMP or RMADS) in writing immediately upon becoming aware of any Breach of Security including an actual, potential or attempted Breach of Security, or Threat to Security, any of the Services.

8.3 Without prejudice to any security incident notification and management process set out in this Consolidated Contract, upon becoming aware of any of the circumstances referred to in Paragraph 8.2 above, the Contractor shall:

8.3.1 immediately take all steps necessary to:

(i) remedy such breach or protect the Services and integrity of the IMP or RMADS against any such potential or attempted Breach of Security or Threat to Security; and

(ii) prevent an equivalent breach in the future,

such steps to include any action or changes required by the Customer Authority including those set out in Clauses 34.9 and 34.10 of this Consolidated Contract. If such action is taken in response to a Breach of Security that is determined by the Customer Authority, acting reasonably, not to be covered by the obligations of the Contractor under this Consolidated Contract, then the Contractor may refer the matter to the Contract Change Procedure, but this shall not delay the Contractor in taking steps to comply with Paragraph 8.2 above; and

8.3.2 provide to the Customer Authority full details using such reasonable reporting mechanisms as may be specified by the Customer Authority from time to time of the Breach of Security or the potential or attempted Breach of Security and of the steps taken to mitigate or resolve them.

8.4 The Contractor shall ensure that the requirements listed in the DCNS Enterprise Security Policy – Cyber Defence Policy and Rule 11 in JSP 604 are met in full.

8.5 The Contractor shall implement measures, in accordance with Customer Authority forensic readiness processes described in the DCNS Enterprise Security Policy, in order to ensure that digital evidence is preserved in support of Customer Authority security investigations.

8.6 The Contractor shall ensure that, and ensure that all Contractor Personnel are aware that, personal electronic devices with a recording, photographic or transmitting capability are not allowed within certain locations that the Customer Authority notifies to the Contractor from time to time.

9 MALWARE & TECHNICAL VULNERABILITY MANAGEMENT

9.1 Without prejudice to any other obligations which the Contractor has under this Consolidated Contract in relation to Malware, including viruses, worms, and spyware the Contractor shall, as an enduring obligation throughout the Term and during any Exit Period in accordance with Consolidated Schedule 20 (*Exit Management*), use its reasonable endeavours to prevent Malware from being introduced into the Customer Authority's ICT environment via the Services. This shall include an obligation to use the latest versions of anti-virus definitions available from industry accepted anti-virus software vendors to check for and investigate Malware. The Contractor shall promptly notify the Customer Authority of any Malware detected and of the results of investigations in relation to such Malware, such notification to be given in accordance with the Standards. If the Customer Authority instructs it to do so, the Contractor shall delete the Malware from the Services. In this Paragraph 9, references to "**anti-virus**" shall mean to software or other data intended to detect, prevent or mitigate the effects of Malware.

9.2 Notwithstanding Paragraph 9.1 above, if Malware is found the Parties shall cooperate with each other and with any affected Other Tower Service Provider and the Customer Authority Third Parties to reduce the effect of the Malware and, particularly if Malware causes loss of operational efficiency or loss or corruption of Customer Authority Data, assist each other to mitigate any losses and to restore the Services to their desired operating efficiency.

9.3 Any cost arising out of the actions of the Parties taken in compliance with the provisions of Paragraph 9.2 above shall be borne by the Parties as follows:

9.3.1 by the Contractor where the Malware originates from:

(i) the Software, except where the Customer Authority has waived the obligation set out in Paragraph 9.1 above by notice in writing (such form of writing to refer to this Paragraph 9.3.1(i)); and

(ii) the Customer Authority's Classified Information, while such Customer Authority's Classified Information was under the control of the Contractor and any Sub-contractor

unless the Contractor can demonstrate that such Malware was present and not quarantined or otherwise identified by the Customer Authority when provided to the Contractor; and

9.3.2 by the Customer Authority if the Malware originates from the Customer Authority's Classified Information whilst the Customer Authority's Classified Information was under the control of the Customer Authority.

9.4 The Contractor shall integrate with the Customer Authority technical vulnerability management mechanisms, where appropriate, as defined in the Standards.

9.5 The Contractor shall ensure that a configuration lockdown policy is maintained in accordance with the Standards for the different components of their ICT environments, including End User and mobile network devices.

9.6 The Contractor shall apply hardening templates endorsed by the SWG to standard builds as part of a defence-in-depth approach in order to:

9.6.1 install only those software components that are supported by a valid business case;

9.6.2 disable all unused services or functions, or both;

9.6.3 configure the component to minimise known vulnerabilities; and

9.6.4 prevent unauthorised alteration of the configuration, including unauthorised alteration of the configuration by End Users.

9.7 Where any actions related to the security of a network, system or application can only be performed by End Users with an elevated level of access to such network, system or application, the Contractor shall:

9.7.1 ensure that such actions cannot be performed by a single individual acting alone; and

9.7.2 implement mechanisms and management structures to segregate such actions.

9.8 For the purpose of Paragraph 9.7 above, "**actions**" shall be deemed to include account creation and deletion, changes to user permissions, access to and processing of protective monitoring data and report outcomes.

9.9 The Contractor shall ensure that the Services are supported by the latest versions of operating systems, applications, security tools, and that security patches are fully tested in an isolated test environment and are Approved before being implemented.

9.10 The Contractor shall only implement software that is under full vendor support, unless otherwise Approved.

9.11 The Contractor shall ensure that all Software and Software updates, including updates to anti-virus software, are subject to a pre-deployment testing regime in an isolated test environment.

9.12 The Contractor shall implement measures and provide evidence of robust privilege management for all administrator/super user accounts in respect of all network devices and infrastructure components.

9.13 The Contractor shall implement measures that ensure that Contractor Personnel with access to computer accounts that enable all discretionary access controls to be bypassed hold Developed Vetting Clearance without caveats.

9.14 The Contractor shall implement measures that ensure scripts provided by the Joint Cyber Unit are run against the configurations of the network routers used to provide the Services, and provide the agreed output to a shared location for use by the Joint Cyber Unit.