CONNECTIVITY CONSOLIDATED CONTRACT SCHEDULE

CONSOLIDATED SCHEDULE 3

SERVICE REQUIREMENTS AND CONTRACTOR SERVICE DESCRIPTIONS

for Contract Number DCNS/080

Table of Contents

Contents **Page**

CONSOLIDATED SCHEDULE 3
SERVICE REQUIREMENTS AND CONTRACTOR SERVICE DESCRIPTIONS

This Consolidated Schedule describes the Services to be provided by the Contractor to the Customer Authority in accordance with the terms of this Consolidated Contract.

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 in Part A, the Customer Authority's Service Requirements; and

1.1.2 in Part B, the Contractor Service Descriptions,

which together describe form part of the Services.

1.2 The Contractor Service Descriptions as set out at Part B of this Consolidated Schedule 3 (*Service Requirements and Contractor Service Descriptions*) shall be interpreted in accordance with the following principles:

1.2.1 Part A shall take precedence over Part B and the Contractor Service Descriptions shall be interpreted in accordance with their corresponding Service Requirements;

1.2.2 the Contractor shall be obliged to provide the Services, carry out the activities and provide the approaches set out in Part B, notwithstanding the fact that terms such as "the Contractor shall" and "by the Contractor" are not used;

1.2.3 unless the context requires otherwise, capitalised terms in Part B which have not been defined shall, where a similar term exists in Consolidated Schedule 1 (*Definitions*), be interpreted in accordance with the similar defined term in Consolidated Schedule 1 (*Definitions*). If there is any ambiguity around the interpretation of capitalised terms in Part B that have not been defined, the Customer Authority shall be entitled to define such capitalised terms in its sole discretion and the Contractor shall accept such Customer Authority definitions;

1.2.4 in accordance with Clause 36.5 of this Consolidated Contract, any activities, tasks or other items described in Part B as being provided by the Customer Authority or being needed from the Customer Authority shall neither be: (i) obligations of the Customer Authority; nor (ii) Customer Authority Dependencies except to the extent expressly stated to be Customer Authority Dependencies in Consolidated Schedule 8 (*Customer Authority Dependencies*). There shall be no obligation on the Customer Authority to provide any advice or assistance to the Contractor save as set out in Consolidated Schedule 8 (*Customer Authority Dependencies*). Except as set out in Clause 36 of this Consolidated Contract and Consolidated Schedule 8 (*Customer Authority Dependencies*), no failure by the Customer Authority to perform or provide any such activities, tasks or other items shall relieve the Contractor of its obligations to deliver the Services or to fulfil any of its obligations under this Consolidated Contract; and

1.2.5 no statements made in Part B about comprehensiveness, ability or quality (whether of the Contractor or of the measures set out in Part B) shall be read as statements that have been approved or accepted by the Customer Authority.

PART A: SERVICE REQUIREMENTS

2 OVERVIEW

2.1 This Part A of this Consolidated Schedule sets out the Customer Authority's Service Requirements as follows:

2.1.1 the common requirements described in Paragraph 3 below;

2.1.2 the Service Management requirements described in Paragraph 4 below;

2.1.3 the technical requirements, including:

(i) the Connectivity Service described in Paragraph 5 below;

(ii) the Point to Point Service described in Paragraph 6 below;

(iii) the Miscellaneous Connectivity Service described in Paragraph 7 below;

(iv) the Domain Name Service and IP Addressing Management Service described in Paragraph 8 below;

(v) the Encryption Service described in Paragraph 9 below;

(vi) the Boundary Protection Service described in Paragraph 10 below;

(vii) the Local Area Network Service described in Paragraph 11 below;

(viii) the Bespoke Engineering Service described in Paragraph 12 below;

(ix) the Cyber Access Service described in Paragraph 13 below; and

(x) the Professional Services described in Paragraph 14 below.

3 COMMON REQUIREMENTS

General

3.1 The Contractor shall ensure that it is PSN Compliant during the Term.

3.2 As part of the Services, the Contractor shall provide Connectivity to the GCN and support the delivery to the Customer Authority and Indirect Customers of other services that are dependent on the Services, including voice, video and application services.

Common Service Requirements

3.3 The Contractor shall:

3.3.1 ensure that a common Stratum 0 (as defined by the Internet Engineering Task Force) clock source, such as global positioning systems is used to synchronise the timing of the Network Infrastructure;

3.3.2 use industry standard methods such as the Network Time Protocol (as such protocol may be published from time to time by the Internet Engineering Task Force) to disseminate timing to the Network Infrastructure; and

3.3.3 ensure that all edge routers used by the Contractor in the provision of the Services are synchronised to a minimum of Stratum Level 2 (as defined by the Internet Engineering Task Force).

3.4 The Contractor shall, on instruction by the Customer Authority, promptly (or within such other timeframe communicated to it by the Customer Authority) disconnect any designated traffic flow for all or part of the Services and reinstate disconnected Services, in accordance with Clause 39.8 of this Consolidated Contract.

3.5 The Contractor shall, except as expressly stated to the contrary in this Consolidated Contract, proactively monitor and manage the Services, including by:

3.5.1 providing a system for monitoring and administering the Services;

3.5.2 deploying network management tools to enable:

(i) provisioning, modification and cessation of the Services remotely;

(ii) detection and rectification of Service Failures; and

(iii) proactive network monitoring of all Services on a twenty-four (24) hours per day, seven (7) days a week, three hundred and sixty five (365) days per year basis;

3.5.3 ensuring that all Contractor Personnel who are responsible for network management and have access rights that allow them to amend the configuration of more than one Service have Developed Vetting Clearance;

3.5.4 ensuring that the network monitoring and management system satisfies the Customer Authority's Business Continuity requirements (as set out in Consolidated Schedule 22 (*Business Continuity and Disaster Recovery Provisions*), so that:

(i) in the event of any failure of the primary network monitoring and management system:

(a) an alternative (or fall-back) network monitoring and management system is available for the affected Service; and

(b) the personnel required to operate the alternative (or fall-back) network monitoring and management system are transferred by the Contractor as soon as reasonably practicable to the alternative Site on which such system is located in order to operate such system; and

(ii) the risk of losing both the primary and fall-back network monitoring and management systems from a single failure or Incident is negligible; and

3.5.5 providing separate network monitoring and management for all TOP SECRET Services and implement in accordance with *JSP 440 STRAP Management Supplement*.

3.6 Unless otherwise directed by the Customer Authority, the Contractor shall ensure that all data traffic associated with the Services is encrypted before such data traffic leaves the boundary of a Customer Authority Site.

3.7 The Contractor shall support the Customer Authority's request, allow the Customer Authority and its authorised nominee (or either of them) to install monitoring and traffic-shaping equipment within any part of the Network Infrastructure, predominately for the purposes of audit and verification. The Contractor shall, within a reasonable period of receiving such request (and in any event within five (5) Working Days of such request) advise the Customer Authority as to the optimal date and time for installation of such equipment and make available a member of the Contractor Personnel to attend and supervise such installation. The optimal date and time advised by the Contractor shall be no later than thirty (30) Working Days after the original request from the Customer Authority.

3.8 The Contractor shall support the management of technical interfaces between the services and technology, communications and infrastructure systems provided by Customer Authority Third Parties to the Customer Authority, including by developing and maintaining interface control documents in a format agreed in writing between the Parties, such form of writing to refer to this Paragraph 3.8.

3.9 The Contractor shall ensure that its solution for the provision of the Services shall be designed, and shall be scalable, in such a way as to ensure that the Services are capable of meeting, as a minimum, the as is geographical footprint and volumes set out in the Service Evaluation Model, as well as handling organic growth.

3.10 The Contractor shall advise the Customer Authority promptly, and in any event prior to the commencement of work, if it believes that:

3.10.1 a suite of Service Elements (whether combined with other Service Elements or not) requested by the Customer Authority is (or are as the case may be) unlikely to be capable of providing the outcome desired by the Customer Authority, once commissioned; or

3.10.2 if there is a better value for money solution to meet the Customer Authority's requirements.

In such circumstances, the Contractor shall identify to the Customer Authority (giving reasons) how the Customer Authority's Service Request may be amended in order to facilitate a successful outcome.

3.11 The Contractor shall ensure that all Services of a critical nature at any given Customer Authority Site are provisioned with power requirements appropriate to supporting that critical Service (for example, UPS, battery back-up or dual feeds).

3.12 Without prejudice to the Customer Authority's entitlement to vary its actual throughput (including as against the Service Evaluation Model) from time to time, the Contractor shall provide a solution for the Services, and plan the Implementation, so that:

3.12.1 once Milestone number 20:*Overall Implementation Acceptance Date* has been Achieved, the Connectivity Service is delivered using Multiprotocol Label Switching (MPLS) technology; and

3.12.2 no later than 1 January 2020, the Contractor Solution is capable of delivering at least seventy per cent. (70%) of the LAN Service through Wireless Local Area

Network (WLAN) technology, in the manner set out in the instructions that accompany the Service Evaluation Model.

3.13 Without prejudice to its obligations under the ISS ITIL Processes and Consolidated Schedule 16 (*Contract Change Procedure*), the Contractor shall:

3.13.1 act as the Installation Design Authority for the Services in accordance with the Standards;

3.13.2 for each Customer Authority Site, engage proactively with, and abide by the decisions made by, the Customer Authority's nominees who represent CIDA and SCIDA (and their successors) in respect of that Customer Authority Site; and

3.13.3 comply with the appropriate HSE Construction (Design and Management) Regulations 2007.

Equipment Management

3.14 The Contractor shall be responsible for ensuring that all Equipment is, and continues to be, sufficient and suitable for delivery of the Services in accordance with this Consolidated Contract, including in accordance with the Service Levels and the Standards.

3.15 Except where expressly stated to the contrary in Consolidated Schedule 8 (*Customer Authority Dependencies*), the Contractor shall manage all matters connected with the lifecycle of all Equipment, including the specification, procurement, construction, installation, commissioning, testing, operation, monitoring, maintenance, support, use, repair, modification, upgrade, refresh, replacement, decommissioning, storage, disposal and recycling of all Equipment. Without prejudice to the generality of the foregoing, the Contractor shall:

3.15.1 proactively liaise with the Customer Authority with respect to the purchase of New Exclusive Equipment in accordance with the Procurement Plan, the Technology Refresh Plan and Clause 11 (*Equipment*) of this Consolidated Contract, and implement Equipment marking, control and inventory management and tracking methodologies, in accordance with Good Industry Practice;

3.15.2 ensure that it holds, manages and controls the distribution of an appropriate pool (or pools, as the case may be) of spare Equipment (the "**Spares Pool**"), including any spare Customer Authority Equipment that the Contractor believes is appropriate (including any equipment required in relation to the Legacy Connections and other Customer Authority Equipment purchased by the Customer Authority from Outgoing Service Providers). The Contractor shall not be entitled, unless otherwise agreed in advance in writing with the Customer Authority, such form of writing to refer to this Paragraph 3.15.2, to house spare Equipment on Customer Authority Premises;

3.15.3 where an item of Customer Authority Equipment is faulty, identify any relevant warranty protection, and progress claims under any such warranty expeditiously with a view to obtaining a repair or replacement of the relevant item or component at no additional charge to the Customer Authority;

3.15.4 where an item of Customer Authority Equipment is faulty and such fault(s) are (or are likely to) impact the provision or receipt of the Services adversely, fix or replace such item or component. Any Charges (if any) for such replacement item or

component shall be handled in accordance with Consolidated Schedule 9 (*Charges and Invoicing*);

3.15.5 from time to time decommission, de-install and remove Equipment that is no longer required to be installed on the Customer Authority Premises (including pursuant to MACs), unless directed otherwise by the Customer Authority. The Contractor shall determine whether such Equipment shall be put back into the Spares Pool or destroyed. Prior to destroying any Customer Authority Equipment, the Contractor shall confirm with the Customer Authority whether the Customer Authority requires the Contractor to:

(i) return such Customer Authority Equipment to the Customer Authority or its nominee at a location in the UK; or

(ii) dispose of such Customer Authority Equipment itself and in accordance with the Standards.

3.16 The Contractor shall ensure that, at the end of the Initial Term (or upon the termination or Partial Termination of this Consolidated Contract, if earlier), each item of Customer Authority Equipment is capable of supporting the Services (or any Replacement Services) for a further eighteen (18) months. This Paragraph 3.16 shall not serve to relieve the Contractor of its obligations to provide the Services in accordance with this Consolidated Contract.

4 SERVICE MANAGEMENT REQUIREMENTS

4.1 The Contractor shall provide Service Management from the Milestone Date for Milestone number 2: *Key Milestone, Service Management Established*.

4.2 In providing Service Management, the Contractor shall:

4.2.1 operate its own service management processes, in accordance with Good Industry Practice, the Service Management Framework and the ISS ITIL Processes;

4.2.2 provide all of the obligations, interfaces, activities and inputs (including data and physical inputs) set out in the ISS ITIL Processes as being carried out by the entity referred to in them as the *MSP*;

4.2.3 provide the Contractor Service Desk;

4.2.4 provide the Key Service Design Plans in relation to each Service to the Customer Authority, in accordance with the ISS ITIL Processes;

4.2.5 deliver the list of Event Management Thresholds to the Customer Authority, in accordance with the ISS ITIL Processes;

4.2.6 provide, to the reasonable satisfaction of the Customer Authority, an initial set of Knowledge Articles in order to establish a base knowledge store for the Customer Authority and update the Knowledge Articles on an on-going basis as required by the ISS ITIL Processes;

4.2.7 provide, to the reasonable satisfaction of the Customer Authority, the Definitive Media Library and update the Definitive Media Library on an on-going basis;

4.2.8 exchange Management Information and operational service management information electronically with the Customer Authority and Customer Authority Third

Parties in near real time and in a format compatible with any Customer Authority OSM Service Management Tooling (the "**Management Information Exchange**"). In particular, the Contractor shall ensure that Customer Authority Authorised Users have access to a range of functions, including:

(i) access to Management Information, including Reports, Monthly Summaries, and information regarding capacity, usage, Incidents and Problems;

(ii) the ability to raise Incidents and monitor the progress of Incident Resolution;

(iii) the ability to call off Services from the Contractor's Call-Off Service Catalogue; and

(iv) access to service bulletins and other information notices; and

4.2.9 present data to the Customer Authority that complies with the minimum data sets listed in the ISS ITIL Processes.

4.3 The Contractor shall provide at least one (1) member of the Contractor Personnel to act as a direct liaison for the GOSCC (such personnel being known as the "**GOSCC Liaison**"). A member of GOSCC Liaison shall:

4.3.1 during Working Hours be located within the GOSCC; and

4.3.2 at all other times outside of Working Hours (three hundred and sixty five (365) days a year) be available to attend the GOSCC on request.

4.4 Each member of the GOSCC Liaison shall have appropriate authority within the GOSCC to facilitate the resolution of Major Incidents between the Contractor Service Desk and any other service desks involved in the provision of information, communications or technology services to the Customer Authority (whether such other service desks are managed and operated by the Customer Authority or a Customer Authority Third Party). The Contractor shall ensure that the GOSCC Liaison shall respond to Incidents that are raised outside the normal Working Hours of the Customer Authority Site on which the GOSCC is located, as follows:

4.4.1 by telephone or email, promptly upon the Customer Authority raising the relevant Incident by sending an email or making a telephone call to the GOSCC Liaison; and

4.4.2 if the GOSCC Liaison is required to attend the GOSCC in person in order to resolve the Incident, the GOSCC Liaison shall attend the GOSCC within two (2) hours of the Customer Authority raising the relevant Incident by sending an email or making a telephone call to the GOSCC Liaison.

4.5 The Contractor shall ensure that the GOSCC Liaison fulfils all of the requirements for, and functions of, the GOSCC Liaison set out in the ISS ITIL Processes. The Contractor shall further ensure that the GOSCC Liaison:

4.5.1 is appropriately empowered and has responsibility and authority over the Contractor's services operation and prioritisation;

4.5.2 works collaboratively with its Sub-contractors, Customer Authority Third Parties and the Customer Authority in order to expedite the resolution of Service Outages, Major Incidents and Problems;

4.5.3 proactively contributes to Service planning; and

4.5.4 supports the delivery and management of the Services effectively.

5 CONNECTIVITY SERVICE

5.1 Connectivity Service Overview

5.1.1 In providing the Connectivity Service, the Contractor shall:

(i) provide new physical presentations at Customer Authority Sites, through which one (1) or more of the Customer Authority's information systems or services at that site is able to access the Connectivity Service at a specified bandwidth and availability (each physical presentation being a "**Connection**"), as required by the Customer Authority from time to time;

(ii) ensure that each Connection (whether or not already commissioned as at the Operational Service Commencement Date for the Connectivity Service) is capable of sending, transporting and receiving traffic (including voice, video and data) as a stream of data packets using IP technology (such capability being known, in respect of each Connection, as "**Connectivity**"); and

(iii) carry out certain MACs,

each as more particularly described in the remainder of this Paragraph 5.

5.1.2 The Contractor shall typically, but not always, provide each Connection using VPNs, access bearers and CPE (as appropriate) provided by the Contractor as part of the network used to provide the Connectivity Services (the "**Connectivity Network**"). However, where required to do so by the Customer Authority from time to time (whether for security reasons or otherwise), the Contractor shall use VPNs, access bearers and CPE provided as Customer Authority Dependencies from time to time.

5.1.3 The Contractor shall, at the Customer Authority's request from time to time, install, commission and support Connections for the following Subscriber Domains, between locations specified by the Customer Authority:

(i) "**UK Connectivity Subscriber Domain**", where both ends of the relevant access bearer is/are (are to be located) within the United Kingdom;

(ii) "**Overseas (Type A)**", where both ends of the relevant access bearer are (or are to be) located within the Overseas (Type A) Country Core Network, where an Overseas (Type A) Country Core Network means either:

(a) the German Country Core Network, which is comprised of Germany, Belgium and the Netherlands; or

(b) the Cyprus Country Core Network, which is comprised of Cyprus;

(iii) "**Overseas (Type B)**", where both ends of the relevant access bearer are (or are to be) located within the Overseas (Type B) Country Core Network, such Overseas (Type B) Country Core Network being comprised of the United States of America and Canada; and

(iv) "**Overseas (Type C)**", where one end of the access bearer is (or is to be) located outside the UK and the other end of the access bearer connects to a Customer Authority Site in the UK,

(each a "**Connectivity Subscriber Domain**").

5.1.4 The Contractor shall install, maintain and support OFFICIAL, SECRET and TOP SECRET Connections in each of the Connectivity Subscriber Domains as required by the Customer Authority from time to time.

5.1.5 The relevant Security Classification for each DSL Access Connection is provided by UAD-based software encryption provided by any Other Tower Service Provider.

5.1.6 The Contractor shall ensure that all Connections provided to Indirect Customers (including Industry Customers), including those Connections routed via the Remote Access Gateways, are routed through the Secure Interfaces and are subject to the constraints these interfaces are designed to impose.

5.2 Connection Types

The Contractor shall provide the Customer Authority with the following choices for each Connection, and shall comply with the Customer Authority's choices, as requested from time to time:

5.2.1 **Access Data Rate Types**. Access data rates determine the maximum End User throughput for IP and non-IP connectivity (the "**Access Data Rate**"). The Contractor shall provide the Customer Authority with a choice of the following Access Data Rate types for each Connection:

Access Data Rate Type	Primary Data Rate	Sub Rates (i.e. the rates within the relevant Primary Data Rate)
DSL Access	• up to 8 Mbit/s • up to 24 Mbit/s	• (none)
Fixed Access	• 10 Mbit/s	• 2 Mbit/s • 4 Mbit/s • 8 Mbit/s
	• 100 Mbit/s	• 20 Mbit/s • 50 Mbit/s
	• 1 Gbit/s	• 200 Mbit/s • 500 Mbit/s
	• 10 Gbit/s	• (none)

Table 1 – Connectivity Service – Access Data Rate types

(i) The Contractor shall ensure that the Customer Authority Authorised User payload throughput is within five per cent (5%) of the maximum throughput that can theoretically be achieved (i.e. taking into account any overheads, including any packet transmission or network protocols, or limitations on such throughput that are outside of the Contractor's control or as a result of any encryption overhead which can be considered Customer Authority

Authorised User payload) for any given frame or packet size or combination of packet sizes.

(ii) Unless otherwise agreed with the Customer Authority in advance, the Contractor shall ensure that it upgrades or downgrades the Access Data Rate for any Connection (as requested by the Customer Authority from time to time) with the minimum level of disruption to the Customer Authority, and in accordance with Clauses 7.3 to 7.17 of this Consolidated Contract.

(iii) All upgrades and downgrades within the Primary Data Rate throughputs shall be available as MACs- Channel Bandwidth Change (soft).

5.2.2 **Interface Types.** The Contractor shall provide a minimum of four (4) interface ports per DSL Access Connection and eight (8) interface ports per Fixed Access Connection and shall provide the Customer Authority with:

(i) a choice of at least the following interface types for each Fixed Access Connection; and

Interface Type	Physical Presentation
Ethernet 10/100/1000 Mbit/s	• RJ45 • STII male connector
Ethernet 100 Mbit/s (100base-FX)	• SC • LC • ST
Ethernet Gbit/s (1000base-X) and (10Gbase-)	
Ethernet Gbit/s (1000base-T) and (10Gbase-T)	• RJ45
TOP SECRET Special Variant Connection	• LEMO 1K 5 pin copper

Table 2a – Connectivity Service – interface types (Fixed Access Connections)

(ii) the following interface types for each DSL Access Connection.

Interface Type	Physical Presentation
Ethernet 10/100 Mbit/s	• RJ45 • STII male connector

Table 2b – Connectivity Service – interface types (DSL Access Connection)

5.2.3 **Availability**. The Contractor shall provide the Customer Authority with a choice of the following availability types for each Connection, in accordance with the requirements shown for that availability type in the table below:

Availability Type	Requirement
Standard Connection (DSL Access)	The Contractor shall provide all Standard Connections via (as a minimum) a non-resilient single DSL-based link and CPE design.
Non-Resilient Connection (Fixed Access)	The Contractor shall provide all Non-Resilient Connections via (as a minimum) a non-resilient single access circuit (excluding DSL) and CPE

Availability Type	Requirement
	design.
Resilient Connection (Fixed Access)	The Contractor shall provide all Resilient Connections via (as a minimum) two (2) access circuits, diversely routed, connecting a dual CPE design to a single site on the Contractor's core network.
Resilient Diverse Connection (Fixed Access)	The Contractor shall provide all Resilient Diverse Connections via (as a minimum) two (2) access circuits, diversely routed, connecting a dual CPE design to different sites on the Contractor's core network.
Resilient Fully Diverse Connection (Fixed Access)	The Contractor shall provide all Resilient Fully Diverse Connections via (as a minimum) two (2) access circuits with full diverse routing, including separate routes (ducting, etc.) onto the relevant Customer Authority Site, connecting a dual CPE design to different sites on the Contractor's core network.
Resilient Fully Diverse (Separation) Connection (Fixed Access)	The Contractor shall provide all Resilient Fully Diverse (Separation) Connections via (as a minimum) two (2) access circuits with full diverse routing, including separate routes (ducting, etc.) onto the relevant Customer Authority Site, connecting a dual CPE design to two (2) separate sites on the Contractor's core network with one of the connections being provided via an access bearer from a totally separately managed network, including totally separate network infrastructure and management systems in order to ensure that there are no shared single points of failure between the two networks.

Table 3 – Connectivity Service – availability types

5.2.4 **PSN Service Classes**. The Contractor shall ensure that the Connectivity Service is aligned with the six (6) PSN Service Classes. For Fixed Access Connections, the Connectivity Service shall conform to the six (6) discrete PSN Service Classes, including support for class selector (CS) precedence and Diffserv marking schemes as described in the *PSN Technical Domain Description* referred to in the Standards to identify and sort different types of applications in order of importance and priority, as follows:

PSN Service Class Name	PSN Diffserv (DSCP)	
	Diffserv PHB	CS
PSN Real Time	EF	

PSN Application Class 1	AF4x	CS4 CS5
PSN Application Class 2	AF3x	CS3
PSN Application Class 3	AF2x	CS2 CS6 CS7
PSN Application Class 4	AF1x	CS1
PSN Default	DF	(CS0)

Table 4 – Connectivity Service – PSN Service Classes

In particular, the Contractor shall ensure that the Connectivity Service provides Customer Authority nominees with the ability to assign each application of quality of service prioritisation clauses to one of the PSN Service Classes identified in the table above and shall also ensure that traffic is prioritised according to the Customer Authority's specification from time to time, including in accordance with any:

(i) source PSN Service Classes or DSCP classifications;

(ii) source or destination application identifiers;

(iii) source or destination logical addressing rules; and

(iv) manual configuration of PSN Service Classes on particular ports identified to the Contractor by the Customer Authority from time to time, in order to support Legacy Equipment,

as specified by the Customer Authority from time to time.

5.2.5 **Border Gateway Protocol**. The Contractor shall design, configure, support and implement the Connectivity Service so that it is able to provide border gateway protocol, such protocol being an inter-autonomous system routing protocol between autonomous systems, such systems being a collection of Subnets which constitute a routing domain under common management, as further described in *JSP 604 v4.1 Leaflet 2112 (IP Routing)* as set out in the Standards, and those identified to the Contractor by the Customer Authority as being autonomous systems from time to time (the "**Autonomous Systems**"), and such system being known as the "**BGP**". Where from time to time the Customer Authority identifies an Autonomous System to be advertised to Connections using BGP, the Contractor shall ensure that this Autonomous System is so advertised, using any of the following additional information about Autonomous System that the Customer Authority may provide to the Contractor from time to time:

(i) the Autonomous System number, the organisational owner of the Autonomous System and contact details for that owner;

(ii) the IP Address range(s) associated with the Autonomous System to be routed, as registered with the Customer Authority;

(iii) the network community string of in-scope Connection(s);

(iv) the protective marking supported by the Autonomous System; and

(v) the IP Address of the peer router advertising the Autonomous System.

5.2.6 TOP SECRET Connections.

(i) **TOP SECRET Connection Types.** The Contractor shall provide the Customer Authority with the choice of two (2) types of TOP SECRET Connections as follows:

(a) **TOP SECRET Standard Connection** – TOP SECRET Standard Connections are generally used in a static fixed environment. When providing a new TOP SECRET Standard Connection, the Contractor shall provide the Customer Authority with (amongst other things required to provide a Connection with Connectivity) a router and cryptographic device housed in a TEMPEST container that conforms to SDIP-27A. Such router shall be equipped with a minimum of two (2) fibre optic Ethernet interfaces of the same type as specified by the Customer Authority; and

(b) **TOP SECRET Special Variant Connection** – TOP SECRET Special Variant Connections are generally intended for use in a specialist user or maritime environments, or both. When providing a new TOP SECRET Special Variant Connection, the Contractor shall provide the Customer Authority with (amongst other things required to provide a Connection with Connectivity) a router and cryptographic device housed in a TEMPEST container that conforms to SDIP-27A and which can be fitted with a 19-inch rack mounting installation kit to fit into an end-user-provided 19-inch rack. Such router shall be equipped with a minimum of seven (7) Ethernet interfaces, which shall comprise five (5) LEMO 1K 5-pin copper interfaces, and two (2) ST fibre optic interfaces (100base FX multi-mode).

In respect of any TOP SECRET Connection, the router (and any relevant cryptographic device) required to be provided in a TEMPEST container for that Connection shall, together with the TEMPEST container, be known as a "**TOP SECRET CPE Box**".

(ii) **TOP SECRET Enclosures.** Where requested to do so by the Customer Authority in connection with a TOP SECRET Connection from time to time, the Contractor shall also provide the Customer Authority with an enclosure that is suitable for housing the TOP SECRET CPE Box (a "**TOP SECRET Enclosure**"). The Contractor shall provide, at the Customer Authority's option:

(a) a **Type 1 Enclosure** – a "**Type 1 Enclosure**" is an enclosure that enables the safe transportation – and operation from within the enclosure – of the router (and cryptographic device (if any)) provided within the TOP SECRET CPE Box. This might be, for example only, a *Secure Systems & Technologies Transportable Shock Mounted Enclosure*; and

(b) a **Type 2 Enclosure** – a "**Type 2 Enclosure**" is an enclosure that enables the safe transportation of the router (and cryptographic device (if any)) provided within the TOP SECRET CPE Box.

(iii) **TOP SECRET Engineering Laptop.** As requested by the Customer Authority from time to time in connection with a TOP SECRET Connection, the Contractor shall provide an engineering laptop that conforms to SDIP-27A and through which the Customer Authority is able to perform key management for the cryptographic device (if any), and configure the router, provided within the relevant TEMPEST container (a "**TOP SECRET Engineering Laptop**").

(iv) **TOP SECRET Bootable CD.** As requested by the Customer Authority from time to time, the Contractor shall provide a bootable CD that contains all software and training materials necessary to enable a Customer Authority representative to install, commission, cryptographic key fill, maintain and support the relevant TOP SECRET Connection using a Customer Authority user access device (for example, a computer or laptop), rather than an engineering laptop provided by the Contractor (a "**TOP Secret Bootable CD**").

(v) **TOP SECRET Cold Spare.** As requested by the Customer Authority from time to time in connection with a TOP SECRET Connection, the Contractor shall provide a duplicate of the relevant TOP SECRET CPE Box (a "**TOP SECRET Cold Spare**"). The Contractor shall provide such duplicate (at the Customer Authority's option) either:

(a) in a fully pre-configured state; or

(b) in an unconfigured state, but which is capable of being fully configured and used to receive the TOP SECRET Connectivity Service by an End User. The Contractor shall provide remote guidance to such End User, so that such End User is able to configure the TOP SECRET CPE Box in order to establish a Connection under direction from the Contractor.

(vi) **TOP SECRET Rack Mounting Kit.** As required by the Customer Authority from time to time in connection with a TOP SECRET CPE Box for a TOP SECRET Special Variant Connection, the Contractor shall provide a 19-inch equipment rack mounting kit and an interface cable (a "**TOP SECRET Rack Mounting Kit**").

(vii) **TOP SECRET Training.** As required by the Customer Authority from time to time in connection with a TOP SECRET Connection, the Contractor shall provide face-to-face training in respect of that TOP SECRET Connection, including a training course (typically two (2) Working Days' duration) designed to provide a technically skilled End User with the skills to configure, commission, maintain and decommission the TOP SECRET Connection ("**TOP SECRET Training**").

(viii) **TOP SECRET Port Activation.** The Contractor shall ensure that only those ports that the Customer Authority notifies the Contractor are in use from time to time are active ("**TOP SECRET Port Activation**").

5.2.7 **Provisioning**. Where a new TOP SECRET Connection (of any type) is requested by the Customer Authority, the Contractor shall provision such new Connections as follows:

(i) the Contractor shall deliver all TOP SECRET CPE Boxes to the required Customer Authority Sites using the Defence Courier Service. For TOP SECRET Connections that require a Type 1 Enclosure or Type 2 Enclosure, the Contractor shall provide the TOP SECRET CPE Box pre-installed in its required enclosure. For TOP SECRET Connections that are not required to be delivered in a Type 1 Enclosure or Type 2 Enclosure, the Contractor shall deliver the TOP SECRET CPE Box in the appropriate industry standard packaging;

(ii) for Overseas (Type A), Overseas (Type B), and Overseas (Type C) Connections, the Contractor shall:

(a) undertake surveys of the Customer Authority Site in order to complete any design documentation required prior to any relevant installation or commissioning works commencing;

(b) install and commission the Connection at the required Customer Authority Site;

(c) provide on-site operational familiarisation training to Customer Authority nominee(s) which gives an overview of how the Connection should be used and operated immediately following installation;

(d) provide system support documentation and fault handling instructions to the Customer Authority's nominee(s);

(e) on request by the Customer Authority's nominee(s), provide a member of the Contractor Personnel to guide the End User through the fault diagnostic and restoration procedure remotely and in real time on a twenty-four (24) hours per day, seven (7) days a week, three hundred and sixty five (365) days a year basis; and

(f) attend the Customer Authority Site to repair or replace faulty equipment delivering the relevant Connection, at a time and date reasonably specified by the Customer Authority; and

(iii) for Overseas (Type B) and Overseas (Type C) Connections only, the Contractor shall:

(a) include in the delivery referred to in Paragraph 5.2.6(v) above, a TOP SECRET Cold Spare, which is to be held on-site as a spare by the Customer Authority;

(b) provide written installation instructions for the equipment which has been delivered;

(c) when requested by the Customer Authority, provide a member of the Contractor Personnel to guide a Customer Authority's nominee(s) through the installation and commissioning of each Connection (and any related equipment) remotely until the Customer Authority has been able to achieve a successful test of the Connection; and

(d) provide system support documentation and fault handling instructions to the Customer Authority's nominee(s).

5.2.8 **Cyprus Alternative Network Capability.** The Contractor shall provide, support, maintain and manage a back-up network for the benefit of Connections to Customer Authority Sites located in Cyprus, such network to be independent of the Cyprus Telecom network, any successors to the Cyprus Telecom network and any Cypriot-owned and Cypriot-controlled networks (the "**Cyprus Alternative Network**"). The Contractor shall ensure that all traffic is capable of being automatically rerouted at all times between the Cyprus Alternative Network and the primary network used to provide the Connectivity Services to Customer Authority Sites located in Cyprus, so that (amongst other things) in the event of a failure in such primary network, traffic can be carried successfully between Connections using the Cyprus Alternative Network;

5.2.9 **Segregated Community Services**. The Contractor shall ensure that the Connectivity Service provides one (1) or more Segregated Community Services and shall:

(i) where requested by the Customer Authority (but only where so requested), advertise the Segregated Community Service(s) to the GCN within twenty (20) Working Days from receipt of such request, in order to enable other PSN providers to integrate their PSN Compliant connectivity services with the Connectivity Service, to give the effect of a single connectivity service;

(ii) for the Segregated Community Service(s), follow published PSN Compliance Conditions for IP Addressing Management on behalf of the Customer Authority, except where such published PSN Compliance Conditions for IP Addressing Management conflict with the Standards and the Customer Authority's instructions with respect to IP Addressing Management from time to time;

(iii) publish an IP Address assignment procedure for the Segregated Community Service, which shall be accessible by authorised End Users in accordance with the Standards and the Customer Authority's instructions with respect to IP Addressing Management from time to time; and

(iv) for the segregated Customer Authority-specific Services, and without prejudice to any other obligations of the Contractor under this Consolidated Contract, resolve technical issues expeditiously and shall co-operate with the Customer Authority and any relevant Customer Authority Third Parties in both resolving and reporting the progress and effect of such resolution.

5.2.10 **Communities of Interest.** The Contractor shall provide a means by which End Users (or groups of End Users) identified to the Contractor by the Customer Authority from time to time may be segregated from each other and other End Users using one (1) or more assured technological techniques (each a "**Community of Interest**" or "**COI**").

5.2.11 **Multi-national Connections.** The Contractor shall provide SECRET Communities of Interest and the Multi-National Connections to support participating nations of the combined communications electronics board (the "**CCEB**") in accordance with

the network design and timing constraints notified by the Customer Authority from time to time.

5.2.12 The Contractor shall provide, manage and support the MNC Red Network and MNC Black Network, including:

(i) acknowledging that the technical design shall conform to the common technical architecture, and adhere to the detailed technical design principles and constraints as developed by the Customer Authority from time to time;

(ii) ensuring that the SECRET Communities of Interest are separated from each other, and from the underlying MNC Black Network using IP cryptographic equipment;

(iii) providing interconnections with black networks that are provided and managed by other participating nations of the CCEB;

(iv) providing network management visibility of the MNC Red Network equipment to other nations within the same Community of Interest on a read-only basis; and

(v) providing technical support to the Customer Authority and attending technical design discussion meetings as directed by the Customer Authority from time to time.

5.3 Connectivity Service MACs

5.3.1 On request by the Customer Authority from time to time, the Contractor shall carry out the types of MACs shown in Table 5 below (each a "**Connectivity Service MAC**").

5.3.2 The activities to be carried out by the Contractor within each Connectivity Service MAC shall include any Site attendance, removal, de-installation, de-commissioning, configuration and administrative work required as a result of such Connectivity Service MAC, including equipment removal, configuration and amendments to the information available through the Management Information Exchange, documentation of the Connectivity Service MAC in accordance with the Standards and communication to the Customer Authority of activity completion by email or telephone, as appropriate.

5.3.3 The Contractor shall obtain all necessary MAC Approvals in accordance with the Standards prior to commencement of work for any of the Connectivity Service MACs, unless otherwise directed by the Customer Authority.

MAC	Non-exhaustive list of activities included within MAC
Connection Move	• All preparatory work, including a Site survey (if required) and design activities; • carry out any MAC Approval Activities; • once any MAC Approvals have been obtained, change the location of the relevant Connection; and • any other activity required to signal completion of, and to document and test, the MAC in accordance with the Standards.

MAC	Non-exhaustive list of activities included within MAC
Channel Bandwidth Change (soft)	• Remote work to up-speed or down-speed the relevant Connection (i.e. the bandwidth change is possible within the capability of the existing equipment and can be completed remotely without a change in hardware); and • any other activity required to signal completion of, and to document and test, the MAC in accordance with the Standards.
Remote/soft Change	• Any change to a Connection configuration that can be performed remotely other than a Channel Bandwidth Change (soft); and • any other activity required to signal completion of, and to document and test, the MAC in accordance with the Standards.
Connection Bandwidth Change (hard)	• All preparatory work, including a Site survey (if required) and design activities; • carry out any MAC Approval Activities; • once any MAC Approvals have been obtained, complete the up-speed or down-speed of the relevant Connection; and • any other activity required to signal completion of, and to document and test, the MAC in accordance with the Standards.
CPE Installation	• All preparatory work, including a Site survey (if required) and design activities; • carry out any MAC Approval Activities; • once any MAC Approvals have been obtained, install and commission additional CPE (for example, where the Customer Authority requires more than eight (8) ports in respect of a Connection); and • any other activity required to signal completion of, and to document and test, the MAC in accordance with the Standards.
Community of Interest (soft)	• Remote work to establish and segregate, or amend, a specified Community of Interest; and • any other activity required to signal completion of, and to document and test, the MAC in accordance with the Standards.
Activation of a TOP SECRET Interface Port	• Remote work to activate an interface port on a TOP SECRET Standard Connection or TOP SECRET Special Variant Connection; and • any other activity required to signal completion of, and to document and test, the MAC in accordance with the Standards.
Deactivation of a TOP SECRET Interface Port	• Remote work to de-activate an interface port on a TOP SECRET Standard Connection or TOP SECRET Special Variant Connection; and • any other activity required to signal completion of, and to document and test, the MAC in accordance with the Standards.
BGP Change	• Remote work to reconfigure a BGP network community string of in-

MAC	Non-exhaustive list of activities included within MAC
(soft)	scope Connection(s) where the requirement for such reconfiguration has resulted from a Customer Authority-initiated change to the routing requirements within an Autonomous System; and • any other activity required to signal completion of, and to document and test, the MAC in accordance with the Standards.
PSN Service Class Allocation Change	• Remote reconfigure PSN Service Class allocation for a CPE associated with a Connection ; and • any other activity required to signal completion of, and to document and test, the MAC in accordance with the Standards.
Cease Connection (soft)	• Remote work to cease a Connection, where such cessation does not require the removal of equipment; and • any other activity required to signal completion of, and to document and test, the MAC in accordance with the Standards.
Cease Connection (hard)	• All preparatory work, including a Site survey (if required) and design activities; • carry out any MAC Approval Activities; • once any MAC Approvals have been obtained, all work necessary to: (a) de-commission, de-install and remove the relevant Connection and all associated hardware, if the relevant Connection is within the UK Connectivity Subscriber Domain; or (b) collect and remove all hardware associated with the relevant Connection from a nominated Customer Authority Site within the UK Connectivity Subscriber Domain, if the relevant Connection is within an Overseas Connectivity Subscriber Domain at the time it is to be ceased, while ensuring that any remaining Services are maintained; and • any other activity required to signal completion of, and to document and test, the MAC in accordance with the Standards.
Community of Interest (hard)	• All preparatory work, including a Site survey (if required) and design activities to establish a new COI; • carry out any MAC Approval Activities; • once any MAC Approvals have been obtained, install and commission additional COI equipment (e.g. crypto equipment and red router in respect of the COI); and • any other activity required to signal completion of, and to document and test, the MAC in accordance with the Standards.

Table 5 – Connectivity Service MACs

6 PPS

6.1 PPS Overview

The PPS encompasses the provision and management of a number of point to point connections between Customer Authority Sites, incorporating a wide range of interface

types, transmission protocols and standards, speeds and other variables. A proportion of the connections provided and managed within the PPS are used to provide connectivity to critical Customer Authority systems with aged (or sometimes near obsolete) interfaces (such connections being more particularly described in Table 6 below and known as "**Legacy Connections**"). New connections are expected to be primarily Ethernet connections.

6.2 Core PPS Requirements

6.2.1 In providing the PPS, the Contractor shall:

(i) provide new one-to-one connections or circuits between Customer Authority Sites (each connection linking two Customer Authority Sites being a "**PPS Connection**"), as required by the Customer Authority from time to time;

(ii) subject to Paragraph 6.3.13 below, ensure that each PPS Connection (whether or not already commissioned as at the Operational Service Commencement Date for the PPS) is able to send, transport and receive analogue or digital traffic (including voice, video and data) as a stream of data packets using predominantly non-IP technology (such ability being known, in respect of a PPS Connection, as "**PPS Connectivity**");

(iii) without prejudice to Paragraph 6.3.13 below, where more than one PPS Connection is present on a Customer Authority Site, rationalise the infrastructure used by these PPS Connections in a manner that is economically advantageous to the Customer Authority (for example, by creating logically separate connections using one physical connection (rather than a number of physically separate connections)). Each set of PPS Connections that has been the subject of such a rationalisation shall be known as a "**PPS Group**";

(iv) carry out certain MACs; and

(v) contribute to discussions with the Customer Authority and Customer Authority Third Parties (as reasonably required by the Customer Authority from time to time) about opportunities and a strategy for retiring PPS Connections and replacing them with appropriate alternative services.

6.2.2 The Contractor shall, at the Customer Authority's request from time to time, provide, install, commission, support, maintain and manage PPS Connections:

(i) wholly within the UK, Germany, Cyprus or North America; and

(ii) from the UK to Germany, Cyprus or North America,

(each a "**PPS Subscriber Domain**").

6.2.3 The Contractor shall provide, install, commission, support, maintain and manage OFFICIAL, SECRET and TOP SECRET PPS Connections in the locations described in Paragraph 6.2.2 above.

6.3 PPS Connection Features

6.3.1 As requested by the Customer Authority from time to time, the Contractor shall provide, install, commission, support, maintain and manage the types of PPS

Connections and infrastructure used to support PPS Connections identified in Table 6 below.

6.3.2 A PPS Connection can be a Flexible PPS Connection or a Fixed PPS Connection, each as more particularly described at Paragraph 6.3.10 below.

6.3.3 The physical presentation of an interface type (as referred to in the table below) for a PPS Connection shall take the form of an appropriate socket on the interface distribution panel or other CPE.

6.3.4 The Contractor shall not use the types of PPS Connection against which a "No" is shown in the "Flexible Configuration Bearer" column below as bearers that provide connectivity to Flexible Configuration Equipment, without the Customer Authority's prior written consent.

PPS Connection Type	Interface/ Transmission Type	Data Rates	Flexible Configuration Bearer	Flexible PPS Connection	PPS Subscriber Domain
Ethernet (Digital)	Ethernet (IEEE 802.3) Base-T	10 Mbit/s 100 Mbit/s 1 Gbit/s	Yes	10 Mbit/s and 100 Mbit/s only	UK North America Germany Cyprus
Ethernet (Digital)	Ethernet (IEEE 802.3) Base-X	10 Mbit/s 100 Mbit/s 1 Gbit/s	Yes	10 Mbit/s and 100 Mbit/s only	UK North America Germany Cyprus
Ethernet (Digital)	Ethernet (IEEE 802.3) Base-(TBD)	10 Gbit/s	Yes	No	UK
Fibre Channel (Digital)	Fibre Channel	1 Gbit/s 4 Gbit/s	No	No	UK
(Digital)	V.11 (RS422) signalling	1.024 Mbit/s 1.536 Mbit/s 2.048 Mbit/s 2.560 Mbit/s 3.840 Mbit/s 7.68 Mbit/s	No	All speeds	UK North America Germany Cyprus
(Digital)	Plesiochronous G.703 75 Ohm unbalanced on	2.048Mbit/s 8.192Mbit/s 34.368Mbit/s	No	All speeds	UK Germany Cyprus

PPS Connection Type	Interface/ Transmission Type	Data Rates	Flexible Configuration Bearer	Flexible PPS Connection	PPS Subscriber Domain
	grounded BNC connectors				
(Digital)	T1 unstructured	1.55 Mbit/s	No	Yes	North America
(Digital)	T3 unstructured	45 Mbit/s	No	Yes	North America
ATM (Digital)	ATM Access Plesiochronous G.703 75 Ohm unbalanced on grounded BNC connectors	2.048 Mbit/s 34.368 Mbit/s	Yes	All speeds	UK Germany Cyprus
ATM (Digital)	ATM Access Synchronous STM-1 optical G957 SC connector	155.520 Mbit/s	Yes	No	UK Germany Cyprus
ATM (Digital)	ATM Access Synchronous STM-4 optical G957 SC connector	622.080 Mbit/s	Yes	No	UK Germany Cyprus

Table 6 –PPS Connections

6.3.5 As requested by the Customer Authority from time to time, and subject to the availability of any relevant equipment required to maintain PPS Connectivity, the Contractor shall support, maintain and manage the types of Legacy Connections and infrastructure used to support Legacy Connections identified in Table 7 immediately below:

PPS Connection Type	Interface/ Transmission Type	Data Rates
(Analogue)	Analogue 2-wire	N/A
(Analogue)	Analogue 4-wire	N/A
(Digital)	Asynchronous V.24	50 bit/s 75 bit/s 100 bit/s 110 bit/s 150 bit/s 200 bit/s 300 bit/s

PPS Connection Type	Interface/ Transmission Type	Data Rates
		600 bit/s 1200 bit/s 2400 bit/s 4800 bit/s 9600 bit/s 19.2 kbit/s
(Digital)	Synchronous V.24	1200 bit/s 2400 bit/s 4800 bit/s 9600 bit/s 19.2 kbit/s
(Digital)	Synchronous X.21	1200 bit/s 2400 bit/s 4800 bit/s 9600 bit/s 19.2 kbit/s 48 kbit/s 56 kbit/s 64 kbit/s
(Digital)	Synchronous V.11 (RS422)	128 kbit/s 192 kbit/s 256 kbit/s 320 kbit/s 384 kbit/s 512 kbit/s

Table 7 - Legacy Connections

6.3.6 No Legacy Connection shall be a Flexible PPS Connection.

6.3.7 No Legacy Connection shall be used to provide connectivity to Flexible Configuration Equipment.

6.3.8 To the extent that the Contractor is not able to repair or replace a Legacy Connection because the relevant equipment is not available (either as part of the Spares Pool or via any other reasonable procurement route), the Contractor shall not be in breach of the relevant Service Levels for that Legacy Connection, but shall provide the Customer Authority promptly with affordable and timely recommendations for maintaining PPS Connectivity between the relevant Customer Authority Sites.

6.3.9 For Fixed PPS Connections, the Contractor shall ensure that the Customer Authority Authorised User payload throughput is within five per cent (5%) of the maximum throughput that can theoretically be achieved (i.e. taking into account any overheads, including any packet transmission or network protocols, or limitations on such throughput that are outside of the Contractor's control or as a result of any encryption overhead which can be considered Customer Authority

Authorised User payload) for any given frame or packet size or combination of packet sizes.

6.3.10 As required by the Customer Authority from time to time:

(i) the Contractor shall provide certain types of PPS Connections rapidly, as indicated in the "Flexible PPS Connection" column in the Table 6 (*PPS Connections*) above (such rapid configuration being known as the "**Flexible Configuration Service**") in accordance with the Service Levels. PPS Connections that are provided under the Flexible Configuration Service shall be known as "**Flexible PPS Connections**" and shall be provided pursuant to a Flexible Configuration – Reconfiguration Activity MAC. PPS Connections that are not Flexible PPS Connections shall be known as "**Fixed PPS Connections**". A Flexible PPS Connection may only be provided where there is capacity on appropriate:

(a) Flexible Configuration Equipment;

(b) Connectivity to the Flexible Configuration Equipment; and

(c) interface cards installed in the Flexible Configuration Equipment;

(ii) the Contractor shall provide, install, commission, support, maintain and manage equipment (for example, a multiplexer) that will enable the delivery of the Flexible Configuration Service in accordance with the Service Levels for the Flexible Configuration Service (with the equipment that is connected to one end of a bearer being known as an item of "**Flexible Configuration Equipment**");

(iii) the Contractor shall provide, install, commission, support, maintain and manage interface cards for use in conjunction with the Flexible Configuration Equipment;

(iv) for each digital Flexible PPS Connection, the Contractor shall ensure that the Customer Authority Authorised User payload throughput is within ten per cent (10%) of the maximum throughput that can theoretically be achieved (i.e. taking into account any overheads or limitations on such throughput that are outside of the Contractor's control or as a result of any encryption overhead which can be considered Customer Authority Authorised User payload) for any given frame or packet size or combination of packet sizes;

(v) for TOP SECRET PPS Connections provided under the Flexible Configuration Service only, the Contractor shall (as required by the Customer Authority from time to time) provide additional duplicate Flexible Configuration Equipment on Customer Authority Sites as spares (each such spare being a "**Cold Standby**"). The Contractor will support this Cold Standby facility with:

(a) operational familiarisation training to a Customer Authority's nominee(s) at the time of delivery which gives an overview of how the equipment delivered should be used and operated;

(b) as required, the provision of a member of the Contractor Personnel to guide a Customer Authority's nominee through the installation and

commissioning of each Cold Standby (and any related equipment) remotely until the Customer Authority has been able to achieve a successful test of the relevant PPS Connection;

(c) the provision of system support documentation and fault handling instructions to the Customer Authority's nominee; and

(d) on request by the Customer Authority's nominee, the provision of a member of the Contractor Personnel to guide the End User through the fault diagnostic procedure remotely and in real time; and

(vi) the Contractor shall provide PPS Connection types that are presented in one of the ways set out below:

(a) **"Non-Resilient PPS Connections**"– PPS Connections provided via (as a minimum) one (1) individual PPS CPE at each end of the connection, each of which PPS CPE is connected by a minimum of one (1) link;

(b) **"Resilient PPS Connections**"– PPS Connections provided via (as a minimum) two (2) individual PPS CPE connected by two (2) links diversely routed; and

(c) **"Resilient Fully Diverse PPS Connections**"– PPS Connections provided via (as a minimum) two (2) individual PPS CPE connected by two (2) links with full diverse routing, including separate routes (ducting etc.) onto the Customer Authority Site and the second link.

6.3.11 **PPARS**. Where requested by the Customer Authority in respect of a particular PPS Connection, the Contractor shall provide and manage point–to-point alternative routing services between relevant Customer Authority Sites and such services shall allow traffic to be re-routed to one (1) or two (2) predefined alternative end points, such end points being CPEs, (the "**PPARS**"). The Contractor shall provide the Customer Authority with two (2) types of PPARS choices as follows:

(i) **PPARS (1)** – a PPARS that provides one (1) additional predefined alternative end point; and

(ii) **PPARS (2)** – a PPARS that provides two (2) additional predefined alternative end points.

6.3.12 In relation to all PPARS, the Contractor shall:

(i) make available to the Customer Authority up-to-date information on the connection status of each of the PPARS end points; and

(ii) inform the Customer Authority's active PPARS network controller (or such other nominee as the Customer Authority may notify the Contractor from time to time) once a switch to a new end-point has been completed.

6.3.13 The Contractor shall ensure that no Legacy Connections (including any infrastructure provided to increase the resilience and availability of such Legacy Connections) that exist as at the Operational Service Commencement Date for the PPS are removed or replaced without the Customer Authority's prior written consent. Such infrastructure may include dual redundancy in equipment and other infrastructure in order to provide greater resiliency.

6.4 Ethernet MAN Connections

6.4.1 As requested by the Customer Authority from time to time, the Contractor shall provide, install, commission, support, maintain and manage PPS Connections that connect:

(a) a particular Customer Authority Site that is identified by the Customer Authority and notified to the Contractor as being a "**MAN Hub**" to

(b) a particular Customer Authority Site identified by the Customer Authority as requiring a low latency connection to the MAN Hub (each such site being a "**MAN Satellite**" and each such PPS Connection being a "**MAN Connection**").

6.4.2 Each MAN Connection shall (unless otherwise agreed with the Customer Authority in advance) be provided by way of an Ethernet connection. Where feasible, the Contractor shall ensure that the end points at each of the MAN Connections connecting to a particular MAN Hub interface with a single item of CPE at the MAN Hub.

6.5 Ethernet and Fibre Channel Very Low Latency (VLL) Connections

As requested by the Customer Authority from time to time, the Contractor shall provide, install, commission, support, maintain and manage PPS Connections that connect the Customer Authority's main data centres (each such PPS Connection being a "**VLL Connection**").

6.6 PPS Synchronisation Requirements

The Contractor shall ensure that each PPS Connection synchronises in accordance with ITU-T (*International Telecommunication Union – Telecommunication Standardisation Sector*) G.811 and G.812 so that cross connections with peer networks operating to the same standards are slip–free unless permitted by the applicable interface control document.

6.7 PPS MACs

6.7.1 On request by the Customer Authority from time to time, the Contractor shall carry out the types of MACs shown in Table 8 below (each a "**PPS MAC**").

6.7.2 The activities to be carried out by the Contractor within each PPS MAC shall include any Site attendance, removal, de-installation, de-commissioning, configuration and administrative work required as a result of such PPS MAC, including equipment removal, configuration and amendments to the information available through the Management Information Exchange, documentation of the PPS MAC in accordance with the Standards and communication to the Customer Authority of activity completion by email or telephone, as appropriate.

6.7.3 The Contractor shall obtain all necessary MAC Approvals in accordance with the Standards prior to commencement of work for any of the PPS MACs, unless otherwise directed by the Customer Authority.

MAC	Non-exhaustive list of activities included within MAC
PPS Connection Move	• All preparatory work, including a Site survey (if required) and design activities;

MAC	Non-exhaustive list of activities included within MAC
	• carry out any MAC Approval Activities; • once any MAC Approvals have been obtained, change the location of the relevant PPS Connection; and • any other activity required to signal completion of, and to document and test, the MAC in accordance with the Standards.
PPS Bandwidth change (soft)	• Remote work to up-speed or down-speed the relevant PPS Connection (i.e. the bandwidth change is possible within the capability of the existing equipment and can be completed remotely without a change in hardware); and • any other activity required to signal completion of, and to document and test, the MAC in accordance with the Standards.
PPS Bandwidth change (hard)	• All preparatory work, including a Site survey (if required) and design activities; • carry out any MAC Approval Activities, including the submission of any documentation/evidence required; • once any MAC Approvals have been obtained, complete the up-speed or down-speed of the relevant PPS Connection; and • any other activity required to signal completion of, and to document and test, the MAC in accordance with the Standards.
PPARS Reconfiguration	• Remote work to reconfigure the relevant PPARS end point (i.e. re-pointing of the end point from one pre-defined location to another); and • any other activity required to signal completion of, and to document and test, the MAC in accordance with the Standards.
Fixed PPS Connection Group Reconfiguration Activity	• Remote work to reconfigure the relevant PPS CPE associated with the PPS Group end point (which can include adjustments to the relative bandwidths of the logically separate PPS Connections or re-routing of those connections from one pre-defined location to another); and • any other activity required to signal completion of, and to document and test, the MAC in accordance with the Standards.
Flexible Configuration Equipment – Reconfiguration Activity	• Remote work to reconfigure Flexible Configuration Equipment (for example, a multiplexer), as required in order to effect one of the following: (i) a bandwidth change; (ii) the provision of a Flexible PPS Connection, such provisioning to include remote setup and configuration of an interface card or unused ports on an already in use interface card;

MAC	Non-exhaustive list of activities included within MAC
	and (iii) cease of a Flexible PPS Connection; and • any other activity required to signal completion of, and to document and test, the MAC in accordance with the Standards.
Cease Fixed PPS Connection (soft)	• Remote work to cease a Fixed PPS Connection which does not require the removal of equipment; and • any other activity required to signal completion of, and to document and test, the MAC in accordance with the Standards.
Cease Fixed PPS Connection (hard)	• All preparatory work, including a Site survey (if required) and design activities; • carry out any MAC Approval Activities; • once any MAC Approvals have been obtained, all work necessary to de-commission, de-install and remove the PPS Connection and all associated hardware, while ensuring that any remaining Services are maintained; and • any other activity required to signal completion of, and to document and test, the MAC in accordance with the Standards.
Cease of Flexible Configuration Equipment and any associated Flexible PPS Connections	• All preparatory work, including a Site survey (if required) and design activities; • carry out any MAC Approval Activities; • once any MAC Approvals have been obtained, all work necessary to de-commission, de-install and remove the Flexible Configuration Equipment and all associated hardware, while ensuring that any remaining Services are maintained; and • any other activity required to signal completion of, and to document and test, the MAC in accordance with the Standards.
Training for Cold Standby	• Delivery of operational familiarisation training to Customer Authority's nominee(s) which gives an overview of how the equipment delivered should be used and operated; and • any other activity required to signal completion of, and to document and test, the MAC in accordance with the Standards.

Table 8 - PPS MACs

7 MISCELLANEOUS CONNECTIVITY SERVICE

7.1 Miscellaneous Connectivity Service Overview

The Contractor shall accept the novation of, procure and manage Commercial Telecoms Contracts in accordance with Paragraph 7.2 below.

7.2 Miscellaneous Connectivity Capability

7.2.1 From the Operational Service Commencement Date for the Miscellaneous Connectivity Service and throughout the Term, the Contractor shall, acting expeditiously:

(i) accept the novation or assignment of one (1) or more commercial contracts for commercial telecoms services;

(ii) enter into one (1) or more commercial contracts for commercial telecoms services, on terms previously agreed by the Contractor with the Customer Authority; and

(iii) procure changes to the services received under such commercial contracts identified in paragraphs (i) and (ii) above,

as required by the Customer Authority from time to time (each such contract, and any other contract identified as such by the Customer Authority, being a "**Commercial Telecoms Contract**").

7.2.2 Subject to Paragraph 7.2.3 below, the Contractor shall proactively manage each Commercial Telecoms Contract, using its best endeavours to ensure that the Customer Authority obtains the full benefit of such Commercial Telecoms Contract in accordance with the terms and conditions of such Commercial Telecoms Contract (including any service levels). In particular, the Contractor shall:

(i) liaise with, and manage, the counterparties to the Commercial Telecoms Contracts, in accordance with the terms and conditions of the Commercial Telecoms Contracts;

(ii) provide to the Customer Authority promptly any reports it receives on the performance of the services under each Commercial Telecoms Contract;

(iii) advise the Customer Authority of the steps to be taken to avoid or mitigate:

(a) any event of which the Contractor is aware (or ought reasonably to be aware) which may significantly adversely affect the performance of a Commercial Telecoms Contract; and

(b) any defect in the service provided under a Commercial Telecoms Contract;

(iv) work with counterparties to Commercial Telecoms Contracts to resolve faults arising in connection with services provided under those Commercial Telecoms Contracts; and

(v) as required by the Customer Authority from time to time, integrate the services provided under the Commercial Telecoms Contracts with the infrastructure used to provide the Services (other than the Miscellaneous Connectivity Service).

7.2.3 Where:

(i) the Customer Authority has identified a contract as a Commercial Telecoms Contract; and

(ii) the Contractor is not a party to that Commercial Telecoms Contract,

the Contractor shall comply with Paragraph 7.2.2 above to the extent possible, and shall immediately notify the Customer Authority of any inability to perform the obligations set out in Paragraph 7.2.2 above, including notifying the Customer Authority of any refusal by a counterparty to the relevant Commercial Telecoms Contract to deal directly with the Contractor.

7.2.4 Where a Commercial Telecoms Contract has been assigned or novated to the Contractor, or the Contractor is otherwise a party to that Commercial Telecoms Contract, each of the counterparties to the Commercial Telecoms Contract shall be a Sub-contractor and such Commercial Telecoms Contract shall be a Transferring Contract.

7.3 MACs

There are no MACs associated with the Miscellaneous Connectivity Service.

8 DNSIP SERVICE

8.1 DNSIP Service Overview

8.1.1 The DNSIP Service is critical to the operation of the Services and the Contractor shall deliver and integrate the DNSIP Service with the Services.

8.1.2 The Contractor shall deliver the DNSIP Service in compliance with the Standards (including *JSP 604 v.4.1 Leaflet 2105 (DNS), Leaflet 2106 (IPv4) and Leaflet 2107 (IPv6)*).

8.1.3 The Contractor shall ensure that all Services that use IP route IP Packets to reachable destinations. Such destinations may include gateways to other networks and End User sub-networks such as any directly connected LANs, including any LANs which are provided as part of the LAN Service as well as any LANs which are outside the scope of the LAN Service.

8.1.4 The Contractor shall manage the part of the Customer Authority's Class A 25.x.x.x Internet Protocol address range that relates to the Services (as allocated by the Customer Authority to the Contractor for use in connection with the Services from time to time, and known as the "**Managed Address Range**"), and shall also manage the Customer Authority's associated domain name service resolution and query processes. In addition, the Contractor shall ensure that the DNSIP Service will:

(i) enable any-to-any communications made or received using the Services;

(ii) provide management of all name resolution functions and will adhere to the generic domain name service hierarchical design set out in the Standards, for both internal and external name resolution functions;

(iii) provide a standardised addressing mechanism for IP Address allocation and management that includes dynamic and static address management;

(iv) provide authorised Customer Authority's nominees and authorised Customer Authority Third Parties (on request from time to time) with one (1) or more predefined globally unique address spaces to allocate IP Addresses from; and

(v) include responsibility for PSN IP Address and domain name service resolution activities as they apply to the Customer Authority.

8.1.5 The DNSIP Service shall comprise:

(i) Domain Name Service Management; and

(ii) IP Addressing Management,

each as more particularly described in Paragraphs 8.2 and 8.3 below (and which together shall be known as the "**DNSIP Capability**").

DNSIP Capability

8.2 Domain Name Service Management

8.2.1 The Contractor shall:

(i) deliver a root domain name service management function;

(ii) provide domain name to IP Address resolution for any end systems connecting via the Services;

(iii) allow authorised Customer Authority's nominees and authorised Customer Authority Third Parties to order domain name registrations and cessations from time to time, which the Contractor shall fulfil; and

(iv) ensure that domain name information changes within a Subnet may only be ordered by the Registered Owner or their authorised representative for that Subnet, and change such domain name information as required by the relevant Registered Owner from time to time.

8.2.2 In providing Domain Name Service Management (including the items referred to in Paragraph 8.2.1 above), the Contractor shall:

(i) provide Domain Name Service Management using Assets located at no less than two (2) geographically diverse locations so as to ensure that there is no single point of failure across both locations for the purposes of Business Continuity and Disaster Recovery purposes; and

(ii) ensure the BCDR Plan (and the design and implementation of the Domain Name Service Management) provides for seamless continuity, so that if assets used to provide such management at one location fail, Domain Name Service Management is immediately provided from assets located at the second location.

8.2.3 The Contractor shall ensure that the Domain Name Service Management is capable of supporting *Internet Protocol version 6 and Domain Name System Security Extensions* (each as specified by the Internet Engineering Task Force (or any successor body)).

8.3 IP Addressing Management

8.3.1 The Contractor shall:

(i) provide IP Addressing Management, including providing and carrying out all activities connected with (and assuming responsibility for) the allocation of:

(a) IP Addresses for internal network management and configuration;

(b) IP Address ranges requested by Registered Owners. The Contractor shall ensure that it provides and manages IP Address ranges from time to time in accordance with any:

(I) specifications that a Registered Owner notifies that Contractor of in relation to his or her IP Address requirements;

(II) request by a Registered Owner to expand a Subnet;

(III) instruction from a Registered Owner to cease one (1) or more specified IP Address(es) that are no longer required; and

(IV) request by a Registered Owner to change an IP Address within a Subnet. The Contractor shall not comply with any instruction to change an IP Address within a Subnet from anyone other than the relevant Registered Owner; and

(c) IP Address ranges for Indirect Customers that are separate from those allocated to the Customer Authority;

(ii) allow each Registered Owner or their authorised representative(s) to view or change (or both) rights to that Registered Owner's name and IP Address allocation;

(iii) provide a Connectivity Service IP Addressing Management function for other networks suitably accredited in accordance with the Standards to transfer information to the Customer Authority at the same Security Classification as the relevant Service, and that accepts and routes IP Addresses from within the 25.x.x.x and 51.x.x.x ranges, and any other authorised ranges that are external to the Managed Address Range (as such other authorised ranges are notified by the Customer Authority to the Contractor from time to time);

(iv) support static routing (i.e. the ability for a Customer Authority's nominee to manually configure network routers with all of the information necessary for successful packet forwarding);

(v) put in place measures designed to ensure that there is no overlapping address space from time to time (and resolve any issues with any address space that is found to be overlapping in consultation with the Customer Authority); and

(vi) maintain a database that records the allocation of:

(a) all IP Addresses used in relation to the Connectivity Services; and

(b) all other IP Addresses associated with other sub-networks within the IP Address range 25.X.X.X, where such addresses are associated with a device using the Services,

and make that database available for inspection by the Customer Authority through the Management Information Exchange.

8.3.2 On request by the Customer Authority from time to time, the Contractor shall provide Dynamic Host Configuration Protocol support for devices identified to the Contractor by the Customer Authority ("**DHCP**"). Such support shall include the provision by the Contractor of dynamic IP Address assignment for such devices, including via a network protocol through which such devices can be connected to the Customer Authority's network (so that they can communicate on that network using IP).

8.3.3 On request by the Customer Authority from time to time, the Contractor shall provide DHCP IP helper function support ("**DHCP IP Helper**") for devices identified to the Contractor by the Customer Authority. The Contractor shall configure the DHCP IP Helper in accordance with the Customer Authority's instructions from time to time.

8.3.4 The Contractor shall:

(i) manage and plan address re-allocations, as well as migrations between address ranges, that the Customer Authority requires from time to time; and

(ii) manage the subnetting of the networks used to deliver the Services in a controlled and structured way, so that structured subnetting is maintained.

8.3.5 The Contractor shall support network address translation as directed (but only as, and to the extent, directed) by the Customer Authority from time to time.

8.3.6 The Contractor shall be responsible for PSN IP Address and domain name service resolution activities as directed by the PSNA.

8.4 MACs

There are no MACs associated with the DNSIP Service.

9 ENCRYPTION SERVICE

9.1 Encryption Service Overview

The Contractor shall provide the Encryption Service. The Encryption Service consists of the supply, handling, installation, commissioning, support, maintenance and management by the Contractor of all encryption (including cryptographic devices and encryption key materials (KEYMAT)) required for the delivery of the Services (including any Service Elements) from time to time in accordance with the Standards and the requirements of this Consolidated Contract.

9.2 Core Encryption Service Requirements

9.2.1 In providing the Encryption Service, the Contractor shall ensure that:

(i) each of the Connectivity Service, PPS, LAN Service and BPS (including any Service Element relating to any such Service) is designed, implemented and delivered with such appropriate encryption and other security techniques as may be required from time to time to ensure that the infrastructure used in the delivery of such Service supports the transfer and handling of information at the Security Classification levels required for that Service (as such Security Classification levels are more particularly set out in this Consolidated Contract (including in the description for such Service set out in this Consolidated Schedule)). The Encryption Service forms an

inherent part of the successful delivery of each of the Connectivity Service, PPS, LAN Service and BPS;

(ii) for Migrated Services only, the minimum encryption standard for all data traffic associated with any of the Services is the CESG full PRIME profile for PSN (also known as the "end state" profile under PSN), as described in the *PSN: Cryptographic Framework* (Version 1.0) that forms part of the Standards;

(iii) it supports the Customer Authority's requirement described in Paragraph 5 of this Consolidated Schedule to establish Communities of Interest through the use of cryptographic separation from time to time;

(iv) the Encryption Service (and all other Services) are implemented so that the Customer Authority has cryptographic access (i.e. access to the encrypted side of any cryptographic device, known within the Customer Authority as the 'black side') from time to time in order to conduct remote electronic key management, updating and monitoring of cryptographic devices;

(v) any cryptographic devices used in the delivery of the Services do not negatively impact the use of the Services or the performance of the Services in accordance with the Service Levels, including in accordance with the requirements for the different PSN Service Classes;

(vi) the Contractor confirms to the Customer Authority (on request from time to time and in any event within thirty (30) Working Days of receiving such request) what cryptographic devices are being used in the delivery of the Services and what the specification for each of such devices is, including its maximum transmission unit (MTU) overhead size;

(vii) any cryptographic device introduced into the infrastructure used in the provision of the Services is interoperable with such infrastructure, as well as any other encryption services offered by the Contractor to support the transfer and handling of information at the same information classification level as is being supported by that cryptographic device;

(viii) it uses the relevant Customer Authority catalogue, or alternative acquisition method as directed by the Customer Authority from time to time, and any associated procedures (once each has been made available) relating to all cryptographic devices and encryption key material;

(ix) the Contractor and its Sub-contractors are able to handle the Customer Authority's Classified Information and that they have been Certified in accordance with the Standards prior to handling any such Classified Information. The Contractor understands that the cryptographic access requirement referred to in Paragraph (iv) above is required within the Customer Authority's risk environment and is subject to all the generic risks identified in CESG Good Practice Guide No.23, entitled *Assessing the Threat of Technical Attack against Information and Communications Technology Systems*;

(x) the Encryption Service uses CESG pre-approved authentication and revocation processes; and

(xi) the Encryption Service uses CESG pre-approved internet protocol security profiles.

9.2.2 The Contractor shall comply with, and shall ensure that the Encryption Service is provided so as to comply with, the Customer Authority's policy describing the Standards relevant to the Encryption Service (as set out in *JSP 490*), except to the extent the Customer Authority has previously (acting in its sole discretion) and expressly waived in writing (such form of writing to refer to this Paragraph 9.2.2) a relevant *JSP 490* requirement.

9.3 Crypto Custodian Service

9.3.1 As requested by the Customer Authority from time to time, the Contractor shall provide cryptographic custodian services in respect of the Services and the IUS Tower services at a Customer Authority Site notified to the Contractor by the Customer Authority, including holding cryptographic materials securely, in accordance with the full range of responsibilities set out in the *JSP 490 Defence Cryptosecurity Operating Instructions* (as amended from time to time) (the "**Crypto Custodian Service**").

9.3.2 In providing the Crypto Custodian Service, the Contractor shall comply at all times with the relevant audit, accounting and reporting requirements described in the Standards.

9.4 MACs

There are no MACs associated with the Encryption Service.

10 BPS

10.1 BPS Overview

10.1.1 In providing the BPS, the Contractor shall provide resilient, geographically separate, load balanced boundary protection gateways or interconnections that are designed to protect the integrity and security of the Connectivity Service, as more particularly described in this Paragraph 10.

10.1.2 The Contractor shall control End User access to the Gateways through the use of accounts that the Contractor shall issue (each a "**BPS Account**", as more particularly described in Paragraph 10.4 below) to those persons that the Customer Authority has authorised from time to time to access the Connectivity Service (each a "**BPS User**"). Such BPS Users may include Customer Authority personnel, personnel of Indirect Customers or Industry Customers or other Government Departments.

10.1.3 A BPS Account may be a:

(i) BPS User Account;

(ii) BPS Business Server Gateway Account;

(iii) BPS Remote Access User Account;

(iv) BPS Industry/OGD Account; or

(v) BPS Gateway Reverse Web Proxy Account,

each as more particularly described in Paragraph 10.4 below.

10.1.4 The Contractor shall ensure that the BPS enables communications and access carried out using the Services to be progressed and completed in accordance with the specific information exchange requirements notified to the Contractor by the Customer Authority from time to time for each of the Connectivity Subscriber Domains. This includes any communications facilitating the exchange of information with external parties, including any industry partners and Customer Authority Third Parties, as well as access via the Services to other resources and capabilities such as the Internet, PSN and collaborative working environments.

10.1.5 The Contractor shall schedule maintenance of the BPS outside the Customer Authority's Working Hours.

10.2 OFFICIAL BPS Capability

10.2.1 On request from the Customer Authority from time to time, the Contractor shall:

(i) provide individual gateways that concurrently provide/support connectivity between the Connectivity Service and certain trusted, untrusted and hostile networks (each being known as a "**Gateway**"); and

(ii) provide remote access to the Network Infrastructure for BPS Users using an external network (for example, using the internet and public switched telephone network) as a communications bearer, such access being known as "**Remote Access**"; and

(iii) provide secure interfaces between the OFFICIAL Connectivity Service and individual OFFICIAL Connections to Indirect Customers, including Industry Customers, as provided by the Contractor in accordance with the requirements of Paragraph 5 of this Consolidated Schedule, from time to time (each such secure interface being an "**OFFICIAL Secure Interface**").

Gateways

10.2.2 On request from the Customer Authority from time to time, the Contractor shall provide Gateways that:

(i) support web browsing and cross-Government email exchange (for both emails that are protectively marked as OFFICIAL or OFFICIAL-SENSITIVE and those without protective marking) for BPS Users through separate gateways to:

(a) the Public Service Network and Government Secure Intranet (the "**PSN/GSI Capability**"); and

(b) the National Health Service N3 service (and any successor(s) to such a service) (the "**N3 Capability**"); and

(ii) support web services and email exchange accessible by the general public and other Government Departments through a gateway to the public internet (the "**Internet Capability**").

10.2.3 In providing and managing the Gateways, the Contractor shall ensure that it provides such assistance to the Customer Authority's Computer Emergency Response Team as is required by the Customer Authority from time to time. Such

assistance may include providing information regarding BPS Account configurations, undertaking transaction log investigations, providing visibility of Gateway configurations and providing details of email attachments.

10.2.4 The Contractor shall ensure that the Gateways, in accordance with Good Industry Practice:

(i) employ a sanction release mechanism requiring BPS Users to verify that an email sent to the Internet does not contain protectively marked information;

(ii) enable BPS Users to send secure/multipurpose internet mail extensions in an encrypted form and signed 'not protectively marked' via email over the Internet;

(iii) enable the encryption of email attachments by any BPS Users that are listed by the Customer Authority in any white lists provided and updated by the Customer Authority from time to time;

(iv) block BPS User access to specified URLs that are listed by the Customer Authority in any black lists provided and updated by the Customer Authority from time to time;

(v) employ techniques to minimise Internet traffic and web content inspection (for example, caching of popular URLs), to make the most efficient use of the bandwidth that the Customer Authority is receiving as part of the Services, in particular so as to ensure that Connections to Overseas Connectivity Subscriber Domains achieve the relevant Service Levels;

(vi) provide a Government Secure Intranet reverse web proxy service to support authorised users on systems connected to the Government Secure Intranet;

(vii) employ anti-spam measures, including measures to filter unsolicited emails sent to the Customer Authority. The Contractor shall ensure that emails identified as being unsolicited are quarantined (i.e. do not appear in the relevant BPS User's inbox, but are available for inspection by the Customer Authority). The Contractor shall ensure that each quarantined email shall be retained, and shall be capable of being viewed by the Customer Authority's nominee(s), for a period not exceeding one (1) month;

(viii) employ anti-virus protection measures, including through scanning incoming web attachments for viruses using two (2) different anti-virus providers; and

(ix) have resilient connection to an internet service provider's core network.

10.2.5 The Contractor shall keep a record of any Gateway, inbound and outbound activity reports which the Contractor shall:

(i) make available to the Customer Authority on a monthly basis; and

(ii) retain for a period of two (2) years.

10.2.6 In providing and managing the Gateways, the Contractor shall:

(i) advise the Customer Authority of suitable capacity and performance levels for the Gateways (including as to whether more capacity is required, for example because usage has increased) and implement the capacity and performance levels required by the Customer Authority from time to time;

(ii) where relevant and permitted, maintain the ability for Domain Name Service Management to function and interwork between Security Classification levels whilst providing inspection or validation of Domain Name Service Management protocols passing between Security Classification levels and is applicable to transparent continuation of IP routing information across the Gateways;

(iii) ensure that the Customer Authority is made aware of, and complies with, the relevant codes of connection of any external networks that the Customer Authority requires to connect to any Gateway;

(iv) ensure that up-to-date security configuration information (for example, protocols, firewall policies, access controls, change history, etc.) of individual Gateways is available for review by the Customer Authority via the Management Information Exchange. Access to this information should only be made available to specified personnel identified and authorised by the Customer Authority; and

(v) where:

(a) the Contractor reasonably believes, or reasonably ought to have believed, that the security of the Network Infrastructure has been (or is likely to be) threatened or compromised; and

(b) the Customer Authority directs the Contractor to do so,

immediately disconnect the relevant source of the security threat identified in (a) above from the relevant Gateway(s) and report such withdrawal and the reasons for it in accordance with the relevant reporting requirements set out in *JSP 541* as set out in the Standards.

10.2.7 The Contractor shall, from time to time at the Customer Authority's request, upgrade or downgrade the bandwidth for the gateway to the public internet provided as part of the Internet Capability, such upgrades to be made within the upper and lower bandwidth limits proposed by the Contractor as part of the Contractor's Response to ITQ and Approved by the Customer Authority (with any subsequent changes to such Approved upper and lower limits being subject to agreement in writing by the Parties, such form of writing to refer to this Paragraph 10.2.7).

Remote Access

10.2.8 On request from the Customer Authority from time to time, the Contractor shall:

(i) provide a Remote Access gateway for BPS Users that require access to applications hosted on the Services and Network Infrastructure remotely from any point in the UK or overseas ("**Remote Access Gateway**") and ensure that the Remote Access Gateway:

(a) is accessible through a range of connectivity types, including public switched telephone network dial-up, mobile data (including WiFi, GPRS, 3G and 4G technologies) as well as DSL (broadband) services; and

(b) supports a contention ratio (i.e. the ratio of the potential maximum demand to the actual bandwidth) of 8:1 without constraint or six thousand (6,000) broadband sessions, where a session is assumed to equal one (1) BPS User access;

(ii) provide the BPS User and their system integrator with all relevant operating instructions for the Remote Access Gateways;

(iii) manage BPS User configuration requirements, including IP Address allocation, port sizing and contention ratio reviews;

(iv) manage the process for providing BPS Remote Access User Accounts security token replacement (if provided), security token theft or loss reporting, annual and emergency cryptographic key change, client software and firmware change and fault/incident reporting with the integrators of Customer Authority Third Parties; and

(v) provide a Remote Access Gateway test facility that:

(a) enables testing before live release of any cryptographic key changes (the scheduled change being annually and known as the cryptographic key date);

(b) enables testing before live release of any Remote Access platform software patches and system testing; and

(c) is available to authorised Customer Authority Third Parties as requested by the Customer Authority from time to time to enable them to perform integration testing with the BPS,

such activities in this Paragraph 10.2.8 being known as the "**Remote Access Capability**".

Secure Interfaces

10.2.9 In order to provide controlled access for Indirect Customers (including Industry Customers) to any network services provided by the Customer Authority and the Customer Authority Third Parties, including the use of e-commerce, human resource and corporate applications and collaborative working environments (CWEs) such as whiteboarding and chat sessions, the Contractor shall (on request by the Customer Authority) provide OFFICIAL Secure Interfaces which shall:

(i) only permit the use of Layer 4 protocols that have been authorised by the Customer Authority; and

(ii) permit the use of any additional protocols that the Customer Authority may require the OFFICIAL Secure Interfaces to support from time to time.

10.3 SECRET BPS Capability

Secure Interfaces

10.3.1 In order to provide controlled access to any network services provided by the Customer Authority and the Customer Authority Third Parties, including the use of e-commerce, human resource and corporate applications and collaborative working environments (CWEs) such as whiteboarding and chat sessions, the Contractor shall provide a secure interface between the SECRET Connectivity Service and individual SECRET Connections, as provided by the Contractor in accordance with the requirements of Paragraph 5 of this Consolidated Schedule to Indirect Customers (including Industry Customers) from time to time (each such secure interface being known as a "**SECRET Secure Interface**").

10.3.2 The Contractor shall ensure that the SECRET Secure Interface shall:

(i) only permit the use of Layer 4 protocols that have been authorised by the Customer Authority; and

(ii) permit the use of any additional protocols that the Customer Authority may require the SECRET Secure Interface to support from time to time.

10.4 BPS Accounts

10.4.1 On request from the Customer Authority from time to time, the Contractor shall:

(i) provide and manage the BPS Accounts in the Connectivity Subscriber Domains or blocks of BPS Accounts, including accounts which control access to the BPS for the following:

(a) BPS Users, such accounts being known as "**BPS User Accounts**". The Contractor shall provide BPS User Accounts that support both primary and secondary email addresses that are associated with BPS Users;

(b) individual Customer Authority Third Party application servers or email servers, such accounts being known as "**BPS Business Server Gateway Accounts**";

(c) BPS Users accessing the Network Infrastructure remotely, such accounts being known as "**BPS Remote Access User Accounts**";

(d) Industry Customers or other Government Departments, such accounts being known as "**BPS Industry/OGD Accounts**"; and

(e) BPS Users connected to the Government Secure Intranet that require access to Customer Authority specified web-based services, such accounts being known as "**BPS Gateway Reverse Web Proxy Accounts**"; and

(ii) ensure that it only activates a BPS User Account after the relevant BPS User has read and agreed to comply with the BPS security operating procedures produced by the Contractor as part of the documentation submitted to achieve Certification (the "**SyOPs**").

10.4.2 As part of the Contractor's management of the BPS Accounts, the Contractor shall:

(i) change BPS User details of any of the BPS Accounts; and

(ii) cease any of the BPS Accounts and reallocate the relevant BPS Account to a new BPS User,

as requested by the Customer Authority from time to time.

10.5 MACs

There are no MACs associated with the BPS.

11 LAN SERVICE

11.1 LAN Service Overview

11.1.1 In providing the LAN Service, the Contractor shall:

(i) provide the Managed Data LAN Service;

(ii) provide the Voice Cabling Service; and

(iii) carry out certain MACs,

each as more particularly described in the remainder of this Paragraph 11.

11.1.2 The Contractor shall, at the Customer Authority's request from time to time, provide the LAN Service to the following subscriber domains:

(i) "**UK**", where the Customer Authority Site to which the Data LAN Connectivity will be provided is (or is to be) located within the UK; and

(ii) "**Overseas**", where the Customer Authority Site to which the Data LAN Connectivity will be provided is (or is to be) located outside the UK,

(each a "**LAN Subscriber Domain**").

11.1.3 The Contractor shall provide the Customer Authority with OFFICIAL, SECRET and TOP SECRET LAN Services in the LAN Subscriber Domains, as required by the Customer Authority from time to time.

11.2 Managed Data LAN Service

The Contractor shall:

11.2.1 provide, install, support, maintain and commission, as applicable, passive and active wired and wireless local area network infrastructure to provide the Data LAN Connectivity to Customer Authority Sites, as set out in the Service Evaluation Model and set out in the recompetition data provided by the Outgoing Service Provider. Such infrastructure, together with any updates or amendments made to it from time to time, shall be known as the "**Data LAN Infrastructure**";

11.2.2 provide, install, support, maintain and commission from time to time the cabling, connectors and any other equipment required to provide Data LAN Connectivity to a Data Device;

11.2.3 ensure that the Data LAN Infrastructure (whether or not already commissioned as at the Operational Service Commencement Date for the LAN Service) is designed, operated, maintained, supported and managed from time to time to ensure that Data Devices located at the relevant Customer Authority Site are capable of sending, transporting and receiving traffic (including voice, video and data) as a stream of data packets using IP technology to, from and between other Data Ports and the Connections provided as part of the Connectivity Service when connected

to the Data LAN Infrastructure ("**Data LAN Connectivity**"). As at the Effective Date, the Data LAN Infrastructure will include some microwave links;

11.2.4 in the case of Data LAN Connectivity that is delivered wirelessly and which is needed to support BPS Users that require access to applications hosted on the Services and Network Infrastructure, ensure that Data Devices can connect through Wireless Access Points, via the Remote Access Gateway to gain access to applications ("**Wireless RA LAN Service**");

11.2.5 in the case of Data LAN Connectivity that is delivered wirelessly and which is needed to support any Users that only require access to the Internet, ensure that Data Devices can connect through Wireless Access Points via an appropriate internet gateway to gain access to the Internet ("**Wireless LAN Service**");

11.2.6 ensure that traffic (including voice, video and data) is managed in conformance with the six (6) PSN Service Classes described in Paragraph 5.2.4 of this Consolidated Schedule in the case of wired infrastructure (except, during the period before the Managed Data LAN Service is Migrated, Legacy Equipment that cannot support the Managed Data LAN Service) and the four (4) access categories defined in the WMM interoperability extension of the IEE 802.11e standard for wireless in accordance with the Standards;

11.2.7 maintain, support and manage all logical virtual local area networks associated with different IP sub-nets within the Data LAN Infrastructure (each a "**VLAN**"). The Contractor shall ensure that the configuration of any part(s) of the Data LAN Infrastructure (including any relevant CPE and any relevant IP access control lists) that exist as at the Operational Service Commencement Date for the LAN Services are preserved, unless otherwise agreed with the Customer Authority in advance, such configuration may include proprietary configuration such as CISCO VLAN trunking protocol;

11.2.8 carry out any configuration management required for the provision of the Services and act as a system design authority for the Managed Data LAN Service. In acting as a system design authority, the Contractor shall be responsible for ensuring that the Data LAN Infrastructure meets Customer Authority's requirements (as such requirements are set out in this Consolidated Contract) in terms of functionality, performance, capacity, security, safety and ergonomics, including by:

(i) defining the environmental conditions in which the Data LAN Infrastructure will be required to operate, including all lighting, ventilation and power requirements;

(ii) producing and submitting master system design drawings and other relevant documentation to the Customer Authority as required by the Standards;

(iii) identifying and specifying the spares required for testing, commissioning and ongoing support of the Managed Data LAN Service;

(iv) preparing and issuing test plans and procedures and providing supervision during commissioning;

(v) designing modifications to the Data LAN Infrastructure and issuing modification details in the form of drawings or instructions;

(vi) providing and supporting industry standard Data LAN Infrastructure interface types and physical presentations, including (as a minimum) the following:

Interface Type	Physical Presentation	Other aspects of the Interface Types
Ethernet 10/100/1000 Mbit/s	• RJ45 • STII male connector	CAT 5, 5e, 6 UTP – Autosensing full duplex, including options for Power over Ethernet
Ethernet 100 Mbit/s (100base-FX)	• SC • LC • ST	full duplex – multi and single mode fibre
Ethernet Gbit/s (1000base-X) and (10Gbase - ***TBD***)	• SC • LC • ST	full duplex – multi and single mode fibre, distribution including SX, LX and ZX
Ethernet Gbit/s (1000base-T) and (10Gbase-T)	• RJ45	CAT 5, 5e, 6 UTP – Autosensing full duplex
Wireless LAN access point		802.11b/g/n/s
Microwave LAN		As shown in the Service Evaluation Model and set out in the recompetition data provided by Outgoing Service Provider

Table 9 – Managed Data LAN Service – interface types

11.2.9 ensure that any parts of the Data LAN Infrastructure which exist as at the Operational Service Commencement Date for the LAN Service and support the delivery of resilient services to Customer Authority Sites are not removed or replaced without the Customer Authority's prior written consent. Such infrastructure may include:

(i) duplicated core switches;

(ii) redundant switch fabrics, processors and power supplies;

(iii) resilient connections between core switches; and

(iv) resilient connections from core to access switches,

the Services in this Paragraph 11.2 being the "**Managed Data LAN Service**".

11.3 Voice Cabling Service

11.3.1 From time to time, the Customer Authority may notify the Contractor, in accordance with the ISS ITIL Processes, that it is unable to send, transport or receive signals to

or from a Voice Port located on a Customer Authority Site using one or more Voice Cables (each such notification being a "**Voice Break Notification**").

11.3.2 Upon receipt of a Voice Break Notification, the Contractor shall, at the Customer Authority's option from time to time, carry out an investigation and either:

(i) make repairs to the relevant Voice Cables so that the Customer Authority is able to send, transport or receive signals using those Voice Cable(s); or

(ii) carry out an investigation and identify correctly to the Customer Authority that there is no fault with the relevant Voice Cable(s),

(the completion of such investigation, repairs and identification being known as a "**Voice Fix**"). Each Voice Fix shall be carried out by the Contractor in accordance with the ISS ITIL Processes.

11.3.3 For the purposes of this Consolidated Schedule, a "**Voice Cable**" means the cable and connectors connecting a telephone line jack unit (the "**Voice Port**") located on a Customer Authority Site to a test jack frame (i.e. a frame supplied by any of the Customer Authority's private automatic branch exchange (PABX) suppliers from time to time, which provides a connection point for exchange lines and extension ports). Cables that form part of the infrastructure used (whether in whole or in part) to deliver the PPS or any other Service (other than the Voice Cabling Service) shall not be considered to be Voice Cables and shall be maintained by the Contractor in accordance with the requirements for the PPS or other Service, as applicable.

11.3.4 The Contractor shall carry out Voice Fixes in relation to industry standard voice infrastructure interface types and physical presentations, including (as a minimum) the following:

Interface Type	Physical Presentation	Other aspects of the Interface Types
Analogue Voice	• RJ11 • RJ14 • BS 6312	Two (2) wire or four (4) wire
Digital Voice	• RJ11 • RJ14 • BS 6312	ISDN 2e (2B+D) Compliant with ITU-T I.420 (1988)

Table 10 – Managed Data LAN Service – Voice Fixes – interface types

11.4 On-Site Support

Where requested by the Customer Authority in relation to an identified Customer Authority Site from time to time, the Contractor shall provide an on-site engineer at a specified UK Customer Authority Site, either during office hours (Monday to Friday, 8am to 5pm excluding UK bank holidays) or on a twenty-four (24) hours, seven (7) days a week basis to carry out support (including End User support) and maintenance in relation to the Services. Such engineer shall primarily be experienced in the delivery of LAN Services, but shall also be capable of supporting other Services on-site, where required. The activities that an on-site engineer may be required to carry out include:

(a) management of Incidents by telephone or email, including updating of status, action and routing calls to other resolver groups or the Customer Authority's service desk as necessary;

(b) assistance in the diagnosis and resolution of basic network faults involving active and passive components, including cables, switches, media converters, small form-factor pluggables and interface connectors;

(c) component configuration checking;

(d) undertaking general Data LAN Infrastructure maintenance, including ensuring compliance with relevant Standards, including minor rectification actions;

(e) periodically auditing site configuration and requesting toolset updates to correct any inaccuracies in order to maintain accurate configuration records;

(f) receiving and marshalling spares onto the relevant Customer Authority Site in readiness to complete Incident Resolution, moves or changes;

(g) acting as point of contact for other engineering resources (including Customer Authority and Customer Authority Third Party engineering resources) to gain access to the Customer Authority Site and any buildings and cabinets, liaising with such engineer resources on task and actions to date and escorting where necessary; and

(h) assisting and advising the Customer Authority on specific Site and LAN issues relating to proposed changes, including confirming port availability and network capacity,

(the above Services together shall be known as the "**On-Site Support**").

11.5 Berthing Telephony Capability

The Berthing Telephony Capability consists of the provision by the Contractor of at least one (1) member of the Contractor Personnel on-site at HMNB Devonport and HMNB Portsmouth twenty-four (24) hours a day, seven (7) days a week. At the Customer Authority's request from time to time, the Contractor shall ensure and procure that such Contractor Personnel carry out the following activities for ships and submarines docked in the United Kingdom as follows:

(a) in respect of ships or submarines which are part of the British armed forces, prior to that ship or submarine docking in port, the Contractor Personnel shall confirm to the Customer Authority whether:

(i) sufficient umbilical cabling is available at the relevant port for the Contractor to perform its obligations under the remaining provisions of this Paragraph 11.5; and

(ii) the relevant cabling is in good working condition or is in need of repair;

(b) in respect of all ships and submarines, the Contractor Personnel shall assist in the connection or disconnection of each relevant ship's or submarine's telephony infrastructure to a shore side junction box or other end point identified for such purpose to the Contractor by the Customer Authority, using:

(i) in the case of ships or submarines which are part of the British armed forces, umbilical cabling carrying multiple services (for example, voice, data or TV, as required by the Customer Authority); and

(ii) in the case of all other ships and submarines, a telephony cable or cables; and

(c) in respect of ships or submarines that the Customer Authority wishes to benefit from a fixed voice service:

(i) ensure that the cabling connected to the shore side junction box or other end point is patched and configured to ensure the correct operation of such fixed voice service; and

(ii) prior to that ship or submarine docking in port, test the relevant shore side junction box or other end point and confirm to the Customer Authority whether such box or end point is correctly configured.

11.6 LAN Service MACs

11.6.1 On request by the Customer Authority from time to time, the Contractor shall carry out the types of MACs shown in Table 11 below (each a "**LAN Service MAC**").

11.6.2 The activities to be carried out by the Contractor in respect of each LAN Service MAC shall include any Site attendance, removal, de-installation, de-commissioning, configuration and administrative work required as a result of such LAN Service MAC, including equipment removal, configuration and amendments to the information available through the Management Information Exchange, testing to ensure the LAN Service MAC is compliant with this LAN Service, documentation of the LAN Service MAC in accordance with the Standards and communication to the Customer Authority of activity completion by email or telephone, as appropriate.

11.6.3 The Contractor shall obtain all necessary MAC Approvals in accordance with the Standards prior to commencement of work for any of the LAN Service MACs, unless otherwise directed by the Customer Authority.

11.6.4 For the purposes of the installation LAN Service MACs in Table 11 below, a Data Port includes the installation of the Data LAN Infrastructure between the access switch and the floor or wall outlet.

11.6.5 For the purposes of the installation LAN Service MACs in Table 11 below, the installation of a Voice Port is identical to the installation of a Data Port, except that the testing required is limited to testing the continuity of the Voice Cable as part of the activities required in relation to the implementation of the LAN Service MAC.

MAC	Non-exhaustive list of activities included within MAC
Remote/soft change	• All preparatory work, including design activities and acting as system design authority (as described in Paragraph 11.2.8 above) in validating a remote change requested by the Customer Authority (i.e. a change that is possible within the capability of the existing equipment and can be completed remotely without a change in hardware), for example changing the structure of a VLAN or a change to spanning tree configuration; • remote work to complete the change requested by the Customer

MAC	Non-exhaustive list of activities included within MAC
	Authority; and • any other activity required to signal completion of, and to document and test, the MAC in accordance with the Standards.
Small move or addition of a Data Device or Voice Device	• All preparatory work, including a Site survey (if required), design activities and any other activities required to ensure that there is the necessary capacity to accommodate the move or change of a Data Device or Voice Device as requested by the Customer Authority (such move or addition not to require additional Data LAN Infrastructure other than patch cables/fly leads); • carry out any MAC Approval Activities; • once any MAC Approvals have been obtained, completion of the move or addition of the relevant Data Device or Voice Device to or at the desired location and physical connection to the intended Data Port (including the provision of any necessary patch cables or fly leads, activation of the newly connected Data Port and (where relevant) de-activation of the previously used Data Port and (in all cases) testing of the Connectivity to the Data Device or Voice Device at its new location); and • any other activity required to signal completion of, and to document and test, the MAC in accordance with the Standards.
Install new Data Port or Voice Port into a floor unit using existing containment infrastructure – UTP	• All preparatory work, including a Site survey (if required) and design activities. Site survey to include an assessment of the availability of spare ports on network access switches; • carry out any MAC Approval Activities; • once any MAC Approvals have been obtained, removal of any redundant cable, or bundle of cables, necessary to allow space for new cabling; • installation of cable into existing containment infrastructure; • installation, and termination, if required, of an RJ-Series connector, Voice Port or socket onto a cable; • installation of new fittings in existing floor box, or removal and replacement of existing floor box and fittings, or installation of new floor box and fittings into false floor; • carry out any necessary patching on the network access switch or patch panel (or both); • where a Data Port is being installed, testing the Data Port to ensure that any subsequent connection of a Data Device to that Data Port is capable of sending, transporting and receiving data traffic; or where a Voice Port is being installed, testing the Voice Port to ensure that it has been installed correctly; and • any other activity required to signal completion of, and to document and test, the MAC in accordance with the Standards.

MAC	Non-exhaustive list of activities included within MAC
Install new Data Port or Voice Port into a wall outlet using existing containment infrastructure – UTP	• All preparatory work, including a Site survey (if required) and design activities. Site survey to include an assessment of the availability of spare ports on network access switches; • carry out any MAC Approval Activities; • once any MAC Approvals have been obtained, removal of any redundant cable, or bundle of cables, necessary to allow space for new cabling; • installation of cable into existing containment infrastructure; • installation, and termination if required, of an RJ-Series connector, Voice Port or socket onto a cable; • installation of new fittings in existing wall outlet enclosure; or removal and replacement of existing wall outlet enclosure and fittings; or installation of new wall outlet enclosure and fittings; • carry out any necessary patching on the network access switch or patch panel (or both); • where a Data Port is being installed, testing the Data Port to ensure that on any subsequent connection the Data Device is capable of sending, transporting and receiving data traffic; or where a Voice Port is being installed, testing the Voice Port to ensure that it has been installed correctly; and • any other activity required to signal completion of, and to document and test, the MAC in accordance with the Standards.
Install new Data Port into a floor unit using existing containment infrastructure - Fibre	• All preparatory work, including a Site survey (if required) and design activities. Site survey to include an assessment of the availability of spare ports on network access switches; • carry out any MAC Approval Activities; • once any MAC Approvals have been obtained, removal of any redundant cable or a bundle of cables necessary to allow space for new cabling; • installation of cable into existing containment infrastructure; • installation, and termination, if required, of an ST, LC or SC fibre optic connector onto a cable; • installation of new fittings in existing floor box, or removal and replacement of existing floor box and fittings, or installation of new floor box and fittings into false floor; • carry out any necessary patching on the network access switch or patch panel (or both); • testing of the new Data Port to ensure that any subsequent connection of a Data Device to that Data Port is capable of sending, transporting and receiving data traffic; and • any other activity required to signal completion of, and to document and test, the MAC in accordance with the Standards.

MAC	Non-exhaustive list of activities included within MAC
Install new Data Port into a wall outlet using existing containment infrastructure - Fibre	• All preparatory work, including a Site survey (if required) and design activities. Site survey to include an assessment of the availability of spare ports on network access switches; • carry out any MAC Approval Activities; • once any MAC Approvals have been obtained, removal of any redundant cable or a bundle of cables necessary to allow space for new cabling; • installation of cable into existing containment infrastructure; • installation, and termination if required, of an ST, LC or SC Fibre optic connector onto a cable; • install new fittings in existing wall outlet enclosure; or remove and replace existing wall outlet enclosure and fittings; or install new wall outlet enclosure and fittings; • carry out any necessary patching on the network access switch or patch panel (or both); • testing of the new Data Port to ensure that any subsequent connection of a Data Device to that Data Port is capable of sending, transporting and receiving data traffic; and • any other activity required to signal completion of, and to document and test, the MAC in accordance with the Standards.
Complex MAC requiring visit	• All preparatory work, including a Site survey (if required) and design activities, and production of a costed proposal for the work involved; • carry out any MAC Approval Activities; • once any MAC Approvals have been obtained, install structured cabling to ensure the connection of the relevant network access points, distribution frames, line drivers, patch panels and CPE (as required by the Customer Authority); and • any other activity required to signal completion of, and to document and test, the MAC in accordance with the Standards.
Fibre Optic Line Extender (FOLE) and Fibre Optic Line Driver (FOLD)	• All preparatory work, including a Site survey (if required) and design activities; • carry out any MAC Approval Activities; • once any MAC Approvals have been obtained, carry out removal or replacement of FOLE/FOLD equipment (excluding any cabling), including any obligations relating to the management of the Spares Pool set out in Paragraphs 3.14 to 3.16 (inclusive) of this Consolidated Schedule; and • any other activity required to signal completion of, and to document and test, the MAC in accordance with the Standards.
Remote/soft cease	• Remote work to cease a Data Port, where no removal of equipment is required (whether to maintain remaining Services or otherwise); and • any other activity required to signal completion of, and to document

MAC	Non-exhaustive list of activities included within MAC
	and test, the MAC in accordance with the Standards.
Cease – engineer visit required	• All preparatory work, including a Site survey (if required) and design activities; • carry out any MAC Approval Activities; • once any MAC Approvals have been obtained, all work necessary to de-commission, de-install and remove the Data Port and all associated hardware in accordance with Paragraphs 3.14 to 3.16 (inclusive) of this Consolidated Schedule, while ensuring that any remaining Services are maintained; and • any other activity required to signal completion of, and to document and test, the MAC in accordance with the Standards.
Complex cease	• All preparatory work, including a Site survey (if required) to scope the proposed cease and production of a costed proposal for the work involved; • carry out any MAC Approval Activities; • once any MAC Approvals have been obtained, all work necessary to cease the relevant Data Port; and • any other activity required to signal completion of, and to document and test, the MAC in accordance with the Standards.
UPS Install	• All preparatory work, including a Site survey (if required) and design activities; • carry out any MAC Approval Activities; • once any MAC Approvals have been obtained, all work necessary to provide UPS equipment, including any necessary configuration with associated devices attached to the UPS equipment and standby power generation facilities; and • any other activity required to signal completion of, and to document and test, the MAC in accordance with the Standards.
UPS Fix	• All preparatory work, including a Site survey (if required) and design activities; • carry out any MAC Approval Activities; • once any MAC Approvals have been obtained, all work necessary to fix UPS equipment at the Customer Authority's request, including any necessary configuration to associated devices attached to the UPS equipment and standby power generation facilities; and • any other activity required to signal completion of, and to document and test, the MAC in accordance with the Standards.
UPS Move per single Data Device	• All preparatory work, including a Site survey (if required) and design activities; • carry out any MAC Approval Activities; • once any MAC Approvals have been obtained, all work necessary to move UPS equipment, including any necessary configuration to

MAC	Non-exhaustive list of activities included within MAC
	associated devices attached to the UPS equipment and standby power generation facilities; and • any other activity required to signal completion of, and to document and test, the MAC in accordance with the Standards.
Miscellaneous Wiring Maintenance – first fix	• Act as a resolver group for the simple fix of faults reported for other site wiring (including any local area networks that are outside the scope of the LAN Service), lifts, alarms, security and CCTV or other maintenance tasking; • fault-find and fix any wiring faults or perform the requested maintenance task and any other activity required to signal completion of, and to document and test, the MAC in accordance with the Standards; or • in the event that no fault is identified by the Contractor or the maintenance task cannot be completed, notify the Customer Authority that no resolution is possible under this MAC, in accordance with the ISS ITIL Processes. All work in relation to this MAC shall be capped at four (4) hours on-site.
Miscellaneous Wiring Maintenance – extended fix	Where the Customer Authority determines that a first fix is likely to require more than four (4) hours' work on-site: • act as a resolver group for the simple fix of faults reported for other site wiring, including lifts, alarms, security and CCTV; • fault-find and fix any wiring faults and any other activity required to signal completion of, and to document and test, the MAC in accordance with the Standards; or • in the event that no fault is identified by the Contractor, notify the Customer Authority that no fix is possible under this MAC, in accordance with the ISS ITIL Processes.
Basic Inspection – physical infrastructure and electrical safety	• All preparatory work, including a Site survey (if required); • carry out any MAC Approval Activities; • once any MAC Approvals have been obtained, all work necessary to carry out such basic inspection of physical infrastructure and electrical safety; • inspect and report on the status of physical LAN containments, pits, ducts poles and catenaries; or • electrical safety testing to support health and safety related tasks such as earthing of cabinets; and • production of documentation or reports and other activities to signal completion of the MAC in accordance with the Standards. All work shall be capped at four (4) hours on-site.
Addition of new switch capacity	• All preparatory work, including a Site survey (if required) and design activities; • carry out any MAC Approval Activities;

MAC	Non-exhaustive list of activities included within MAC
	• once any MAC Approvals have been obtained, removal of the existing network switch(es) if being replaced; • installation of new network switch(es) into existing racking; • carry out any necessary configuration and patching on the installed network switch(es); • testing of the new network switch(es) and any other equipment impacted by this MAC to ensure that existing Data LAN Connectivity is unaffected and any subsequent connection of a Data Device supported by the new switch(es) is capable of sending, transporting and receiving data traffic; and • any other activity required to signal completion of, and to document and test, the MAC in accordance with the Standards.
Addition of new switch capacity – complex	In relation to a Site which the Contractor has notified the Customer Authority as having insufficient power, air conditioning, space or other constraints: • all preparatory work, including a Site survey (if required), design activities, and work with the Customer Authority to address the constraints identified in relation to that Site; • carry out any MAC Approval Activities; • once any MAC Approvals have been obtained, removal of the existing network switch(es) if being replaced; • installation of new network switch(es) into existing racking; • carry out any necessary configuration and patching on the installed network switch(es); • testing of the new network switch(es) and any other equipment impacted by this MAC to ensure that existing Data LAN Connectivity is unaffected and on any subsequent connection the Data Device supported by the new switch(es) is capable of sending, transporting and receiving data traffic; and • any other activity required to signal completion of, and to document and test, the MAC in accordance with the Standards.

Table 11 – LAN Service MACs

12 BESPOKE ENGINEERING SERVICE

12.1 Bespoke Engineering Service Overview

12.1.1 The Bespoke Engineering Service consists of the provision by the Contractor of:

(i) the Core Bespoke Engineering Capability (as more particularly described at Paragraph 12.2 below);

(ii) the System 1 Capability (as more particularly described at Paragraph 12.3 below);

(iii) the BES Help Desk (as more particularly described at Paragraph 12.4 below); and

(iv) all other activities performed by the personnel to be named by the Customer Authority at or around the Effective Date (the "**Legacy BES Personnel**") immediately prior to the relevant Operational Service Commencement Date (such activities being known as the "**BES Activities**").

12.1.2 The Contractor shall provide all of the BES Activities at secure enclaves at:

(i) the Customer Authority Site in Northwood;

(ii) the Customer Authority Site at Whitehall; and

(iii) the Customer Authority Sites in Germany and Cyprus,

(each such secure enclave being known as a "**BES-Supported Enclave**").

12.1.3 The Contractor shall use all reasonable endeavours to retain the Legacy BES Personnel. Failure to retain such Legacy BES Personnel shall not relieve the Contractor of its obligations to provide the Bespoke Engineering Service in accordance with the Service Levels.

12.1.4 The Contractor shall ensure that the activities performed by the Legacy BES Personnel are fully documented in writing by the Legacy BES Personnel and submitted to the Customer Authority for Approval within six (6) months of the Operational Service Commencement Date for the BES. If the Customer Authority does not Approve such documentation, the Contractor shall ensure that the Legacy BES Personnel revise such documentation, taking into account the Customer Authority's comments, and shall re-submit the revised documentation to the Customer Authority until it has received the Customer Authority's Approval. Once such documentation has been Approved, the Contractor shall (and ensure that all BES Personnel) comply with such documentation immediately.

12.2 Core Bespoke Engineering Capability

12.2.1 The Contractor shall ensure that the Contractor Personnel (including any Legacy BES Personnel) used in the delivery of the Bespoke Engineering Service (the "**BES Personnel**") are appropriately qualified, trained and security cleared in accordance with the requirements of this Consolidated Contract.

12.2.2 The Contractor shall ensure and procure that each of the BES Personnel acts as the local configuration authority for the following critical systems:

(i) the system currently known as the transport management system (as updated and amended from time to time), such system being an intelligent multiplexer network used for voice and data communications (the "**TMS**"); and

(ii) the systems currently known as the matrix switches, such switches being intelligent switching systems for internal local site and external switching, which provide the backbone for data services without loss of cryptographic synchronisation (the "**Matrix Switches**").

12.2.3 In acting as such a local configuration authority, the Contractor and the BES Personnel shall be responsible for ensuring that the TMS and Matrix Switches meet the Customer Authority's requirements (as such requirements are set out in

this Consolidated Contract) from time to time, in terms of functionality, performance, capacity, security, safety and ergonomics, including by:

(i) defining the environmental conditions in which the TMS and Matrix Switches will be required to operate, including all lighting, ventilation and power requirements;

(ii) producing and submitting master system design drawings and other relevant documentation to the Customer Authority as required by the Standards;

(iii) identifying and specifying the spares required for testing, commissioning and ongoing support of the TMS and Matrix Switches;

(iv) preparing and issuing test plans and procedures, including annual maintenance plans, and providing supervision during commissioning;

(v) designing modifications to the TMS and Matrix Switches and issuing modification details in the form of drawings or instructions; and

(vi) in relation to the TMS, designing the routing mechanism for traffic over the TMS network.

12.2.4 The Contractor shall provide additional maintenance and other activities as directed by the Customer Authority, which include the following:

Group/Activity	**Examples of Typical Activities**
Management of encryption devices (outside the scope of the Encryption Service described at Paragraph 9 of this Consolidated Schedule)	Activities including the physical checking of assets, first line maintenance support, refill of cryptographic key material and resynchronisation.
Non-Contractor provided circuits and connectivity services	Includes second line support to: (a) circuits, equipment and assets which are not provided by the Contractor under this Consolidated Contract, for example routers supporting other organisations and services such as NATO and Allies; and (b) Customer Authority multiplexers, switches, promina terminals (and other similar equipment) supporting operational systems deployed worldwide.
BES LAN services	Co-ordination and procurement of LAN services for the BES-Supported Enclaves

Table 12 – Bespoke Engineering Service – support to Service and Assets

12.2.5 The Contractor shall, in accordance with the ITIL guidelines, provide service management services for the Bespoke Engineering Service. Such service

management shall be limited to Incident management, Problem management and change management and shall be provided by the Contractor as self-contained processes within the Bespoke Engineering Service. The provision of this service management will require the Contractor to coordinate with a wide range of Customer Authority personnel and Customer Authority Third Parties who provide components and services that are part of the Customer Authority's information services and systems in the specified enclaves.

12.3 System 1 Capability

The Contractor shall ensure and procure that each of the BES Personnel also provides configuration of an additional system, as more particularly described in the TOP SECRET documentation provided to the Contractor by the Customer Authority, (the receipt of which is hereby acknowledged), upon request from the Customer Authority from time to time (the "**System 1 Capability**").

12.4 BES Help Desk

12.4.1 In providing the Core Bespoke Engineering Capability and the System 1 Capability, the Contractor shall ensure that:

(i) it provides support twenty-four (24) hours a day, seven (7) days a week, including via dedicated help desks equipped with a telephone at Northwood and Whitehall, and remotely via telephone and email virtual help desks, which are capable of managing, responding to and resolving requests, Incidents and providing assistance to End Users, in connection with the BES Activities (each helpdesk being known as a "**BES Help Desk**")*;*

(ii) each BES Help Desk is only accessible to specifically authorised End Users via telephone, electronically or face-to-face requests;

(iii) each BES Help Desk responds to and resolves requests based on the priority levels described in the below table; and

BES Priority Level	Systems, Services and Activities Included	Locations
Level 1	System 1	Northwood and Whitehall locations
Level 2	TMS Matrix Switches	Northwood and Whitehall locations
Level 3	All systems and services covered by the BES Activities	Northwood, Whitehall, Cyprus and Germany locations

Table 13 – Bespoke Engineering Service – system priority levels

(iv) it has at least two (2) staff on duty at all times to support BES Priority Level 1 systems.

12.4.2 The list of activities set out in this Paragraph 12.4 is without prejudice to the generality of this Paragraph 12, including the description of the BES Activities to be provided by the Contractor.

12.5 MACs

There are no MACs associated with the Bespoke Engineering Service.

13 CYBER ACCESS SERVICE

13.1 Cyber Access Service Overview

13.1.1 The Cyber Access Service is one component of the Customer Authority's cyber defence activities. It specifically supports the Customer Authority sponsored Enhanced Computer Network Defence capability to monitor and report malicious and non-malicious attacks in the UK and Cyprus on the Customer Authority's OFFICIAL, SECRET and TOP SECRET Connectivity Networks. ECND relies on feeds of information from various providers of Customer Authority's ICT and critically its various data networks.

13.1.2 In providing data feeds and other information to the ECND capability, the Contractor shall ensure that the Cyber Access Service infrastructure supporting the Cyber Access Service (the "**Cyber Access Infrastructure**") is installed in different strategic locations across the Connectivity Networks so that one hundred per cent (100%) of all IP traffic passing through and into or out of the Connectivity Networks is monitored by the Cyber Access Infrastructure.

13.1.3 For the purposes of providing the Cyber Access Service the Contractor can deploy sensors and other equipment at either Edge Nodes or Core Nodes.

13.1.4 In providing the Cyber Access Service, the Contractor shall:

(i) provide the Cyber Access Capability as more particularly described in Paragraph 13.2 below;

(ii) provide the Buffering Capability as more particularly described in Paragraph 13.3 below; and

(iii) provide the Content Inspection Service as more particularly described in Paragraph 13.4 below.

13.2 Cyber Access Capability

13.2.1 In providing the Cyber Access Capability, the Contractor shall:

(i) maintain, replace and manage the Cyber Access Infrastructure supporting the Cyber Access Service;

(ii) provide information to the Customer Authority on security events and situational awareness through the use of wide area network monitoring, including configuration information from open systems interconnection (OSI) network (layer 3) equipment, firewall logs (including dropped packet information, information gained from the Services described at Paragraph 13.2.6(iii) below and SFTP data collection such as gateway and mail logs), such information being provided through support to the various Customer Authority-provided ECND tools (all such monitoring to be on Plaintext);

(iii) provide, install and manage sensors on the Network Infrastructure, and manage configuration changes, and ensure that such sensors shall have the following level of functionality:

(a) end-to-end traffic flow analysis (including analysis for malicious behaviour or activities) using the Customer Authority's extant solution (or any other solution that the Contractor has obtained the Approval of the Customer Authority to use);

(b) whole network flow trend analysis (worms and DDoS) using the Customer Authority's extant solution (or any other solution that the Contractor has obtained the Approval of the Customer Authority to use); and

(c) in the case of IDS and IPS, allow deep packet published vulnerability detection;

(iv) facilitate network situational awareness by provision of simple network management protocol community strings (read-only) for all OSI network (layer 3) equipment;

(v) restrict the possibility of a denial of service incident occurring on the Connectivity Networks through enforcing a limit to the amount of JFlow information, or equivalent, that can be carried across the Connectivity Networks; and

(vi) employ equipment capable of running a SNORT signature engine.

13.2.2 The Contractor shall ensure that:

(i) the OFFICIAL Cyber Access Service is capable of monitoring the:

(a) IP traffic flow at any OFFICIAL Core Node or Edge Node will be presented to the Customer Authority's extant whole network flow trend analysis solution using 1:100 flow sampling;

(b) IP traffic flow at any OFFICIAL location on which Cyber Access Infrastructure has been installed will be presented to the Customer Authority's extant end to end traffic flow analysis solution using 1:1 flow sampling only for the OFFICIAL Connectivity Network; and

(c) all IP traffic on all OFFICIAL Core Node or Edge Node interfaces will be subject to inspection by the IDS/IPS;

(ii) the SECRET Cyber Access Service is capable of monitoring the:

(a) IP traffic flow at all SECRET Core Nodes or Edge Nodes using 1:100 flow sampling; and

(b) of all IP traffic on all SECRET Core Nodes or Edge Nodes interfaces will be subject to inspection by the IDS/IPS;

(iii) the TOP SECRET Cyber Access Service is capable of monitoring the:

(a) IP traffic flow at all TOP SECRET Core Nodes or Edge Nodes using 1:100 flow sampling; and

(b) of all IP traffic on all TOP SECRET Core Nodes or Edge Nodes interfaces will be subject to inspection by the IDS/IPS.

13.2.3 The Contractor shall configure the Cyber Access Infrastructure such that an alert is sent immediately to the Customer Authority's ECND security information manager (or such other nominee as the Customer Authority may notify the Contractor from time to time) when:

(i) Customer Authority traffic matches a Common Signature (for example a Common Signature that matches a computer network attack or computer network exploitation, such as a TCP port scan);

(ii) traffic level between defined end-points reaches a defined percentage above a baseline defined by the Customer Authority;

(iii) the whole network traffic matches an Approved Distributed Denial of Service Common Signature. A DDoS Common Signature is traffic from multiple Hosts, any one of which would be normal, but which together could trigger a denial of service;

(iv) a Host breaches one of the Customer Authority's policies relating to the parameters, constraints, criteria or other items that are used to help detect malicious and non-malicious attacks on the Network Infrastructure networks. Such policies may be notified to the Contractor by the Customer Authority from time to time and provide the Contractor with guidance on achieving compliance with the Standards in respect of the Cyber Access Service, for example, where a Host identified by an IP Address is a web server only and should not be the source of any traffic; or

(v) traffic within any Gateway or interconnection point from the BPS that is monitored by the Cyber Access Service matches a Common Signature of a security attack.

13.2.4 In providing the Cyber Access Service, the Contractor shall ensure that hostile traffic detected in the BPS is blocked immediately following detection. For alerts generated elsewhere such as the LAN Service or Connectivity Service boundary, the Contractor shall, where directed by the Customer Authority, immediately block Connectivity Network data flows by specific IP Address(es).

13.2.5 The Contractor shall comply with the latest versions of the policies as they are amended by the Customer Authority from time to time.

13.2.6 The Contractor shall:

(i) allow interactive access to traffic and security alert systems on a role-based level to ECND End Users such that:

(a) ECND End Users are able to add to or amend any policies which are capable of being amended by ECND End Users directly from time to time; and

(b) ECND End Users are able to provide updated commercial security databases, patches (or similar), via the Internet or downloaded update;

(ii) run any scripts provided by the Customer Authority's ECND team (and any of its successors) against the configurations of the Connectivity Networks routers, and provide the output in a format agreed with the Customer Authority from time to time to a shared location for use by the Customer Authority's ECND team (and any of its successors). In providing the Cyber Access Service, the Contractor shall comply with any changes and developments to such scripts that may be specified by the Customer Authority from time to time; and

(iii) enable the Connectivity Service to allow network configuration and end system scanning through tools such as Tripwire (IP360) and Lumeta (IPsonar) toolsets.

13.2.7 In respect of the Cyber Access Capability, the Customer Authority shall retain control over the IDS and IPS equipment, such that the Customer Authority is able to configure, write and upload the Common Signatures to the IDS and IPS at any time, without having to request any assistance or permission from Contractor Personnel.

13.3 Buffering Capability

13.3.1 The Contractor shall provide a buffering capability to:

(i) all Core Nodes or Edge Nodes, MAN Hubs or Gateways (collectively referred to here as "**Nodes**"); and

(ii) all Nodes or other locations to which the Contractor provides the Content Inspection Service in accordance with Paragraph 13.4 below,

and ensure ongoing integration with the Customer Authority's ECND systems.

13.3.2 The buffering capability consists of:

(i) buffering in Plaintext all IP traffic at the Nodes;

(ii) providing the Customer Authority with a means of requesting the buffered data packets that immediately surround a network event detected by an IPS/IDS sensor. The buffered data packets may, upon receipt from the Customer Authority's ECND systems, be provided to the boundary with the Customer Authority's ECND system such that additional measures may be performed by the Customer Authority;

(iii) configuring each of the Nodes such that the Nodes transport any buffer traffic requested by the Customer Authority from time to time, even if the monitored part of the network is isolated from the rest of the network, back to the Customer Authority ECND systems for eventual processing and storage; and

(iv) buffering data for a maximum of seventy (70) days (rolling), but with buffering capacity that shall be agreed in writing between the parties, such form of writing to refer to this Paragraph 13.3.2(iv), and in any event such buffering capacity shall be no less than 50TB at MAN Hubs, Gateways and Core Nodes and 4TB at Edge Nodes. If the achievable level of data buffering is deemed insufficient by the Customer Authority's ECND team

(and any of its successors), then a formal Contract Change Request to increase the capacity will be required.

together, the "**Buffering Capability**".

13.4 Content Inspection Service

13.4.1 On request by the Customer Authority from time to time, the Contractor shall install and operate a Content Inspection Service that allows the Customer Authority ECND capability to monitor data streams, including HTTPS data streams, that traverse any Gateways or other locations identified as being required by the Customer Authority.

13.4.2 The Content Inspection Service consists of:

(i) provision of a monitoring function that can inspect data streams for:

(a) keywords and phrases;

(b) destination URL;

(c) port;

(d) protocol;

(e) IP Address;

(f) application,

(g) sender; and

(h) destination;

(ii) provision of a monitoring function on HTTPS tunnelled web traffic by means of SSL interception; and

(iii) management of an HTTPS interception white list, populated by the Customer Authority, describing websites that are accessed by Customer Authority applications using client certificates, or known trusted financial institutions/banks etc. in order to allow normal tunnelling of HTTPS data traffic. The Contractor shall submit such white list, and any subsequent changes to such white list, to the Customer Authority for Approval.

13.5 MACs

There are no MACs associated with the Cyber Access Service.

14 PROFESSIONAL SERVICES

14.1 Professional Services Overview

14.1.1 From time to time, the Contractor shall provide Contractor Personnel with appropriate experience and qualifications to carry out, and conclude successfully, the tasks described in the Rate Card. The Contractor's provision of Contractor Personnel to carry out each of such tasks, together with the carrying out of that task, shall be known as a "**Professional Service**".

14.1.2 Activities included as part of any other Service shall not be considered part of the Professional Services or charged for as a Professional Service. The Contractor

shall not carry out and shall not be entitled to invoice for any Professional Service, unless that Professional Service has been specifically requested in advance by the Customer Authority and identified by the Customer Authority as being a Professional Service.

14.1.3 The Contractor shall, at the Customer Authority's request from time to time, provide the Professional Services in the following Subscriber Domains:

(i) "**UK**", where the Contractor Personnel carrying out the relevant Professional Service is (or are, as the case may be) to be located within the United Kingdom;

(ii) "**Overseas (Rate Card Locations 1)**", where the Contractor Personnel carrying out the relevant Professional Service is (or are, as the case may be) to be located within Cyprus, Germany or North America; and

(iii) "**Overseas (Rate Card Locations 2)**", where the Contractor Personnel carrying out the relevant Professional Service is (or are, as the case may be) to be located in any location that is not the UK or Overseas (Rate Card Locations 1).

(each a "**Rate Card Subscriber Domain**").

PART B: CONTRACTOR SERVICE DESCRIPTIONS

APPENDIX 1
NOT USED