FUTURE SERVICE DELIVERY CONTACT

SCHEDULE 2.3

STANDARDS

CONTENTS

Clause	Heading	Page
1	GENERAL	3
2	TECHNOLOGY AND DIGITAL SERVICES PRACTICE	3
3	OPEN DATA STANDARDS & STANDARDS HUB	3
4	TECHNOLOGY ARCHITECTURE STANDARDS	4
5	ACCESSIBLE DIGITAL STANDARDS	4
6	SERVICE MANAGEMENT SOFTWARE & STANDARDS	4
7	ENVIRONMENTAL STANDARDS	5
8	HARDWARE SAFETY STANDARDS	6
9	OTHER STANDARDS	6

STANDARDS

1 GENERAL

1.1 Throughout the Term of this Agreement, the Parties shall monitor and notify each other of any new or emergent standards which could affect the Contractor's provision, or the Authority's receipt, of the Services.

1.2 Subject to Clause 16, any changes to the Standards, including the adoption of any such new or emergent standard, shall be agreed in accordance with the Change Control Procedure.

1.3 Where a new or emergent standard is to be developed or introduced by the Authority, the Contractor shall be responsible for ensuring that the potential impact on the Contractor's provision, or the Authority's receipt, of the Services is explained to the Authority (in a reasonable timeframe), prior to the implementation of the new or emergent standard.

1.4 Where Standards referenced conflict with each other or with Good Industry Practice, then the later Standard or best practice shall be adopted by the Contractor. Any such alteration to any Standard(s) shall require the prior written agreement of the Authority and shall be implemented within an agreed timescale.

2 TECHNOLOGY AND DIGITAL SERVICES PRACTICE

2.1 The Contractor shall (when designing, implementing and delivering the Services) adopt the applicable elements of HM Government's Technology Code of Practice as documented at https://www.gov.uk/service-manual/technology/code-of-practice.html.

3 OPEN DATA STANDARDS & STANDARDS HUB

3.1 The Contractor shall, to the extent it is within its control, comply with UK Government's Open Standards Principles as documented at https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles, as they relate to the specification of standards for software interoperability, data and document formats in the IT Environment.

3.2 Without prejudice to the generality of Paragraph 1.3, the Contractor shall, when implementing or updating a technical component or part of the Software or Contractor Solution where there is a requirement under this Agreement or opportunity to use a new

or emergent standard, submit a Suggested Challenge compliant with the UK Government's Open Standards Principles (using the process detailed on Standards Hub and documented at http://standards.data.gov.uk/). Each Suggested Challenge submitted by the Contractor shall detail, subject to the security and confidentiality provisions in this Agreement, an illustration of such requirement or opportunity within the IT Environment, Contractor Solution and Government's IT infrastructure and the suggested open standard.

3.3 The Contractor shall ensure that all documentation published on behalf of the Authority pursuant to this Agreement is provided in a non-proprietary format (such as PDF or Open Document Format (ISO 26300 or equivalent)) as well as any native file format documentation in accordance with the obligation under Paragraph 3.1 to comply with the UK Government's Open Standards Principles, unless the Authority otherwise agrees in writing.

4 TECHNOLOGY ARCHITECTURE STANDARDS

4.1 The Contractor shall produce full and detailed technical architecture documentation for the Contractor Solution in accordance with Good Industry Practice. If documentation exists that complies with The Open Group Architecture Forum (TOGAF) 9.1 or its equivalent, then this shall be deemed acceptable.

5 ACCESSIBLE DIGITAL STANDARDS

5.1 The Contractor shall comply with (or with equivalents to):

(a) the World Wide Web Consortium (W3C) Web Accessibility Initiative (WAI) Web Content Accessibility Guidelines (WCAG) 2.0 Conformance Level AA; and

(b) ISO/IEC 13066-1: 2011 Information Technology – Interoperability with assistive technology (AT) – Part 1: Requirements and recommendations for interoperability.

6 SERVICE MANAGEMENT SOFTWARE & STANDARDS

6.1 Subject to Paragraphs 1 to 3 (inclusive), the Contractor shall reference relevant industry and HM Government standards and best practice guidelines in the management of the Services, including the following and/or their equivalents:

(a) ITIL v3 2011;

(b) ISO/IEC 20000-1 2011 "ITSM Specification for Service Management";

(c) ISO/IEC 20000-2 2012 "ITSM Code of Practice for Service Management";

(d) ISO 10007 "Quality management systems – Guidelines for configuration management"; and

(e) BS25999-1:2006 "Code of Practice for Business Continuity Management" and, ISO/IEC 27031:2011, ISO 22301. ISO22313, ISO27031 and ISO/IEC 24762:2008 in the provision of "IT Service Continuity Strategy" or "Disaster Recovery" plans.

6.2 For the purposes of management of the Services and delivery performance the Contractor shall make use of Software that complies with Good Industry Practice including availability, change, incident, knowledge, problem, release & deployment, request fulfilment, service asset and configuration, service catalogue, service level and service portfolio management. If such Software has been assessed under the ITIL Software Scheme as being compliant to at least "**Bronze Level**", then this shall be deemed acceptable.

7 ENVIRONMENTAL STANDARDS

7.1 The Contractor warrants that it has obtained ISO 14001 (or equivalent) certification for its environmental management and shall comply with and maintain certification requirements throughout the Term. The Contractor shall follow a sound environmental management policy, ensuring that any Goods and the Services are procured, produced, packaged, delivered, and are capable of being used and ultimately disposed of in ways appropriate to such standard.

7.2 The Contractor shall comply with relevant obligations under the Waste Electrical and Electronic Equipment Regulations 2006 in compliance with Directive 2002/96/EC and subsequent replacements (including those in compliance with Directive 2012/19/EU).

7.3 The Contractor shall (when designing, procuring, implementing and delivering the Services) ensure compliance with Article 6 and Annex III of the Energy Efficiency Directive 2012/27/EU and subsequent replacements.

7.4 The Contractor shall comply with the EU Code of Conduct on Data Centres' Energy Efficiency. The Contractor shall ensure that any data centre used in delivering the Services are registered as a Participant under such Code of Conduct.

7.5 The Contractor shall comply with the Authority and HM Government's objectives to reduce waste and meet the aims of the Greening Government: IT strategy contained in the document "Greening Government: ICT Strategy issue (March 2011)" at https://www.gov.uk/government/publications/greening-government-ict-strategy.

8 HARDWARE SAFETY STANDARDS

8.1 The Contractor shall comply with those British Standards or other standards relevant to the provision of the Services, including the following or their equivalents:

(a) any new hardware required for the delivery of the Services (including printers), shall conform to BS EN 60950-1:2006+A12:2011 or subsequent replacements. In considering where to site any such hardware, the Contractor shall consider the future working user environment and shall position the hardware sympathetically, wherever possible;

(b) any new audio, video and similar electronic apparatus required for the delivery of the Services, shall conform to the following standard: BS EN 60065:2002+A12:2011 or any subsequent replacements;

(c) any new laser printers or scanners using lasers, required for the delivery of the Services, shall conform to either of the following safety Standards: BS EN 60825-1:2007 or any subsequent replacements ; and

(d) any new apparatus for connection to any telecommunication network, and required for the delivery of the Services, shall conform to the following safety Standard: BS EN 41003:2009 or any subsequent replacements.

8.2 Where required to do so as part of the Services, the Contractor shall perform electrical safety checks in relation to all equipment supplied under this Agreement in accordance with the relevant health and safety regulations.

9 OTHER STANDARDS

9.1 The Contractor shall comply with the standards set out in Annex 1 (Other Standards) to this Schedule and which are relevant to the provision of the Services.

ANNEX 1

OTHER STANDARDS

1950 Royal Warrant Indian Army Pension Code
2007DIN02-010 Death-in-Service, all benefits, spouse's Additional Voluntary Contributions and Added Years Contracts
2011DIN01-037 Introduction of Additional Paternity/Adoption Leave and Pay for Members of the Regular Armed Forces
2011DIN01-15 Revised Maternity Policy for Servicewomen in the Regular Armed Forces
2011DIN06-008 Sustainable ICT policy
2014DIN01-74 Tri-Service Arrangements for the Administration of Service Wills
2014DIN02- 007 Software Patching and the use of the Defence Out of Band Update Service (DOBUS)
2015DIN05-017 Complaints Handling in the Ministry of Defence
2016DIN02-004 Statement of Defence Risk Appetite
2016DIN03-029 Contact with the Media and Communicating in Public
2017DIN03-015 Protection of Information Relating to UK Special Forces
Attributable Benefits Reserves Scheme (ABRS) Policy
Audit Commission Guidelines
BIP 0008-1:2008 (Evidential Weight and Legal Admissibility of Electronic Information)
Business Continuity Training in accordance with MOD Summary of Mandatory Training (v16.0-April

2018
Cabinet Office Bulk Data Requirement
Cabinet Office Digital First Strategy
Centre for the Protection of National Infrastructure (CPNI) Secure Destruction Standard 2017
Centre for the Protection of National Infrastructure (CPNI) Standard for Secure Destruction of Sensitive Items
Communications Electronic Security Group (CESG) GPG 12 - Security Procedures VMware vSphere 4.0 & 4.1
NCSC - Protective Monitoring for HMG ICT Systems (GPG 13)
CESG GPG 18 - Forensic Readiness
National Cyber Security Centre (NCSC) - Security Incident Management
CESG GPG 47 - Information Risk Management
CESG Information Assurance Standards 1 and 2
CESG IS1 - Technical Risk Assessment and Risk Treatment
Civil Service Policy Rules and Guidance
Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) v3.0
Code of Practice for Information Security Management System
Code of Practice for the Legal Admissibility of Information Stored on Electronic Document Management Systems
Payment Card Industry Data Security Standard (PCI DSS)

NCSC Commercial Product Assurance Security Characteristics
CPA SC Overwriting Tools for Magnetic Media V2-1
Defence Business Service (DBS) Accreditation and Approvals Policy
DBS Accreditation and Approvals Process
DBS Confidentiality Agreement
DBS Critical Cyber Security Incident Document
DBS Cyber Incident Response Plan
DBS Security Incident Response Plan
DBS Data Retention Policy
DBS DFCR Process and Procedures
DBS Government Furnished Assets Procedure
DBS Guidance 'Applying the Brand'
DBS Information Asset Owner (IAO) Network & Governance Policy
DBS IT Security Health Check (ITSHC) Planning Procedures Document
DBS Military Personnel & Veterans CANNEL Alert State Procedure
DBS Military Personnel & Veterans Design Standards & Principles
DBS Military Personnel & Veterans Security Information Assurance Risk Governance
DBS Military Personnel & Veterans General Security Instruction
DBS Military Personnel & Veterans Customer Correspondence Review

DBS Military Personnel & Veterans Management Information Technical Information Service Request Process
DBS Procedure - Reporting Breach of Security
DBS Protective Health Check Procedures
DBS Protective Security Health Check Policy
DBS Public Key Infrastructure
DBS Retention and Disposal Schedule
DBS Risk Management Framework
DBS Risk Management Strategy
DBS Risk Review Process
DBS Safety Health Environment and Fire (SHEF) Policy
DBS Security Policy
DBS Security Processes and Procedures
DBS SyOps
DBS Vetting Policy
Def Commercial Security & Personal Data Aspects Letter
Defence Business Services (DBS) Business Continuity (BC) Management Strategy
Defence Cyber Protection Partnership Requirements
Defence Data Management Framework

Defence Data Management Strategy 2016
Defence Data Quality Guide
Defence Information Strategy
Defence Management Information Strategy
Defence Operating Board Military Human Rescources (HR) Benchmarking standards
Defence Standard 05-138 (DEFSTAN 05-138) Cyber Security for Defence Suppliers
DIAN 16 - Dealing with Aggregation of Non-Personal Information
Extant MODMO Desk Instructions
Future Defence Business Services Programme - Statement of Requirement for Industry Partner Data Management Services
Good Practice Guide (GPG) 44 (Authentication credentials for online government services)
Good Practice Guide (GPG) 45 (Identity proofing and verification of an individual)
Government Digital Service - Digital by Default
Government Financial Reporting Manual (FReM)
Guide for Defence Data Authorities
HM Treasury - Managing Public Money
HMG IA Standard No. 7 - Authentication of Internal Users of ICT Systems Handling Government Information
HMRC Guidelines and CoCo for Administering and Reporting under Real Time Information (RTI) and MOD Security Rules for the PD2 population with the Special Handling Flag set

HMRC Guidelines for Earlier Year Updates
HMRC Guidelines for Employer Payment Summary
HMRC Guidelines for Full Payment Submission
HMRC Guidelines for Real Time Information Reporting
HMRC Guidelines for Student Loans (Collection of Student Loans Manual)
HMRC Publications CWG5 (Class 1A National Insurance contributions on Benefits in kind)
Electricity at Work Regulations
IAMM guidance
Information Security (InfoSec) Standard 5 - MOD Data Destruction Standard
International Financial Reporting Standards
International Payroll Benchmarking
International Standard for Assurance Engagements (ISAE) 3402 - Assurance Reports on Controls at a Service Organization
ISO 8000 - Data Quality and Enterprise Master Data
ISO 44001
ISO/IEC 20000 - IT Service Management
ISO/IEC 22301 - Business Continuity Management Systems
ISO/IEC 22313 - Business Continuity Management Systems
ISO/IEC 27001 - Information Security Management System

ISO/IEC 27002 - Code of Practice for Information Security Controls
ISO/IEC 27031 - Guidelines for Information and Communication Technology Readiness for Business Continuity
ISO/IEC 27034 - Application Security guidelines
ISO/IEC 27035 - Information Security Incident Management
ISO/IEC 30111 - Vulnerability Handling Processes
ISO/PAS 28000 - Specification for Security Management Systems for the Supply Chain
ITIL v3 2011
Joint Personnel Administration (JPA) Documentations (Business Process Guides and Self-Service User Guides) Standards
JPA Documentations (Business Process Guides and Self-Service User Guides)
JPA System SyOps
Joint Service Publication (JSP) 101 - The Defence Writing Guide
JSP 332 - Low Value Purchasing
JSP 367 - Defence Postal and Courier Services
JSP 418 - Management of Environmental Protection in Defence
JSP 440 - Defence Manual of Security, Resilience and Business Continuity
JSP 440 Leaflet 4 - Physical Security 01/05/2018
JSP 440 Part 2 - Leaflet 16 - Business Continuity Guidance
JSP 441 - Managing Information in Defence

JSP 462 - Financial Management and Charging Policy Manual
JSP 464 - Tri-Service Accommodation Regulations (TSARs)
JSP 472 - Financial Accounting and Reporting Manual
JSP 490 - Defence Cryptosecurity Operating Instructions
JSP 491 - Cryptographic Handling Instructions
JSP 525 - Corporate Governance
JSP 541 - MoD Information Security and Computer Network Defence (Organisation and Reporting Procedures)
JSP 604 - Defence Manual of Information and Communications Technology
JSP 604 Pt 1 Volume 2 - Leaflet 3001 Computer Network Defence.
JSP 752 - Tri-Service Regulations for Expenses and Allowances
JSP 753 - Regulations for the Mobilisation of UK Reserve Forces
JSP 754 - Tri-Service Regulations for Pay
JSP 757 - Tri-Service Appraisal Reporting Instructions
JSP 760 - Tri-Service Regulations for Leave and Other Types of Absence
JSP 761 - Honours and Awards in the Armed Forces
JSP 764 - The Armed Forces Pension Scheme 2005 (AFPS 05)
JSP 822 Defence Direction and Guidance for Training and Education Part 1 and Part 2 (published July 2018)
JSP 891 - Imprest Accounting, Banking and Control Accounts Manual

JSP 892 - Risk Management
JSP 905 - Armed Forces Pension Scheme 2015 (AFPS 15) and Early Departure Payments Scheme 2015 (EDP 15)
Letter: D/AG Sec2/25/2/2 dated 21 April 1992
List X Site Security
Ministry of Defence Architecture Framework (MODAF)
MOD CIO Architecting and wider ICT Policy
MOD Corporate Services Relationship Management Plan
MOD Data Management Framework
MOD Data Management Strategy
MOD Data Protection Guidance Notes
MOD Data Quality Guidance
MOD Information Assurance (IA) Strategy
MOD Information Strategy
MOD ISS Application Developer's Guide
MOD Management Information Strategy
MOD Memorandum of Understanding with the Child Maintenance and Enforcement Commission (Child Support Agency (CSA)) CMEC (CSA)
MOD Regulations and Procedures for Handling Ministerial Correspondence
MOD Retention and Disposal Policy

MOD Sustainable Procurement Strategy
MOD Medals Office Engraving Policy (including Annexes covering historic engraving guidelines and policies)
MOD Medals Office Intestacy Policy
MORI / Industry standards
National Audit Office Customer Liaison Schedule and Regulations
National Cyber Security Centre (NCSC) Bulk Data Measures on MoD Bulk Data Systems.
National Cyber Security Centre (NCSC) Bulk Data Requirement
National Cyber Security Centre (NCSC) Cloud Security Principles
National Cyber Security Centre (NCSC) Commercial Product Assurance (CPA) Build Standard
National Cyber Security Centre (NCSC) Guidance for Secure Development
National Cyber Security Centre (NCSC) Protecting Bulk Personal Data Guidance
National Cyber Security Centre (NCSC) Risk Management Guidance
National Cyber Security Centre (NCSC) Secure Sanitisation of Storage Media Guide
Naval Orders In Council
Office of Efficiency and Performance Benchmarking
Op Augite - Network User Instructions
Parliamentary & Health Service Ombudsman (PHSO) Principles of Administration
Parliamentary & Health Service Ombudsman (PHSO) Principles of Good Complaints

Parliamentary & Health Service Ombudsman (PHSO) Principles of Remedy
Personal Injuries (Civilian) Scheme 1983 (PICS)
Queens Regulations for the Royal Air Force (QRRAF)
Royal Warrants for Medallic Recognition
Saratoga HR Shared Services
Security Operating Procedures (SyOps)
Security Policy Framework (SPF)
Site Co-Ordination and Installation Design Authority (SCIDA) Standards & Regulations
Site Specific Safety Health Environment and Fire (SHEF) Instructions
Service Personnel and Veterans Agency (AFPS)/ Divorce/4 (revised 07 June 2011)
Statement on Standards for Attestation Engagements (SSAE) 16 - Reporting on Controls at a Service Organisation
The Gazette of the Democratic Socialist Republic of Sri Lanka dated 15 June 1989
The National Archives - Digital Continuity Framework
The National Archives - Understanding Digital Continuity
The Open Group Architecture Forum
The Pensions (Polish Forces) Scheme 1964
The SysAdmin, Audit, Network and Security (SANS) Critical Security Controls
The War Pensions (Coastguards) Scheme 1944, Home Guard (From 1952)

The War Pensions (Mercantile Marine) Scheme 1964
The War Pensions (Naval Auxiliary Personnel) Scheme 1964
Tower Order from the Constable of the Tower of London
UK HM Government Green ICT Workbook
Vets UK Complaints Procedure