SCHEDULE 8

Security and Information Management

1. Definitions

1.1 In this Schedule the definitions set out in Schedule 1 (Definitions) shall apply.

2. Introduction

2.1 This Schedule sets out:

(a) the arrangements the Contractor must implement before, and comply with when, providing the Services and performing its other obligations under this Agreement to ensure the security of the Authority Data and the Contractor System;

(b) the Certification Requirements applicable to the Contractor and each of those Sub-Contractors which handles and/or processes Authority Data;

(c) the tests which the Contractor shall conduct on the Contractor System during the contract duration; and

(d) the Contractor's obligations to return or destroy Authority Data on the expiry or earlier termination of this Agreement; and

(e) the process to be followed in the event of a Breach of Security.

3. Principles of Security

3.1 The Contractor acknowledges that the Authority places great emphasis on the confidentiality, integrity and availability of the Authority Data.

3.2 Notwithstanding the involvement of the Authority in assessing the arrangements which the Contractor implements to ensure the security of the Authority Data and the Contractor System, the Contractor shall be, and shall remain, responsible for:

(a) the security, confidentiality, integrity and availability of the Authority Data whilst that Authority Data is under the control of the Contractor or any of its Sub-Contractors; and

(b) the security of the Contractor System.

3.3 The Contractor shall:

(a) comply with the security requirements in as set out in the Security Aspects Letter at Annex B to this Schedule;

(b) ensure that each Sub-Contractor that Processes Authority Data complies with the Sub-Contractor Security Requirements at Annex C to this schedule;

(c) provide the name of the Contractor's security officer to the Authority;

(d) ensure the Contractor's security officer liaises with the Authority’s security officer in relation to any security matters at Government Establishments; and

(e) ensure that all Contractor Personnel (including Sub-Contractors, Agents and Representatives) have the required UKAS Security Clearances required to enable them to carry out their duties in providing the Services as set out in the Security Aspects Letter.

4. Information Security Approval Statement

4.1 The Contractor's Transition Plan and Service Delivery Plan sets out how the Contractor shall ensure compliance with the requirements of this Schedule 8 (Security and Information Management), including the requirements imposed on Sub-Contractors by Annex C, from Effective Date.

4.2 The Contractor may not use the Contractor System to Process Authority Data unless and until:

(a) the Contractor has procured the conduct of an IT Health Check of the Contractor System by a CHECK Service Provider or a CREST Service Provider in accordance with paragraph 7.1; and

(b) the Authority has issued the Contractor with an Information Security Approval Statement in accordance with the process set out in this paragraph 4.

4.3 The Authority may require, and the Contractor shall provide the Authority and its authorised Representatives with:

(a) access to the Contractor Personnel;

(b) access to the Contractor System to audit the Contractor and its Sub-Contractors' compliance with this Agreement; and

(c) such other information and/or documentation that the Authority or its authorised Representatives may reasonably require,

to assist the Authority to establish whether the arrangements which the Contractor and its Sub-Contractors have implemented to ensure the security of the Authority Data and the Contractor System are consistent with the representations in the Transition Plan and the Service Delivery Plan. The Contractor shall provide the access required by the Authority in accordance with this paragraph within twenty (20) Business Days of receipt of such request, except in the case of a Breach of Security in which case the Contractor shall provide the Authority with the access that it requires within twenty-four (24) hours of receipt of such request.

5. Compliance

5.1 The Contractor shall regularly review and update the Security and Information Management Plan, and provide such to the Authority, at least once each year pursuant to Clause 28.5 (Change) of the Contract.

5.2 The Contractor shall notify the Authority within ten (10) Business Days after becoming aware of:

(a) a significant change to the components or architecture of the Contractor System;

(b) a new risk to the components or architecture of the Contractor System;

(c) a change in the risk profile;

(d) a significant change to any risk component;

(e) a significant change in the quantity of Personal Data held within the Service;

(f) a proposal to change any of the Sites from which any part of the Services are provided; and/or

(g) an ISO27001 audit report produced in connection with the Certification Requirements indicates significant concerns,

and such notice shall include a summary of any Changes the Contractor reasonably believes are required as a result of (a) to (g) (as applicable) above. If the Authority considers that a Change is required then it shall proceed in accordance with the Change Control Procedure.

5.3 The Contractor shall, upon written request by the Authority, provide the Authority with evidence of its and its Sub-Contractor's compliance with the requirements set out in this Schedule 8 (Security and Information Management).

6. Certification Requirements

6.1 The Contractor and all relevant Sub-Contractors shall be certified as compliant with:

(a) ISO/IEC 27001:2013 by a United Kingdom Accreditation Service-approved certification body or is included within the scope of an existing certification of compliance with ISO/IEC 27001:2013; and

(b) Cyber Essentials PLUS,

and shall provide the Authority with a copy of each such certificate of compliance before the Contractor shall be permitted to receive, store or Process Authority Data.

6.2 The Contractor shall ensure that each Higher Risk Sub-Contractor is certified as compliant with either:

(a) ISO/IEC 27001:2013 by a United Kingdom Accreditation Service-approved certification body or is included within the scope of an existing certification of compliance with ISO/IEC 27001:2013; or

(b) Cyber Essentials PLUS,

and shall provide the Authority with a copy of each such certificate of compliance before the Higher-Risk Sub-Contractor shall be permitted to receive, store or Process Authority Data.

6.3 The Contractor shall ensure that each Medium Risk Sub-Contractor is certified compliant with Cyber Essentials.

6.4 The Contractor shall ensure that they and each Sub-Contractor who is responsible for the secure destruction of Authority Data;

(a) securely destroys Authority Data only on Sites which are included within the scope of an existing certification of compliance with ISO/IEC 27001:2013; and

(b) are certified as compliant with the NCSC Assured Service (CAS) Service Requirement Sanitisation Standard or an alternative standard as agreed by the Authority.

6.5 The Contractor shall notify the Authority as soon as reasonably practicable and, in any event within ten (10) Business Days, if the Contractor or any Sub-Contractor ceases to be compliant with the Certification Requirements and, on request from the Authority, shall or shall procure that the relevant Sub-Contractor shall:

(a) immediately ceases using the Authority Data; and

(b) procure that the relevant Sub-Contractor promptly returns, destroys and/or erases the Authority Data in accordance with the requirements set out in this paragraph.

7. Security Testing

7.1 The Contractor shall, at its own cost and expense procure and conduct:

(a) testing of the Contractor System by a CHECK Service Provider or a CREST Service Provider ("**IT Health Check**"); and

(b) such other security tests as may be required by the Authority,

The IT Health Check shall be repeated not less than once every 12 months during the Contract Term and the results of each such test submitted to the Authority for review in accordance with this paragraph.

7.2 In relation to each IT Health Check, the Contractor shall:

(a) agree with the Authority the aim and scope of the IT Health Check;

(b) promptly, and no later than ten (10) Business Days, following the receipt of each IT Health Check report, provide the Authority with a copy of the full report;

(c) in the event that the IT Health Check report identifies any vulnerabilities, the Contractor shall:

(i) prepare a remedial plan for approval by the Authority (each a "**Vulnerability Correction Plan**") which sets out in respect of each vulnerability identified in the IT Health Check report:

(A) how the vulnerability will be remedied;

(B) unless otherwise agreed in writing between the Parties, the date by which the vulnerability will be remedied, which must be:

(1) within three (3) months of the date the Contractor received the IT Health Check report in the case of any vulnerability categorised with a severity of “medium”;

(2) within one (1) month of the date the Contractor received the IT Health Check report in the case of any vulnerability categorised with a severity of “high”; and

(3) within five (5) Business Days (or such other time period as agreed in writing between the Parties) of the date the Contractor received the IT Health Check report in the case of any vulnerability categorised with a severity of “critical”;

(C) the tests which the Contractor shall perform or procure to be performed (which may, at the discretion of the Authority, include a further IT Health Check) to confirm that the vulnerability has been remedied;

(ii) comply with the Vulnerability Correction Plan; and

(iii) conduct such further tests on the Service as are required by the Vulnerability Correction Plan to confirm that the Vulnerability Correction Plan has been complied with.

7.3 The Contractor shall ensure that any testing which could adversely affect the Contractor System shall be designed and implemented by the Contractor so as to minimise the impact on the delivery of the Services and the date, timing, content and conduct of such tests shall be agreed in advance with the Authority.

7.4 If any testing conducted by or on behalf of the Contractor identifies a new risk, new threat, vulnerability or exploitation technique that has the potential to affect the security of the Contractor System, the Contractor shall within five (5) Business Days (or such other time period as agreed in writing between the Parties) of becoming aware of such risk, threat, vulnerability or exploitation technique provide the Authority with a copy of the test report and:

(a) propose interim mitigation measures to vulnerabilities in the Contractor System known to be exploitable where a security patch is not immediately available; and

(b) where and to the extent applicable, remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in

order to reduce the attack surface of the Contractor System) within the timescales set out in the test report or such other timescales as may be agreed with the Authority.

7.5 The Contractor shall conduct such further tests of the Contractor System as may be required by the Authority from time to time to demonstrate compliance with its obligations set out this Schedule and the Agreement.

8. Monitoring and Reporting

8.1 The Contractor shall:

(a) ensure that the Joint Risk Register reflects any security risks identified in relation to the operation of the Services and the handling of Authority Data and is kept up to date; and

(b) report Breaches of Security in accordance with the approved Incident Management Process and paragraph 10.3 below.

9. Malicious Software

9.1 The Contractor shall install and maintain Anti-Malicious Software or procure that Anti-Malicious Software is installed and maintained on any part of the Contractor System which may Process Authority Data and ensure that such Anti-Malicious Software is configured to perform automatic software and definition updates as well as regular scans of the Information Management System to check for, prevent the introduction of Malicious Software or where Malicious Software has been introduced into the Contractor System, to identify, contain the spread of, and minimise the impact of Malicious Software.

9.2 If Malicious Software is found, the parties shall cooperate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Authority Data, assist each other to mitigate any Losses and to restore the Services to their desired operating efficiency.

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

(a) by the Contractor where the Malicious Software originates from the Contractor Software, the Third Party Software supplied by the Contractor or the Authority Data (whilst the Authority Data was under the control of the Contractor) unless the Contractor can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Authority when provided to the Contractor; and

(b) by the Authority, in any other circumstance.

10. Breach of Security

10.1 The Contractor shall monitor security risk impacting upon the operation of the Service.

10.2 If either Party becomes aware of a Breach of Security, it shall notify the other in accordance with the Incident Management Process.

10.3 The Contractor shall, upon it becoming aware of a Breach of Security or attempted Breach of Security, immediately take all reasonable steps necessary to invoke its Incident Management Process which shall:

(a) minimise the extent of actual or potential harm caused by such Breach of Security;

(b) remedy such Breach of Security to the extent possible;

(c) apply a tested mitigation against any such Breach of Security; and

(d) prevent a further Breach of Security in the future which exploits the same root cause failure;

10.4 Following the Breach of Security or attempted Breach of Security, the Contractor shall as soon as reasonably practicable and, in any event, within five (5) Business Days (or such other time period as agreed in writing between the Parties), provide to the Authority full details of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Authority.

10.5 In the event that any action is taken in response to a Breach of Security or attempted Breach of Security as a result of non-compliance by the Contractor, its Sub-Contractors and/or all or any part of the Contractor System with this Contract, then such remedial action shall be completed at no additional cost to the Authority.

ANNEX A

BASELINE SECURITY REQUIREMENTS

1 Security Classification of Information

1.1 If the provision of the Services requires the Contractor to Process Authority Data which is classified as:

(a) OFFICIAL-SENSITIVE, the Contractor shall implement such additional measures as agreed with the Authority from time to time in order to ensure that such information is safeguarded in accordance with the applicable Standards; and/or

(b) SECRET or TOP SECRET, the Contractor shall only do so where it has notified the Authority prior to receipt of such Authority Data and the Contractor shall implement additional measures as agreed with the Authority from time to time in order to ensure that such information is safeguarded in accordance with the applicable Standards.

2 End User Devices

2.1 The Contractor must manage, and must ensure that all Sub-Contractors manage, all end-user devices used by the Contractor on which Authority Data is Processed in accordance the following requirements:

(a) the operating system and any applications that Process or have access to Authority Data must be in current support by the vendor, or the relevant community in the case of open source operating systems or applications;

(b) users must authenticate before gaining access;

(c) all Authority Data must be encrypted using an encryption tool agreed to by the Authority;

(d) the end-user device must lock and require any user to re-authenticate after a period of time that is proportionate to the risk environment, during which the end-user device is inactive;

(e) the end-user device must be managed in a way that allows for the application of technical policies and controls over applications that have access to Authority Data;

(f) the Contractor or Sub-Contractor, as applicable, can, without physical access to the end-user device, remove or make inaccessible all Authority Data on the device and prevent any user or group of users from accessing the device;

(g) all end-user devices are within in the scope of any current Cyber Essentials Plus certificate held by the Contractor, or any ISO/IEC 27001 (at least ISO/IEC 27001:2013) certification issued by a UKAS-approved certification body, where the scope of that certification includes the Services.

2.2 The Contractor must comply, and ensure that all Sub-Contractors comply, with the recommendations in NCSC Device Guidance, as updated, amended or replaced from time to time, as if those recommendations were incorporated as specific obligations under this Agreement.

2.3 Where there any conflict between the requirements of this Schedule 8 (Security and Information Management) and the requirements of the NCSC Device Guidance, the requirements of this Schedule will take precedence.

3 Encryption

3.1 The Contractor must ensure, and must ensure that all Sub-Contractors ensure, that Authority Data is encrypted:

(a) when stored at any time when no operation is being performed on it; and

(b) when transmitted.

3.2 Where the Contractor, or a Sub-contractor, cannot encrypt Authority Data the Contractor must:

(a) immediately inform the Authority of the subset or subsets of Authority Data it cannot encrypt and the circumstances in which and the reasons why it cannot do so;

(b) provide details of the protective measures the Contractor or Sub-Contractor (as applicable) proposes to take to provide equivalent protection to the Authority as encryption; and

(c) provide the Authority with such information relating to the Authority Data concerned, the reasons why that Authority Data cannot be encrypted and the proposed protective measures as the Authority may require.

3.3 The Authority, the Contractor and, where the Authority requires, any relevant Sub-Contractor shall meet to agree appropriate protective measures for the unencrypted Authority Data.

3.4 Where the Authority and Contractor reach agreement, the Contractor must update the Security and Information Management Plan to include:

(a) the subset or subsets of Authority Data not encrypted and the circumstances in which that will occur; and

(b) the protective measure that the Contractor and/or Sub-Contractor will put in place in respect of the unencrypted Authority Data.

3.5 Where the Authority and Contractor do not reach agreement within forty (40) Business Days of the date on which the Contractor first notified the Authority that it could not encrypt certain Authority Data, either Party may refer the matter to be determined in accordance with Schedule 30 (Dispute Resolution Procedure).

4 Personnel Security

4.1 All Contractor Staff shall be subject to a pre-employment check before they may participate in the provision and or management of the Services. Such pre-employment checks must include all pre-employment checks which are required by the HMG Baseline Personnel Security Standard including: verification of the individual's identity; verification of the individual's nationality and immigration status; and, verification of the individual's employment history; and verification of the individual's criminal record.

4.2 The Authority and the Contractor shall review the roles and responsibilities of the Contractor Personnel in order to enable the Authority to determine which roles require additional vetting and a specific national security vetting clearance (e.g. a Counter Terrorist Check). Roles which are likely to require additional vetting and a specific national security vetting clearance include system administrators whose role would provide those individuals with privileged access to IT systems which Process Authority Data or data which, if it were Authority Data, would be classified as OFFICIAL-SENSITIVE.

4.3 The Contractor shall not permit Contractor Staff who fail the security checks required by paragraphs 4.1 and 4.2 to be involved in the management and/or provision of the Services except where the Authority has expressly agreed in writing to the involvement of the named individual in the management and/or provision of the Services.

4.4 The Contractor shall ensure that Contractor Staff are only granted such access to Authority Data as is necessary to enable the Contractor Staff to perform their role and to fulfil their responsibilities.

4.5 The Contractor shall ensure that Contractor Staff who no longer require access to the Authority Data (e.g. they cease to be employed by the Contractor or any of its Sub-Contractors), have their rights to access the Authority Data revoked within one (1) Business Day.

4.6 The Contractor shall ensure that Contractor Staff that have access to the Sites, the Shared Data Environment or the Authority Data receive regular training on security awareness that reflects the degree of access those individuals have to the Sites, the Shared Data Environment or the Authority Data.

4.7 The Contractor shall ensure that the training provided to Contractor Staff under paragraph 4.6 includes training on the identification and reporting fraudulent communications intended to induce individuals to disclose Personal Data or any other information that could be used, including in combination with other Personal Data or information, or with other techniques, to facilitate unauthorised access to the Sites, the Shared Data Environment or the Authority Data ("phishing").

5 Identity, Authentication and Access Control

5.1 The Contractor shall operate an access control regime to ensure:

(a) all users and administrators of the Contractor System are uniquely identified and authenticated when accessing or administering the Services; and

(b) all persons who access the Sites are identified and authenticated before they are allowed access to the Sites.

5.2 The Contractor shall apply the 'principle of least privilege' when allowing persons access to the Contractor System and Sites so that such persons are allowed access only to those parts of the Sites and the Contractor System they require.

5.3 The Contractor shall retain records of access to the Sites and to the Contractor System and shall make such record available to the Authority on request.

6 Audit and Protective Monitoring

6.1 The Contractor shall collect audit records which relate to security events in Contractor System or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Contractor audit records should (as a minimum) include regular reports and alerts setting out details of access by users of the Contractor System, to enable the identification of (without limitation) changing access trends, any unusual patterns of usage and/or accounts accessing higher than average amounts of Authority Data.

6.2 In addition to any requirement in Clause 37 (Cyber), the Contractor shall

(a) Implement audit and monitoring of the Contractor System sufficient to comply with any applicable Relevant Requirements and to prevent or detect any Prohibited Act;

(b) Keep sufficient records to demonstrate compliance with the requirements of paragraph 6.2(a) to the Authority; and

(c) Make those records and any documents describing the audit and monitoring undertaken to the Authority on request.

6.3 The Contractor and the Authority shall work together to establish any additional audit and monitoring requirements for the Contractor System.

6.4 The retention periods for audit records and event logs must be agreed with the Authority and documented in the Security and Information Management Plan.

7 Secure Architecture

7.1 The Contractor shall design the Contractor System in accordance with:

(a) the NCSC "Security Design Principles for Digital Services", a copy of which can be found at: https://www.ncsc.gov.uk/guidance/security-design-principles-digital-services-main;

(b) the NCSC "Bulk Data Principles", a copy of which can be found at: https://www.ncsc.gov.uk/guidance/protecting-bulk-personal-data-main; and

(c) the NSCS "Cloud Security Principles", a copy of which can be found at: https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles and which are summarised below:

(i) "Cloud Security Principle 1: data in transit protection" which, amongst other matters, requires that user data transiting networks should be adequately protected against tampering and eavesdropping;

(ii) "Cloud Security Principle 2: asset protection and resilience" which, amongst other matters, requires that user data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure;

(iii) "Cloud Security Principle 3: separation between users" which, amongst other matters, requires that a malicious or compromised user of the service should not be able to affect the service or data of another;

(iv) "Cloud Security Principle 4: governance framework" which, amongst other matters, requires that the Contractor should have a security governance framework which coordinates and directs its management of the Services and information within it;

(v) "Cloud Security Principle 5: operational security" which, amongst other matters, requires that the Services need to be operated and managed securely in order to impede, detect or prevent a Breach of Security;

(vi) "Cloud Security Principle 6: personnel security" which, amongst other matters, requires that where Contractor Staff have access to Authority Data and/or the Authority System that those personnel be subject to appropriate security screening and regular security training;

(vii) "Cloud Security Principle 7: secure development" which, amongst other matters, requires that the Services be designed and developed to identify and mitigate threats to their security;

(viii) "Cloud Security Principle 8: supply chain security" which, amongst other matters, requires the Contractor to ensure that appropriate security controls are in place with its Sub-Contractors and other Contractors;

(ix) "Cloud Security Principle 9: secure user management" which, amongst other matters, requires the Contractor to make the tools available for the Authority to securely manage the Authority's use of the Service;

(x) "Cloud Security Principle 10: identity and authentication" which, amongst other matters, requires the Contractor to implement appropriate controls in order to ensure that access to Service interfaces is constrained to authenticated and authorised individuals;

(xi) "Cloud Security Principle 11: external interface protection" which, amongst other matters, requires that all external or less trusted interfaces with the Services should be identified and appropriately defended;

(xii) "Cloud Security Principle 12: secure service administration" which, amongst other matters, requires that any IT system which is used for administration of a cloud service will have highly privileged access to that service;

(xiii) "Cloud Security Principle 13: audit information for users" which, amongst other matters, requires the Contractor to be able to provide the Authority

with the audit records it needs to monitor access to the Service and the Authority Data held by the Contractor and/or its Sub-Contractors;

(xiv) "Cloud Security Principle 14: secure use of the service" which, amongst other matters, requires the Contractor to educate Contractor Staff on the safe and secure use of the Contractor System.

ANNEX B

SECURITY ASPECTS LETTER

Defence Marine Services
Rm 221, 24 Store, Bldg 1/117
HM Naval Base Portsmouth
Hampshire
PO1 3LT

Reference: DMS-NG SAL

Date: 1 Dec 2022

Dear Sir / Madam,

DEFENCE MARINE SERVICES NEXT GENERATION ITN
CONTRACT 3 – SUPPLY AND MAINTENANCE OF MOORINGS, MARKERS AND TARGETS
CONTRACT NO: 703249457

SECURITY ASPECTS LETTER – Redacted under FOIA section 23 & 23 security bodies and national security