**ANNEX E – SECURITY ASPECTS LETTER**

|  |  |  |
| --- | --- | --- |
| **REDACTED** | **Defence Marine Services**  Rm 221, 24 Store, Bldg 1/117  HM Naval Base Portsmouth  Hampshire  PO1 3LT  **Reference:** DMS-NG SAL  **Date:** 21 Dec 22 |  |
|  | Our Reference: 073247450 |  |
|  |  |  |

**Dear Sir / Madam,**

**DEFENCE MARITIME SERVICES NEXT GENERATION ITN**

**CONTRACT 1 - SUPPORT TO IN-PORT MARINE SERVICES AND DELIVERY OF A VESSEL REPLACMENT**

**CONTRACT NO: 073247450**

**SECURITY ASPECTS LETTER**

1. On behalf of the Secretary of State for Defence, I hereby give the Tenderer notice of the information or assets connected with, or arising from, the referenced Invitation to Negotiate (ITN) that constitute classified material.
2. Aspects that constitute OFFICIAL-SENSITIVE for the purposes of DEFCON 660 are specified below. These aspects must be fully safeguarded. The Security Condition at Appendix 1 (UK Official and UK Official-Sensitive Contractual Security Conditions) to this Annex E outlines the minimum measures required to safeguard OFFICIAL-SENSITIVE assets and information.

|  |  |
| --- | --- |
| **ASPECT** | **CLASSIFICATION** |
| **REDACTED** | **REDACTED** |
| **REDACTED** | **REDACTED** |
| **REDACTED** | **REDACTED** |
| **REDACTED** | **REDACTED** |
| **REDACTED** | **REDACTED** |
| **REDACTED** | **REDACTED** |
| **REDACTED** | **REDACTED** |
| **REDACTED** | **REDACTED** |
| **REDACTED** | **REDACTED** |
| **REDACTED** | **REDACTED** |
| **REDACTED** | **REDACTED** |
| **REDACTED** | **REDACTED** |
| **REDACTED** | **REDACTED** |
| **REDACTED** | **REDACTED** |
| **REDACTED** | **REDACTED** |
| **REDACTED** | **REDACTED** |
| **REDACTED** | **REDACTED** |
| **REDACTED** | **REDACTED** |
| **REDACTED** | **REDACTED** |

1. The Tenderer's attention is drawn to the provisions of the Official Secrets Act (OSA) 1911-1989 in general, and specifically to the provisions of Section 2 of the Official Secrets Act 1911 (as amended by the Act of 1989). In particular the Tenderer should take all reasonable steps to make sure that all individuals employed on any work in connection with this ITN have notice of the above specified aspects and that the aforementioned statutory provisions apply to them and will continue to apply should the ITN be unsuccesful.
2. Will the Tenderer please confirm that:
   1. this definition of the classified aspects of the referenced ITN has been brought to the attention of the person directly responsible for security of classified material;
   2. the definition is fully understood;
   3. measures can, and will, be taken to safeguard the classified aspects identified herein in accordance with applicable national laws and regulations. The requirement and obligations set out above and in any contractual document can and will be met and that the classified information shall be protected in accordance with applicable national laws and regulations; and
   4. all employees of the company who will have access to classified information have either signed the OSA Declaration Form in duplicate and one (1) copy is retained by the Company Security Officer or have otherwise been informed that the provisions of the OSA apply to all classified information and assets associated with this ITN.
3. Clyde Naval Base security policy states that access requests for Foreign/Dual National Contractors or Naturalised British Citizens (born outside the UK) must only be made in exceptional circumstances where they are for highly specialised engineering techniques utilising SQEP that is unavailable in the UK. Only suitably cleared UK Nationals will be permitted to work in or visit Clyde Naval Base.
4. If the Tenderer has any difficulty either in interpreting this definition of the classified aspects or in safeguarding them, will the Tenderer please let me know immediately.
5. Classified Information associated with this ITN must not be published or communicated to anyone without the approval of the MOD Contracting Authority.
6. Any access to classified information or assets on MOD premises that may be needed will be subject to MOD security regulations under the direction of the MOD Project Officer in accordance with DEFCON 76 – attached at Appendix 2 (Contractor's Personnel at Government Establishments) of this Annex E.

Yours faithfully,

DMS-NG Contract Lead

Copy via email to:

[ISAC-Group (MULTIUSER)](mailto:ISAC-Group@mod.gov.uk)

[COO-DSR-IIPCSy (MULTIUSER)](mailto:COO-DSR-IIPCSy@mod.gov.uk)

[UKStratComDD-CyDR-CySAAS-021](mailto:Heather.Uzzell848@mod.gov.uk)

**APPENDIX 1 - UK OFFICIAL AND UK OFFICIAL-SENSITIVE CONTRACTUAL SECURITY CONDITIONS**

**Contract no: 798934450**

**In-Port Marine Services and Delivery of a Vessel Replacement Programme**

**21 Dec 22**

**Purpose**

1. This document provides guidance for Contractors where classified material provided to or generated by the Contractor is graded UK OFFICIAL or UK OFFICIAL-SENSITIVE. Where the measures requested below cannot be achieved or are not fully understood, further advice should be sought from the UK Designated Security Authority (Email: COO-DSR-IIPCSy@mod.gov.uk).

**Definitions**

1. The term "**Authority**" for the purposes of this Annex means the HMG Contracting Authority.
2. The term "**Classified Material**" for the purposes of this Annex means classified information and assets.

**Security Grading**

1. The SENSITIVE caveat is used to denote UK OFFICIAL material that is of a particular sensitivity and where there is a need to reinforce the ‘need to know’. The Security Aspects Letter, issued by the Authority shall define the UK OFFICIAL-SENSITIVE material that is provided to the Contractor, or which is to be developed by it, under this Contract. The Contractor shall mark all UK OFFICIAL and UK OFFICIAL-SENSITIVE documents which it originates or copies during the Contract with the applicable security grading.

**Security Conditions**

1. The Contractor shall take all reasonable steps to adhere to the provisions specified in the Contract or listed in this Annex E. The Contractor shall make sure that all individuals employed on any work in connection with the Contract have notice that these provisions apply to them and shall continue to apply after the completion or earlier termination of the Contract. In accordance with Part D (Records) of Schedule 6 (Governance, Management Information, Reports, Records and Audit) the Authority must state the data retention periods to allow the Contractor to produce a data management policy. If Tenderers are a Contractor located in the UK their attention is also drawn to the provisions of the Official Secrets Acts 1911 to 1989 in general, and to the provisions of Section 2 of the Official Secrets Act 1911 (as amended by the Act of 1989) in particular.

**Protection of UK OFFICIAL and UK OFFICIAL-SENSITIVE Classified Material**

1. The Contractor shall protect UK OFFICIAL and UK OFFICIAL-SENSITIVE material provided to or generated by it in accordance with the requirements detailed in this Security Condition and any other conditions that may be specified by the Authority. The Contractor shall take all reasonable steps to prevent the loss or compromise of classified material whether accidentally or from deliberate or opportunist attack.
2. Once the Contract has been awarded, where Contractors are required to store or process UK MOD classified information electronically, they are required to register the IT system onto the Defence Assurance Risk Tool (DART). Details on the registration process can be found in the ‘Industry Security Notices (ISN)’ on Gov.UK website. ISNs 2017/01, 04 and 06, Defence Condition 658 and Defence Standard 05-138 details the DART registration, IT security accreditation processes, risk assessment/management and Cyber security requirements which can be found in the following links:

<https://www.gov.uk/government/publications/industry-security-notices-isns>.

<http://dstan.gateway.isg-r.r.mil.uk/standards/defstans/05/138/000002000.pdf>

<https://www.gov.uk/government/publications/defence-condition-658-cyber-flow-down>

1. All UK classified material including documents, media and other assets must be physically secured to prevent unauthorised access. When not in use UK OFFICIAL and UK OFFICIAL-SENSITIVE material shall be handled with care to prevent loss or inappropriate access. As a minimum UK OFFICIAL-SENSITIVE material shall be stored under lock and key and shall be placed in a lockable room, cabinets, drawers or safe and the keys/combinations shall be subject to a level of control.
2. Disclosure of UK OFFICIAL and UK OFFICIAL-SENSITIVE material must be strictly controlled in accordance with the "need to know" principle. Except with the written consent of the Authority, the Contractor shall not disclose the Contract or any provision thereof to any person other than to a person directly employed by the Contractor or Sub-Contractor.
3. Except with the consent in writing of the Authority the Contractor shall not make use of the Contract or any information issued or provided by or on behalf of the Authority otherwise than for the purpose of the Contract, and, same as provided for in paragraph 8 above, the Contractor shall not make use of any article or part thereof similar to the articles for any other purpose.
4. Subject to any intellectual property rights of third parties, nothing in this Security Condition shall restrict the Contractor from using any specifications, plans, drawings and other documents generated outside of this Contract.
5. Any samples, patterns, specifications, plans, drawings or any other documents issued by or on behalf of the Authority for the purposes of the Contract remain the property of the Authority and must be returned on completion of the Contract or, if directed by the Authority, destroyed in accordance with paragraph 35.

**Access**

1. Access to UK OFFICIAL and UK OFFICIAL-SENSITIVE material shall be confined to those individuals who have a “need-to-know”, have been made aware of the requirement to protect the information and whose access is essential for the purpose of their duties.
2. The Contractor shall ensure that all individuals requiring access to UK OFFICIAL-SENSITIVE information have undergone basic recruitment checks. This should include establishing proof of identity; confirming that they satisfy all legal requirements for employment by the Contractor; and verification of their employment record. Criminal record checks should also be undertaken where permissible under national/local laws and regulations. This is in keeping with the core principles set out in the UK Government (HMG) Baseline Personnel Security Standard (BPSS) which can be found at:

<https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/714002/HMG_Baseline_Personnel_Security_Standard_-_May_2018.pdf>

**Hard Copy Distribution**

1. UK OFFICIAL and UK OFFICIAL-SENSITIVE documents may be distributed, both within and outside Contractor premises in such a way as to make sure that no unauthorised person has access. It may be sent by ordinary post in a single envelope. The words UK OFFICIAL or UK OFFICIAL-SENSITIVE must not appear on the envelope. The envelope must bear a stamp or marking that clearly indicates the full address of the office from which it was sent. Commercial Couriers may be used.
2. Advice on the distribution of UK OFFICIAL-SENSITIVE documents abroad or any other general advice including the distribution of UK OFFICIAL-SENSITIVE shall be sought from the Authority.

**Electronic Communication and Telephony and Facsimile Services**

1. UK OFFICIAL information may be emailed unencrypted over the internet. UK OFFICIAL-SENSITIVE information shall normally only be transmitted over the internet encrypted using either a National Cyber Security Centre (NCSC) Commercial Product Assurance (CPA) cryptographic product or a UK MOD approved cryptographic technique such as Transmission Layer Security (TLS). In the case of TLS both the sender and recipient organisations must have TLS enabled. Details of the required TLS implementation are available at:

<https://www.ncsc.gov.uk/guidance/tls-external-facing-services>

Details of the CPA scheme are available at:

<https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa>

1. Exceptionally, in urgent cases UK OFFICIAL-SENSITIVE information may be emailed unencrypted over the internet where there is a strong business need to do so, but only with the prior approval of the Authority. However, it shall only be sent when it is known that the recipient has been made aware of and can comply with the requirements of these Security Conditions and subject to any explicit limitations that the Authority require. Such limitations including any regarding publication, further circulation or other handling instructions shall be clearly identified in the email sent with the material.
2. UK OFFICIAL information may be discussed on fixed and mobile telephones with persons located both within the country of the Contractor and overseas. UK OFFICIAL-SENSITIVE information may be discussed on fixed and mobile telephones only where there is a strong business need to do so and only with the prior approval of the Authority.
3. UK OFFICIAL information may be faxed to recipients located both within the country of the Contractor and overseas, however UK OFFICIAL-SENSITIVE information may be transmitted only where there is a strong business case to do so and only with the prior approval of the Authority.

**Use of Information Systems**

1. The detailed functions that must be provided by an IT system to satisfy the minimum requirements cannot all be described here in specific detail; it is for the implementers to identify possible means of attack and ensure proportionate security mitigations are applied to prevent a successful attack.
2. The Contractor should ensure 10 steps to Cyber Security (link below) is applied in a proportionate manner for each IT and communications system storing, processing or generating UK OFFICIAL or UK OFFICIAL-SENSITIVE information. The Contractor should ensure competent personnel apply 10 steps to Cyber Security.

<https://www.ncsc.gov.uk/guidance/10-steps-cyber-security>.

1. As a general rule, any communication path between an unauthorised user and the data can be used to carry out an attack on the system or be used to compromise or ex-filtrate data.
2. Within the framework of the 10 steps to Cyber Security, the following describes the minimum security requirements for processing and accessing UK OFFICIAL-SENSITIVE information on IT systems.
   1. Access. Physical access to all hardware elements of the IT system is to be strictly controlled. The principle of “least privilege” will be applied to System Administrators. Users of the IT system (administrators) should not conduct ‘standard’ user functions using their privileged accounts.
   2. Identification and Authentication (ID&A). All systems are to have the following functionality:
      1. up-to-date lists of authorised users; and
      2. positive identification of all users at the start of each processing session.
   3. Passwords. Passwords are part of most ID&A security measures. Passwords are to be “strong” using an appropriate method to achieve this, e.g. including numeric and “special” characters (if permitted by the system) as well as alphabetic characters.
   4. Internal Access Control. All systems are to have Internal Access Controls to prevent unauthorised users from accessing or modifying the data.
   5. Data Transmission. Unless the Authority authorises otherwise, UK OFFICIAL-SENSITIVE information may only be transmitted or accessed electronically (e.g. point to point computer links) via a public network like the Internet, using a CPA product or equivalent as described in paragraph 16 (Hard Copy Distribution) above.
   6. Security Accounting and Audit. Security relevant events fall into two categories, namely legitimate events and violations.
      1. The following events shall always be recorded:
         1. all log on attempts whether successful or failed;
         2. log off (including time out where applicable);
         3. the creation, deletion or alteration of access rights and privileges; and
         4. the creation, deletion or alteration of passwords.
      2. For each of the events listed above, the following information is to be recorded:
         1. type of event;
         2. user ID;
         3. date & time; and
         4. device ID.

The accounting records are to have a facility to provide the System Administrator with a hard copy of all or selected activity. There also must be a facility for the records to be printed in an easily readable form. All security records are to be inaccessible to users without a need to know. If the operating system is unable to provide this then the equipment must be protected by physical means when not in use i.e. locked away or the hard drive removed and locked away.

* 1. Integrity & Availability. The following supporting measures are to be implemented:
     1. provide general protection against normally foreseeable accidents/mishaps and known recurrent problems (e.g. viruses and power supply variations);
     2. defined Business Contingency Plan;
     3. data backup with local storage;
     4. anti-virus software (implementation, with updates, of an acceptable industry standard anti-virus software);
     5. operating systems, applications and firmware should be supported; and
     6. patching of operating systems and applications used are to be in line with the manufacturers recommended schedule. If patches cannot be applied an understanding of the resulting risk will be documented.
  2. Logon Banners. Wherever possible, a *“*Logon Banner*”* will be provided to summarise the requirements for access to a system which may be needed to institute legal action in case of any breach occurring. A suggested format for the text (depending on national legal requirements) could be:

*“Unauthorised access to this computer system may constitute a criminal offence”*

* 1. Unattended Terminals. Users are to be automatically logged off the system if their terminals have been inactive for some predetermined period of time, or systems must activate a password protected screen saver after 15 minutes of inactivity, to prevent an attacker making use of an unattended terminal.
  2. Internet Connections. Computer systems must not be connected direct to the Internet or *“*un-trusted*”* systems unless protected by a firewall (a software based personal firewall is the minimum but risk assessment and management must be used to identify whether this is sufficient).
  3. Disposal. Before IT storage media (e.g. disks) are disposed of, an erasure product must be used to overwrite the data. This is a more thorough process than deletion of files, which does not remove the data.

**Laptops**

1. Laptops holding any UK OFFICIAL-SENSITIVE information shall be encrypted using a CPA product or equivalent as described in paragraph 17 (Electronic Communication and Telephony and Facsimile Services) above.
2. Unencrypted laptops and drives containing personal data are not to be taken outside of secure sites[[1]](#footnote-2). For the avoidance of doubt the term “drives” includes all removable, recordable media e.g. memory sticks, compact flash, recordable optical media (CDs and DVDs), floppy discs and external hard drives.
3. Any token, touch memory device or password(s) associated with the encryption package is to be kept separate from the machine whenever the machine is not in use, left unattended or in transit.
4. Portable CIS devices holding the Authorities’ data are not to be left unattended in any public location. They are not to be left unattended in any motor vehicles either in view or in the boot or luggage compartment at any time. When the vehicle is being driven the CIS is to be secured out of sight in the glove compartment, boot or luggage compartment as appropriate to deter opportunist theft.

**Loss and Incident Reporting**

1. The Contractor shall immediately report any loss or otherwise compromise of any OFFICIAL or OFFICIAL-SENSITIVE material to the Authority. In addition any loss or other compromise of any UK MOD owned, processed or UK MOD Contractor generated UK OFFICIAL or UK OFFICIAL-SENSITIVE material is to be immediately reported to the UK MOD Defence Industry Warning, Advice and Reporting Point (WARP). This will assist the MOD in formulating a formal information security reporting process and the management of any associated risks, impact analysis and upward reporting to the UK MOD’s Chief Information Officer (CIO) and, as appropriate, the Contractor concerned. The UK MOD WARP will also advise the Contractor what further action is required to be undertaken.

**WARP Contact Details**

**Email:** [DefenceWARP@mod.gov.uk](mailto:DefenceWARP@mod.gov.uk) (OFFICIAL with no NTK restrictions)

**RLI Email:** [defencewarp@modnet.rli.uk](mailto:defencewarp@modnet.rli.uk) (MULTIUSER)

**Telephone (Office hours):** +44 (0) 30 6770 2185

**Mail:** Defence Industry WARP, DE&S PSyA Office

MOD Abbey Wood, NH2 Poplar-1 #2004, Bristol, BS34 8JH

1. Reporting instructions for any security incidents involving MOD classified material can be found in Industry Security Notice 2017/03 as may be subsequently updated at:

<https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/651683/ISN_2017-03_-_Reporting_of_Security_Incidents.pdf>

**Sub-Contracts**

1. Where the Contractor wishes to sub-contract any elements of a Contract to Sub-Contractors within its own country or to Contractors located in the UK such sub-contracts will be notified to the contracting Authority. The Contractor shall ensure that these Security Conditions are incorporated within the sub-contract document.
2. The prior approval of the Authority shall be obtained should the Contractor wish to sub-contract any UK OFFICIAL-SENSITIVE elements of the Contract to a Sub-Contractor facility located in another (third party) country. The first page of Appendix 5 (MOD Form 1686 (F1686) of the GovS 007 Security Contractual Process chapter is to be used for seeking such approval. The MOD Form 1686 can be found at Appendix 5 at:

<https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/710891/2018_May_Contractual_process.pdf>

1. If the sub-contract is approved, the Contractor will flow down the Security Conditions in line with paragraph 31 (Sub-Contracts) above to the Sub-Contractor. Contractors located overseas may seek further advice and/or assistance from the Authority with regards the completion of F1686.

**Publicity Material**

1. Contractors wishing to release any publicity material or display assets that arise from a Contract to which these Security Conditions apply must seek the prior approval of the Authority. Publicity material includes open publication in the Contractor’s publicity literature or website or through the media; displays at exhibitions in any country; lectures or symposia; scientific or technical papers, or any other occasion where members of the general public may have access to the information even if organised or sponsored by the UK Government.

**Physical Destruction**

1. As soon as no longer required, UK OFFICIAL and UK OFFICIAL-SENSITIVE material shall be destroyed in such a way as to make reconstitution very difficult or impossible, for example, by burning, shredding or tearing into small pieces. Advice shall be sought from the Authority when information/material cannot be destroyed or, unless already authorised by the Authority, when its retention is considered by the Contractor to be necessary or desirable. Unwanted UK OFFICIAL-SENSITIVE information/material which cannot be destroyed in such a way shall be returned to the Authority.

**Interpretation/Guidance**

1. Advice regarding the interpretation of the above requirements should be sought from the Authority.
2. Further requirements, advice and guidance for the protection of UK classified information at the level of UK OFFICIAL-SENSITIVE may be found in Industry Security Notices at:

<https://www.gov.uk/government/publications/industry-security-notices-isns>

**Audit**

1. Where considered necessary by the Authority the Contractor shall provide evidence of compliance with this Security Condition and/or permit the inspection of the Contractors processes and facilities by representatives of the Contractors’ National/Designated Security Authorities or the Authority to ensure compliance with these requirements.

**APPENDIX 2 - DEFCON 76: CONTRACTOR’S PERSONNEL AT GOVERNMENT ESTABLISHMENTS**

**Contract no: 798934450**

**In-Port Marine Services and Delivery of a Vessel Replacement Programme**

**21 Dec 22**

**Contractor's Representatives**

1. The Contractor shall submit in writing to the Authority for approval, initially and as necessary from time to time, a list of those of its Representatives who may need to enter a Government Establishment for the purpose of, or in connection with, work under the Contract, giving such particulars as the Authority may require, including full details of birthplace and parentage of any such Representative who:
   1. was not born in the United Kingdom; or
   2. if they were born in the United Kingdom, was born of parents either or both of whom were not born in the United Kingdom.
2. The Authority shall issue passes for those Representatives who are approved by it in accordance with paragraph 1 herein for admission to a Government Establishment and a Representative shall not be admitted unless in possession of such a pass. Passes shall remain the property of the Authority and shall be surrendered on demand or on completion of the work.
3. Notwithstanding the provisions of paragraphs 1 and 2 hereof if, in the opinion of the Authority, any Representative of the Contractor shall misconduct themselves, or it shall not be in the public interest for any person to be employed or engaged by the Contractor, the Contractor shall remove such person without delay on being required to do so and shall cause the work to be performed by such other person as may be necessary.
4. The decision of the Authority upon any matter arising under paragraphs 1 to 3 inclusive shall be final and conclusive.

**Observance of Regulations**

1. The following provisions apply:
   1. The Contractor shall ensure that his Representatives have the necessary probity (by undertaking the Government’s Baseline Personnel Security Standard) and, where applicable, are cleared to the appropriate level of security when employed within the boundaries of a Government Establishment.
   2. Where the Contractor requires information on the Government’s Baseline Personnel Security Standard (the Standard) or security clearance for his Representatives or is not in possession of the relevant rules, regulations or requires guidance on them, he shall apply in the first instance to the Project Manager/Equipment Support Manager.
   3. On request, the Contractor shall be able to demonstrate to the Authority that the Contractor’s processes to assure compliance with the standard have been carried out satisfactorily. Where that assurance is not already in place, the Contractor shall permit the Authority to inspect the processes being applied by the Contractor to comply with the Standard.
   4. The Contractor shall comply and shall ensure that his Representatives comply with the rules, regulations and requirements that are in force whilst at that Establishment which shall be provided by the Authority on request.
   5. When on board ship, compliance with the rules, regulations, and requirements shall be in accordance with the Ship's Regulations as interpreted by the Officer in Charge. Details of those rules, regulations and requirements shall be provided on request by the Officer in Charge.

1. Secure Sites are defined as either Government premises or a secured office on the contractor premises. [↑](#footnote-ref-2)