**CCS FRAMEWORK RM 3816**

**ESTATES PROFESSIONAL SERVCIES**

**FOR**

**FEASIBILITY STUDY – STRATTON**

**LONDON RESERVE ESTATE**

**STATEMENT OF REQUIREMENT**

**EPS\_00047\_2017 (DIOCB3/218)**

**Introduction**

1. The purpose of the feasibility study is to assess the current laydown of the Reserve sites across London and Windsor and to determine the optimal laydown of the estate which will encompass the use of the Regular Barracks, development of Super Reserve Centres (SRC) and a small number of retained key Reserve Centres.

1. This requirement is requesting a feasibility study that must consider the current real estate with the Defence Estate Optimisation (DEO) business objectives that will:
   1. Produce a baseline position for each Reserve Centre (RC) establishing the condition, costs and value of each of the sites;
   2. Through modelling scenario’s with differing concentrations of SRC and analytical advice propose the optimal operational future laydown options that provides Value for Money (VfM) for the continuing running of the Reserve Estate for the next 25 years;
   3. Consider the operational, future and strategic factors impacting on the London Reserve estate located in London;
   4. Achieve delivery of a feasibility study to the highest level that will add value across the lines of development for DEO business objectives for project Stratton;
   5. Realisation of capital receipts considering the net operating costs; and
   6. Determine implementation costs and income receipts for options that concur with DEO business objectives.

**Background**

1. The current reserve estate in London, both in terms of building design as well as physical location has evolved through time rather than of intent, and whilst the estate has evolved to meet the requirement, they are not necessarily optimised to do so. Utilising the inclusion of the SRC concept the MOD has a potential opportunity to optimise its functionality with new fit for purpose facilities.
2. Project Stratton has been initiated to optimise the London reserve estate in order to meet the needs of the reserve forces in the modern operating environment. This will be achieved by undertaking investment in core sites and either disposing or commercialising of surplus estate where identified.
3. The Reserve Centre of the 21st Century should be designed and built ‘smarter’, incorporating the latest technological and ergonomic standards enabling flexible and collaborative working environments and best practice from industry and government, all of which will contribute to the reduction of operating costs and aid the overall reduction of the Defence estate. The reserve centre of the future must also acknowledge changes in working practices and recognise the benefits of colocation, both with regular and reserve units. This forms the basis of the SRC and Joint Cadet Centre (JCC) concept which presents an opportunity to address deficiencies in the current estate and presents a sustainable vision for the future.
4. Similarly, as the regular estate footprint within London decreases the reserve estate must be optimised to meet the wider needs of defence, supporting the whole force concept, as well as other government departments (OGDs) as may be required. It should be recognised that there are Pan Defence Lines of Development (DLOD) benefits to investing in and rationalising the reserve estate.
5. This is a tri-service review; the scope of which includes all reserve and a number of the larger cadet centres within the London area, as defined by those sites within the M25 and also including Windsor.

**Objectives**

1. The feasibility study will evaluate opportunities that will inform the strategic decision for the optimisation of the Reserve estate in London. This will;
   1. Enable open discussion, challenge and clarity on each option development, providing the flexibility to meet priorities as they mature;
   2. Understanding land and assets are key to success at this stage of the project, accounting for constraints, planning, leases, and restrictions for disposing of assets – there must be clear links to Operational service delivery to the estate optimisation strategy.
   3. This will inform DEO of the viability to progress this project to the next stage of delivery, which will deliver an improved, effective but smaller estate footprint that is more cost effective to sustain and is funded through realisation of capital receipts from surplus estate.
2. The contractor must work closely with DEO throughout the development of the feasibility study, ensuring opportunities are identified and considered at an early stage without compromising the operational capability and business as usual.

**Scope**

1. The goal is to achieve and maximise the capital receipts from those buildings or land parcels identified that will no longer be required from optimising the estate that is currently used by the Reserves in London.
2. The contractor must have the expertise as a real estate professional understanding the geographical dynamics within London, identifying opportunities and options for a successful outcome considering such tasks as;
   1. Identifying estate solutions that will provide value for money options when down selecting the location(s) of the Reserve estate;
   2. Making strategic recommendations from factual evidence that considers;
      1. Understanding the role of the Reserve Force with the Regular Forces;
      2. Current and future laydown plan for the Reserves;
      3. Impact on the Units and the Reservists with any proposed laydown;
      4. Transportation and accessibility for implementing viable options;
      5. Base line value of the Reserve Forces estate;
      6. Market analysis considering the total revenue that will be gained from receipts, generated income, property and land valuations maximising the optimum solution for the Reserve Force estate;
      7. Space management analysis ensuring an efficient estate, utilising all land and buildings while taking into account the current and future capability needs;
      8. Financial analysis using an agreed process supporting the down selection of options;
      9. SWOT analysis that considers the impact of option ranking with the enduring capability;
      10. Identifying the planning, legislative, statutory, environmental, ecological, operational and sustainable support for viable options;
      11. Master Data Assumptions List (MDAL); and
      12. Clear decision and communications structure for developing the feasibility study making known to DEO any benefits and / or opportunities
3. There are 43 reserve estate sites within the London cluster. These sites, managed by the Greater London Reserve Forces and Cadets Association (GLRFCA), are a mixture of freehold and leasehold to GLRFCA or MOD. Site particulars are available in the Feasibility Study brief, including location and minimum space requirements. In Addition, there are 145 Cadet Centres some are which located in the Reserve sites. Cadets are excluded from this feasibility study unless they are currently co-located with on an effected Reserve site.
4. Project Stratton is part of the London District Sub-programme board that will require regular updates on progress and project achievements for the delivery of the feasibility study, which must be completed by, but no later than 31st March 2018.
5. OFFICIAL and OFFICIAL- SENSITIVE Security Condition for UK Contracts Definitions is detailed at Annex A to this statement of requirement. Security, escorting and relevant clearances including access to the sites must be by prior arrangement with the appropriate DIO authority noting that;
   1. The contractor must complete the Baseline Personal Security Standard (BPSS) in all instances that will allow individuals to access most establishments unescorted;
   2. The contractor shall ensure that all material, including maps, blueprints, sketches and written material, is handled and stored in accordance with the Government Security Classification (GSC) Policy and the JSP 440 – Defence Manual of Resilience, Business Continuity and Security ensuring full compliance with the confidentiality clause for this contract;
   3. Where release is required to a sub-contracted partner then the contractor will seek approval for the release of classified information.
   4. Documents are only to be addressed to those authorised for access.
   5. For this contract the control and management of the Feasibility Study Report including relevant supporting information, will be classified as “**OFFICIAL – SENSITIVE**” Government Furnished Information (GFI).
   6. For the purposes of this Contract a Security Aspects Letter (SAL) is a requirement for the Invitation to Tender and provided with this Invitation to Tender.
6. The feasibility study, supporting plans, drawings, and spreadsheets if issued as part of the feasibility study must use the software that is compatible with the MOD;
   1. Report – Word
   2. Financial spread sheets – Excel
   3. Project plans – Microsoft Project
   4. Drawings – PDF
7. Whilst undertaking the study the following must be fully addressed:
   1. Conformance with Relevant construction JSP/BPS;
   2. Obtain all necessary and appropriate security passes (personal and vehicular);
   3. H & S compliance;
   4. Ensure all operatives attend mandatory 4C’s Induction Safety Training; and
   5. The supplier, owner, maintainer, operator, interfaces of all service supplies must be thoroughly recorded and considered.

**Requirements**

1. The programme for the feasibility study will commence 8 January 2018 concluding 30 March 2018, duration of three months. Progress will be reported monthly at Andover or London MOD Main Building, with key decisions taking place at London MOD Main Building Whitehall, where delivery progress can be assessed against the strategic objectives of the DEO programme.
2. The acceptance process will be in two parts. The contractor will present to DIO the draft feasibility study report including development analysis of viable options for endorsement. On receiving that endorsement, the contractor will present the final feasibility study report to the project Stratton sub-programme board that are the authority to accept this study – this is in addition to the monthly progress meetings and the key decision meetings at Andover and London.
3. Engagement with key stakeholders and, pre-agreement of all analysis models used in the development of the feasibility study, will enhance the quality of the final report. Technical advice on the scrutiny and approval process including the quality of project deliverables will build a solid foundation and acceptance of the final feasibility study report by the wider MOD Subject Matter Experts. Early engagement of the Army Front Line Command (FLC) is also a recommendation in building that strong foundation, seeking strategic advice and guidance on the current and future lay down plan for Reserves in London.
4. The feasibility study is the key deliverable supported by relevant information that underpins the analysis outputs for the down selection of options to the few. Performance against this key deliverable will be assessed at the monthly meetings and presentations by the contractor.
5. A specific requirement will be the governance, management and control of project delivery (including safety) arrangements used by the contractor for this phase of the project programme. DEO will expect, at mobilisation, appointments of key project staff including a Project Execution Plan (PEP) to include MDAL, risk register and a Level 0 schedule.

**Outputs/deliverables/milestones**

**Outputs**

1. The results from the feasibility study must provide the sufficient technical information to enable them to support DEO on the London Reserve estate that provides:
   1. A baseline position for the current Reserve Estate
   2. Provide six (6) proposed alternative future laydowns for the London Reserve Estate

**Milestones**

1. A lump sum contract with relevant payments on project achievements against each milestone detailed in the table below.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Milestone No** | **Milestone** | **Payment** | **Programme Submission Timeline** | **Verification** |
| 1 | Appointment of team and presentation of Project Execution Plan | 10% | Week 1 | DIO Progress Board |
| 2 | Completion and acceptance of the baseline report for the current reserve estate | 50% | Week 8 | DIO Progress Board |
| 3 | Acceptance of draft final feasibility study report | 20% | Week 10 | DIO Progress Board |
| 4 | Acceptance of final feasibility study report | 20% | Week 12 | STRATTON Sub-programme Board |

**Deliverables**

1. The programme for the delivery of the feasibility study will identify the deliverables, milestones including scheduled tasks that will be required for this stage of the project. Therefore the deliverables are;
   1. Baseline report for each Reserve site establishing the condition, utilisation, costs to run and maintain (inc. backlog), and the current estimated value of each of the sites;
   2. For each Reserve site understand if there are any key capability requirements that need to be addressed in any future location for the unit;
   3. For each site identified in the future laydown include;
   4. Indicative build cost for each of the proposed sites
   5. Condition of the property that any development
   6. Any listings to be considered
   7. Town planning considerations
   8. Proportion of new build versus reuse required to accommodate the proposed SRC
   9. Future Revenue Departmental Expenditure Limit (RDEL) costs, i.e. planned and outstanding maintenance.
   10. Impact on the units / reservists to be moved (e.g. increase travel time, parking etc.)
   11. Note where there are current differences between the current provision and that defined in the relevant Joint Service Publication (JSP);
   12. At least a minimum of 6 scenarios modelled with a different number of SRCs and geographical dispersement that will be assessed to define the optimal laydown;
   13. Facilitated workshops which review and refine the scenarios to deliver the proposed future Reserve laydown for London; (A maximum of 6 workshops divided equally between Andover and London.
   14. Risk register;
   15. MDAL;
   16. Progress reports, presentations including development of analyses of viable options;
   17. Monthly meetings at either Andover and / or London;
   18. Project Execution Plan; and
   19. Pre-start meeting.
2. The contractor will, in the development of the feasibility study, travel between London and Andover, the responsibility for transport and T&S costs remaining with the contractor.
3. Variations may give rise to additions or deductions from the contracted lump sum and must include not only the work which the variation order describes, but other expenses that may result from the variation i.e. impact on scope, programmed work tasks including T&S using CCS RM3816 Framework Rates from the lump sum contract.
4. Payments shall follow CP&F e-invoicing following approval by DIO against the agreed milestones.
5. A soft copy as well as hard copy will be required with all project information collated and saved on disk.

**Acceptance**

1. Acceptance of the feasibility study will be through the project STRATTON sub-programme board.
2. Monthly progress meetings will assess the quality of the Feasibility Study outputs the Financial Appraisal following the conventions detailed in JSP 507. This is the required standard for the Feasibility Report, a key user requirement for this stage of the project.

**Intellectual Property (IP) Rights (Known as IPR)**

1. Intellectual property rights will be a condition of the contract for this service provision. DIO will have full rights to the Feasibility Study Report and supporting information.
2. This report will be furnished as Government Information for those contracts that will be used for the next project stage, delivery of the Assessment Study.

**Government Furnished Supplies**

1. The following Government Furnished Information (GFI) will be available on appointment of the winning contractor:
   1. JSP 313 – Combined Cadet Force Manual
   2. JSP 315 - Building Performance Standards (BSP)
   3. Scale 80 - TAVRA Accommodation Reserve and Cadet Forces
   4. JSP 426 – Defence Fire Safety and Fire Risk Management
   5. JSP 440 – Defence Manual of Security
   6. JSP 507 – Investment Appraisal and Evaluation
   7. JSP 516 – The Reserve Forces Act 1996
   8. JSP 752 – Tri service Regulations for Expenses and Allowances
   9. JSP 814 – Policy and regulations for MOD Sponsored Cadet Forces
   10. JSP 815 – Defence Health and Safety and Environment
   11. JSP 892 – Risk Management
   12. DEO Feasibility Brief – Listing of sites, reserve estate review, specification for SRC sizing requirement, feasibility scenario assessment matrix.

**Approach**

1. DIO will facilitate Subject Matter Expert advice during the market, financial and risk analysis.

**Payment**

1. The contractor will be paid at each milestone achievement, when DIO consider that project progress or development of the analysis, final report is of a standard for acceptance to the DEO;
   1. MS1 – Appointment of team and presentation of Project Execution Plan
   2. MS2 – Completion and acceptance of the baseline report for the current Reserve Estate.
   3. MS3 – Acceptance of the draft final feasibility study report.
   4. MS4 – Acceptance of the final feasibility study report.
2. Payment will only be made on successful delivery of the milestones and never in advance.

**Contract management arrangements**

1. Stakeholder engagement is the responsibility of all those involved in the development and delivery of the feasibility report. Regular consultation is essential to ensure that the requirements are agreed and a delivery solution is negotiated that is acceptable to DEO. It is expected that the winner contractor will demonstrate strong governance providing clarity in stakeholder engagement across all boundaries and what will be expected of people involved when engaged in developing the feasibility study report.
2. Change request must be provided by the winning contractor in a timely submission using the recognised template (issued on contract award) to DEO PPD. This is part of the formal process in seeking a change request approval which must consider affordability and impact on the agree scope for this study. Decisions resulting from submissions that require an official approval will be in full consultation with DEO who can advise on affordability and impact on the scope for this study.
3. All change requests must be submitted on the PPD DEO Project Change Request Form and submitted to the Project Manager detailed in Section 2 of the DEFFORM 111.
4. The contractor will be monitored throughout the duration of the contract at the monthly meetings planned at Andover, where progress and the quality of the deliverable will be assessed.
5. At each meeting the contractor will provide a power point presentation on project progress including achievements, responding in a timely manner actions that are captured as recorded of decisions.
6. The acceptance of the feasibility study will be by the STRATTON Sub-programme Board.

**ANNEX A to**

**Statement of Requirement**

**OFFICIAL and OFFICIAL- SENSITIVE Security Condition for UK Contracts**

**Definitions**

**1. The term "Authority" means a Ministry of Defence (MOD) official acting on behalf of the Secretary of State for Defence.**

**Security Grading**

**2. All aspects associated with this Contract are classified OFFICIAL. Some aspects are more sensitive and are classified as OFFICIAL-SENSITIVE. The Authority shall issue a Security Aspects Letter which shall define the OFFICIAL- SENSITIVE information that is furnished to the Contractor, or which is to be developed by it, under this Contract. The Contractor shall mark all OFFICIAL-SENSITIVE documents which it originates or copies during the Contract clearly with the OFFICIAL-SENSITIVE classification. However, the Contractor is not required to mark information/material related to the contract which is only OFFICIAL.**

**Official Secrets Acts**

**3. The Contractor's attention is drawn to the provisions of the Official Secrets Acts 1911-1989 in general, and to the provisions of Section 2 of the Official Secrets Act 1911 (as amended by the Act of 1989) in particular. The Contractor shall take all reasonable steps to make sure that all individuals employed on any work in connection with the Contract (including sub-contractors) have notice that these statutory provisions, or any others provided by the Authority, apply to them and shall continue so to apply after the completion or earlier termination of the Contract.**

**Protection of OFFICIAL and OFFICIAL- SENSITIVE Information**

**4. The Contractor shall protect OFFICIAL and OFFICIAL-SENSITIVE information provided to it 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 the information or from deliberate or opportunist attack.**

**5. The contractor shall apply Industry Security Notice (ISN) 2017/01 requirements to every industry owned IT and communication system used to store, process or generate MOD information including those systems containing OFFICIAL and/or OFFICIAL-SENSITIVE information. ISN 2017/01 details Defence Assurance and Risk Tool (DART) registration, IT security accreditation processes, risk assessment and risk management requirements. The ISN is available at:**

**<https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/594320/DART_ISN_-_V2_3.pdf>**

**6. OFFICIAL and OFFICIAL-SENSITIVE information shall be protected in a manner to avoid unauthorised access. The Contractor shall take all reasonable steps to prevent the loss, compromise or inappropriate access of the information or from deliberate or opportunist attack.**

**7. All OFFICIAL and OFFICIAL-SENSITIVE material including documents, media and other material shall be physically secured to prevent unauthorised access. When not in use OFFICIAL and OFFICIAL- SENSITIVE documents/material shall be handled with care. As a minimum, when not in use, OFFICIAL-SENSITIVE material shall be stored under lock and key and in a lockable room, cabinets, drawers or safe and the keys/combinations are themselves to be subject to a level of physical security and control.**

**8. Disclosure of OFFICIAL and OFFICIAL-SENSITIVE information shall be strictly in accordance with the "need to know" principle. Except with the written consent of the Authority, the Contractor shall not disclose any of the classified aspects of the Contract detailed in the Security Aspects Letter other than to a person directly employed by the Contractor or sub-Contractor, or Service Provider.**

**9. 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 shall be returned on completion of the Contract or, if directed by the Authority, destroyed in accordance with paragraph 32.**

**Access**

**10. Access to OFFICIAL and OFFICIAL-SENSITIVE information 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 his or her duties.**

**11. The Contractor shall ensure that all individuals having access to OFFICIAL-SENSITIVE information have undergone basic recruitment checks. Contractors shall apply the requirements of HMG Baseline Personnel Security Standard (BPSS) for all individuals having access to OFFICIAL-SENSITIVE information. Further details and the full requirements of the BPSS can be found at the Gov.UK website at:**

[**https://www.gov.uk/government/publications/government-baseline-personnel-security-standard**](https://www.gov.uk/government/publications/government-baseline-personnel-security-standard)**.**

**Hard Copy Distribution**

**12. OFFICIAL and OFFICIAL-SENSITIVE documents shall be distributed, both within and outside company premises in such a way as to make sure that no unauthorised person has access. It may be sent by ordinary post or Commercial Couriers in a single envelope. The words OFFICIAL or OFFICIAL-SENSITIVE shall not appear on the envelope. The envelope should bear a stamp or details that clearly indicates the full address of the office from which it was sent.**

**13. Advice on the distribution of OFFICIAL-SENSITIVE documents abroad or any other general advice including the distribution of OFFICIAL-SENSITIVE hardware shall be sought from the Authority.**

**Electronic Communication, Telephony and Facsimile Services**

**14. OFFICIAL information may be emailed unencrypted over the internet. OFFICIAL-SENSITIVE information shall normally only be transmitted over the internet encrypted using either a CESG Commercial Product Assurance (CPA) cryptographic product or a 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**](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**](https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa)

**Exceptionally, in urgent cases, OFFICIAL-SENSITIVE information may be emailed unencrypted over the internet where there is a strong business need to do so and only with the prior approval of the Authority.**

**15. OFFICIAL-SENSITIVE information 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 shall require. Such limitations, including any regarding publication, further circulation or other handling instructions shall be clearly identified in the email sent with the material.**

**16. OFFICIAL information may be discussed on fixed and mobile telephones with persons located both within the UK and overseas. OFFICIAL-SENSITIVE information may be discussed on fixed and mobile types of telephone within the UK, but not within earshot of unauthorised persons.**

**17. OFFICIAL information may be faxed to recipients located both within the UK and overseas, however OFFICIAL-SENSITIVE information may be faxed only to UK recipients.**

**Use of Information Systems**

**18. The detailed functions that must be provided by an IT system to satisfy the minimum requirements cannot all be described here; it is for the implementers to identify possible means of attack and ensure proportionate security mitigations are applied to prevent a successful attack.**

**19. The contractor shall ensure 10 Steps to Cyber Security is applied in a proportionate manner for each IT and communications system storing, processing or generating MOD UK OFFICIAL or OFFICIAL-SENSITIVE information. 10 Steps to Cyber Security is available at:**

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

**The contractor shall ensure competent personnel apply 10 Steps to Cyber Security.**

**20. 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.**

**21. Within the framework of the 10 Steps to Cyber Security, the following describes the minimum security requirements for processing and accessing OFFICIAL-SENSITIVE information on IT systems.**

a. **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.**

b. **Identification and Authentication (ID&A). All systems shall have the following functionality:**

(1) **Up-to-date lists of authorised users.**

(2) **Positive identification of all users at the start of each processing session.**

c. **Passwords. Passwords are part of most ID&A, Security Measures. Passwords shall be ‘strong’ using an appropriate method to achieve this, for example including numeric and “special” characters (if permitted by the system) as well as alphabetic characters.**

d. **Internal Access Control. All systems shall have internal Access Controls to prevent unauthorised users from accessing or modifying the data.**

e. **Data Transmission. Unless the Authority authorises otherwise, OFFICIAL- SENSITIVE information shall 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 13 above,**

f. **Security Accounting and Audit. Security relevant events fall into two**

**categories, namely legitimate events and violations.**

(1). **The following events shall always be recorded:**

(a) **All log on attempts whether successful or failed,**

(b) **Log off (including time out where applicable),**

(c) **The creation, deletion or alteration of access rights and privileges,**

(d) **The creation, deletion or alteration of passwords,**

(2) **For each of the events listed above, the following information is to be**

**recorded:**

(e) **Type of event,**

(f) **User ID,**

(g) **Date & Time,**

(h) **Device ID, The accounting records shall have a facility to provide the System Manager with a hard copy of all or selected activity. There shall also 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 shall be protected by physical means when not in use i.e. locked away or the hard drive removed and locked away.**

g. **Integrity & Availability. The following supporting measures shall 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,**

(6). **Patching of Operating Systems and Applications used shall be in line with the manufacturers recommended schedule. If patches cannot be applied an understanding of the resulting risk will be documented,**

h. **Logon Banners Wherever possible, a “Logon Banner” shall 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”**

i. **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.**

j. **Internet Connections. Computer systems shall not be connected direct to the Internet or ‘untrusted’ 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).**

k. **Disposal Before IT storage media (e.g. disks) are disposed of, an erasure product shall be used to overwrite the data. This is a more thorough process than deletion of files, which does not remove the data.**

**Laptops**

**22. Laptops holding any MOD supplied or contractor generated OFFICIAL-SENSITIVE information are to be encrypted using a CPA product or equivalent as described in paragraph 14 above.**

**23. Unencrypted laptops not on a secure site[[1]](#footnote-1) are to be recalled and only used or stored in an appropriately secure location until further notice or until approved full encryption is installed. Where the encryption policy cannot be met, a Risk Balance Case that fully explains why the policy cannot be complied with and the mitigation plan, which should explain any limitations on the use of the system, is to be submitted to the Authority for consideration. Unencrypted laptops and drives containing personal data are not to be taken outside of secure sites. For the avoidance of doubt the term “drives” includes all removable, recordable media (e.g. memory sticks, compact flash, recordable optical media e.g. CDs and DVDs), floppy discs and external hard drives.**

**24. 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.**

**25. Portable CIS devices 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**

**26. The contractor shall immediately report any loss or otherwise compromise of any OFFICIAL or OFFICIAL-SENSITIVE information to the Authority.**

**27. Accordingly, in accordance with Industry Security Notice 2014/02 as may be subsequently updated at:**

[**https://www.gov.uk/government/uploads/system/uploads/attachment\_data/file/293480/ISN 2014\_02\_Incident\_Reporting.pdf**](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/293480/ISN%202014_02_Incident_Reporting.pdf)

**any security incident involving any MOD owned, processed, or Contractor generated OFFICIAL or OFFICIAL-SENSITIVE information defined in the contract Security Aspects Letter shall be immediately reported to the MOD Defence Industry Warning, Advice and Reporting Point (WARP), within the Joint Security Co-ordination Centre (JSyCC). This will assist the JSyCC in formulating a formal information security reporting process and the management of any associated risks, impact analysis and upward reporting to the MOD’s Chief Information Officer (CIO) and, as appropriate, the company concerned. The MOD WARP will also advise the contractor what further action is required to be undertaken.**

**JSyCC WARP Contact Details**

**Email: For those with access to the RLI: CIO-DSAS-JSyCCOperations**

**Email: For those without access to the RLI: CIO-DSAS-JSyCCOperations@mod.gov.uk**

**Telephone: Working Hours: 0306 770 2187**

**Out of Hours/Duty Officer Phone: 07768 558863**

**Fax: 01480 446328**

**Mail: Joint Security Co-ordination Centre (JSyCC), X007 Bazalgette Pavilion, RAF Wyton,**

**Huntingdon, Cambs, PE28 2EA.**

**Sub-Contracts**

**28. The Contractor may Sub-contract any elements of this Contract to Sub-contractors within the United Kingdom notifying the Authority. When sub-contracting to a Sub-contractor located in the UK the Contractor shall ensure that these Security Conditions shall be incorporated within the Sub-contract document. The prior approval of the Authority shall be obtained should the Contractor wish to Sub-contract any OFFICIALSENSITIVE elements of the Contract to a Sub-contractor located in another country. The first page of Appendix 5 (MOD Form 1686 (F1686)) of the Security Policy Framework 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/367494/Contractual\_Process\_-\_Appendix\_5\_form.doc**](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/367494/Contractual_Process_-_Appendix_5_form.doc)**.**

**If the Sub-contract is approved, the Authority shall provide the Contractor with the security conditions that shall be incorporated within the Sub-contract document. Chapter 2: Contract Security – Annex N**

**Publicity Material**

**29. Contractors wishing to release any publicity material or display hardware that arises from this contract shall 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 MOD, Services or any other government department.**

**Private Venture**

**30. Any defence related Private Venture derived from the activities of this Contract are to be formally assessed by the Authority for determination of its appropriate classification. Contractors are to submit a definitive product specification for PV Security Grading in accordance with the requirement detailed at:**

[**https://www.gov.uk/government/uploads/system/uploads/attachment\_data/file/414857/20150310\_PV\_Ex\_Guidance\_Document.pdf**](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414857/20150310_PV_Ex_Guidance_Document.pdf)

**Promotions and Potential Export Sales**

**31. Contractors wishing to promote, demonstrate, sell or export any material that may lead to the release of information or equipment classified OFFICIAL-SENSITIVE (including classified tactics, training or doctrine related to an OFFICIAL-SENSITIVE equipment) are to obtain the prior approval of the Authority utilising the MOD Form 680 process, as identified at:**

[**https://www.gov.uk/mod-f680-applications**](https://www.gov.uk/mod-f680-applications)**.**

**Destruction**

**32. As soon as no longer required, OFFICIAL and OFFICIAL-SENSITIVE information/material shall be destroyed in such a way as to make reconstitution unlikely, 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 OFFICIAL-SENSITIVE information/material which cannot be destroyed in such a way shall be returned to the Authority.**

**Interpretation/Guidance**

**33. Advice regarding the interpretation of the above requirements should be sought from the Authority.**

**34. Further requirements, advice and guidance for the protection of MOD information at the level of OFFICIAL-SENSITIVE may be found in Industry Security Notices at:**

[**https://www.gov.uk/government/publications/industry-security-notices- isns.**](https://www.gov.uk/government/publications/industry-security-notices-%20isns.)

**Audit**

**35. 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 Authority to ensure compliance with these requirements.**

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