SC1A PO
(Edn 12/21)

Ministry of Defence

PURCHASE ORDER

Contract No: DGM/2010

Contract Name: Supply of 7.62 x 35mm Ammunition Samples for Trial Evaluation

Dated: 22nd February 2022

Supply the Deliverables described in the Schedule to this Purchase Order, subject to the attached MOD Terms and Conditions for Less Complex Requirements (up to £122,979).

Contractor	**Quality Assurance Requirement (Clause 8)**
Name: EPA Manufacturing Limited Registered Address: EPA Manufacturing Limited Units 1 & 154 Faldingworth Base, Spridlington Road, Faldingworth, Lincolnshire, LN8 3SQ, United Kingdom	The Contractor shall conform with AQAP 2110. Further Quality Assurance requirements for this Purchase Order shall be as per Annex A.

Consignor (if different from Contractor's registered address)	**Transport Instructions (Clause 10)**
Name: Address:	Select method of transport of Deliverables To be Delivered by the Contactor ☒ Delivery of Contractor Deliverables shall be made to [Redacted in accordance with FOIA Part II, Section 26]: FAO [Redacted in accordance with FOIA Part II, Section 40], [Redacted in accordance with FOIA Part II, Section 26]. To be Collected by the Authority ☐ [Special Instructions] Each consignment of the Deliverables shall be accompanied by a delivery note.

Progress Meetings (Clause 13)	Progress Reports (Clause 13)
The Contractor shall be required to attend the following meetings: None required.	The Contractor is required to submit the following Reports: None required.

Payment (Clause 14)
Payment is to be enabled by CP&F.

Forms and Documentation	Supply of Data for Hazardous Deliverables (Clause 9)
Forms can be obtained from the following websites: https://www.aof.mod.uk/aofcontent/tactical/toolkit (Registration is required). https://www.gov.uk/government/organisations/ministry-of-defence/about/procurement#invoiceprocessing https://www.dstan.mod.uk/ (Registration is required). The MOD Forms and Documentation referred to in the Conditions are available free of charge from: Ministry of Defence, Forms and Pubs Commodity Management PO Box 2, Building C16, C Site Lower Arncott Bicester, OX25 1LP (Tel. 01869 256197 Fax: 01869 256824) Applications via email: DESLCSLS-OpsFormsandPubs@mod.uk If you require this document in a different format (i.e. in a larger font) please contact the Authority's Representative (Commercial Officer), detailed below.	Not required.

SC1A PO
(Edn 12/21)

DEFFORM 111
(Edn 07/21)

1. Commercial Officer
Name: [Redacted in accordance with FOIA Part II, Section 40]
Address:
MOD Abbey Wood,
DGM PT,
Fir 1C, #4115
Bristol
BS34 8JH

Email: [Redacted in accordance with FOIA Part II, Section 40]@mod.gov.uk, [Redacted in accordance with FOIA Part II, Section 40]@mod.gov.uk
Tel: [Redacted in accordance with FOIA Part II, Section 40]

2. Project Manager, Equipment Support Manager or PT Leader (from whom technical information is available)
Name: [Redacted in accordance with FOIA Part II, Section 40]
Address:
MOD Abbey Wood,
DGM PT,
Fir 1C, #4115
Bristol
BS34 8JH

Email: [Redacted in accordance with FOIA Part II, Section 40]@mod.gov.uk
Tel: [Redacted in accordance with FOIA Part II, Section 40]

3. Packaging Design Authority

Organisation & point of contact: See box 2.

4. (a) Supply / Support Management Branch or Order Manager: Branch/Name:

See box 2.

(b) U.I.N.

5. Drawings/Specifications are available from

See box 2.

6. Intentionally Blank

7. Quality Assurance Representative:

Name: [Redacted in accordance with FOIA Part II, Section 40], address as per Box 2.

Email: [Redacted in accordance with FOIA Part II, Section 40]@mod.gov.uk
Tel: [Redacted in accordance with FOIA Part II, Section 40]

AQAPS and **DEF STANs** are available from UK Defence Standardization, for access to the documents and details of the helpdesk visit http://dstan.gateway.isg-r.r.mil.uk/index.html [intranet] or https://www.dstan.mod.uk/ [extranet, registration needed].

8. Public Accounting Authority

1. Returns under DEFCON 694 (or SC equivalent) should be sent to DBS Finance ADMT – Assets In Industry 1, Level 4 Piccadilly Gate, Store Street, Manchester, M1 2WD
Tel: +44 (0) 161 233 5397
Email: DBSFin-FAADMT-AiiTeam@mod.gov.uk.

2. For all other enquiries contact DES Fin FA-AMET Policy, Level 4 Piccadilly Gate, Store Street, Manchester, M1 2WD
Tel: +44 (0) 161 233 5394

9. Consignment Instructions

The items are to be consigned as follows:

Contract Articles as per Purchase Order Schedule of Requirements.

10. Transport. The appropriate Ministry of Defence Transport Offices are:

A. DSCOM, DE&S, DSCOM, MoD Abbey Wood, Cedar 3c, Mail Point 3351, BRISTOL BS34 8JH
Air Freight Centre
IMPORTS 030 679 81113 / 81114 Fax 0117 913 8943
EXPORTS 030 679 81113 / 81114 Fax 0117 913 8943
Surface Freight Centre
IMPORTS 030 679 81129 / 81133 / 81138 Fax 0117 913 8946
EXPORTS 030 679 81129 / 81133 / 81138 Fax 0117 913 8946

B. JSCS

JSCS Helpdesk No. 01869 256052 (select option 2, then option 3)
JSCS Fax No. 01869 256837
Users requiring an account to use the MOD Freight Collection Service should contact UKStratCom-DefSp-RAMP@mod.gov.uk in the first instance.

11. The Invoice Paying Authority
Ministry of Defence 0151-242-2000
DBS Finance
Walker House, Exchange Flags Fax: 0151-242-2809
Liverpool, L2 3YL **Website is:**
https://www.gov.uk/government/organisations/ministry-ofdefence/about/procurement#invoice-processing

12. Forms and Documentation are available through *:
Ministry of Defence, Forms and Pubs Commodity Management
PO Box 2, Building C16, C Site
Lower Arncott
Bicester, OX25 1LP (Tel. 01869 256197 Fax: 01869 256824)
Applications via fax or email: DESLCSLS-OpsFormsandPubs@mod.uk

*** NOTE**
1. **Many DEFCONs and DEFFORMs can be obtained from the MOD Internet Site:** https://www.aof.mod.uk/aofcontent/tactical/toolkit/index.htm

2. If the required forms or documentation are not available on the MOD Internet site requests should be submitted through the Commercial Officer named in Section 1.

Contractor Commercially Sensitive Information (Clause 5). Not to be published.
Description of Contractor's Commercially Sensitive Information: [Redacted in accordance with FOIA Part II, Section 26].
Cross reference to location of sensitive information: [Redacted in accordance with FOIA Part II, Section 26].
Explanation of Sensitivity: [Redacted in accordance with FOIA Part II, Section 26].
Details of potential harm resulting from disclosure: [Redacted in accordance with FOIA Part II, Section 26].
Period of Confidence (if Applicable): [Redacted in accordance with FOIA Part II, Section 26].
Contact Details for Transparency / Freedom of Information matters: Name: [Redacted in accordance with FOIA Part II, Section 40] Position: MD Address: 34 Chancery Lane, West Street, Retford, DN22 6ES Telephone Number: [Redacted in accordance with FOIA Part II, Section 40] E-mail Address: [Redacted in accordance with FOIA Part II, Section 40]

Offer and Acceptance	
[Redacted in accordance with FOIA Part II, Section 40]	B) Acceptance [Redacted in accordance with FOIA Part II, Section 40] Name (Block Capitals): [Redacted in accordance with FOIA Part II, Section 40] Position: Commercial Manager For and on behalf of the Authority Authorised Signatory Date: 2nd March 2022
C) **Effective Date of Contract:** 2nd March 2022	

SCHEDULE OF REQUIREMENTS FOR DGM/2010 – Supply of 7.62 x 35mm Ammunition Samples for Trial Evaluation

Contract Deliverables								
Item Number	**ADAC Number**	**Specification**	**Consignee Address Code**	**Packaging Requirements**	**Delivery Date**	**Total Qty**	**Firm Price (£) Ex VAT**	
							Per Item	**Total inc. packaging (and delivery if specified in the Purchase Order)**
1	N/A	Supply of 7.62 x 35mm Ammunition Suite Natures as per Annex A	XY	As per Annex A	[Redacted under FOIA Section 43, Commercially Sensitive Information]	As set out at Table 1 to Annex A	[Redacted under FOIA Section 43, Commercially Sensitive Information]	[Redacted under FOIA Section 43, Commercially Sensitive Information]
2	N/A	Delivery Costs associated with Line Item 1	N/A	N/A		N/A	[Redacted under FOIA Section 43, Commercially Sensitive Information]	[Redacted under FOIA Section 43, Commercially Sensitive Information]
							Firm Price (ex VAT)	[Redacted under FOIA Section 43, Commercially Sensitive Information]

- Delivery shall be in accordance with the Statement of Requirement for Supply of 7.62 x 35mm Ammunition Samples for Trial Evaluation at Annex A to this Contract.
- The Acceptance Criteria for these Contract Deliverables shall be as per Annex A to this Contract.

Item Number	Consignee Address (XY code only)
1 and 2	FAO [Redacted in accordance with FOIA Part II, Section 40], [Redacted in accordance with FOIA Part II, Section 26].

Annex A to DGM/2010 SC1A PO

Statement of Requirement for Supply of 7.62 x 35mm Ammunition Samples for Trial Evaluation

1. Objectives of the Contract

1.1. The objectives of this procurement are outlined as follows:

1.1.1 Supply quantities of 7.62 x 35mm Ammunition Suite natures for use under competitive Tender DGM/1917 for the Trial Technical Evaluation;

1.1.2 Supply 7.62 x 35mm Ammunition Suite natures that are representative of the ammunition that has been tendered by the Contractor under Tender DGM/1917; and

1.1.3 Supply technical data for the ammunition deliverables to support the safe handling and use of the ammunition.

2. Contract Deliverables

2.1. The Contractor shall deliver quantities of 7.62 x 35mm Ammunition Suite, as set out at Table 1, to the Authority's consignee address and in accordance with the delivery schedule set out in the Schedule of Requirements.

Nature	Part Number/Drawing Number	Quantity
[Redacted in accordance with FOIA Part II, Section 26]	[Redacted in accordance with FOIA Part II, Section 26]	6,236
[Redacted in accordance with FOIA Part II, Section 26]	[Redacted in accordance with FOIA Part II, Section 26]	6,457
[Redacted in accordance with FOIA Part II, Section 26]	[Redacted in accordance with FOIA Part II, Section 26]	5,605
[Redacted in accordance with FOIA Part II, Section 26]	[Redacted in accordance with FOIA Part II, Section 26]	6,073
[Redacted in accordance with FOIA Part II, Section 26]	[Redacted in accordance with FOIA Part II, Section 26]	5,572
[Redacted in accordance with FOIA Part II, Section 26]	[Redacted in accordance with FOIA Part II, Section 26]	2,734

Table 1: Contract Deliverables for the Supply of 7.62 x 35mm Ammunition Suite

2.2. The Contract Deliverables set out at in Table 1 shall be representative of the ammunition tendered under Tender DGM/1917 and shall have the same speficiation as per the Part Number/Drawing Numbers within Table 1.

2.3. The Contractor shall deliver the Contract Deliverables to the Authority's specified Consignee Address no later than [Redacted in accordance with FOIA Part II, Section 26].

2.4. The Authority has not specified the packaging configuration that the Contractor should use for this delivery of Contract Deliverables. The Authority may accept the Contract Deliverables being supplied in commercial packaging, subject to the Contractor supplying evidence that the packaging configuration selected meets the relevant standards set out in the UN Recommendations on the Transport of Danerous Goods Model Regulations, the HSE Classification of Explosives for UK or the relevant Competent Authority certification for any other countries (e.g. DoT Ex etc.).

2.5. In addition to the Ammunition Contract Deliverables outlined at paragraphs 2.1 – 2.4, the Contractor shall provide Technical Documentation and information as follows, to be made available upon request by the Authority:

2.5.1. Supply of Material Safety Data Sheets for each ammunition nature;

2.5.2. Supply of Energetic Material composition data for each ammunition nature;

2.5.3. Supply of Explosives Safety Transport Certificate or Healthy and Safety Executive number or equivalent relevant Competent Authority certification;

2.5.4. Confirm the pack type and method of pack that is proposed for the Ammunition Contract Deliverables, providing drawings of the ammunition and packaging where possible; and

2.5.5. Technical Data to include but not be limited to, the Hazard Division, compatibility groups, Net Explosive Quantity (NEQ) for each ammunition round, NEQ for the overall delivery, the method of transport and any special instructions that will apply.

3. Instructions for Delivery of Contract Deliverables

3.1. The Contractor shall be responsible for delivery of the Ammunition Contract Deliverables as set out in the Schedule of Requirements and this Statement of Requirements to the Consignee Address specified.

3.2. Prior to delivery of the Ammunition to the [Redacted in accordance with FOIA Part II, Section 26], the proposed delivery date and time must be agreed in advance with the Authority's Project Manager. The Contractor shall also provide information about the consignment, including the hazard division and compatibility group, the Net Explosive Quantity for each round and the overall delivery and (if possible) the size and quantity of containers to be delivered.

3.3. The Authority will liaise with the Consignee to secure the delivery slot on behalf of the Contractor. The delivery slot must be within normal business hours (to be defined as 08:00 to 16:00 between Monday to Thursday, 08:00 to 15:00 on Fridays for the purpose of this Contract). No deliveries will be accepted on weekends or public bank holidays.

3.4. A Consignee Can Accept (CCA) number will be granted for the delivery once agreed on behalf of the Contractor. This CCA number must be quoted with the delivery to the [Redacted in accordance with FOIA Part II, Section 26].

3.5. The Contractor must have supplied the information required at paragraph 2.5 and any further information specified prior to being granted a CCA number and an agreed delivery slot. If this information is not provided, the request for a delivery date, time and CCA will be rejected and it will the Contractor's responsibility to re-arrange delivery with the Authority's Project Manager.

3.6. For technical documentation or data deliverables (e.g. paragraph 2.5 to this Statement of Requirements), the Contractor shall send electronic copies (unless otherwise submitted under Tender DGM/1917) via email to the Authority's Commercial Manager and Project Manager.

4. Acceptance Criteria

4.1. The acceptance criteria for the Ammunition Contract Deliverables shall be as follows:

4.1.1. Delivery of the quantity and specification of Ammunition Contract Deliverables set out at Table 1 to this Statement of Requirements, in accordance with the delivery schedule set out in the Schedule of Requirements.

4.2. The acceptance criteria for the Technical Documentation Contract Deliverables shall be as follows:

4.2.1. Delivery of the Technical Documentation Contract Deliverables and associated data in its entirety, in accordance with the delivery timescale set out at paragraph 2.5 to the Statement of Requirements.

Security Aspects Letter

Ministry of Defence

de&s

UK Strategic Command Munitions
Defence General Munitions Project Team

[Redacted in accordance with FOIA Part II, Section 40]

[Redacted in accordance with FOIA Part II, Section 40]@mod.gov.uk

Defence Equipment & Support
Fir 1c, #4115
MOD Abbey Wood
Bristol BS34 8JH

Our Reference: DE&S PT/DGM/7/27/2/4
5 Apr 22

CONTRACT DGM/2010 - Supply of 7.62 x 35mm Ammunition Samples for Trial Evaluation

1. On behalf of the Secretary of State for Defence, I hereby give you notice of the information or assets connected with, or arising from, the referenced Contract that constitute classified material.

2. Aspects that constitute OFFICIAL-SENSITIVE for the purpose of DEFCON 660 are specified below. These aspects must be fully safeguarded. The enclosed Security Condition at Appendix 1 to Annex B outlines the minimum measures required to safeguard OFFICIAL-SENSITIVE assets and information.

SER	SECURITY ASPECTS	CLASSIFICATION
	Operational	
1	Existence of Contract	UK OFFICIAL
2	Third part trials and testing	UK OFFICIAL-SENSITIVE
	Commercial	
3	Contract	UK OFFICIAL – SENSITIVE
4	Schedule of requirements	UK OFFICIAL - SENSITIVE
5	Contract costs quotes	UK OFFICIAL – SENSITIVE COMERCIAL
6	Shipping and movement	UK OFFICIAL - SENSITIVE LIMCIRC
	Technical	
7	Design specifications	UK OFFICIAL - SENSITIVE
8	Top level drawings	UK OFFICIAL - SENSITIVE
9	Ammunition Marking Drawings	UK OFFICIAL
10	Packaging drawings and specifications	UK OFFICIAL
11	All Up Round (AUR)	UK OFFICIAL- SENSITIVE

3. Your attention is drawn to the provisions of the Official Secrets Act 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 you should take all reasonable steps to make sure that all individuals employed on any work in connection with this Contract have notice of the above specified aspects and that the aforementioned statutory provisions apply to them and will continue to apply after completion or earlier termination of the contract.

4. Will you please confirm that:

a. This definition of the classified aspects of the referenced Contract has been brought to the attention of the person directly responsible for security of classified material.

b. The definition is fully understood.

c. 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.

d. All employees of the company who will have access to classified information have either signed the OSA Declaration Form in duplicate and one 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 contract.

5. If you have any difficulty either in interpreting this definition of the classified aspects or in safeguarding them, will you please let me know immediately.

6. Classified Information associated with this Contract must not be published or communicated to anyone without the approval of the MOD Contracting Authority.

7. 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.

Yours faithfully

<Signed electronically>

[Redacted in accordance with FOIA Part II, Section 40]
DES WpnsDGM ATL-UKStratCom

Copy via email to:
ISAC-Group (MULTIUSER)
SPO DSR-IIPCSy (MULTIUSER)
ISS Des-DAIS-SRAAcc4-IA

Appendix 1 to Annex B
to SC1APO DGM/2010

Security Condition

Security Grading

1. All aspects associated with this Contract are classified OFFICIAL. Some aspects are more sensitive and are classified as OFFICIAL-SENSITIVE. The Security Aspects Letter at Annex B issued by the Authority defines 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 OFFICIALSENSITIVE 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

2. 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

3. The Contractor shall protect OFFICIAL and OFFICIAL-SENSITIVE information provided to it or generated by it in accordance with the requirements detailed in this Appendix 1 to Annex B 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.

4. 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.

5. 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.

6. 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.

7. 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.

8. 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 31.

Access

9. Access to OFFICIAL and OFFICIAL-SENSITIVE information shall be managed in accordance with paragraph 7 to this Appendix 1 to Annex B.

10. The Contractor shall ensure that all individuals having access to OFFICIALSENSITIVE 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.

Hard Copy Distribution

11. OFFICIAL and OFFICIAL-SENSITIVE documents shall be distributed, both within and outside the Contractor's 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.

12. 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

13. 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. 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.

14. 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.

15. 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.

16. 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

17. 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.

18. 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. The Contractor shall ensure competent personnel apply 10 Steps to Cyber Security.

19. 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.

20. 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:

i Up-to-date lists of authorised users.

ii 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,

g 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.

h Integrity & Availability. The following supporting measures shall be implemented:

(1). Provide general protection against normally foreseeable accidents/mishaps and known recurrent problems (e.g. viruse 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,

i. 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"

j. 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.

k. 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).

l. 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

21. Laptops holding any MOD supplied or Contractor generated OFFICIALSENSITIVE information shall be encrypted using a CPA product or equivalent as described in paragraph 13 above.

22. Unencrypted laptops not on a secure site[1] shall 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 shall be submitted to the Authority for consideration. Unencrypted laptops and drives containing personal data shall not 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.

[1] Secure Sites are defined as either Government premises or a secured office on the contractor premises

23. Any token, touch memory device or password(s) associated with the encryption package shall be kept separate from the machine whenever the machine is not in use, left unattended or in transit.

24. Portable CIS devices shall not be left unattended in any public location or 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 shall be secured out of sight in the glove compartment, boot or luggage compartment as appropriate to deter opportunist theft.

Loss and Incident Reporting

25. The Contractor shall immediately report any loss or otherwise compromise of any OFFICIAL or OFFICIAL-SENSITIVE information to the Authority.

26. Accordingly, in accordance with Industry Security Notice 2014/02, any security incident involving any MOD owned, processed, or Contractor generated OFFICIAL or OFFICIAL-SENSITIVE information defined in the Contract Security Aspects Letter at Annex B shall be immediately reported to the MOD's Project Manager and Commercial Manager (as per DEFFORM 111).

Sub-Contracts

27. The Contractor may Sub-contract any elements of this Contract to Subcontractors within the United Kingdom, notifying the Authority. When subcontracting 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 OFFICIAL SENSITIVE 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. If the Sub-contract is approved, the Contractor shall incorporate these security conditions within the Sub-contract document.

Publicity Material

28. In the event the Contractor wishes to release any publicity material or display hardware that arises from this Contract, he 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

29. Any defence related Private Venture derived from the activities of this Contract shall be formally assessed by the Authority for determination of its appropriate classification. Contractors shall submit a definitive product specification for PV Security Grading as directed by the Authority.

Promotions and Potential Export Sales

30. In the event the Contractor wishes to promote, demonstrate, sell or export any material that may lead to the release of information or equipment classified OFFICIALSENSITIVE

(including classified tactics, training or doctrine related to an OFFICIAL-SENSITIVE equipment), the Contractor shall obtain the prior approval of the Authority utilising the MOD Form 680 process.

Destruction

31. 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 OFFICIALSENSITIVE information/material which cannot be destroyed in such a way shall be returned to the Authority.

Interpretation/Guidance

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

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

Audit

34. 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.