

Framework Schedule 6 (Order Form and Call-Off Schedules)

[REDACTED]

Order Form

CALL-OFF REFERENCE: 708269450_(DInfoCom/0242)

THE BUYER: D Info Commercial

BUYER ADDRESS: Blenheim Building,
Army Headquarters,
Monxton Road,
Andover,
Hampshire
SP11 8HJ

THE SUPPLIER: **[Boxxe Limited]**

SUPPLIER ADDRESS: **[Boxxe Limited Floor 2 & 3 Artemis House,
Eboracum Wy, York YO317RE]**

REGISTRATION NUMBER: **[2109168]**

DUNS NUMBER: 390294056

SID4GOV ID: **[N/A]**

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated 06 December 2023

It's issued under the Framework Contract with the reference number RM6068 for the provision of Technology Products and Associated Services.

CALL-OFF LOT(S):

Lot 4: Information Assured Products and Associated Services.

CALL-OFF INCORPORATED TERMS

The following documents are incorporated into this Call-Off Contract. Where numbers are missing we are not using those schedules. If the documents conflict, the following order of precedence applies:

1. **This Order Form including the Call-Off Special Terms and Call-Off Special Schedules.**
2. **Joint Schedule 1(Definitions and Interpretation) RM6068.**
3. The following Schedules in equal order of precedence:

3.1 **Joint Schedules for RM6068**

Joint Schedule 2 (Variation Form)
Joint Schedule 3 (Insurance Requirements)
Joint Schedule 4 (Commercially Sensitive Information)
Joint Schedule 5 (Corporate Social Responsibility)
Joint Schedule 6 (Key Subcontractors) – **N/A**
Joint Schedule 7 (Financial Difficulties)
Joint Schedule 8 (Guarantee) – **N/A**
Joint Schedule 9 (Minimum Standards of Reliability) – **N/A**
Joint Schedule 10 (Rectification Plan)
Joint Schedule 11 (Processing Data)
Joint Schedule 12 (Supply Chain Visibility) – **N/A**

3.2 **Call-Off Schedules for 702751450 (DInfoCom/0242)**

Call-Off Schedule 1 (Transparency Reports) – **N/A**
Call-Off Schedule 2 (Staff Transfer) – **N/A**
Call-Off Schedule 3 (Continuous Improvement) – **N/A**
Call-Off Schedule 4 (Call Off Tender)
Call-Off Schedule 5 (Pricing Details)
Call-Off Schedule 6 (ICT Services)
Call-Off Schedule 7 (Key Supplier Staff)
Call-Off Schedule 8 (Business Continuity & Disaster Recovery) – **N/A**
Call-Off Schedule 9 (Security) **Part A** –Short Form
Call-Off Schedule 10 (Exit Management) **Part B** – Short Form
Call-Off Schedule 11 (Installation Works)
Call-Off Schedule 12 (Clustering) – **N/A**
Call-Off Schedule 13 (Implementation Plan and Testing) – **N/A**
Call-Off Schedule 14 (Service Levels) – **N/A**
Call-Off Schedule 15 (Call-Off Contract Management) – **N/A**
Call-Off Schedule 16 (Benchmarking) – **N/A**
Call-Off Schedule 17 (MOD Terms)
Call-Off Schedule 18 (Background Checks)
Call-Off Schedule 19 (Scottish Law) – **N/A**
Call-Off Schedule 20 (Call-Off Specification)
Call-Off Schedule 21 (Northern Ireland Law) – **N/A**
Call-Off Schedule 22 (Lease Terms) – **N/A**
Call-Off Schedule 23 (Optional Provisions) – **N/A**

4. **CCS Core Terms (version 3.0.6).**

No Supplier terms are part of the Call-Off Contract. That includes any terms written on the back of, added to this Order Form, or presented at the time of delivery.

CALL-OFF SPECIAL TERMS

The following Special Terms are incorporated into this Call-Off Contract:

1. AUTHORISATION BY THE CROWN FOR USE OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

- (a) Notwithstanding any other provisions of the Contract and for the avoidance of doubt, award of the Contract by the Authority and placement of any contract task under it does not constitute an authorisation by the Crown under Sections 55 and 56 of the Patents Act 1977 or Section 12 of the Registered Designs Act 1949.
- (b) The Contractor acknowledges that any such authorisation by the Authority under its statutory powers must be expressly provided in writing, with reference to the acts authorised and the specific intellectual property involved.

2. ATTACHMENTS

- (a) Attachment 1 – Cyber Implementation Plan
- (b) Attachment 2 – Security Aspect Letter (SAL) and Appendix 1 to SAL Official and Official-Sensitive Contractual Security Conditions
- (c) Attachment 3– Personal Data Aspect Letter

CALL-OFF START DATE:

7 December 2023

CALL-OFF EXPIRY DATE:

6 December 2026

CALL-OFF INITIAL PERIOD:

36 Months

(7 December 2023 to 6
December 2026);

Hardware inclusive of Year 1-3:
36 Month initial hardware support
including disc replacement
warranty: (includes purchase and
delivery of prepared and ready to
use Hardware + Manufacturer's
Warranty for delivery as soon as
possible and by NLT 7 December
2023).

CALL-OFF EXTENSION PERIOD (OPTIONAL):

Not Applicable N/A

CALL-OFF DELIVERABLES

~~Option A: see details in Annex A (Statement of Requirement)~~

Option B: See details in Call Off Schedule 20 (Order Specification)

LOCATION FOR DELIVERY

~~Option A: See details in Annex A (Statement of Requirement).~~

Option B: See details in Call-Off Schedule 20 (Order Specification)

DATES FOR DELIVERY OF THE DELIVERABLES

~~Option A: See details in Annex A (Statement of Requirement).~~

Option B: See details in Call-Off Schedule 20 (Order Specification)

TESTING OF DELIVERABLES

Option A: None

WARRANTY PERIOD

The warranty period for the purposes of Clause 3.1.2 of the Core Terms shall a Minimum is 90 days.

MAXIMUM LIABILITY

The limitation of liability for this Call-Off Contract is stated in Clause 11.2 of the Core Terms.

The Estimated Year 1 Charges used to calculate liability in the first Contract Year is £249,847.60 excluding VAT Estimated Charges in the first 12 months of the Contract. The Buyer must always provide a figure here]

CALL-OFF CHARGES

Option A: See details in Annex C (Pricing Schedule)

~~Option B: See details in Call-Off Schedule 5 (Pricing D~~
~~etails)~~

The Charges will not be impacted by any change to the Framework Prices. The Charges can only be changed by agreement in writing between the Buyer and the Supplier because of a Specific Change in Law or Benchmarking using Call-Off Schedule 16 (Benchmarking) where this is used.

REIMBURSABLE EXPENSES

None.

PAYMENT METHOD

CP&F.

BUYER'S INVOICE ADDRESS:

[REDACTED] and [REDACTED]

Digital Support Team, Service Police Crime Bureau, Bassett Wilson Building, Southwick Park, Fareham, Hampshire, PO17 6EJ

BUYER'S AUTHORISED REPRESENTATIVE

[REDACTED]

SO3 Commercial

[REDACTED]

Information Directorate, Blenheim Building, Army Headquarters, Marlborough Lines, Monxton Road, Andover, Hampshire, SP11 8HJ.

BUYER'S ENVIRONMENTAL POLICY – N/A**BUYER'S SECURITY POLICY- N/A****SUPPLIER'S AUTHORISED REPRESENTATIVE**

[REDACTED]

Account Director

[REDACTED]

Boxxe Limited

Floor 2 & 3 Artemis House,

Eboracum Wy,

York

YO317RE

SUPPLIER'S CONTRACT MANAGER

[REDACTED]

[Account Director

[REDACTED]

Boxxe Limited

Floor 2 & 3 Artemis House,

Eboracum Wy,

York

YO317RE

PROGRESS REPORT FREQUENCY- N/A

PROGRESS MEETING FREQUENCY- N/A

SUPPLIER KEY STAFF

[REDACTED]

Account Director

[REDACTED]

Boxxe Limited

Floor 2 & 3 Artemis House,

Eboracum Wy,

York

YO317RE

KEY SUBCONTRACTOR(S) - N/A

COMMERCIALLY SENSITIVE INFORMATION

Suppliers Pricing

SERVICE CREDITS - N/A

ADDITIONAL INSURANCES- N/A

GUARANTEE- N/A

SOCIAL VALUE COMMITMENT – N/A

For and on behalf of the Supplier:		For and on behalf of the Buyer:	
Signature:	[REDACTED]	Signature:	[REDACTED]
Name:	[REDACTED]	Name:	[REDACTED]
Role:	Account Director	Role:	D Info Comrcl – SO2b
Date:	7/12/2023	Date:	07 Dec 2023

Attachment 1 – Cyber Implementation Plan

Contract Title:	The Provision of SPCB – SERVICE POLICE CYBERCRIME CENTRE - FORENSIC DATA HANDLING NETWORK – ARES HARDWARE REFRESH.
MOD Contract Number:	702107454 (DInfoCom/0242)
CSM Risk Acceptance Reference:	[REDACTED]
CSM Cyber Risk Level:	Not Applicable (N/A)
Name of Supplier (to be shared with the MOD only):	BOXXE Limited
Current Level of Supplier Compliance:	[REDACTED]
Reasons why Supplier is unable to achieve full compliance:	[REDACTED]
Measures planned to achieve compliance/ mitigate the risk with associated dates:	[REDACTED]
Anticipated date of compliance/mitigations will be in place:	[REDACTED]
Current Cyber Essential Plus Certification No:	[REDACTED]
Expiry Date:	[REDACTED]
Renewal certification to be issued to the Authority:	[REDACTED]
Name:	[REDACTED]
Position: Account Director	Account Director
Date:	23/11/23

Attachment 2 – Security Aspect Letter (SAL)

Date of Issue: 21/02/2023

Army Commercial (DInfo) Information
Directorate Army Headquarters
Blenheim Bldg Marlborough Lines
Monxton Road Andover SP11 8HT

For the attention of:

Dell Technologies
44 Kidmore Road
Caversham
Berkshire
RG4 7LU

Security Aspects Letter – Supplier Ref Number – 7008269450 - DinfoCom/0242 for the Provision of SPCB – SERVICE POLICE CYBERCRIME CENTRE - FORENSIC DATA HANDLING NETWORK – ARES HARDWARE REFRESH

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 ITT 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 this Security Aspects Letter, outlines the minimum measures required to safeguard OFFICIAL-SENSITIVE assets and information.

ASPECTS	CLASSIFICATION
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

(Note: Add more rows as required)

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 ITT have notice of the above specified aspects and that the aforementioned statutory provisions apply to them and will continue to apply should the ITT be unsuccessful.
4. Will you please confirm that:
 - a. This definition of the classified aspects of the referenced Invitation to Tender 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 ITT.

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 ITT 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

[REDACTED]
[REDACTED]
[REDACTED]

Copy via email to:

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Attachment 2 – Appendix 1 to Security Aspect Letter (SAL)

Appendix 1: UK OFFICIAL AND UK OFFICIAL-SENSITIVE CONTRACTUAL SECURITY CONDITIONS

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

2. The term "*Authority*" for the purposes of this Annex means the HMG Contracting Authority.

3. The term "*Classified Material*" for the purposes of this Annex means classified information and assets.

Security Grading

4. 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

5. The Contractor shall take all reasonable steps to adhere to the provisions specified in the Contract or listed in this Annex. 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 so to apply after the completion or earlier termination of the Contract. The Authority must state the data retention periods to allow the Contractor to produce a data management policy. If you are a Contractor located in the UK your 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

6. 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.

7. 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>

8. 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.

9. 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.

10. 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.

11. 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.

12. 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 34.

Access

13. 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.

14. 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/71400/2/HMG_Baseline_Personnel_Security_Standard_-_May_2018.pdf

Hard Copy Distribution

15. 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.

16. 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

17. 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>

18. 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.

19. 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.

20. 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

21. 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.

22. 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>.

23. 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.

24. 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.

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 are to 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 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.

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

e. 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 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:

- (a) Type of event,
- (b) User ID,
- (c) Date & Time,
- (d) Device ID.

The accounting records are to have a facility to provide the System Manager 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.

g. 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,
- (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.

h. 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”

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 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).

k. 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

25. Laptops holding any UK OFFICIAL-SENSITIVE information shall be encrypted using a CPA product or equivalent as described in paragraph 17 above.

26. Unencrypted laptops and drives containing personal data are not to be taken outside of secure sites¹. 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.

27. 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.

28. 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

29. 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 otherwise compromise of any UK MOD owned, processed or UK MOD Contractor generated UK OFFICIAL or UK OFFICIAL-SENSITIVE material is to be immediately

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

reported to the UK MOD Defence Industry Warning, Advice and Reporting Point (WARP), within the Joint Security Co-ordination Centre (JSyCC) below. 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 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.

JSyCC WARP Contact Details

Email: [REDACTED] (OFFICIAL with no NTK restrictions)

RLI Email: [REDACTED] (MULTIUSER)

Telephone (Office hours): [REDACTED]

JSyCC Out of hours Duty Officer: [REDACTED]

Mail: JSyCC Defence Industry WARP

X007 Bazalgette Pavilion,

RAF Wyton, HUNTINGDON, Cambridgeshire, PE28 2EA.

30. 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

31. 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.

32. 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

33. If the sub-contract is approved, the Contractor will flow down the Security Conditions in line with paragraph 31 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

34. Contractors wishing to release any publicity material or display assets that arises 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

35. 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

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

37. 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

38. 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.

Attachment 3 – Personal Data Aspect Letter (PDAL)

ANNEX B: PERSONAL DATA ASPECTS LETTER FOR CONTRACTS INVOLVING THE HANDLING OF OFFICIAL-SENSITIVE PERSONAL DATA

For the personal attention of:

Dell Technologies
44 Kidmore Road
Caversham
Berkshire
RG4 7LU

Personal Data Aspects Letter – Supplier Ref Number – 7008269450 - DinCom/0242 for the Provision of SPCB – SERVICE POLICE CYBERCRIME CENTRE - FORENSIC DATA HANDLING NETWORK – ARES HARDWARE REFRESH

1. On behalf of the Secretary of State for Defence, I hereby give you notice that the Privacy Impact Assessment conducted has identified that this contract involves the requirement to handle UK MOD personal data. This data is subject to the provisions of the Data Protection Act 2018,² the Data Handling Review,³ and the GovS 007 Security. Your attention is also drawn to the specific aspects of personal data handling set out in Industry Security Notices which must be fully implemented.

2. Will you please confirm that:

- a. This definition of the personal data aspects of the above contract has been brought to the attention of the person directly responsible for the protection of data in this contract.
- b. The definition is fully understood.
- c. Measures can, and will, be taken to protect the personal data.
- d. Any problems in meeting these requirements will be notified to MOD immediately.

Yours faithfully

[REDACTED]
[REDACTED]
[REDACTED]

Copy to:
CIO-Advisor

² <https://www.gov.uk/data-protection>

³ <https://www.gov.uk/government/publications/data-handling-procedures-in-government>