MOD Commercial

702193450
Managed Learning Services Framework

SANS 500 Series Courses

This Contract is made

BETWEEN (1) **HER BRITANNIC MAJESTY'S SECRETARY OF STATE FOR DEFENCE**, acting through the Director Commercial, Strategic Command, Defence Academy, Trenchard Building, Shrivenham, SN6 8LA ("the Authority")

AND (2) **CAPITA BUSINESS SERVICES LIMITED,** 1st Floor, Reading Bridge House, George Street, Reading, RG1 8LS ("THE Contractor")

1. The Contractor shall provide the Services described in the Statement of Requirement, in accordance with the Conditions of Contract (as detailed in Framework Schedule 4 – Order Form and Call-Off Terms for the Managed Learning Service dated 04 July 2017 – to the Framework Agreement entered into between the Authority and the Supplier on RM3822), the firm prices attached and the Contractor's Work Order (WO) reference **WO_PSGW01787 dated 22 November 2021.**

2. The Contract shall come into effect on **20th December 2021 until 31st March 2022.**

3. Except where there is prior written approval from the Contracts Branch no payment shall be made for work performed which is outside the scope or period of the Contract. All prices contained within this Contract exclude VAT.

4. If there is a conflict between the documents described in 1. above, the order of precedence shall be:

1. Work Order/SOW reference **WO_PSGW01787 dated 22 November 2021**
2. Statement of Requirements at Schedule 1
3. Conditions of Contract (as detailed in Framework Schedule 4 – Order Form and Call-Off Terms for the Managed Learning Service dated 04 July 2017 - to the Framework Agreement entered into between the Authority and the Supplier on RM3822)

Index to Schedules

SCHEDULE 1 **STATEMENT OF REQUIREMENTS**

SCHEDULE 2 **PRICING SCHEDULE**

APPENDIX 1 (DEFFORM 111) **ADDRESSES & OTHER INFORMATION**

Schedule 1

Statement of Requirements

Proposal

Given current restrictions and timescales, it is proposed that all four courses are undertaken virtually at prescribed timings as agreed with DCS. Attendees can attend remotely or work together in a classroom. The Instructor will be live on screen.

Course Outline and Content

- SEC 503: Intrusion Detection in Depth GCIA
- SEC 504: Hacker Tools, Techniques, Exploits and Incident Handling. GCIH
- SEC 508: Advanced Incident Response, Threat Hunting, and Digital Forensics GCFA
- SEC 511: Continuous Monitoring and Security Operations GMON

SEC503: Continuous Monitoring and Security Operations

You Will Learn:

- How to analyse traffic traversing your site to avoid becoming another "Hacked!" headline
- How to identify potentially malicious activities for which no IDS has published signatures
- How to place, customize, and tune your IDS/IPS for maximum detection
- Hands-on detection, analysis, and network forensic investigation with a variety of open-source tools
- TCP/IP and common application protocols to gain insight about your network traffic, enabling you to distinguish normal from abnormal traffic
- The benefits of using signature-based, flow, and hybrid traffic analysis frameworks to augment detection.
-

You Will Be Able To:

- Configure and run open-source Snort and write Snort signatures
- Configure and run open-source Bro to provide a hybrid traffic analysis framework
- Understand TCP/IP component layers to identify normal and abnormal traffic
- Use open-source traffic analysis tools to identify signs of an intrusion
- Comprehend the need to employ network forensics to investigate traffic to identify a possible intrusion
- Use Wireshark to carve out suspicious file attachments
- Write tcp dump filters to selectively examine a particular traffic trait
- Craft packets with Scapy
- Use the open-source network flow tool SiLK to find network behaviour anomalies
- Use your knowledge of network architecture and hardware to customize placement of IDS sensors and sniff traffic off the wire

SEC 504: Hacker Tools, Techniques, Exploits and Incident Handling

You will learn:

- How to best prepare for an eventual breach
- The step-by-step approach used by many computer attackers
- Proactive and reactive defences for each stage of a computer attack
- How to identify active attacks and compromises
- The latest computer attack vectors and how you can stop them
- How to properly contain attacks
- How to ensure that attackers do not return
- How to recover from computer attacks and restore systems for business
- How to understand and use hacking tools and techniques

- Strategies and tools to detect each type of attack
- Application-level vulnerabilities, attacks, and defences
- How to develop an incident handling process and prepare a team for battle
- Legal issues in incident handling

SANS supports its students with a wealth of additional courseware. This includes:

- A library of expertly written textbooks. These books are written by the same authors who create the SANS course they support. The books follow the course's structure and add supplementary technical detail to what's taught.

- Complete toolkits. SANS equips students with copies of all the tools and applications that are explored in class. This means students will be able to deploy their new skills as soon as they return to the office.

SEC 508 - Advanced Incident Response, Threat Hunting, and Digital Forensics **REDACTED**

You will learn to:

- Detect how and when a breach occurred
- Quickly identify compromised and affected systems
- Perform damage assessments and determine what was stolen or changed
- Contain and remediate incidents
- Develop key sources of threat intelligence
- Hunt down additional breaches using knowledge of the adversary

SEC 511 - Continuous Monitoring and Security Operations

You will learn to:

- Analyse a security architecture for deficiencies
- Apply the principles learned in the course to design a defensible security architecture
- Understand the importance of a detection-dominant security architecture and Security Operations Centres (SOC)
- Identify the key components of Network Security Monitoring (NSM)/Continuous Diagnostics and Mitigation (CDM)/Continuous Monitoring (CM)
- Determine appropriate security monitoring needs for organizations of all sizes
- Implement robust Network Security Monitoring/Continuous Security Monitoring
- Determine requisite monitoring capabilities for a SOC environment
- Determine capabilities required to support continuous monitoring of key CIS Controls

Full details of the Customers requirement are detailed within the WO_PSGW01787 dated 22 November 2021.

Schedule 2 to 702193450

Pricing Schedule

Milestone	Maximum delegates per cohort	Number of tutors per cohort	Number of Days per cohort	TOTAL (ex VAT) and including Capita Service Fee at 5.95%	Delivery Date: Week commencing:
SEC 504	25	1	6	**REDACTED**	22 November 2021
SEC 508	25	1	6	**REDACTED**	13 December 2021
SEC 511	25	1	6	**REDACTED**	31 January 2022
SEC 503	25	1	6	**REDACTED**	7 March 2022
TOTAL				£695,849.17	

***Dates are indicative and will be discussed and agreed at the Start-Up Meeting, however noting the final milestone must be delivered before contract end date.**

As an exception to the RM3822 Payment Terms and Conditions, Milestone Payments will be processed to enable payment to be made 7 days after each course delivery; however, there is no penalty to the Authority if this timescale is not met.

Appendix 1 to 702193450

DEFFORM 111
(Edn 18/11/16)

Appendix - Addresses and Other Information

1. Commercial Officer:

Name: **REDACTED**

Address: Room 103 Trenchard
Defence Academy of the United Kingdom,
Shrivenham,
SN6 8LA

Email: **REDACTED**

☎ **REDACTED**

2. Project Manager, Equipment Support Manager or PT Leader (from whom technical information is available):

Name: **REDACTED**

Address: CO Defence Cyber School, Information Warfare Group,
Defence College for Military Capability Integration, Room 1030
Heaviside Building, Defence Academy of the United Kingdom
Shrivenham, Wiltshire. SN6 8LA

Email: **REDACTED**

☎ **REDACTED**

3. Packaging Design Authority:

Organisation and point of contact:

(where no address is shown please contact the Project Team in Box 2)

☎

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

Branch/Name:

☎

(b) U.I.N. D5357B

5. Drawings/Specifications are available from:

7. Intentionally Left Blank

8. Quality Assurance Representative:

Commercial staff are reminded that all Quality Assurance requirements should be listed under the General Contract Conditions.

AQAPS and **DEF STANs** are available from UK Defence Standardization, for access to the documents and details of the helpdesk visit http://dstan.uwh.diif.r.mil.uk/ [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
   ☎ 44 (0) 161 233 5397
2. For all other enquiries contact DES Fin FA-AMET Policy, Level 4 Piccadilly Gate, Store Street, Manchester, M1 2WD
   ☎ 44 (0) 161 233 5394

9. Consignment Instructions:

The items are to be consigned as follows:

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 ☎ 01869 256052 (option 2, then option 3); JSCS Fax No 01869 256837 www.freightcollection.com

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-of-defence/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.

NOTES
***** Many **DEFCONs and DEFFORMs** can be obtained from the MOD Internet Website [extranet, registration needed]:
https://www.aof.mod.uk/aofcontent/tactical/toolkit/index.htm