Annex 3 – Statement of Requirements

Contract Reference: CCIT22A48

Provision of Vulnerability Exposure Platform

CONTENTS

1. PURPOSE 3

2. BACKGROUND TO THE CONTRACTING AUTHORITY 3

3. BACKGROUND TO REQUIREMENT/OVERVIEW OF REQUIREMENT 4

4. DEFINITIONS 5

5. SCOPE OF REQUIREMENT 5

6. THE REQUIREMENT 5

7. KEY MILESTONES AND DELIVERABLES 6

8. MANAGEMENT INFORMATION/REPORTING 7

9. VOLUMES 8

10. CONTINUOUS IMPROVEMENT 8

11. SUSTAINABILITY 8

12. QUALITY 8

13. PRICE 8

14. STAFF AND CUSTOMER SERVICE 9

15. SERVICE LEVELS AND PERFORMANCE 9

16. SECURITY AND CONFIDENTIALITY REQUIREMENTS 9

17. PAYMENT AND INVOICING 10

18. CONTRACT MANAGEMENT 10

19. LOCATION 11

1. PURPOSE

1.1 The purpose of this document is to provide a statement of requirements for a 12 month contract, for the provision of a new vulnerability exposure management platform licence for use by the Cabinet Office Cyber Defence team, which is essential to the Cabinet Office’s CO Digital Cyber Security team in order to ensure the ongoing delivery of core tasks and capabilities.

2. BACKGROUND TO THE CONTRACTING AUTHORITY

2.1 The Cabinet Office supports the Prime Minister and ensures the effective running of government. The Cabinet Office is also the corporate headquarters for government, in partnership with HM Treasury, and takes the lead in certain critical policy areas. The Cabinet Office has responsibility for:

2.1.1 Supporting collective government, helping to ensure the effective development, coordination and implementation of policy

2.1.2 Supporting the National Security Council and the Joint Intelligence Organisation, coordinating the government’s response to crises and managing the UK’s cyber security

2.1.3 Promoting efficiency and reform across government through innovation, better procurement and project management, and by transforming the delivery of services

2.1.4 Promoting the release of government data, and making the way government works more transparent

2.1.5 Creating an exceptional Civil Service, improving its capability and effectiveness

2.1.6 Political and constitutional reform

2.2 The Cabinet Office’s Chief Digital and Information Office (CO Digital) is the department’s IT and digital shared services function.

2.3 CO Digital Cyber Security is the internally-facing cyber security team for the Cabinet Office, with a mission to secure the Cabinet Office against cyber threats. It delivers on this mission through four core tasks:

2.3.1 Define the cyber security policies and standards that Cabinet Office services, teams and staff must meet

2.3.2 Deliver cyber security capabilities to services, teams and staff to help and support them to meet those policies and standards

2.3.3 Assess and report on compliance against cyber security policies and standards

2.3.4 Enable an effective and efficient cyber security function

3. BACKGROUND TO REQUIREMENT/OVERVIEW OF REQUIREMENT

3.1 The National Cyber Security Strategy 2022, Pillar 2 focuses on Cyber Resilience containing primary objectives on Central Government leading by example with direct reference to Vulnerability Management. “Government’s critical functions are significantly hardened to cyber attack and all government organisations – across the whole public sector – will be resilient to known vulnerabilities and attack methods by 2030.”

3.2 The CO Digital Cyber Security Strategy (FY 22-23) has a number of goals and objectives around improving cyber security capabilities, one of the main focuses is around improving vulnerability assessment and management. The procurement of a Vulnerability Exposure Platform is integral to achieving this goal.

3.3 CO Digital Cyber Security’s FY22 strategy identifies six strategic goals, with lower-level strategic objectives underpinning these. While many of these objectives are broadly relevant to Vulnerability Management (and other areas of technology and processes), there are three specific objectives which are directly relevant to Vulnerability Management:

3.3.1 Objective 1.4: “Develop our vulnerability management capability beyond MVP.”

3.3.2 Objective 1.5: “Improve the technology stack that supports the delivery of our capabilities so that it is simple, supportable, sustainable and reliable (including, where necessary, removing elements of it).”

3.3.3 Objective 2.4: “Where appropriate, fill in the remaining gaps that exist with our existing capabilities.”

3.3.4 Goal 2: “Expand the cyber security services we deliver”

3.3.5 Goal 4: “Work with delivery partners to augment our capabilities”

3.4 The Cyber Security team currently utilises an on premise vulnerability scanner with a very small number of licences provided by Tenable. This scanner is only capable of performing vulnerability assessments on public facing domains. Onboarding a cloud based Vulnerability Exposure Platform will enable the team to significantly increase their capability to ensure vulnerability assessments are performed across the entire infrastructure.

3.5 The chosen solution will be used to perform vulnerability assessments on assets hosted within the GDS and CO environments. Currently this is estimated to be approximately 15,000 assets, broken down, this comprises of;

● 12,500 end user devices

● 1,000 AWS accounts

● 1,000 on site physical assets

● 300 public facing domains

4. DEFINITIONS

VM means Vulnerability Management

VEP means Vulnerability Exposure Platform

GDS means Government Digital Service

CO Digital means Cabinet Office Digital, the Cabinet Office directorate providing IT and digital shared services across the department

Supplier means the provider of the chosen solution

Reseller means the entity providing commercial procurement services

5. SCOPE OF REQUIREMENT

5.1

5.1.1 CO Digital Cyber Security has a requirement to procure a Vulnerability Exposure Platform through an authorised reseller and accredited Professional Services provider. This requirement shall include licensing and support, training and provide delivered professional services to deliver successful onboarding of the platform.

5.1.2 The scope of this requirement is the successful implementation of a Vulnerability Exposure Platform. The full details of this requirement are included in Section 6 below.

6. THE REQUIREMENT

6.1 CO Digital Cyber Security requires the Supplier to provide the following products and services for a 12 month period:

6.1.1 A cloud-based VEP with a licence count suitable for supporting a minimum of 5000 assets in a hybrid infrastructure composing of multiple AWS cloud environments, physical on-premises devices and web applications

6.1.2 A cloud-based VEP capable of asset discovery and tracking

6.1.3 A cloud-based VEP capable of risk-based prioritisation based on a range of factors such as asset criticality, known vulnerabilities and exposure

6.1.4 A cloud-based VEP capable of assessing container Cloud Container Security

6.1.5 A cloud-based VEP providing a unified exposure view comprising vulnerability management, web application scanning, cloud and attack surface management.

6.1.6 Professional Services capable of delivery and implementation of the chosen solution to a minimum agreed operational level

6.1.7 The solution must provide an elastic licensing model to ensure the product continues to function without interruption when the licence limit is temporarily exceeded.

6.1.8 The solution must provide the capability to produce technical and executive level metrics

6.1.9 The solution must be capable of creating custom reporting widgets

6.1.10 The solution must have extensive vulnerability intelligence updated daily

6.1.11 Assigned Customer Success Manager

6.1.12 Assigned Technical Platform Engineer

6.2 Skills transfer to buyer user base to a minimum agreed level to enable BAU use of the chosen solution in addition to any separately purchased specialist training course

6.3 The Reseller must be an authorised agent acting on behalf of the Supplier

6.4 The Supplier must be able to demonstrate experience delivering comparable products and services to similar organisations

7. KEY MILESTONES AND DELIVERABLES

7.1 The following Contract milestones/deliverables shall apply:

o Commencement of Contract (Estimated) - 31st January 2023. Contract expiry 31st January 2024.

On Boarding The Supplier will provide the Services within the times agreed and to the minimum agreed standards and service levels and these will be formally accepted when completed to the satisfaction of the Buyer. Within week 1 of contract award

Professional Services The Supplier will provide the Services within the times agreed and to the minimum agreed standards and service levels and these will be formally accepted when completed to the satisfaction of the Buyer.

The Supplier will provide the Buyer with Monthly reports detailing all work planned, forecast and completed with any issues/recommendations during the Professional Services engagement with the Buyer staff. As required through the duration of the Professional Services engagement

Contract Management The Supplier will work with the Buyer and provide the Services including agreed reports, actions, service levels and timescales and these will be formally accepted when completed to the satisfaction of the Buyer. Throughout the contract

Off Boarding Planning The supplier will work with the Buyer throughout the engagement to ensure the transfer of relevant skills to the CO Digital Cyber Security team. Throughout the contract

8. MANAGEMENT INFORMATION/REPORTING

8.1 MI reporting to be agreed at the Inception meeting of the successful supplier.

8.2 Where the Supplier has agreed to deliver tasks, the Supplier shall provide updates on these tasks including:

8.2.1 Task completion, measured against agreed delivery date for that task

8.2.2 Current documented challenges that have potentially impacted on delivery of agreed tasks including but not limited to:

8.2.2.1 Actions taken by the supplier to resolve documented challenges

8.2.2.2 Estimate of delay on agreed delivery date of the task

8.3 The Supplier shall provide data on uptime of the service and performance against the stated SLAs.

9. VOLUMES

9.1 Approximate number of assets included in this scope is 15,000. During the initial implementation stages it is expected that 5,000 assets will be able to be onboarded within the first year, with the expected completion of all 15,000 assets during the second year of service.

9.2 Initial Licence requirement of 5,000 with a planned uplift to 15,000 in the next contracting year following successful implementation.

10. CONTINUOUS IMPROVEMENT

10.1 The Supplier will be expected to work with the team to continually improve the way in which the required Services are to be delivered throughout the Contract duration.

10.2 The Supplier should present any suggestions on new ways of working to the Authority during quarterly Contract review meetings.

10.3 Changes to the way in which the Services are to be delivered must be brought to the Authority’s attention and agreed prior to any changes being implemented.

11. SUSTAINABILITY

11.1 None noted

12. QUALITY

12.1 The Supplier will deliver the Services in a way that enables the Authority to comply with its obligations under the Technology Code of Practice, which is available at https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice.

12.2 The quality standards required for this Call-Off Contract are ISO/IEC 27001 and CSA STAR, see Security Standards, and the Supplier shall maintain appropriate internal systems and processes to ensure the quality of service delivered under this agreement.

13. PRICE

13.1 The Supplier shall provide pricing showing a detailed breakdown of Vulnerability Exposure platform licensing, additional platform costs, delivered professional services, any additional reseller costs, and any other costs.

13.2 Prices are to be submitted via the e-Sourcing Suite Attachment 4 – Price Schedule excluding VAT and including all expenses relating to Contract delivery.

14. STAFF AND CUSTOMER SERVICE

14.1 The Supplier shall provide a sufficient level of resource throughout the duration of the Contract in order to consistently deliver a quality service.

14.2 The Supplier’s staff assigned to the Contract shall have the relevant qualifications and experience to deliver the Contract to the required standard.

14.3 The Supplier shall ensure that staff understand the Authority’s vision and objectives and will provide excellent customer service to the Authority throughout the duration of the Contract.

15. SERVICE LEVELS AND PERFORMANCE

15.1 The Authority will measure the quality of the Supplier’s delivery by:

User Support Email, web chat or online ticketing: Response within 1 hour

Phone support: available Mon-Fri 9am-5pm 99%

Incident support Support for P1 to P4 incidents where a part of the software, appliance or licence was previously working and is not working as expected or at all. 100%

Issue escalation Supplier to resolve 80% of service desk tickets without requiring the involvement of our Partners 80%

Staff Security clearance All staff to have the relevant security clearance 100%

Availability The platform is considered available if the user is able to log into the service account and perform VM assessments and access reporting methods 100%

o

16. SECURITY AND CONFIDENTIALITY REQUIREMENTS

16.1 Security clearance is not a necessary requirement for supplier support staff providing technical or user assistance remotely when not accessing the authority environment.

16.2 The Supplier shall ensure that all staff accessing the authority environments and whilst professional services are engaged hold UK National Security Vetting to “Security Check” (SC) level.

16.3 The Supplier shall ensure that collection, processing and storage of data is hosted within the UK.

16.4 The Supplier shall maintain compliance with ISO 27001:2013 and ISO 27018:2014 or equivalent, and shall also ensure that any third parties used by it in the course of the service provision and deemed critical to the service, shall adopt a systematic approach to managing information so that it remains secure.

17. PAYMENT AND INVOICING

17.1 A PO will be raised once the Contract has been signed. The PO is a vehicle for payment and not a firm commitment of spend.

17.2 There is no guarantee to the Supplier of the volume of services required and the Buyer may increase or decrease the volume of Services to meet its flexible requirements.

17.3 Payment can only be made following satisfactory delivery of pre-agreed certified products and deliverables.

17.4 Before payment can be considered, each invoice must include a detailed elemental breakdown of work completed and the associated costs.

17.5 The Supplier shall submit invoices in PDF format by email to **REDACTED TEXT under FOIA Section 40, Personal Information.**

17.6 All Invoices must include the WP number and PO number. Each invoice must be accompanied by a breakdown of the deliverables and services, quantity thereof, applicable unit charges and total charge for the invoice period, in sufficient detail to enable the Customer to validate the invoice.

18. CONTRACT MANAGEMENT

18.1 The Supplier will facilitate monthly (or as otherwise agreed) status review meetings between CO Digital Cyber Security and the supplier.

18.2 In months where the Supplier has provided professional services, the Supplier shall provide a written monthly status update to a nominated representative of CO Digital Cyber Security.

18.2.1 The monthly status update must be provided no later than the end of the first full working week of the next month.

18.2.2 The monthly status update shall detail the tasks delivered during that month, and (if applicable) the tasks planned for delivery during the next month.

19. LOCATION

19.1 The Services will be delivered to the Cabinet Office, at **REDACTED TEXT under FOIA Section 40, Personal Information.**

19.2 The Supplier is not required to be on site as BAU but may be required to attend on-site meetings as part of the Professional Services phase.