**Commonwealth Secretariat**

**Tender Ref 497-2019**

**Invitation to tender for the provision of Managed Information Securiry Services**

**Clarification Questions** Deadline for questions: Noon on 21 January 2020

Deadline for Secretariat to publish responses: 5 pm on 24 January 2020

|  |
| --- |
| Q1: What cloud services is/are currently being used? |
| A1: We have a presence in Microsoft Azure with several VMs hosted there. Also use Microsoft Office 365 for business Apps and Email. |
| Q2: What type of Wireless AP is currently being used? |
| A2: Ruckus R610 Access Points connected to a virtualised SmartZone controller |
| Q3: What type of Firewall equipment is/are currently being used? How many firewalls and in what topology are deployed? |
| A3: There are a pair of Cisco ASA 5525s deployed as active/passive failover pair |
| Q4: What type of specialized applications are currently being used? |
| A4: Not detailed enough definition of “specialized applications” to give definitive answers. We have one bespoke, custom-designed, business application if that is what is meant? |
| Q5: Is it possible to share your network diagrams? |
| A5: We can share such network diagrams as we have |
| Q6: How many business applications are in use (e.g. SAP, SQL, Oracle, ERP solutions)? |
| A6: The main business applications are Unit4 Coda Financials, Advanced OpenHR, a custom Project/Program management tool. All databases are MS SQL standard (2102, 2016 or 2017) |
| Q7: How many live external facing IPs would be targeted during any Penetration tests? |
| A7: About 15 |
| Q8: Has a security control framework been adopted? If yes, which one (e.g. ISO, PCI, TOGOF etc.)? |
| A8:Our policies base on ISO 27001 |
| Q9: When was your last information security assessment performed? |
| A9:a comprehensive assessment was done in Jun 2018, the last network penetration test was done in December 2019 |
| Q10: Are there documented policies, procedures, standards, and guidelines in place? |
| A10: Yes |
| Q11: What is the approximate number of routers / switches? What is the mix of Vendors of these devices? |
| A11: No routers and 20 Cisco Catalyst 9300 layer 3 switches |
| Q12: How many web applications? |
| A12: About 10 internal systems utilising web-based user interfaces and about 15 external facing web-sites hosted in the cloud |
| Q13: How many servers in the environment? |
| A13: 28 Physical and 61 Virtual |
| Q14: How many workstations in the environment? |
| A14: about 320 |
| Q15: Number of workstations (physical and virtual) including laptops |
| A15: about 320 |
| Q16: How many databases / instances and SQL/Oracle? |
| A16: All MS SQL – 4 instances – 22 databases |
| Q17: How many Admin are responsible to make any Infrastructure changes |
| A17: 3 |
| Q18: What would be total no. of EPS (Events -per-second), which would cater by SIEM solution |
| A18: Not certain at this stage but possibly about 25 EPS |
| Q19: What is approx data per day from all network/workstatation/server/applications? |
| A19: Not certain at this stage but possibly about 2GB/day |
| Q20: What is log retention period as per organization Information security policies? |
| A20: 365 days |
| Q21: Is solution PAM and SIEM solution needed for Cloud application as well? |
| A21: Not in general but maybe for a few machines (all Azure hosted) |
| Q22: Is session recording required for Admin activities? |
| A22: Maybe advantageous but not required |
| Q23: How many desktops |
| A23: See Q14 |
| Q24: How many database servers? |
| A24: See Q16 |
| Q25: How many email servers? |
| A25: None on-premise, Office365 service |
| Q26:How many HQ firewall clusters (if HA count as 1)? |
| A26: See Q3 |
| Q27: Do you have AS400, if so, how many partitions? |
| A27: No we don’t - N/A |
| Q28: Is AD in scope? If so, how many Domain Controllers? |
| A28: Certain aspects may be advantageous – 5 DCs but only 1 forest and 1 domain |
| Q29: How many office locations are in scope? |
| A29: initially only 1 |
| Q30: Is cloud in scope? If so, please indicate cloud providers in use? |
| A30: See Q 21 |
| Q31: How many DMZ servers? |
| A31: |
| Q32: Is FIM (File Integrity Monitoring a requirement for the SOC service)? If yes, is there a requirement of FIM on all of the server estate or a portion? |
| A32: Just access auditing on change |
| Q33: Number of assets on the network? |
| A33: Probably about 500 in total depending on definition used |
| Q34: Number of internal physical/office locations where an internal scanner (VM) will be required? |
| A34: 1 initially |
| Q35: Number of Web Applications (URLs) to be scanned? |
| A35: About 15 |
| Q36: With reference to the 5th requirement listed on Page 4, please can you elaborate on your requirements for dashboards? |
| A36: Discrete dashboards for both technical and non-technical staff, customisable as to parameters displayed. |
| Q37: With reference to the 10th requirement listed on Page 4, please can you elaborate on your requirements for access to research and threat intelligence? |
| A37: Make us aware of any new threats emerging |
| Q38: With reference to Part 3, Question 6, please could you outline the energy efficiency of your existing systems/equipment and designs? |
| A38: We comply to ISO 50001 Energy management standard |