TO:	**BIDDERS**
FROM:	**RAF**
DATE:	**13 December 2013**
SUBJECT:	**RAF/2013/00043 – ICT SECURITY SERVICES QUESTIONS AND ANSWERS**

Question 1:

Out of the 3000 devices, could we please have a breakdown so we may better recommend the suitable services to be provided against those devices in their different categories.

This is to say that not all devices require the same type of attention and Firewall rule changes for instance cannot apply to a windows file or web server as an example.

Thus it is very important for us to know what the 3000 devices are so that we can better provide pricing on the relevant services and skills.

Answer 1:

Approximately 140 Windows Servers, 180 Citrix servers, 30 Unix Servers, 10 Linux Servers, 600 endpoints using Windows7/8, – the remaining IPs are windows thin clients, printers, routers, switches and phones.

Question 2

How many external IPs are required to be scanned?

Answer 2:

No more than 20

Question 3:

What are the locations for scanning?

Answer 3:

The server farm is at the Midrand Data Centre while remote scanning is possible for all branches via the RAF WAN.

Question 4:

How many firewalls are there?

Answer 4:

Two Cisco ASA Firewalls in HA Mode (One Primary and One Standby) with AIP-SSM40 IPS blades.

Question 5:

Will the firewalls require a full managed service from the vendor.

Answer 5:

No, the day to day management is handled with the RAF in compliance with RAF change and configuration management procedures. The vendor shall be responsible for security monitoring and ensuring the firewall is free from vulnerabilities as well as making recommendations on best practise.

Question 6:

How many internet facing sites to be monitored from a firewall perspective?

Answer 6:

The sites which are pubic facing and require security monitoring are less than 10 but may increase to 20.

Question 7:

Is there a SOC to integrate with or must the security events from the firewall be outsourced?

Answer 7:

Alerts pulled from Firewall IDS events and logs and need be handled fully by the vendor as there is no onsite SOC.