PFA

Pension Funds Adjudicator

PROVISIONING OF ICT SECURITY SUPPORT SERVICES REF NO: OPFA/SCSS2017/T4

No.	Question	Answers
1.	What is the number IPs	7 external IP addresses.
2.	Is HA required?	Yes.
3.	How many events per second?	2500 events per second and over.
4.	How many sites and do they all have connectivity into HO? If so what are the line speeds?	2 sites – Head Office and Disaster Recovery site. Link Speed: 32Mbps current.
5.	Is storage for logs required? If so, what is the retention period?	Yes.
6.	Are the PFA looking for historical and real-time events?	Real-time events, but must be able to search for historical data.
7.	Please could we have a current network diagram.	Diagram to be provided to the awarded bidder.
8.	**1. Would the PFA allow us to tender on only the ICT Security components of the bid and not on the support? As a global ICT service provider to both public and private sector, we would be best positioned to bid only on the following:** - 3.1.1 ICT Security monitoring - 3.1.2 Advisory Threat Intelligence - - 3.1.3 Penetration Testing and Social Engineering (Annually)	No, the service provider needs to provide a full solution including all components in the scope.
	2. ICT Security monitoring 1. Do you have an estimate of your Events per Second (EPS) this has a direct effect on cost of monitoring?	2500 events per second and over.
	2. Can you provide us with a breakdown of the technology vendors and products you would like to integrate into the SIEM, together with quantities i.e. 2xCisco ASA Firewalls, 1xMcAfee EPO etc?	• Checkpoint Gateways, • Checkpoint Manager, • Checkpoint SmartEvent, • Dell OpenManager • Dell Server Hardware • Dell network switches, • HP switches • HPE Aruba switch • MS SharePoint servers

		• Kaspersky Anti-Virus servers • SQL Databases. • DHCP Server, • Domain Controllers • Exchange servers
	3. What are the log retention requirements if any (for both raw and correlated)?	6 months.
	4. How many Data Centres are there?	2 Data Centre – Head Office and Disaster Recovery site.
	▪ The service provider will be required to perform an external vulnerability assessment aimed at identifying potential weaknesses in the perimeter network and external facing systems of the organisation annually. **Questions:** 1. How many IP addresses are in scope for the external vulnerability assessment?	This will be the external IP addresses. 7 external IP addresses.
	2. Please confirm that the requirement is to run the external vulnerability assessment **once** a year for a period of 3 years?	As per the tender the vulnerability scans in the perimeter network and external facing systems must be done annually. (section 3.1.1).
	▪ The service provider will be required to assess the vulnerability status of one (1) external facing website and/or portal, which the organisation manages and maintains. **Questions:** 1. Please clarify if the requirement is for a vulnerability scan or a web application security review? a. If a web application security review is required, how many different user profiles/types are there? (e.g. normal user, super user, admin user)	Only for Vulnerability scan.
	3. Penetration Testing and Social Engineering (Annually) 1. Please confirm if an internal or external penetration test is required, or both?	Both.
	2. How many IP addresses are in scope? (Internal, External)	7 external IP addresses.
	3. How many email addresses should we target for the phishing exercise?	65 email addresses.