Annex A

S/N	Tender Doc Ref Clause	Questions & Answers
1	Clause 3.5	Could you confirm if the computing equipment (example: workstation, servers) allows to communicate with security tools hosted in public cloud?
		Yes
2	Clause 6	What is the required SLA for maintenance for the core switches?
		Please refer to clause 23.10
3	Clause 6	Please share number of Core Switches to replace
		Refer to clause 24
4	Clause 7	Please share Number of User Access Switches to replace
		Refer to clause 24
5	Clause 7	What is the required SLA for maintenance of the access switches?
		Please refer to clause 23.10
6	Clause 7	How many end user endpoints will be connected to the access switches?
		Currently approximately 40
7	Clause 7	Will there be any IP phones connecting to the access switches? How many?
		None
8	Clause 7	Will there be printers connecting to the access switches? How many?
		Yes, less than 10 printers
9	Clause 7	Will all the access switches be installed at the same server room together with other networking devices?
		Yes
10	Clause 7	What is the existing network access control solution?
		None
11	Clause 7	Do you have network access control solution?
		You may propose, but it is not part of the tender.
12	Clause 8	How many access points required?
		Up to 6
13	Clause 8	Can we request for the detailed floor plan?
		Will be provided on award of contract.

14	Clause 8	What is the required SLA for maintenance of the access points?
		8x5xNBD (Next Business Day) for hardware
15	Clause 9	What is the existing internet gateway solution?
		Fortinet Fortiproxy
16	Clause 9	Can we remove the internet gateway solution?
		Yes, as long as URL filtering is in place in your solution.
17	Clause 9	What do you mean by Advanced Load Balancing for firewall?
		ISP load balancing for future proofing.
18	Clause 9	How many years of support and what is the SLA required?
		5 years support, for SLA please refer to clause 23.10
19	Clause 9	The new firewall will be replacing both tier-1 and tier-2 firewall?
		Yes
20	Clause 9	What is the current throughput of the current tier-1 firewall?
		Tier 1 Firewall is a Fortigate 200E, Tier 2 Firewall is a Checkpoint SG5400
21	Clause 9	Please share Number of Firewalls to replace
		Refer to clause 24
22	Clause 10.2	Is the AD VM a mandatory requirement? Microsoft offers Microsoft Entra ID.
		Yes, It is preferred option
21		Why is it preferred to use an AD rather than services such as Entra ID.
		This is preferred as we would like to avoid formatting the end-devices
22	Clause 10.2	What is the purpose of the monitoring server? What needs to be monitored?
		Servers, VM, network devices (switches, access points, firewalls)
23	Clause 10.2	Can we propose a need of a bastion host if any case?
		Yes, it can be included in the tender proposal.
24	Clause 10.4	Is Backup as a Service (BaaS) an option? Or they prefer to manage the backup software in the cloud?
		Not preferred for BaaS as ReCAAP ISC wants to have full control of the data

25	Clause 12.1	Instead of Software-as-a-Service (SaaS), is the customer also considering Backup as a Service (BaaS) as a solution?
		Not preferred for BaaS as ReCAAP ISC wants to have full control of the data
26	Clause 14.1	Could you confirm Endpoint Protection is require to manage mobile platform?
		No. Only for desktop and laptop as of the moment.
27	Clause 14.1	Could you provide the breakdown of operating system and the quantity of the endpoints?
		Currently we have total 40 devices, 20 x Laptops, and 20 x Desktops. All Windows platform.
28	Clause 14.1	Mentioned 10 VM's and Given 4 VM's specifications. Please clarify.
		4 x VM's are for the confirmed system. The additional six is a buffer.
29	Clause 14.2	Is the customer currently using any antivirus solution, or should the proposed EDR solution also include endpoint protection (antivirus)?
		It should be included.
30	Clause 14.3	Trellix product integrate with SIEM to aggregate logs and alerts for advanced threat correlation. Such information could be correlation with NetFlow or network logs through the SIEM. Could you let us know if customer is looking to import hashes into firewall/gateway equipment or a XDR solution which allows 3rd parties logs to be forward and aggregate through the XDR platform.
		Solution should have the capability to integrate with other security solutions
31	Clause 15	MFA authentication for which application or services?
		IFN System, VPN Authentication, O365 Authentication
32	Clause 16	Is there any requirement on data locality as it needs to monitor both onpremise and on the cloud?
		This is not part of the tender requirement
33	Clause 17	Is the SMS gateway focuses on the IFN application? Or to the entire system hosted in both cloud and onpremise?
		The SMS gateway must be able to integrate with other apps that may require the SMS gateway, such as Monitoring Systems and MFA Systems. The solution shall be hosted on Cloud.
34	Clause 19	How many remote offices that will be connecting to the IFN?
		Minimum 25 Countries with minimum 2 Users
35	Clause 19	How many remote users outside the remote offices that will be connecting to the IFN?
		Minimum 25 Countries with minimum 2 Users
36	Clause 19	Will you also need a rack and UPS?
		No, we will re-use the existing racks.

37	Clause 19	How much UPS power would you need?
		No UPS required
38	Clause 19	Is the current IFN referring to this URL ? https://www.recaap.org/lodge-incident-report
		No
39	Clause 19	What is the current IFN data size?
		Estimated about 2.12TB, with projected growth 20% year on year.
40	Clause 20.1	Are those reporting the incidents part of the Active Directory?
		Refer to Clause Ref 20.11
41	Clause 20.1	Currently it looks like Focal Points are able to submit without Login. How will Focal Points get registered in the new system
		Focal Points will need to login to enter into the IFN System
42	Clause 20.3	What is ReCAAP Recover Time Objective (RTO) and Recovery Point Objective (RPO) policies?
		RPO, 1 day / RTO, 4 hours
43	Clause 20.7	Who is the person logging in , a public person or internal staff? From mobile app, it seems to be via a public ship contact. Please confirm
		Refer to Clause 19. Mobile App is not link to IFN
44	Clause 20.9	We note that there is a training module and we see training videos on the website. Can we have more details of the training module?
		Training videos are not the Training Modules
45	Clause 20.11	Login information is mentioned. Is the directory referring to this URL? https://www.recaap.org/focal-points or are there more info?
		No
46	Clause 21.1	Could you confirm if a cloud-hosted (example: AWS) EDR solution is included as a preferred option in clause “3.5 Solutions leveraging on Cloud or Software as a Solution (SaaS) are preferred.”
		Yes
47	Clause 23.2	Please elaborate "scalable and adaptable to meet changing organization
		The full proposal must be easily able to scale and grow with the company, may it be in terms of company size, or new technology requirements.
48		Please share details on "scalable and adaptable to meet changing organization needs".
		The full proposal must be easily able to scale and grow with the company, may it be in terms of company size, or new technology requirements.
49		Is there a ReCAAP policy on Preventive Maintenance; what the number of times required per year? Is this done 2X yearly?
		Quarterly for VMs, Twice a year for Network devices, but not limited, in case there are zero day attacks that required to be patched.

50	Clause 23.4	What are the requested support hours for managed services in Day 2 operations?
		Operating hours are 8x5, On Call Support is required as well
51	Clause 23.5	What is ReCAAP's policy PLAN Patch Management? Are patching required to be done, monthly, quarterly, half yearly (apart from critical patching)?
		Quarterly for VMs, Twice a year for Network devices, but not limited, in case there are zero day attacks that required to be patched.
52	Clause 23.5	Would you kindly elaborate on Vulnerability Assessment requirements?
		We would propose the following 1. Vulnerability Assessment and Remediation is for Cloud instances/VMs, and; 2. Penetration Testing and Remediation are for IFN system. Tenderer should suggest the number of times in a year the Client should be doing for the test. These services should be included in the Managed Services (Maintenance) proposal, with an option to do on need basis.
53		How many internet lines will be provided?
		One at the moment
54		Are there any MPLS lines? How many?
		None
55		How much bandwidth is the internet line?
		1Gbps
56		How does the member country focal point connects, via VPN?
		Focal points only need access to IFN, they are required to connect via a web portal to access the IFN.
57		How many users in each member country's focal point office?
		Minimum 2
58		How many users in Singapore office?
		Minimum 20
59		Are there any remote users outside the site offices that needs to connect to the VPN? If yes how many remote users?
		Yes, minimum 20
60		Will you need cabling and AP mounting services?
		Yes
61		Please share the SLA required in terms of system uptime/availability.
		Please refer to clause 23.10

62		Do you accept remote support for managed services within Singapore location?
		Yes, support team preferably to be based in Singapore
63		Do you accept remote support for managed services outside Singapore location?
		No, support team preferably to be based in Singapore
64		Do you accept remote support for managed services after normal office hours?
		Yes, onsite support shall be activated if required.
65		GDPR or HIPAA are regulatory compliance found in Data Loss Prevention (DLP) products. Could we find out if DLP is part of the requirement?
		Data Loss Prevention (DLP) is not a requirement as of the moment.
66		Does the monitoring platform need to be virtualized?
		Yes, as we would like to transition most, if not all, services to Cloud
67		Is there a requirement to monitor the applications as well?
		None as of the moment.
68		How many cloud environment is expected? PROD, DR, etc?
		Currently, only for PROD
69		Is there an existing cloud environment in ReCAAP?
		None as of the moment.
70		What is the backup retention period?
		We would like to keep the yearly data as long as possible.
71		Is the cloud platform to be multi-region?
		Single region in SG, however, must be multi AZ.
72		For the EDR solution, is there a need to support mobile devices?
		No as of the moment.
73		What is the patching frequency?
		Based on patch-release cycle of the proposed product.
74		Any security requirements for the IFN services if we propose a SAAS-based solution?
		The backend infrastructure of the SAAS service must have a robust security protection in place, such as, but not limited to firewalls, WAF, and other security measures to prevent malicious attacks.