Response to the vendor queries for the tender for Information & Cyber Security Consultant for ECGC Ltd.

Sr No.	Page No (Tender Ref)	Clause (Tender Ref)	Description in the tender (Tender Ref)	Query	ECGC's Response
1	8	Section 13	Presentation cum-Interaction: The Bidders who are qualified in eligibility evaluation, have to give presentation/interactions before panel of representatives of ECGC on the methodology/ approach, time frame for various activities, strengths of the Bidders in carrying out the tasks as per the scope of the RFP.	The presentation/interaction date and time are not given in this sub-section. Can that be cleared out please?	The tentative date for presentation/interaction by eligible bidders will be scheduled between 14th February 2018 to 16th February 2018 inclusive of both the dates
2	16	Section 32 > Sub-Section A	GAP Assessment Area - Physical and Environmental Security	Since this aspect of GAP Assessment deals with Physical and Environmental Security, the geographic locations where our services would be needed for this haven't been included in the tender. Can we know about them please.	The cyber security assessment will need to be conducted at ECGC HO, one Branch Office and data centre all located at Mumbai and Regional office at Bangalore.
3	16	Section 32 > Sub-Section A	GAP Assessment will cover the following areas listed in IRDA Information Security (IS) guidelines Ref. No. IRDA/IT/ GDL/MISC/082/04/2017 dated 07.04.2017.	Can we receive the technology stack along with count and areas included in the Scope of Work highlighting different Operating Systems, Network Devices, Virtualization and mobility solutions that are already implemented at ECGCs end? Including details about Remote Access and whether it's implemented and if yes, which remote access solution has been deployed or greenlit for use.	As per Annexure I
4	17-18	Section 32 > Sub-section C > Point i	Drafting Information and Cyber Security Policy for ECGC containing areas listed in IRDA information security guidelines Ref. No. IRDA/IT/GDL/MISC/082/04/2017 dated 07.04.2017.	In point (I) of sub-section C - under the 'Drafting Information and Cyber Security Policy for ECGC', it states a guideline for "Reviewing existing Information & Cyber Security policy of ECGC". This only mentions the review, but we would like some clarification regarding this. Is there a pre-drafted existing policy that just needs reviewing OR a new policy has to be drafted afresh?	ECGC already has IT Security Policy, approved by its Board. This needs to be reviewed and augemented for conforming with IRDAI guidelines.
5				Kindly let us know the tentative dates of project start and completion for Part “A” and start date of Part B.	(i) The tentative date for project start for Part A is 15th March 2018 and completion date is 14th June 2018. (ii) The tentative Start Date of Part B is 16th June 2018 and completion date is 16th August 2018
6	16	Scope of Work	A : Gap Assessment Network Security	Number of Network Devices	Please refer to response at Sr.No.3
7	16	Scope of Work	A : Gap Assessment Information Security Risk Management	Please confirm that the bidder has to review the existing information risk management being performed at ECGC and not conduct a risk assessment	Bidder has to conduct Information Risk Management as per IRDAI regulatory guidelines.

Sr No.	Page No (Tender Ref)	Clause (Tender Ref)	Description in the tender (Tender Ref)	Query	ECGC's Response
8	16	Scope of Work	A : Gap Assessment Application Security	Number of Applications in-scope	Please refer to response at Sr.No.3
9	16	Scope of Work	A : Gap Assessment Endpoint	Number of endpoints to be reviewed in-scope	As per Annexure I
10	16	Scope of Work	A : Gap Assessment Vulnerability Assessment and Penetration Testing	Provide the number of public facing IP addresses on which black box penetration testing needs to be performed Total number of IPs for which the VAPT is to be conducted (External/Internal)	As per Annexure I
11	16	Scope of Work	Scope of Work	Please confirm that the scope of the assessment in strictly to the IT Department	The scope of assessment is for IT services at ECGC Head Office, One Branch Office, Data Centre all located at Mumbai and Regional Office at Bangalore.
12	16	Scope of Work D :Drafting Cyber Security Assurance programme.	Deliverables: Cyber Security Assurance programme for ECGC as per IRDAI Guidelines.	Please provide more information of what exactly is required in the Cyber Security Assurance program	Please refer to IRDAI circular No.IRDA/IT/GDL/MISC/082 Dated 07.04.2017 which include guidelines on Information & Cyber Security for Insurers
13	16	Scope of Work	NA	All gap resolution would be the responsibility of ECGC and the bidder would be playing an oversight role during the implementation phase	Vendor will have to guide ECGC in resolving and closing all the GAPs identified in PART A
14	16	Scope of Work	NA	Please confirm that there is no Application Security Testing and Configuration Testing	Vendor will need to carry out Application Security Testing and Configuration Testing also.
15	19	Scope of Work	The vendor is expected to provide ISO:27001 Lead Auditor for completing part B activity on monthly basis. Activity is estimated to be completed in two months.	The vendor is expected to provide ISO:27001 Lead Auditor for completing part B activity on monthly basis. : Please let us know how many team members would need to be placed on site and for how long ?	One Lead Auditor for approximately two months.
16	16	Scope of Work	The backbone IT infrastructure of the Company is located at Mumbai and DR center at Faridabad.	Please let us know the locations from where the project needs to be executed.	Please refer to response at Sr.No.11 above
17	22	Annexure I: Eligibility Criteria Point 3, 4	Should have minimum average annual turnover of Rs.5 crore (Rupees five crore) during last three financial years 2014-15, 2015-16 and 2016-17. Should have made net profits for the last three financial years viz. 2014-15, 2015-16 and 2016-17.	Please confirm that the CA certification is acceptable instead of the P&L statements	CA certification is also acceptable.
18	2	Last Date of Tender submission	Last Date of Tender submission 09.02.2018 up to 5.00 pm	Please extend the bid submission date	Not Possible.

Annexure I

ECGC IT stack for Cyber Security Assessment

ECGC Ltd has its data centre hosted at third party tier III DC of BSNL, Mumbai. The setup has six physical servers of Dell make, out of which four physical severs have been virtualised using VMWARE. There are around 20 VMs created for various kinds of IT applications. The remaining two physicals servers are used for installing the Oracle database with (Real Application Cluster (RAC). The entire environment is running on MS Windows Server operating system, except two VMs which uses Linux.

ECGC branches are connected to the Data centre through MPLS connectivity. The dual internet connectivity is provided from two different vendors. The connectivity is used for accessing the ECGC web portal, email exchange with inside / outside world and for centralised internet browsing by the employees.

The details of technical stack are as below:

	Installation	Vendor	Technology
Application Software (ERP)	VM (1 No.)	In-house developed	Bespoke development. Classic ASP and Oracle as data base
Proxy	VM (1 No.)		Open source, Wbsense Proxy with Linux
Mailing Solution	VM (4 Nos.)	Synacor	Zimbra
Mail gateway and AntiSpam	VM (1 No.)	TrendMicro	IMSS
Antivirus	VM (1 No.)	Symantec	Symantec with end point security
Web Filtering	VM (1 No.)	Forcepoint	Websense
WSUS	VM (1 No.)	Microsoft	Windows Patch Management
Firewall	Physical (2 Nos.)	Fortinet	Fortinet
Authentication/SSO	VM (2 Nos.)	Microsoft	Active Directory
Network	CISCO switches (2 Nos)	CISCO	
Virtualization			VMWARE
Treasury App	VM (1 No.)	Intellect	Treasury APP
Treasury DB	VM (1 No.)		Oracle
IGMS	VM (1 No.)	Dhruv	IRDA
Mobility APP			None
Remote Access			MSTSC
Web Portal	VM (1 No.)		Wordpress with PostgreSQL
Client Portal	VM (1 No.)		Java with Linux

Number of endpoints to be reviewed in-scope : On sample basis around 25.

Total number of IPs for which the VAPT is to be conducted : Internal IPs 20 and External IPs (Public facing) 10.