Supplemental/Bid Bulletin No. 1

SUPPLY, DELIVERY, INSTALLATION AND CONFIGURATION OF NEXT GENERATION FIREWALL FOR THE DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY (DICT)

Bid Reference No.: GPG-B1-2018-173

Approved Budget for the Contract: P 20,000,000.00

This **Supplemental/Bid Bulletin No. 1** is being issued to advise concerned parties on reply to queries raised by suppliers through letters/emails for the information of all bidders for the aforecited project.

A) AMENDMENT TO BIDDING DOCUMENTS

FROM	TO
SECTION II. BID DATA SHEET Under Clause 12.1	
In accordance with Clause 19.4 of the Instructions to Bidders, the bid, except for the unamended printed literature, shall be signed, and each and every page thereof shall be initialed, by the duly authorized representative/s of the Bidder.	**DELETED**

FROM	TO
SECTION V. SPECIAL CONDITIONS OF CONTRACT (SCC) (k)	
Delivery Place: LSS Warehouse, Camp Crame, QC	**Delivery/Installation Place: DICT designated sites within Metro Manila.**

B) REPLIES TO BIDDER'S QUERIES:

MICROGENESIS BUSINESS SYSTEMS

I. Hardware Requirements : Must support SB 3G modem	
Microgenesis	**DICT**
Question #1 Can we confirm that the main purpose of this requirement is for the agency to have a backup internet link should the only ISP connection goes down? Furthermore, that this backup connection should be via 3G cellular network?	**Reply No.1** Yes, to backup the ISP connection while it is having problem like broken of Fiber line or copper link damage with ISP transit terminal. In theory, 4G LTE can go up to 100Mbps downloading and 50Mbps uploading speed, in case of disaster of ISP connectivity issue, 3G/4G can be used for backup.
Question #2 If the answer to question #1 is both yes, then, would you consider a NGFW solution with external (not built in) USB 3G modem support as long as we can prove that an internet backup link is achievable?	**Reply #2** We require that the Next Generation Firewall (NGFW) must have a usb port that can accept USB 3G modems. The USB port must be built-in with the firewall.
Question #3 3G modem is not a reliable back up for an enterprise NGFW. This is applicable to smaller boxes for branch/remote offices. For your consideration to remove the 3G USB Modem from the TOR	**Reply #3** We could not accept your request since we need the said feature for emergency purposes.

II. Performance : Must be able to Support a sustained Firewall throughput of the Firewall system at least 15Gbps	
Question #4 Since this is a NGFW procurement, can we clarify if the “15Gbps sustained firewall throughput” refers to a real-world Layer-7 Application Firewall throughput and not the traditional firewall Layer 3/4 throughput?	**Reply #4** The 15Gbps throughput should refers to traditional firewall L3/4 throughput (firewall throughput). We require the maximum performance of a traditional SPI firewall, indicates how much traffic the firewall can handle within one second, it is a main indicator to indicate the firewall maximum performance. A “real-world” L7 throughput it is not a “real world” indicator as it is hard to measure and there is no standard indication for “real world” throughput. It based on various factors like the traffic types, the average packet sizes, the protocols, the applications, network overhead, etc.
Question #5 If not, in alignment with your explicit definition of a NGFW in section 1.b.i, the NGFW should have application firewalling. “NGFW is a firewall that is a part of the third generation of firewall technology, combining a traditional firewall with other network device filtering functionalities, such as an application firewall using in line deep packet inspection (DPI), and IPS....” Since the required 15Gbps is referring to traditional Layer-4 firewall ONLY, can the proposed solution have a slightly lower throughput with a reasonable degradation of 50% from the specified Layer-4 only 15 Gbps throughput? For your consideration, to lower down the **Firewall throughput to 7.5Gbs.** “Must be able to support a sustained firewall throughput of at least 15Gbps OR combined firewall and Application aware throughput of at least **7.5Gbps**”.	**Reply #4** Please refer to the Terms of Reference for the minimum required specifications.

II. Performance : Must be able to Support a sustained Intrusion Prevention System Throughput of the Firewall system of at least 5 Gbps	
Question #6 In the TOR, DICT also require other deep packet inspection capabilities such as application usage control, Anti-virus, and web filtering. In real production network, all these features when enabled together simultaneously will result to a slightly lower IPS throughput. Since this requirement is explicitly referring to IPS throughput ONLY, can the proposed solution have a slightly lower throughput with a reasonable degradation of 30% from the specified IPS only 5Gbps? For your consideration, to lower down the IPS throughput to 3.5Gbps. “Must be able to support a sustained IPS of at least 5Gbps OR combined IPS and Anti-virus throughput of at least 3.5Gbps”.	**Reply #6** Please refer to the Terms of Reference for the minimum required specifications.
III. Software Feature : Must have a LINUX command line interface SSL VPN	
Question #7 Most, if not all, enterprise-class NGFW will have proprietary Operating System that is hardened and tested secure. This is in alignment with the required industry certifications of FIPS 140-2 and Common Criteria. So, for clarification, do you mean to say “Must have a Linux-style Command line interface SSL VPN”? Linux-style means that the CLI must operate in a similar way with Linux Operating System. LINUX command line is applicable only with open-source, software-based, and non-enterprise grade NGFW. Can LINUX be removed from the phrase? “Must have a command line interface SSL VPN.”	**Reply #7** We require the NGFW has a VPN client that can be downloaded on the NGFW manufacturer’s website, is Linux compatible and in command line interface format.

III. Software Feature : Must have a capacity to scan unlimited file size without buffering them	
Question #8 Most of the firewalls has a limit file size for scanning depends on the model of NGFW. Kindly elaborate. What type of scanning? E.g. AV, IPS, etc.....	**Reply #8** Scan packet payloads for vulnerabilities and exploits, covering a broad spectrum of attacks and vulnerabilities. AV engine should scan all inbound, outbound and intra-zone traffic for viruses, Trojans, key loggers and other malware in files of unlimited length and size across all ports and TCP streams. For AV and IPS, scanning should have no buffering (No proxy-based), no file size limit, and no protocol limitations.
IV. Monitoring of the FW : The solution must have hardware appliance deployment Option.	
Question #9 Do you mean that the proposed solution should be a hardware/appliance based?	**Reply #9** The proposed firewall monitoring solution should be external to the NGFW. It should be installed on a separate hardware, not built in with the firewall.
IV. Monitoring of the FW : The winning bidder must provide the recommended system hardware required with redundant power supplies for the monitoring solutions	
Question #10 Is a software-based/virtual edition is welcome. This will be installed in a dedicated PC/server/VM for monitoring and management purposes.	**Reply #10** We are expecting that the monitoring solution is software based and it is installed in a dedicated hardware that adheres with the monitoring solution's manufacturer's recommended system hardware requirements. Please refer to the Terms of Reference for more info.
V. Industry Certifications : Voluntary Product Accessibility template	
Question #11 Can this be removed? Or can we comply any 2 industry certifications in the list	**Reply #11** We require that the NGFW is certified on each of the industry certifications stated on the Terms of Reference.

c. Warranty and Support : Voluntary Product Accessibility template	
May we request for your consideration to modify the 24x7x2 to 24x7x4 response time of 4 hours after receiving the call or email request for support	DICT is supporting a mission-critical environment, thus we require a 24 x 7 x 2 response time via email or phone during system failure and downtime.
Others : Fail-over option from Head Office to DR site.	
Question #12 Is this required as part of our proposal? This requires a third party solution to handle it. 2 options as follows : 1. Fiber cabling from HO to DR Site (not feasible due to the distance issue e.g. Makati to QC) 2. A third party load balancer solution is required to handle this requirement.	**Reply #12** 1. We do not require fiber cabling from QC to Makati since we already have an existing connection to it. 2. We only require what is stated on the Terms of reference

This Supplemental/Bid Bulletin No. 1 shall form part of the Bidding Documents. Any provisions in the Bidding Documents inconsistent herewith is hereby amended, modified and superseded accordingly.

For guidance and information of all concerned.

Issued this 11th day of June, 2018 in Makati City.

Reviewed and Approved by:

(SGD)ATTY. MA. VICTORIA C. MAGCASE
Chairperson, Bids and Awards Committee – I

(SGD)ATTY. MA. GUDELIA C. GUESE
Vice Chairman

(SGD)CHRISTABELLE P. EBRIEGA
Member

(SGD)MYRA CHITELLA T. ALVAREZ
Member

(SGD)DAVID A. INOCENCIO
Member

Concurred by:

ASEC. ALLAN S. CABANLONG
Provisional Member- DICT

Received by:	
______________________________	______________________________
(SIGNATURE OVER PRINTED NAME & DATE)	**NAME OF COMPANY**
(PLEASE RETURN OR FAX THIS PAGE ONLY TO THE PITC BAC-I)	