REPUBLIC OF THE PHILIPPINES
SOCIAL SECURITY SYSTEM
East Avenue, Diliman, Quezon City

BIDS AND AWARDS COMMITTEE (BAC) I

PROJECT : **SUPPLY, DELIVERY, TESTING AND INSTALLATION OF ENTERPRISE FIREWALL IN SSS MAIN OFFICE AND DISASTER RECOVERY (DR) SITES**

ITB NO. : **Goods 2019-041**

SUBJECT : **BID BULLETIN NO. 1**

DATE : **09 August 2019**

Details of the bidding, as advertised:

Advertisement:	**Posting at Websites & Conspicuous Places – July 20 to 27, 2019**
Approved Budget for the Contract (ABC) and Source of Fund	**P26,990,000.00** **COB – CAPEX**
Price of BD (non-refundable)	P15,000.00
Delivery Period	90 calendar days from receipt of Notice to Proceed

This addendum/Bid Bulletin No. 1 is issued to clarify, modify or amend items in the Bidding Documents (BD) as a result of the pre-bidding conference on 29 July 2019. This shall form an integral part of the BD.

Under Section 22.5.3 of the RIRR of RA 9184, it shall be the responsibility of all those who have properly secured the BD to inquire and secure Supplemental/Bid Bulletins that may be issued by the BAC.

1. **Schedule of activities as discussed in the Pre-bidding Conference:**

   - Deadline for the submission of written queries: Thursday, 01 August 2019
   - Issuance of Bid Bulletin No. 1 – reply to written queries: Tuesday, 6 August 2019
   - **Submission and opening of 2 envelopes: Thursday, 15 August 2019, 2:00 p.m. at the Green Room, 12th floor, SSS Main Building, East Avenue, Diliman, Quezon City**

   Revised schedule of activities:

   - Issuance of Bid Bulletin No. 1 – reply to written queries: Friday, 9 August 2019
   - **Submission and opening of 2 envelopes: Tuesday, 20 August 2019, 3:00 p.m. at the Green Room, 12th floor, SSS Main Building, East Avenue, Diliman, Quezon City**

2. **Clarification and Amendments - Annex "A".**

3. **Documentary Requirements**

   a. **1st Envelope**

      a.1 PhilGEPS Certificate of Registration and membership.

      In case of uploaded document/s, which validity period had already expired, submit the updated document/s.

      a.2 Statement of all its Ongoing Government and Private Contracts, including contracts awarded but not yet started, if any, whether similar or not similar in nature and complexity to the contract to be bid;

a.3 Statement of Single Largest Completed Contract **within five (5) years** prior to the submission and opening of bids **with supporting documents,** which should be equivalent to at least **50% of the ABC.**

a.4 JVA, in case of Joint Venture – Class "B" Documents (Each partner of the joint venture shall submit the legal eligibility documents. The submission of technical and financial eligibility documents by any of the joint venture partners constitutes compliance, except for SSS Clearance that must be complied by all JV partners);

a.5 Omnibus Sworn Statement (form supplied)

a.6 NFCC Computation or committed Line of Credit (form supplied)

a.7 Bid Security (2% of the ABC for Cash or Manager's/Cashier's Check payable to SSS or Bank Draft of the ABC, 5% of the ABC for Surety Bond **or** Bid Securing Declaration – form supplied).

a.8 Technical Documents – project requirements
- Section VI – Schedule of Requirements
- Section VII – Statement of Compliance with the Technical Specifications

b. Checklist of the 2nd envelope:

b.1 Bid Form (form supplied) – pages 69 to 70
b.2 Bid Breakdown pages (form supplied) - page 71

c. Additional Requirements to be submitted by the bidder with the Lowest Calculated Bid

c.1 2018 Income Tax Return filed through Electronic Filing and Payment System (EFPS) corresponding to the submitted Audited Financial Statement;
c.2 Quarterly VAT for the period January to June 2019;
c.3 Documents listed in the Platinum Membership and updates, if any;
- SEC/DTI Registration
- 2019 Mayor's Permit
- Valid Tax Clearance
- 2018 Audited Financial Statement filed through EFPS

4. Awarding shall be made to the bidder with the Lowest Calculated and Responsive Bid (LCRB).

Prepared by:

ROSALYN AZUL-CONDAT
OIC, Administrative Support Section
BAC Secretariat Department

Concurred by:

MA. SALOME E. ROMANO
Chairperson, TWG

Approved by:

ERNESTO D. FRANCISCO, JR.
Senior Vice-President & Chairperson
Bids and Awards Committee I

Annex "A"
BAC Resolution No. BB-2019-081
dated 09 August 2019

ANNEX "A"

PROJECT: Supply, Delivery and Installation of Enterprise Firewall in SSS Main Office and Disaster Recovery (DR) Site

ANNEX A: TWG RESPONSE TO QUERIES/CLARIFICATIONS

I. ISSUES RAISED DURING THE PRE-BID CONFERENCE

ITEM	QUERY/CLARIFICATIONS	TWG/BAC Reply
1.	On Technical Specifications, page 56, item 1.1.5 – New Sessions per second - Is it 150 million or 150,000?	1. The correct value is 150,000 New Sessions per second. This amends Item 1.1.5 "Firewall components" of Section VII. "Technical Specifications"
2.	On Technical Specifications, item 1.1.13 - 4-Port 10/100/1000BASE-TX interfaces with built-in bypass port - Why is there a need for bypass? This defeats the essence of a firewall, maybe the correct term should be fail-close.	2. Bypass is no longer required. This amends Section VII. Technical Specifications.
3.	On Technical Specifications, item 1.1.1 - Firewall throughput: Minimum 60 Gbps and 1.1.2 - Threat Prevention throughput: Minimum 10 Gbps - Can you allow a Threat Prevention throughput of 20 Gbps but lower than 60 Gbps Firewall Throughput?	3. No.
4.	On Technical Specifications, item 1.1.15 – 2 USB Ports - Why is there a need for 2 USB Ports?	4. For backup.
5.	On Technical Specifications, item 1.2.5 – USB Port/s : 6 On-board USB ports ; At least two (2) ports located at the front panel; At least two (2) USB 3.0 ports - Can we offer an Appliance-based solution for the Management Console instead of a separate device?	5. Yes. This amends Section VII. Technical Specifications.
6.	On Technical Specifications, item 1.1.7 – Interface supported: (12 Ports) 10/100/1000 (8 Gigabit) SFP, (4) 10 Gigabit SFP+, with network expansion slot for 40G QSF + port card - Will you be requiring the same specifications in the DR site? - Should the specifications of the firewall in the MO be completely similar to the DR site?	 No. No. Refer to ITEM 1, Question 1.2 of RESPONSE TO WRITTEN QUERIES.
6.	On Technical Specifications, item 1.7 – User Identification - Will you be using AD for user authentication? - Can you consider a product that does not support e-Directory and LDAP?	6. Yes. No.

ITEM	QUERY/CLARIFICATIONS	TWG/BAC Reply
7.	On Technical Specifications, item 1.3.5 – Platform - ASIC requirement - Only selected firewalls can support such requirement, can you consider others that do not have it?	7. Yes.

II. RESPONSE TO WRITTEN QUERIES

A. TRENDS AND TECHNOLOGIES, INC.

ITEM NO.	QUERIES/CLARIFICATIONS	TWG RESPONSE
1.	Under Section VII Technical Specifications, page 56 Items 1.1.5, 1.1.7, 1.1.8, 1.1.13 and 1.1.14 **1.1 Firewall Components** 1.1.5. New sessions per second: 150,000,000 1.1.7.Interface supported (12 ports) 10/100/1000 (8 Gigabit) SFP, (4) 10 Gigabit SFP+, with network expansion slot for 40G QSF + port card 1.1.8. Management I/O: (2) 10/100/1000, (1) 40G/100G QSFP28 HA, (1) 10/100/1000 out-of-band management, (1) RJ45 console port or (1) db9 console port 1.1.13. 4-Port bypass 10/100/1000BASE-TX interfaces with built-in 1.1.14 2-Port 10/100/1000BASE-TX interface with RJ-45 connector *Question 1.1* ***For us to better understand the interface requirement, we would like to request for a copy of the existing firewall infra diagram (e.g. Core Back bone, ISP, and DMZ connectivity) and your proposed set up as well?*** *Question 1.2* **How would these firewall appliances connect to SSS network infrastructure? What would be the links/connection? On the same manner what is the connectivity type and bandwidth in DR?**	1.1) Please see attached diagram ***(Annex B)*** for the existing and proposed firewall diagram. 1.2) Links/Connections for Main Office and DR are as follows:(Please see Annex B) **Main Office (MO)** *4 x 40G to the Core layer switch,* *2 x 10G to proposed WAN Switch,* *2 x 10G to existing DMZ A and 12 x 1G for DMZ* **DRSite** *1 x 10G to DR Core Switch* *8 x 1GE existing 1 WAN Switch and DMZ Switch* *Additional requirement for Head Office. Supply, delivery, installation and testing of the following equipment below:*

		1. *Two (2) units of Cisco Nexus 7000 F3-Series 12 Port 40GbE (QSFP) line card* 2. *Four (4) units of 40GBASE-SR4 QSFP Transceiver* 3. *One (1) Unit Wide Area Network Edge Switch (24 Ports) 10/100/1000 Mbps UTP with 2 10G Transceiver Ports (10G ports is separate from the 24 ports* 4. *1 lot Fiber Patch Cords* *Note: Bidder must submit Manufacturer certification stating the bidder is authorized reseller of the cisco equipment mentioned above.*
	Question 1.3 **For item 1.1.7, please validate if the interface supported (12-ports) 10/100/1000, is just the total of the subsequent 8 SFP fiber interface and 4x10Gb SFP+?**	1.3) Yes, it is the total of the interfaces. Please see below list of interface. **SSSMO (per appliance)** ▪ *8x10/100/1000 Ethernet (RJ-45) ports* ▪ *2 x 10G SFP+ ports* ▪ *2 x 40G QSFP ports* **SSS DRSite** ▪ *8 x10/100/1000 Ethernet (RJ-45) ports* ▪ *1 x 10G SFP+ ports* **Firewall Management Console @ MO** ▪ 1 x 10G ports
	Question 1.4 **For items 1.1.13 bypass requirement, can this be removed since NGFW deployment that uses bypass ports is an in-line/transparent and not in a gateway/routed configuration which will be the setup of this system?**	1.4) Refer to ITEM 2, ISSUES RAISED DURING THE PRE-BID CONFERENCE.
	Question 1.5 **For item 1.1.8, can the 40/100G QSFP28HA management port be changed to (1) 10G ? The 40/100G is not a common approach for a Firewall High-availability and management architecture, dedicated 10/100/1000 Mbps ports usually suffice clustering heartbeat and management segment.**	1.5) Yes.
	Question 1.6 ***Item 1.1.5, New sessions per second: 150,000,000. We want to clarify if this 150 Million or 150 Thousand?***	1.6) Refer to ITEM 1, ISSUES RAISED DURING THE PRE-BID CONFERENCE.
2.	Section VII Technical Specifications, page 57 Items 1.2.3, 1.2.5, 1.2.6 and 1.2.7 1.2.3 **Storage:** (HHD) Hot-swappable: Minimum 2 TB 1.2.5. **USB Port/s :** 6 On-board USB ports ; At least two (2) ports located at the front panel; At least two (2) USB 3.0 ports 1.2.6. **Form Factor :** SFF Desktop: Maximum height is	

	6 inches SFF Tower: Maximum width is 6 inches 1.2.7. **Monitor :** 23" Wide LED, 1920 X 1080, DVI or HDMI or Display Port ***Question 2.1*** ***Items 1.2.5, 1.2.6 and 1.2.7 depict a Small Form Factor server specification which presumably the management is an application based that runs on it, will you consider an appliance-based management console setup?*** ***Question 2.2*** ***Item 1.2.3 Will SSS allow to lower the minimum HDD to 1TB?***	2.1 Yes 2.2. No
3.	Section VI. Technical Specification, Page 57,Item 1.3.5 Have the hardened Operating System (OS) and built as a firewalls appliance (i.e. not an generic server hardware) and shall handle traffic in a single pass stream-based manner with all features turned on. It shall be optimized for layer 7 application level content processing and have special Application-Specific Integrated Circuit (ASIC) to handle signature matching and processing in a single pass parallel processing architecture. ***Question 3.1*** ***ASIC is not common features or technology for firewall; can we offer standard based multi core network processor that is capable of accelerating the network traffic? Multicore network processor is more efficient and capable of scaling the performance in accordance with the growth of general computing, chipset, which life cycle and performance improved much better than the ASIC Chipset. By leveraging on the advantage of the development of multicore CPU, our firewall scale up the performance very well.***	3.1 Refer to ITEM 8, ISSUES RAISED DURING THE PRE-BID CONFERENCE.
4.	Section VII. Technical Specification, Page 58 Item 1.4.7 Support the ability to circumvent the route lookup process and the subsequent Policy-Based Forwarding (PBF) lookup for return traffic (server to client). The firewalls shall use the original incoming interface as the egress interface. However, if the source IP is in the same subnet as the incoming interface on the firewalls, symmetric return shall not take effect. ***Question 4.1*** ***Is policy based routing (PBR) acceptable as this also supports the ability*** **circumvent the route lookup process?**	4.1. Yes

5.	Section VII. Technical Specification, page 60 1.9.5 Client Remote Access (c) Remote access agent shall be provide host information profile (i.e. patch level of OS, status of Anti-Virus software or Host-based IPS, etc.) to the firewalls to ascertain whether the host meets the required security requirement before allowing access into the internal corporate network. d) Remote access agent shall be able to determine whether the client is within the internal corporate network. If its not, it shall be able automatically connect to the firewalls and establish a secure tunnel (via SSL or IPSec VPN). **Question # 5.1** **Requirement item c and d is more of a Network Access Control (NAC) technology rather than an Enterprise Firewall project. Kindly remove item c and d.**	5.1This specification will be removed. This amend Section VII. Technical Specifications.
6.	Page 62 Item 1.12.4. **Capability** (c) Should have experienced and certified personnel for the proposed solution ***Question # 6.1*** ***What type of certification and how many certified personnel is needed ?***	6.1. Network or Security Certification. 6.2 At least two(2) certified personnel.
7.	Page 65 Item 5.5.7 If within 24 hours, upon arriving onsite, the service contractor fails to restore / repair the malfunctioning part / component, the service contractor must supply and install a service unit within the next 12 hours. SSS use of service units must not exceed 15 calendar days from the date the problem was first reported to the supplier, defective units must be fixed or replaced within 15 days. All shipment / delivery fees must be charged against the account of the service contractor. ***Question # 7.1*** ***Since the requirement is HA already, can you extend the 12 hours requirement for the service unit to 48 hours ? Likewise, can you also extend the 15 days replacement to 30days? Standard replacement process is 30 days since the replacement unit will be comingoutside the country.***	7.1 No

8.	Page 49 Item 4 DURING POST QUALIFICATION. The Supplier with the lowest calculated bid shall ensure that the proposed solution is compatible with the existing SSS IT Infrastructure during the Post-Qualification *Question 8.1* ***Since the requirement is an enterprise grade firewall appliance, would SSS allow us to use a virtualized environment (VM) version for the demo/ proof of concept?***	8.1 Yes

B. ACCENT MICRO TECHNOLOGIES INC.

ITEM NO.	QUERIES/CLARIFICATIONS	TWG RESPONSE
9.	*Question 1* ***Under line item 1.1.5 New Sessions per second:150,000,000*** ***The new session per second with the value of 150,000,000 is over the maximum sessions as stated on line item 1.1.4 which is 6,000,000 sessions per second.*** ***Is this a type error? If it is, what is the correct value?***	9. Yes, it is a typographical error. The correct value is 150,000 New Sessions per second. This amends Item 1.1.5 "Firewall components" of Section VII. "Technical Specifications"
10.	*Question 2* ***Under line item 1.1.13 4-Port 10/100/1000 Base-TX interfaces with built-in bypass.*** ***We would like to clarify why SSS needs built-in bypass in the firewall?*** ***Bypass traffic allows all internet traffic (in and out) to pass without checking its identity, either it contains malicious software, viruses or any other threats. This is not recommended and not a good security setup. We highly recommend that this (built-in bypass) be removed.***	10. Please refer toITEM 1, Question 1.4. of RESPONSE TO WRITTEN QUERIES.

11.	*Question 3* *Under line item 1.1.1 Firewall throughput : Minimum of 60 Gbps.* Under line item 1.1.2 Threat Prevention throughput: Minimum of 10 Gbps *The firewall throughput performance is based on stateful packet inspection which decides either on incoming/outgoing traffic is allowed to pass or block. These re two (2) most widely protocols being use and those are http/https where user uses it for browsing the internet and smtp for email.* *Since users are using these protocols, we cannot simply block it. Hence we need to open it. This is where the threat prevention comes in. The next generation firewalls open those ports (http/https.smtp) but uses threat prevention like IPS, AV and URL filtering to deter malware, virus and all forms of attacks. Majority of traffic rules are based on these (2) protocols. With this, we highly recommend to lower the value of firewall throughput from sixty (60) to forty (40) and increase the threat prevention, throughput from ten (10) to twenty (20) Gbps as this is mostly being used.*	11. We maintain the minimum requirement of 60Gbps firewall throughput.

C. PALO ALTO NETWORKS

ITEM NO.	QUERIES/CLARIFICATIONS	TWG RESPONSE
12.	Question 1 Under line item 1.1.5 New Sessions per second:150,000,000 Please reconfirm if this a typo error and it is actually 150,000 thousand New Session Per Sec.	12. Please refer toITEM 1.of ISSUES RAISED DURING THE PRE-BID CONFERENCE.
13.	Question 2 Under line item 1.1.13 4-Port 10/100/1000 Base-TX interfaces with built-in bypass. We would like to clarify the requirement of SSS for built-in bypass in the firewall? The value of a Firewall by default is used as perimeter device that routes our internal traffic to the internet either by NAT of L3 routing. When a firewall fails and interface goes to a by-pass port, the internet bound traffic will remain down because there will be no device to process NAT or even routing. In a transparent deployment wherein a firewall only performs traffic inspection and	13. Refer to ITEM 2 of ISSUES RAISED DURING THE PRE-BID CONFERENCE.

	as main perimeter defense, network for all traffic can freely go in and out of SSS network without security inspections when the firewall is on a by-pass mode. Our proposed designed is based on HA, wherein the event of a device failure your traffic would still pass through and maintaining your security posture without any compromise. We are requesting that "Line item 1.1.13 4-Port 10/100/1000 Base-TX interfaces with built-in bypass" be removed.	
14.	Question 3 Under line item 1.1.1 Firewall throughput: Minimum of 60 Gbps. Under line item 1.1.2 Threat Prevention throughput: Minimum of 10 Gbps Palo Alto Firewall has two unique features, the Application-based enforcement (App-ID) & User Identification (User-ID) that provides Layer 7 visibility. Our firewall throughput performance is measured with 64Kb HTTP transactions, and Firewall Throughput already includes App-ID and User-ID all tests are done under real enterprise traffic scenarios. Our Threat Prevention throughput measured with App-ID, IPS, antivirus, anti-spyware, WildFire and logging enabled utilizing 64KB HTTP/appmix transactions. All features are turned ON and performance is not measured individually. With this, we highly recommend to lower the value of firewall throughput from 60 to 40 and increase the threat prevention throughput from 10 to 20 Gbps which is mostly being used.	14. Refer to ITEM 11 of RESPONSE TO WRITTEN QUERIES.

D. ePLDT

ITEM NO.	QUERIES/CLARIFICATIONS	TWG RESPONSE
15.	Question 1 Line item 1.1.13 4Port 10/100/1000BASE-TX interfaces with built-in bypass Based on the discussion last prebid, bypass traffic allows all internet traffic (in and out) to pass without checking its identity, either it contains malicious software, viruses or any other threats. Our proposed design is based on HA, in which case this is more than enough to protect our DATA's without bypassing our security. We would like to request that line item 1.1.13	15. Refer to ITEM 2 of ISSUES RAISED DURING THE PRE-BID CONFERENCE.

	4-Port 10/100/1000BASE-TX interfaces with built-in bypass" be removed	
16.	Question 2 Line item 1.1.1 Firewall throughput: Minimum of 60Gbps., Based also on the discussion during PBC, firewall throughput performance is based on stateful packet inspection which decides either an incoming/outgoing traffic is allowed to pass or block. Two of the most widely used protocols in the internet are http/https where user uses it for browsing the internet and smtp for email. Since users are using these protocols, we cannot simply block it. With that said, we need to open it. This is where the threat prevention comes in. The next generation firewalls open those ports and uses threat prevention like IPS, AV and URL filtering to prevent any malware, virus and all forms of attacks. We would like to highly recommend and request to lower the value of firewall throughput from 60 to 40 and increase the threat prevention throughput from 10 to 20Gbps as this is mostly being used to support the statements above.	16. Refer to ITEM 11 of RESPONSE TO WRITTEN QUERIES.