REPUBLIC OF THE PHILIPPINES
SECURITIES & EXCHANGE COMMISSION
SEC Building, EDSA, Greenhills
City of Mandaluyong, Metro Manila

Project Title: **Supply, Delivery, Installation, Testing and Commissioning of Three (3) Units of Next Generation Firewall**

BID BULLETIN No. 4

All prospective bidders are hereby informed of the following clarifications:

	Query	Clarification
1 InfoBahn	While most appliance can conform to 3 to 4 items, this however does not make them a next generation FW, as it still fails to meet or exceeds all the requirement. Kindly check the ones that need to be injected in the TOR. • Our recommendation is that the proposed firewall shall support policy based forwarding based on zone, source or destination address, source or destination port, application and Active Directory(AD)/Lightweight Directory Access Protocol (LDAP) Remote Authentication Dial in User Service (RADIUS) user or user groups • Our recommendation is that the proposed firewall shall have modern malware protection that identifies unknown malicious files by directly and automatically executing them in a virtual cloud-based environment to expose malicious behavior even if the malware has never been seen in the wild before without the need for additional hardware. • Our recommendation o The proposed FW solution shall be managed from Web-based Graphical User Interface (GUI) and Command-line Interface (CLI) o The proposed FW shall be able to manage itself without the need for external servers or appliances, at the same time with an option to be managed centrally o The proposed FWs shall have dedicated management port that has separate routing tables from the other production interfaces o The proposed FWs management shall be able to granularly assigned management function for each management user group or for individual user	CIC cannot accommodate requests just to meet vendor capabilities or limitation.. CIC adopted the Gartner definition of Next Generation Firewall, as follows: "Next-generation firewalls (NGFWs) are deep-packet inspection firewalls that move beyond port/protocol inspection and blocking to add application-level inspection, intrusion prevention, and bringing intelligence from outside the firewall. An NGFW should not be confused with a stand-alone network intrusion prevention system (IPS), which includes a commodity or non-enterprise firewall, or a firewall and IPS in the same appliance that are not closely integrated." (Source: http://www.gartner.com/it-glossary/next-generation-firewalls-ngfws)

	Query	Clarification
	○ The proposed FWs are able to schedule lof exports using SCP or FTP protocol ○ The proposed FW s hall have a reporting management system capable of generating reports on a manual ad-hoc or schedule (daily, weekly, monthly, etc.) basis • The proposed FW shall be able to generate reports on individual user ID with (but not limited to) the following activities, Application Usage, accessed websites & URL Categories • The proposed FW shall support at least TWO HINDRED (200) megabits per second per second throughput with threat prevention, application awareness, URL filtering, antivirus, with SSL VPN turned on simultaneously. FIVEHUNDRED (500) sessions of SS VPN clients shall be supported. Please provide 3rd party test to substantiate performance • The proposed FW shall have the hardened Operating System (OS) and built as a firewall appliance (i.e. not on 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 • With all functions on at layer 7 (application layer) the appliance should be able to handle traffic at low latency and performance will not drop and still maintain its advertised throughput. Other appliance could do this at layer 3 but true test for Next Generation FEW should be at layer 7.	
2 AG Datacom Phil., Inc.	Denial of Service (DDOS) Protection of Layer 4 to 7 – Removal or Relaxed of DDOS Protection of Layers 4 to 7	CIC cannot accommodate requests just to meet vendor capabilities or limitation.
3 TIM Corp	1. In the Technical Specifications, item A.1. Functional Description. "Email Security including Anti-Spam, Anti-Phishing (applies only to Business Office Firewall)" – We would just like to confirm if "Email Security" requirement is only in the Business Office? Is this not required in the Data Center? 2. In the Technical Specifications, item A.2. Performance Requirements B. Business Office –	Email security is required only for the business office, not for the data center as company's email is hosted in a cloud, not in the data center. 200mb of data refers to file size limit

	Query	Clarification
	"ii. Control access to cloud-based services including email, external websites and internal applications with 200 megabytes (MB) of data" – Is the 200 MB of data the "session limit" or the "file size limit" that the firewall will handle?	
	3. In the Technical Specifications, item A.6. Certification – Can other firewall certifications such as "ICSA Labs". "Checkmark" or "Virtual Private Network Consortium (VPNC)" be also accepted in the "Certification" criteria?	CIC cannot accommodate requests just to meet vendor capabilities or limitation.

This Bid Bulletin No. 4 shall form an integral part of the Bid Documents.

December 12, 2014 Mandaluyong City.

Jose P. Aquino
Chairman, BAC

Suite 1705 17/F Atlanta Centre, # 31 Annapolis St., Greenhills, San Juan, Metro Manila, Philippines
Tel: (63-2) 584 0988, 584 1173, 564 1157
Fax: (63-2) 744 3244
info@agdatacom.com; www.agdatacom.com

December 9, 2014

To: Secretariat, Bids and Awards Committee
Securities and Exchange Commission
9th Floor, SEC Building, EDSA
Greenhills, Mandaluyong City

To whom it may concern;

a. This letter serves as to request and appeal to the SECRETARAT, BIDS AND AWARDS COMMITTEE for the Project "***Supply, Delivery, Installation, Configuration and Commissioning of Three (3) units of Next Generation Firewalls" With*** (SEC PB No. 2014-12)

Reference Number	Description from SEC	Recommendation	Advantages
Technical Specifications **Item A** **No. 1 of Funtional Description**	Denial of Service (DDOS) Protection of Layers 4 to 7	Removal or Relaxed of Denial of Service (DDOS) Protection of Layers 4 to 7	• Intrusion Prevention System functionality of Next Generation Firewalls has already DDOS Protection which is good enough for the Agency. • You will Lessen the Cost because Looking for DDOS Protection for Layer 4 to7 will require you to Buy a STAND ALONE Separate Appliance of DDOS. • Removing Protection Layer 4 to 7 will open the doors to other prospective bidders to join and let this project be successful.

We Hope for your Favorable Response.

Very truly yours,

Thanks and Best Regards!

Roxanne DL. Carpio
VP for Sales

AG Datacom Philippines Inc.
Suite 1705 17th Floor, Atlanta Centre #31 Annapolis St.,
Greenhills, San Juan Metro Manila 1502 Philippines
Tel : (+632)5840988, 7443244

InfoBahn Communications, Inc.
Positive Change Through Technology

2/F DRB (Fil-American) Bldg.
Aurora Blvd.Cor La Salle St.
Cubao, Quezon City, 1109
T : 913-9888 F : 315-8890

December 3, 2014

Office of the BAC Secretariat
Human Resources and Administrative Department
Securities and Exchange Commission
9th Floor SEC Bldg Edsa, Mandaluyong City

Dear Sir/Madam,

We are writing for the clarification on the bid documents stated in the Terms of Reference for the project "***Supply, Delivery, Installation, Configuration, Testing and Commissioning of Three (3) Units of Next generation Firewall***".

Since the requirement calls that we supply Next Generation Firewall, it is just but proper that we adhere to 5 definitions of what a Next Gen FW should be.

While most appliance can conform to 3 to 4 items, this however does not make them a next generation FW, as it still fails to meet or exceeds all the requirement.
Kindly check the ones that needs to be injected in the TOR (especially the ones in red).

1. Identify application regardless of ports, protocol, or evasive tactics or SSL.

2. Identify Users regardless of IP address.

- **Our recommendation is that the proposed firewalls shall support policy based forwarding based on zone, source or destination address, source or destination port, application and Active Directory (AD)/ Lightweight Directory Access Protocol (LDAP) Remote Authentication Dial In User Service (RADIUS) user or user groups**

3. Protect in real time against threats embedded across applications.

- **Our recommendation is that the he proposed firewall shall have modern malware protection that identifies unknown malicious files by directly and automatically executing them in a virtual cloud-based environment to expose malicious behavior even if the malware has never been seen in the wild before without the need for additional hardware.**

(This justify that real threat prevention means protecting your network not just for unknown threats but most importantly new/or unknown threats, inclusion of this, is what will really protect network)

4. Fine grained visibility and policy control over application access and functionality.

Our Recommendation:

1.1.1 The proposed firewalls solution shall be managed from Web-based Graphical User Interface (GUI) and Command-Line Interface (CLI).

1.1.2 The proposed firewalls shall be able to manage itself without the need for external servers or appliances, at the same time with an option to be managed centrally.

1.1.3 The proposed firewalls shall have a dedicated management port that has separate routing tables from the other production interfaces.

1.1.4 The proposed firewalls management shall be able to granularly assigned management functions for each management user group or for individual user.

1.1.5 The proposed the firewalls are able to schedule log exports using SCP or FTP protocol.

1.1.6 The proposed firewalls shall have a reporting management system capable of generating reports on a manual ad-hoc or schedule (daily, weekly, monthly, etc) basis.

- **The proposed firewalls shall be able to generate reports on individual user ID with (but not limited to) the following activities, Application Usage, accessed websites & URL Categories.**

5. Multi gigabit in deployment with no performance degradation.

- **The proposed firewalls shall support at least TWO HUNDRED (200) megabit per second per second throughput with threat prevention, application awareness, URL filtering, antivirus, with SSL VPN turned on simultaneously. FIVE HUNDRED (500)sessions of SSL VPN clients shall be supported. Please provide 3rd party test reports to substantiate performance.**

- The proposed firewalls shall have the hardened Operating System (OS) and built as a firewall appliance (i.e. not on 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

(the means with all functions on at layer 7 (application layer) the appliance should be able to handle traffic at low latency and performance will not drop and still maintain its advertised throughput. Other appliance could do this at layer 3, but true test for Next Generation FW should be at layer 7 (with all functions on)

For your information and approval

Very truly yours,

BLAIR BENJAMIN C. IGNACIO
Account Manager
INFOBAHN COMM. INC.

December 11, 2014

Secretariat
Bids and Awards Committee
Securities and Exchange Commission (SEC)
4th Floor SEC Building , EDSA Greenhills Mandaluyong City
Philippines

Dear Sir / Madam,

Greetings!

I would like to extend my most sincere appreciation for allowing Total Information Management (TIM) Corporation the opportunity to participate in the bid for the Firewall Project for Credit Information Corporation (CIC). During the evaluation of the Technical Bid Documents supplied by the procuring entity to TIM, we have found a number of clarifications which we would like to bring up to the Bids and Awards Committee. Listed below are our clarificatory inquiries for the project bid.

1. In the Technical Specifications, item A.1. Functional Description,"Email Security including Anti-Spam, Anti-Phishing (applies only to Business Office firewall)" – We would just like to confirm if 'Email Security' requirement is only in the Business office? Is this not required in the Data Center?

2. In the Technical Specifications, item A.2. Performance Requirements B. Business office –"ii. Control access to cloud-based services including email, external websites and internal applications with 200 megabytes (MB) of data" - Is the 200 MB of data the 'session limit' or the 'file size limit' that the firewall will handle?

3. In the Technical Specifications, item A.6. Certification –Can other firewall certifications such as 'ICSA Labs', 'Checkmark' and 'Virtual Private Network Consortium (VPNC)' be also accepted in the "Certification" criteria?

   We are requesting reconsideration for item no. 4 above because in our opinion, by accepting other types of valid and publicly recognized certifications, it will be beneficial for the government agency for it will encourage other suitable & reputable vendors to propose and participate in the bidding. In the end, this will be in the best interest of the government agency as it spouses the spirit of fairness and competitiveness.

I hope that the good committee finds our inquiries in good order. I thank you for taking the time and attention towards this matter.

Much Regards,

Karen Santos
Account Manager – Financial Services and Institutions
Total Information Management Corporation