



Bids and Awards Committee for ICT

November 8, 2022

BID BULLETIN NO. 1

This Bid Bulletin No. 1 is issued to modify or amend items in the Bid Document with Solicitation No.: 22-10-105 for the **Procurement of Firewall Subscription**.

In the Pre-Bid Conference conducted last November 4, 2022 for the above-mentioned project, the following revisions in the bidding documents were effected:

1) Amendments to Section I – INVITATION TO BID

<i>No.</i>	<i>Before</i>	<i>Revised</i>
2	The <i>PHILIPPINE SCIENCE HIGH SCHOOL – MAIN CAMPUS</i> now invites bids for the above Procurement Project. Delivery of the Goods is required by thirty (30) calendar days . Bidders should have completed, within five (5) years from the date of submission and receipt of bids, a contract similar to the Project. The description of an eligible bidder is contained in the Bidding Documents, particularly, in Section II (Instructions to Bidders).	The <i>PHILIPPINE SCIENCE HIGH SCHOOL – MAIN CAMPUS</i> now invites bids for the above Procurement Project. Delivery of the Goods is required by sixty (60) calendar days . Bidders should have completed, within five (5) years from the date of submission and receipt of bids, a contract similar to the Project. The description of an eligible bidder is contained in the Bidding Documents, particularly, in Section II (Instructions to Bidders).
4	Prospective Bidders may obtain further information from <i>PHILIPPINE SCIENCE HIGH SCHOOL – MAIN CAMPUS</i> and inspect the Bidding Documents at the address given below during <i>[insert office hours]</i> .	Prospective Bidders may obtain further information from <i>PHILIPPINE SCIENCE HIGH SCHOOL – MAIN CAMPUS</i> and inspect the Bidding Documents at the address given below during 8:00 a.m. to 3:00 p.m.

2) Amendments to Section VI – SCHEDULE OF REQUIREMENTS

Item Number	Description	Quantity	Total	Delivered, Weeks/Months
1	PROCUREMENT OF FIREWALL SUBSCRIPTION	1	1	60 CD

3) Amendments to Section VII – TECHNICAL SPECIFICATIONS

<i>Before</i>	<i>Revised</i>
PROCUREMENT OF FIREWALL SUBSCRIPTION	PROCUREMENT OF FIREWALL SUBSCRIPTION
Performance	Performance
The proposed solution must have at least 25 Gbps Firewall Layer 3 throughput.	The proposed solution must have at least 25 Gbps Firewall Layer 3 throughput.
The proposed solution must support at least 3,000,000 concurrent sessions.	The proposed solution must support at least 3,000,000 concurrent sessions.

The proposed solution must support atleast 200,000 new connections per second.	The proposed solution must support atleast 200,000 new connections per second.
Security Capabilities and Update	Security Capabilities and Update
The proposed solution must provide non-interruptable basic functionality for Access Control, Intrusion Prevention, Botnet Detection and Content Security ON PERPETUAL LICENSE (i.e. no License Expiry/ no loss of aforementioned functionality and accessibility after license expiry)	The proposed solution must provide non-interruptable basic functionality for Access Control, Intrusion Prevention, Botnet Detection and Content Security ON PERPETUAL LICENSE (i.e. no License Expiry/ no loss of aforementioned functionality and accessibility after license expiry)
The proposed solution must provide non-interruptable basic functionality for known and unknown malware detection	The proposed solution must provide non-interruptable basic functionality for known and unknown malware detection
Interface	Interface
The proposed solution must have at least 4*10/100/1000 Base-T, 4*1G Fiber SFP Interface, 2*10G Fiber SFP+ Interface	The proposed solution must have at least 4*10/100/1000 Base-T, 4*1G Fiber SFP Interface, 2*10G Fiber SFP+ Interface
Management	Management
Management console must be managed through Web interfaces via secure encrypted connection.	Management console must be managed through Web interfaces via secure encrypted connection.
<p>The proposed solution must support policy configuration modules for the following functions from a single appliance</p> <ul style="list-style-type: none"> - Stateful firewall - DDos Prevention, ARP spoofing prevention - Anti-Virus - Anti-Malware, On-premise artificial intelligence based malware detection engine - Anti-phishing - Intrusion Prevention System - Web Application Firewall, semantic detection method - SSL Decryption - Risk assessment by on-demand and real-time scanner - Cloud sandboxing - Cloud threat intelligence - IPsec VPN - SSL VPN 	<p>The proposed solution must support policy configuration modules for the following functions from a single appliance</p> <ul style="list-style-type: none"> - Stateful firewall - DDos Prevention, ARP spoofing prevention - Anti-Virus - Anti-Malware, On-premise artificial intelligence based malware detection engine - Anti-phishing - Intrusion Prevention System - Web Application Firewall, semantic detection method - SSL Decryption - Risk assessment by on-demand and real-time scanner - Cloud sandboxing - Cloud threat intelligence - IPsec VPN - SSL VPN

- User authentication and grouping - Web(URL) filtering, Application control, Bandwidth management - Report center / dashboard with emailable and printable reports	- User authentication and grouping - Web(URL) filtering, Application control, Bandwidth management - Report center / dashboard with emailable and printable reports
The proposed solution must support security protection features for pre-attack, during-attack and post-attack.	The proposed solution must support security protection features for pre-attack, during-attack and post-attack.
Firewall	Firewall
The proposed solution must support static and dynamic package filtering, Inspection on well-known protocols including FTP, HTTP, SMTP, RTSP, H.323 (Q.931, H.245, RTP/RTCP), SQLNET, SNMP, PPTP, TCP, UDP	The proposed solution must support static and dynamic package filtering, Inspection on well-known protocols including FTP, HTTP, SMTP, RTSP, H.323 (Q.931, H.245, RTP/RTCP), SQLNET, SNMP, PPTP, TCP, UDP
The proposed solution must be able to protect against popular and common attacks including LAND attacks, Smurf, Teardrop, IP spoofing, SYN/ICMP/UDP flood, HTTP GET flood, DNS query flood, ARP cheating, ICMP redirection	The proposed solution must be able to protect against popular and common attacks including LAND attacks, Smurf, Teardrop, IP spoofing, SYN/ICMP/UDP flood, HTTP GET flood, DNS query flood, ARP cheating, ICMP redirection
GeoLocation Block, create rules to allow or block traffic from IP addresses in specific countries, regions and states, reduce the attack possible.	GeoLocation Block, create rules to allow or block traffic from IP addresses in specific countries, regions and states, reduce the attack possible.
Application Control	Application Control
The proposed solution should support application control feature and meet the following specifications:	The proposed solution should support application control feature and meet the following specifications:
Support application control and can identify & control over 5000+ applications.	Support application control and can identify & control over 5000+ applications.
Support admin customization (i.e. add their own application types)	Support admin customization (i.e. add their own application types)
Control common and popular applications including game, P2P, shopping and social networking	Control common and popular applications including game, P2P, shopping and social networking
Should be able to control applications via source/destination IP, username, Schedule	Should be able to control applications via source/destination IP, username, Schedule
URL Filtering	URL Filtering
The proposed product must support URL filtering:	The proposed product must support URL filtering:
Provide at least 50+ URL categories , include game, gambling, finance, Pornography etc.	Provide at least 50+ URL categories , include game, gambling, finance, Pornography etc.
Support manual creation of customized URL categories.	Support manual creation of customized URL categories.
Should provide on-premise URL signature database (i.e. not only rely on cloud).	Should provide on-premise URL signature database (i.e. not only rely on cloud).
Intrusion Prevention System	Intrusion Prevention System
The proposed solution must support vulnerability database with at least 5000+ entries	The proposed solution must support vulnerability database with at least 5000+ entries
The IPS system must be able to block common and popular intrusions including worms,	The IPS system must be able to block common and popular intrusions including worms,

Trojans, spyware, scanning, DoS, DDoS, vulnerability exploits, buffer overflow attacks, abnormal protocol (protocol anomaly) and attacks with evasive tactics employed.	Trojans, spyware, scanning, DoS, DDoS, vulnerability exploits, buffer overflow attacks, abnormal protocol (protocol anomaly) and attacks with evasive tactics employed.
The IPS supports brute-force attack prevention for common and popular protocols including FTP, IMAP MSSQL, POP3 SMTP, ORACLE, RDP, SMBv1, SMBv2, SMBv3	The IPS supports brute-force attack prevention for common and popular protocols including FTP, IMAP MSSQL, POP3 SMTP, ORACLE, RDP, SMBv1, SMBv2, SMBv3
APT prevention	APT prevention
The proposed solution must support APT detection of intruder presence including identifying botnet, remote control trojans, malicious link	The proposed solution must support APT detection of intruder presence including identifying botnet, remote control trojans, malicious link
The proposed solution must support anti-malware database with more than 100,000+ entries	The proposed solution must support anti-malware database with more than 100,000+ entries
The proposed solution must be able to lock a suspicious IP when malicious behavior from that IP is detected by any of the modules.	The proposed solution must be able to lock a suspicious IP when malicious behavior from that IP is detected by any of the modules.
APT supports to detect ddos attack from intranet	APT supports to detect ddos attack from intranet
Support honeypot feature and locate the real host IP address of the intranet infected botnet virus	Support honeypot feature and locate the real host IP address of the intranet infected botnet virus
Risk Assessment and Prevention	Risk Assessment and Prevention
The proposed solution must provide risk assessment module that allows to scan and identify security loopholes such as open port, system vulnerabilities, weak passwords and other risks of the protected servers	The proposed solution must provide risk assessment module that allows to scan and identify security loopholes such as open port, system vulnerabilities, weak passwords and other risks of the protected servers
The proposed solution must support real-time vulnerability analysis, includes the underlying software vulnerability analysis, Web application risk analysis, Web unsafe configuration detection and server weak password detection, and generate real-time analysis report. That can be deployed in mirror mode to discover system vulnerabilities within protected network in real-time.	The proposed solution must support real-time vulnerability analysis, includes the underlying software vulnerability analysis, Web application risk analysis, Web unsafe configuration detection and server weak password detection, and generate real-time analysis report. That can be deployed in mirror mode to discover system vulnerabilities within protected network in real-time.
The real-time vulnerability is also to support to detect for the website if it exited backlink, and we can record the type of the backlink and the location of backlink.	The real-time vulnerability is also to support to detect for the website if it exited backlink, and we can record the type of the backlink and the location of backlink.
Risk assessment and scanning results must be shown and generated with corresponding reports with description of the issues and recommended solution.	Risk assessment and scanning results must be shown and generated with corresponding reports with description of the issues and recommended solution.
Risk assessment module must be able to be affiliated with the IPS and server protection module to automatically generate the protection policies	Risk assessment module must be able to be affiliated with the IPS and server protection module to automatically generate the protection policies
Threat Alerts is able to actively push the current popular 0 day or high-risk vulnerabilities, and can provide vulnerability detection tools for	Threat Alerts is able to actively push the current popular 0 day or high-risk vulnerabilities, and can provide vulnerability detection tools for

business scan, according to the results of scan, it can generate safety protection policies.	business scan, according to the results of scan, it can generate safety protection policies.
Web application	Web application
The proposed solution should support a built-in WAF capability in Firewall but not separate appliance and supports the following features:	The proposed solution should support a built-in WAF capability in Firewall but not separate appliance and supports the following features:
Defense against the 10 major web-based attacks identified by the Open Web Application Security Project (OWASP) , including SQL injection, XSS, CSRF, by semantic detection engine.	Defense against the 10 major web-based attacks identified by the Open Web Application Security Project (OWASP) , including SQL injection, XSS, CSRF, by semantic detection engine.
WAF database that hosts not less than 5000 Web-based attacks rules	WAF database that hosts not less than 5000 Web-based attacks rules
Perform inspection of the content at the perimeter for incoming traffic. Only to allow input parameters that conform to the application functionalities required of the web application and no malicious input parameters	Perform inspection of the content at the perimeter for incoming traffic. Only to allow input parameters that conform to the application functionalities required of the web application and no malicious input parameters
Restrict suspicious file uploading with file types of asp, asa, exe, jsp, php,aspx,php3,php4,phtml, vbs etc.	Restrict suspicious file uploading with file types of asp, asa, exe, jsp, php,aspx,php3,php4,phtml, vbs etc.
CC, CSRF and Cookie attack prevention.	CC, CSRF and Cookie attack prevention.
Password protection, including FTP weak password detection, WEB login weak password detection, WEB login plaintext transmission detection, password brute force protection	Password protection, including FTP weak password detection, WEB login weak password detection, WEB login plaintext transmission detection, password brute force protection
Data Breach Prevention	Data Breach Prevention
Allow to define multiple types of sensitive information based on the characteristics of stored data, the sensitive information includes email account information, MD5 encrypted passwords.	Allow to define multiple types of sensitive information based on the characteristics of stored data, the sensitive information includes email account information, MD5 encrypted passwords.
The proposed solution must be able to restrict suspicious file downloading with file types of dat, bak,dmp,backup, asa,log, fp, frx, frm, CNF, ade,mde, db, ldb,etc.,	The proposed solution must be able to restrict suspicious file downloading with file types of dat, bak,dmp,backup, asa,log, fp, frx, frm, CNF, ade,mde, db, ldb,etc.,
Anti-Virus	Anti-Virus
Stream-based anti-virus for HTTP, FTP, SMTP and POP3 , SMBv3 protocols	Stream-based anti-virus for HTTP, FTP, SMTP and POP3 , SMBv3 protocols
The proposed solution must support built-in capability to detect malware, virus and ransomware variants and provide the malware analysis report	The proposed solution must support built-in capability to detect malware, virus and ransomware variants and provide the malware analysis report
Should support compressed file malware inspection, up to 16 layers	Should support compressed file malware inspection, up to 16 layers
Support scan of the files up to at least 20MB	Support scan of the files up to at least 20MB
Content Security	Content Security
Mail protection supports for pop3, smtp, imap, pop3s, smtps, imaps and other specified ports.	Mail protection supports for pop3, smtp, imap, pop3s, smtps, imaps and other specified ports.
Mail protection supports mail collision attack prevention and anti-phishing.	Mail protection supports mail collision attack prevention and anti-phishing.
Mail attachment can be detected by anti-virus.	Mail attachment can be detected by anti-virus.
Support mail attachment filter and http/ftp download/upload filter.	Support mail attachment filter and http/ftp download/upload filter.

When users receive a Malicious Mail, The proposed solution will tamper the mail subject	When users receive a Malicious Mail, The proposed solution will tamper the mail subject
Access Management	Access Management
The proposed solution must support up to at least 5 user identification methods including active directory (AD) authentication and Remote Authentication Dial-In User Service (RADIUS) and LDAP	The proposed solution must support up to at least 5 user identification methods including active directory (AD) authentication and Remote Authentication Dial-In User Service (RADIUS) and LDAP
The proposed solution must support security policy optimizer, which helps: 1) Identify the redundant policy, expired policy, conflict policy etc. 2) Be able to track the ACL policy life cycle, help to track every changes that have been done to the policy in a specific period of time	The proposed solution must support security policy optimizer, which helps: 1) Identify the redundant policy, expired policy, conflict policy etc. 2) Be able to track the ACL policy life cycle, help to track every changes that have been done to the policy in a specific period of time
The proposed solution must support link load balance per traffic load as well as application type in occasion of multiple Internet lines	The proposed solution must support link load balance per traffic load as well as application type in occasion of multiple Internet lines
Reporting	Reporting
The proposed solution must support built-in report center, which provides comprehensive security analysis reports	The proposed solution must support built-in report center, which provides comprehensive security analysis reports
The proposed solution must support business model learning, which will help to simplify the security operation for web servers, and reduce the false positive.	The proposed solution must support business model learning, which will help to simplify the security operation for web servers, and reduce the false positive.
Support the detailed logs for security issues as DOS attack, web attack, IPS, viruses, website access, application control, user login and OS configuration.	Support the detailed logs for security issues as DOS attack, web attack, IPS, viruses, website access, application control, user login and OS configuration.
Support detailed threats analysis for specific attack by Description, Target, Solution	Support detailed threats analysis for specific attack by Description, Target, Solution
The report center must provide full visibility to network, endpoint clients and the business servers with multi-dimensional analysis of risks, vulnerabilities, attacks, threats, traffic and behaviors	The report center must provide full visibility to network, endpoint clients and the business servers with multi-dimensional analysis of risks, vulnerabilities, attacks, threats, traffic and behaviors
Support PDF format and automatically send to pre-defined mailbox on daily/weekly/monthly basis	Support PDF format and automatically send to pre-defined mailbox on daily/weekly/monthly basis
Supports automatic generation of comprehensive security risk reports. The content of the report should reflect but not limited: <ul style="list-style-type: none"> ▪ The overall security level of the protected network object The vulnerability information & forensic evidence each attack	Supports automatic generation of comprehensive security risk reports. The content of the report should reflect but not limited: <ul style="list-style-type: none"> ▪ The overall security level of the protected network object The vulnerability information & forensic evidence each attack
Deployment	Deployment

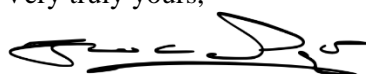
<p>The proposed solution must support following deployment options</p> <ul style="list-style-type: none"> - Gateway (Route mode) - Bridge mode - Mirror mode - Multiple Bridge mode (2- 4 bridges) 	<p>The proposed solution must support following deployment options</p> <ul style="list-style-type: none"> - Gateway (Route mode) - Bridge mode - Mirror mode - Multiple Bridge mode (2- 4 bridges)
<p>The proposed solution must support build-in auto hardware bypass in the event of hardware failure</p>	<p>The proposed solution must support build-in auto hardware bypass in the event of hardware failure</p>
<p>VPN</p>	<p>VPN</p>
<p>The proposed solution must support to build Proprietary VPN tunnel between HQ and branches</p>	<p>The proposed solution must support to build Proprietary VPN tunnel between HQ and branches</p>
<p>IPSEC VPN</p> <p>Authentication algorithm: MD5/SHA-1</p> <p>Encryption algorithm: DES/3DES/AES128 Hash:MD5/SHA</p>	<p>IPSEC VPN</p> <p>Authentication algorithm: MD5/SHA-1</p> <p>Encryption algorithm: DES/3DES/AES128 Hash:MD5/SHA</p>
<p>SSL VPN :</p> <p>Source Type: L3VPN resources, TCP resources.</p> <p>Operating System Supported: Win XP/Win 7/Win 8/Win 10/MAC/Win 11/ Ubuntu Linux</p> <p>Supports 2FA with google authenticator, microsoft authenticator</p>	<p>SSL VPN :</p> <p>Source Type: L3VPN resources, TCP resources.</p> <p>Operating System Supported: Win XP/Win 7/Win 8/Win 10/MAC/Win 11/ Ubuntu Linux</p> <p>Supports 2FA with google authenticator, microsoft authenticator</p>
<p>Real-time visibility</p>	<p>Real-time visibility</p>
<p>Real time provides CPU, memory, disk usage, session number, the number of online users, the network interface</p>	<p>Real time provides CPU, memory, disk usage, session number, the number of online users, the network interface</p>
<p>The proposed solution must be provide real-time user ranking / real-time application ranking</p>	<p>The proposed solution must be provide real-time user ranking / real-time application ranking</p>
<p>The proposed solution must be provide real-time attack map, include top attack country and counting, real-time attack and threat detail</p>	<p>The proposed solution must be provide real-time attack map, include top attack country and counting, real-time attack and threat detail</p>
<p>Provide information security incidents, including recently security incidents, server security incidents, terminal security incidents displays the current network risks need to be handled, and top attacks</p>	<p>Provide information security incidents, including recently security incidents, server security incidents, terminal security incidents displays the current network risks need to be handled, and top attacks</p>
<p>Routing</p>	<p>Routing</p>
<p>Supports static route, RIPv1 & v2, OSPFv2 and BGP</p>	<p>Supports static route, RIPv1 & v2, OSPFv2 and BGP</p>
<p>The proposed solution must be able to support but not limited to intelligent route selection based on source and destination IP, Port, Protocol and country based IP address</p>	<p>The proposed solution must be able to support but not limited to intelligent route selection based on source and destination IP, Port, Protocol and country based IP address</p>

Support DNS-Mapping	Support DNS-Mapping
Certification	Certification
In order to ensure the maturity of solution technology, the principal must be CMMI L5 certified	In order to ensure the maturity of solution technology, the principal must be:
<ul style="list-style-type: none"> ● ISO 9001:2015 ● ISO/IEC 27001:2013 ● ISO 14001:2015 ● ISO/IEC 20000-1:2018 	<ul style="list-style-type: none"> ● at least CMMI L3 certified or ISO 9001:2015 ● ISO 9001:2015 ● ISO/IEC 27001:2013 ● ISO 14001:2015 ● ISO/IEC 20000-1:2018 or ITIL v.4
Warranty and support	Warranty and support
At least one (1) year for the hardware and software components of the project.	At least one (1) year for the hardware and software components of the project.
Vendor must have direct local support in the Philippines.	Vendor must have direct local support in the Philippines.
Provide on-call technical support	Provide on-call technical support
VI. Training Requirements	VI. Training Requirements
- Provide comprehensive training for MIS People with Certificates with regards to the use of the device and the software.	- Provide comprehensive training for MIS People with Certificates with regards to the use of the device and the software.
VII. Installation, Configuration and Testing	VII. Installation, Configuration and Testing
- Configure the device for installation based on the specification provided by the MIS example (load balancing, packet filtering, etc.)	- Configure the device for installation based on the specification provided by the MIS example (load balancing, packet filtering, etc.)
- Installation and Testing. - Perform 13 Steps Firewall Testing and also test the set configurations of the firewall. - Provide documentation of the tools, methods used for the test and the results. Included in the document, are recommendations to further improve the configuration and how to set them.	- Installation and Testing. - Perform 13 Steps Firewall Testing and also test the set configurations of the firewall. - Provide documentation of the tools, methods used for the test and the results. Included in the document, are recommendations to further improve the configuration and how to set them.
-Documentation of the configuration and instructions on how to set them.	-Documentation of the configuration and instructions on how to set them.

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

For guidance and information of all concerned.

Very truly yours,



LEO ANDREI A. CRISOLOGO
Chairperson, BAC for ICT