

Republic of the Philippines Department of Science and Technology **PHILIPPINE SCIENCE HIGH SCHOOL MAIN CAMPUS** Agham Road, Diliman, Quezon City (02) 8929-1606



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

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

## 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

Before	Revised
PROCUREMENT OF FIREWALL	PROCUREMENT OF FIREWALL
SUBSCRIPTION	SUBSCRIPTION
Performance	Performance
The proposed solution must have atleast 25	The proposed solution must have atleast 25
Gbps Firewall Layer 3 throughput.	Gbps Firewall Layer 3 throughput.
The proposed solution must support atleast	The proposed solution must support atleast
3,000,000 concurrent sessions.	3,000,000 concurrent sessions.

The sum of the left of sum of sum of states	The sum of the last of the second second set of the set	
The proposed solution must support atleast	The proposed solution must support atleast	
200,000 new connections per second.	200,000 new connections per second.	
Security Capabilities and Update	Security Capabilities and Update	
The proposed solution must provide non-	The proposed solution must provide non-	
interruptable basic functionality for Access	interruptable basic functionality for Access	
Control, Intrusion Prevention, Botnet Detection	Control, Intrusion Prevention, Botnet Detection	
and Content Security ON PERPETUAL	and Content Security ON PERPETUAL	
LICENSE (i.e. no License Expiry/ no loss of	LICENSE (i.e. no License Expiry/ no loss of	
aforementioned functionality and accessibility	aforementioned functionality and accessibility	
after license expiry)	after license expiry)	
The proposed solution must provide non-	The proposed solution must provide non-	
interruptable basic functionality for known and	interruptable basic functionality for known and	
unknown malware detection	unknown malware detection	
Interface	Interface	
The proposed solution must have at least	The proposed solution must have at least	
4*10/100/1000 Base-T, 4*1G Fiber SFP	4*10/100/1000 Base-T, 4*1G Fiber SFP	
Interface, 2*10G Fiber SFP+ Interface	Interface, 2*10G Fiber SFP+ Interface	
Management	Management	
Management console must be managed through	Management console must be managed through	
Web interfaces via secure encrypted connection.	Web interfaces via secure encrypted connection.	
The proposed solution must support policy	The proposed solution must support policy	
configuration modules for the following	configuration modules for the following	
functions from a single appliance	functions from a single appliance	
renetiono nom a singre appriance	ranetions from a single apphance	
- Stateful firewall	- Stateful firewall	
- DDos Prevention, ARP spoofing prevention	- DDos Prevention, ARP spoofing prevention	
- Anti-Virus	- Anti-Virus	
- Anti-Malware, On-premise artificial intelligence based malware detection engine	- Anti-Malware, On-premise artificial intelligence based malware detection engine	
- Anti-phishing	- Anti-phishing	
- Intrusion Prevention System	- Intrusion Prevention System	
- Web Application Firewall, semantic detection method	- Web Application Firewall, semantic detection method	
- SSL Decryption	- SSL Decryption	
- Risk assessment by on-demand and real-time scanner	- Risk assessment by on-demand and real-time scanner	
- Cloud sandboxing	- Cloud sandboxing	
- Cloud threat intelligence	- Cloud threat intelligence	
- IPsec VPN	- IPsec VPN	
- SSL VPN	- SSL VPN	

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

Trojans, spyware, scanning, DoS, DDoS,	Trojans, spyware, scanning, DoS, DDoS,
vulnerability exploits, buffer overflow attacks,	vulnerability exploits, buffer overflow attacks,
abnormal protocol (protocol anomaly) and	abnormal protocol (protocol anomaly) and
attacks with evasive tactics employed.	attacks with evasive tactics employed.
The IPS supports brute-force attack prevention	The IPS supports brute-force attack prevention
for common and popular protocols including	for common and popular protocols including
FTP, IMAP MSSQL, POP3 SMTP, ORACLE,	FTP, IMAP MSSQL, POP3 SMTP, ORACLE,
RDP, SMBv1, SMBv2, SMBv3	RDP, SMBv1, SMBv2, SMBv3
APT prevention	APT prevention
The proposed solution must support APT	The proposed solution must support APT
detection of intruder presence including	detection of intruder presence including
identifying botnet, remote control trojans,	identifying botnet, remote control trojans,
malicous link	malicous link
The proposed solution must support anti-	The proposed solution must support anti-
malware database with more than 100,000+	malware database with more than 100,000+
entries	entries
The proposed solution must be able to lock a	The proposed solution must be able to lock a
suspicious IP when malicious behavior from that	suspicious IP when malicious behavior from
IP is detected by any of the modules.	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	Support honeypot feature and locate the real
host IP address of the intranet infected botnet	host IP address of the intranet infected botnet
virus	virus
<b>Risk Assessment and Prevention</b>	Risk Assessment and Prevention
The proposed solution must provide risk	The proposed solution must provide risk
assessment module that allows to scan and	assessment module that allows to scan and
identify security loopholes such as open port,	identify security loopholes such as open port,
system vulnerabilities, weak passwords and	system vulnerabilities, weak passwords and
other risks of the protected servers	other risks of the protected servers
The proposed solution must support real-time	The proposed solution must support real-time
vulnerability analysis, includes the underlying	vulnerability analysis, includes the underlying
software vulnerability analysis, Web application	software vulnerability analysis, Web application
risk analysis, Web unsafe configuration	risk analysis, Web unsafe configuration
detection and server weak password detection,	detection and server weak password detection,
and generate real-time analysis report. That can	and generate real-time analysis report. That can
be deployed in mirror mode to discover system	be deployed in mirror mode to discover system
vulnerabilities within protected network in real-	vulnerabilities within protected network in real-
time.	time.
The real-time vulnerability is also to support to	The real-time vulnerability is also to support to
detect for the website if it exited backlink, and	detect for the website if it exited backlink, and
we can record the type of the backlink and the	we can record the type of the backlink and the
location of backlink.	location of backlink.
Risk assessment and scanning results must be	Risk assessment and scanning results must be
shown and generated with corresponding reports	shown and generated with corresponding
with description of the issues and recommended	reports with description of the issues and
solution.	recommended solution.
Risk assessment module must be able to be	Risk assessment module must be able to be
affiliated with the IPS and server protection	affiliated with the IPS and server protection
module to automatically generate the protection	module to automatically generate the protection
policies	policies
Threat Alerts is able to actively push the current	Threat Alerts is able to actively push the current
popular 0 day or high-risk vulnerabilities, and	popular 0 day or high-risk vulnerabilities, and
can provide vulnerability detection tools for	can provide vulnerability detection tools for
2	2

business seen according to the results of seen it	business scan, according to the results of scan, it	
business scan, according to the results of scan, it can generate safety protection policies.	can generate safety protection policies.	
Web application	Web application	
The proposed solution should support a built-in	The proposed solution should support a built-in	
WAF capability in Firewall but not separate	WAF capability in Firewall but not separate	
appliance and supports the following features:	appliance and supports the following features:	
Defense against the 10 major web-based attacks	Defense against the 10 major web-based attacks	
identified by the Open Web Application	identified by the Open Web Application	
Security Project (OWASP), including SQL	Security Project (OWASP), including SQL	
injection, XSS, CSRF, by semantic detection	injection, XSS, CSRF, by semantic detection	
engine.	engine.	
WAF database that hosts not less than 5000	WAF database that hosts not less than 5000	
Web-based attacks rules	Web-based attacks rules	
Perform inspection of the content at the	Perform inspection of the content at the	
perimeter for incoming traffic. Only to allow	perimeter for incoming traffic. Only to allow	
input parameters that conform to the application	input parameters that conform to the application	
functionalities required of the web application	functionalities required of the web application	
and no malicious input parameters	and no malicious input parameters	
Restrict suspicious file uploading with file types	Restrict suspicious file uploading with file types	
of asp, asa, exe, jsp, php,aspx,php3,php4,phtml,	of asp, asa, exe, jsp, php,aspx,php3,php4,phtml,	
vbs etc.	vbs etc.	
CC, CSRF and Cookie attack prevention.	CC, CSRF and Cookie attack prevention.	
Password protection, including FTP weak	Password protection, including FTP weak	
password detection, WEB login weak password	password detection, WEB login weak password	
detection, WEB login plaintext transmission	detection, WEB login plaintext transmission	
detection, password brute force protection	detection, password brute force protection	
Data Breach Prevention	Data Breach Prevention	
Allow to define multiple types of sensitive	Allow to define multiple types of sensitive	
information based on the characteristics of	information based on the characteristics of	
stored data, the sensitive information includes	stored data, the sensitive information includes	
email account information, MD5 encrypted	email account information, MD5 encrypted	
passwords.	passwords.	
The proposed solution must be able to restrict	The proposed solution must be able to restrict	
suspicious file downloading with file types of	suspicious file downloading with file types of	
dat, bak,dmp,backup, asa,log, fp, frx, frt, CNF,	dat, bak,dmp,backup, asa,log, fp, frx, frt, CNF,	
ade, mde, db, ldb, etc.,	ade, mde, db, ldb, etc.,	
Anti-Virus	Anti-Virus	
Stream-based anti-virus for HTTP, FTP, SMTP	Stream-based anti-virus for HTTP, FTP, SMTP	
and POP3, SMBv3 protocols	and POP3, SMBv3 protocols	
The proposed solution must support built-in	The proposed solution must support built-in	
capability to detect malware, virus and	capability to detect malware, virus and ransomware variants and provide the malware	
ransomware variants and provide the malware	•	
analysis report Should support compressed file malware	analysis report Should support compressed file malware	
inspection, up to 16 layers	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,	Mail protection supports for pop3, smtp, imap,	
pop3s, smtps, imaps and other specified ports.	pop3s, smtps, imaps and other specified ports.	
Mail protection supports mail collision attack	Mail protection supports mail collision attack	
prevention and anti-phishing.	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	Support mail attachment filter and http/ftp	
support man attachment inter and http/11p		
download/upload filter.	download/upload filter.	

When years reasing a Maligious Mail The	When years receive a Malicious Mail The	
When users receive a Malicious Mail, The	When users receive a Malicious Mail, The	
proposed solution will tamper the mail subject	proposed solution will tamper the mail subject	
Access Management	Access Management	
The proposed solution must support up to at	The proposed solution must support up to at	
least 5 user identification methods including active directory (AD) authentication and Remote	least 5 user identification methods including active directory (AD) authentication and	
- · · · · · · · · · · · · · · · · · · ·	Remote Authentication Dial-In User Service	
Authentication Dial-In User Service (RADIUS)		
and LDAP	(RADIUS) and LDAP	
The proposed solution must support security	The proposed solution must support security	
policy optimizer, which helps:	policy optimizer, which helps:	
1) Identify the redundant policy, expired policy,	1) Identify the redundant policy, expired policy,	
conflict policy etc.	conflict policy etc.	
2) Be able to track the ACL policy life cycle,	2) Be able to track the ACL policy life cycle,	
help to track every changes that have been done	help to track every changes that have been done	
to the policy in a specific period of time	to the policy in a specific period of time	
The proposed solution must support link load	The proposed solution must support link load	
balance per traffic load as well as application	balance per traffic load as well as application	
type in occasion of multiple Internet lines	type in occasion of multiple Internet lines	
Reporting	Reporting	
The proposed solution must support built-in	The proposed solution must support built-in	
report center, which provides comprehensive	report center, which provides comprehensive	
security analysis reports	security analysis reports	
The proposed solution must support business	The proposed solution must support business	
model learning, which will help to simplify the	model learning, which will help to simplify the	
security operation for web servers, and reduce	security operation for web servers, and reduce	
the false positive.	the false positive.	
Support the detailed logs for security issues as DOS attack, web attack, IPS, viruses, website	Support the detailed logs for security issues as DOS attack, web attack, IPS, viruses, website	
access, application control, user login and OS	access, application control, user login and OS	
configuration.	configuration.	
Support detailed threats analysis for specific	Support detailed threats analysis for specific	
attack by Description, Target, Solution	attack by Description, Target, Solution	
The report center must provide full visibility to	The report center must provide full visibility to	
network, endpoint clients and the business	network, endpoint clients and the business	
servers with multi-dimensional analysis of risks,	servers with multi-dimensional analysis of risks,	
vulnerabilities, attacks, threats, traffic and	vulnerabilities, attacks, threats, traffic and	
behaviors	behaviors	
Support PDF format and automatically send to	Support PDF format and automatically send to	
pre-defined mailbox on daily/weekly/monthly	pre-defined mailbox on daily/weekly/monthly	
basis	basis	
Supports automatic generation of comprehensive	Supports automatic generation of	
security risk reports. The content of the report	comprehensive security risk reports. The	
should reflect but not limited:	content of the report should reflect but not	
• The overall security level of the	limited:	
protected network object	• The overall security level of the	
protected network object	protected network object	
The vulnerability information & forensic	protected lictwork object	
evidence each attack	The vulnerability information & forensic	
	evidence each attack	
Deployment	Deployment	
2 - Projinent	1. Projinchi	

The proposed solution must support following deployment options	The proposed solution must support following deployment options
- Gateway (Route mode)	- Gateway (Route mode)
- Bridge mode	- Bridge mode
- Mirror mode	- Mirror mode
- Multiple Bridge mode (2- 4 bridges)	- Multiple Bridge mode (2- 4 bridges)
The proposed solution must support build-in	The proposed solution must support build-in
auto hardware bypass in the event of hardware	auto hardware bypass in the event of hardware
failure	failure
VPN	VPN
The proposed solution must support to build Proprietary VPN tunnel between HQ and branches	The proposed solution must support to build Proprietary VPN tunnel between HQ and branches
IPSEC VPN	IPSEC VPN
Authentication algorithm: MD5/SHA-1	Authentication algorithm: MD5/SHA-1
Encryption algorithm: DES/3DES/AES128 Hash:MD5/SHA	Encryption algorithm: DES/3DES/AES128 Hash:MD5/SHA
SSL VPN :	SSL VPN :
Source Type: L3VPN resources, TCP resources.	Source Type: L3VPN resources, TCP resources.
Operating System Supported: Win XP/Win 7/Win 8/Win 10/MAC/Win 11/ Ubuntu Linux	Operating System Supported: Win XP/Win 7/Win 8/Win 10/MAC/Win 11/ Ubuntu Linux
Supports 2FA with google authenticator,	Supports 2FA with google authenticator,
microsoft authenticator	microsoft authenticator
Real-time visibility	Real-time visibility
Real time provides CPU, memory, disk usage,	Real time provides CPU, memory, disk usage,
session number, the number of online users, the	session number, the number of online users, the
network interface	network interface
The proposed solution must be provide real-time	The proposed solution must be provide real-
user ranking / real-time application ranking	time user ranking / real-time application ranking
The proposed solution must be provide real-time	The proposed solution must be provide real-
attack map, include top attack country and	time attack map, include top attack country and
counting, real-time attack and threat detail	counting, real-time attack and threat detail
Provide information security incidents,	Provide information security incidents,
including recently security incidents, server	including recently security incidents, server
security incidents, terminal security incidents	security incidents, terminal security incidents
displays the current network risks need to be handled, and top attacks	displays the current network risks need to be handled, and top attacks
handled, and top attacks  Pouting	handled, and top attacks
<b>Routing</b> Supports static route, RIPv1 & v2, OSPFv2 and	<b>Routing</b> Supports static route, RIPv1 & v2, OSPFv2 and
BĜP	BĜP
The proposed solution must be able to support	The proposed solution must be able to support
but not limited to intelligent route selection	but not limited to intelligent route selection
based on source and destination IP, Port,	based on source and destination IP, Port,
Protocol and country based IP address	Protocol and country based IP address

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: • at least CMMI L3 certified or ISO 9001:2015
•ISO 9001:2015	•ISO 9001:2015
•ISO/IEC 27001:2013	•ISO/IEC 27001:2013
•ISO 14001:2015 •ISO/IEC 20000-1:2018	• <del>ISO 14001:2015</del>
•150/1LC 20000-1.2018	•ISO/IEC 20000-1:2018 or ITIL v.4
Warranty and support	Warranty and support
At least one (1) year for the hardware and	At least one (1) year for the hardware and
software components of the project.	software components of the project.
Vendor must have direct local support in the	Vendor must have direct local support in the
Philippines.	Philippines.
Provide on-call technical support	Provide on-call technical support
VI. Training Requirements	VI. Training Requirements
- Provide comprehensive training for MIS	- Provide comprehensive training for MIS
People with Certificates with regards to the use	People with Certificates with regards to the use
of the device and the software.	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.	- Installation and Testing.
- Perform 13 Steps Firewall Testing and also test	- Perform 13 Steps Firewall Testing and also
the set configurations of the firewall.	test the set configurations of the firewall.
- Provide documentation of the tools, methods	- Provide documentation of the tools, methods
used for the test and the results. Included in the	used for the test and the results. Included in the
document, are recommendations to further	document, are recommendations to further
improve the configuration and how to set them.	improve the configuration and how to set them.
-Documentation of the configuration and	-Documentation of the configuration and
instructions on how to set them.	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