PASEGURUHAN NG MGA NAGLILINGKOD SA PAMAHALAAN
(GOVERNMENT SERVICE INSURANCE SYSTEM)
Financial Center, Pasay City, Metro Manila 1308

GSIS BIDS AND AWARDS COMMITTEE
FOR INFRASTRUCTURE AND INFORMATION TECHNOLOGY

Project Title: **Maintenance of Existing Enterprise Security**

Bid Bulletin No. 2
30 April 2015

This bid bulletin is issued to respond to the bidder's queries and to provide the new procurement for the project "*Maintenance of Existing Enterprise Security*". This shall form an integral part of the Bidding Documents.

A. Bidder's Queries

Bidder's Queries	GSIS Response
Item No.17.4 under GCC Clause of Section V - Special Conditions of the Contract	
• On "*The period for correction of defects is within 10 calendar days.*"- May we respectfully clarify if the period being referred to is that of a resolution time?	This refers to 10 calendar days resolution time once a defect is reported.
Item No.2 under Section VI - Schedule of Requirements	
• On "*Preventive Maintenance: House Keeping, Optimization, Fine Tuning and Diagnostic Reports.*" This provision is new.	Yes
• If *House Keeping* means the routine task of a System Administrator in order for the system to function or function efficiently, we deem to understand that you are referring to the role of GSIS's System Administrators. If however, expectation on housekeeping involves	Housekeeping refers to quarterly housekeeping that the provider will perform as basis for quarterly maintenance billing. For instance, SEP is to evaluate its DB, determine capacity and performance thresholds, and if necessary, provides indexing.

service to conduct Quarterly Health Checks, it can be provided with the following scope: Status of Symantec Endpoint Protection Manager; Check the virus definitions of clients through SEPM; Gathering of reports such as Licensing Status report, Risk Summary, and Computer Status Report and Recommendation based on the analysis of gathered data.	
• On *Optimization and fine tuning*. We usually provide further recommendations in our Health Check. The suggested recommendations may be applied by GSIS's Systems Administrator.	If necessary, once issues/concerns are identified in diagnostic health checks, the service provider will submit recommendations on how to improve system performance or to mitigate failures, which will then be applied by GSIS personnel.
• On *Diagnostic Reports*. May we know of the expectations of GSIS in this report?	This includes system/components health checks, (such us, but not limited to, state of system batteries [either in good condition or needs replacement], CPU and memory usage, and other diagnostics) to ensure optimal operation of SEP, CCS, SWG, SMG (*e.g.,* to determine if SEP database needs to be indexed). This will be part of the documentary requirements, which will serve as a basis for quarterly billing activities.
Item No.2.1.6 under 2.1 General Requirements of 2.Detailed Requirements, Section VII – Technical Specifications	
• On *"2.1.6. Provide support procedure and problem escalation."* - It is not clear now in the current provision whether these are for Managed Security Services, as previously they were. Please specify if these provisions will remain to be the same as "only for Managed Services".	Please refer to **Annex A** of his Bid Bulletin.
• On 2.1.6.23 and 2.1.6.24 - *"Unlimited request for minor changes" and "Significant Changes"* respectively pertains to remediation	Please refer to **Annex A** of his Bid Bulletin.

within Symantec Solution that will address a Symantec product issue. This will be applied to the Symantec Manager Console and up to 10 pilot endpoints. The rest will be managed by GSIS's systems administrators.	

ANNEX A

Below are the amendments made to the numbering/sequence for Item Nos. 2.1.6.1 up to 2.1.6.31 of Section VII (Technical Specifications) in the Bidding Documents:

From	To
2.1.6.1. Managed Security Services	**2.2 Managed Security Services**
2.1.6.2. Service Level Warranty Metrics	
2.1.6.3. Managed Device Availability Up-Time Percentage 99.90%	**2.2.1 Service Level Warranty Metrics**
2.1.6.4. Security Operation Center (SOC) availability uptime percentage 99.90%	2.2.1.1 Managed Device Availability Up-Time Percentage 99.90%
2.1.6.5. Should provide phone escalation in the event of a critical incident	2.2.1.2 Security Operation Center (SOC) availability uptime percentage 99.90%
2.1.6.6. Emergency change or assistance response(offsite) time 30 minutes	2.2.1.3 Should provide phone escalation in the event of a critical incident
2.1.6.7. Should provide a security analyst (off-site) and available 24 x 7 x 365	2.2.1.4 Emergency change or assistance response(offsite) time 30 minutes
2.1.6.8. Log retention should be three (3) months online and one(1) year offline	2.2.1.5 Should provide a security analyst (off-site) and available 24 x 7 x 365
2.1.6.9. Monthly Reporting available on SII	2.2.1.6 Log retention should be three (3) months online and one(1) year offline
2.1.6.10. Service Features	2.2.1.7 Monthly Reporting available on SII
2.1.6.11. Provide Management and configuration assistance but not limited to the following	**2.2.2 Service Features**
2.1.6.12. Firewall	2.2.2.1 Provide Management and configuration assistance but not limited to the following: • Firewall • IPS and IDS • Symantec Endpoint Protection
2.1.6.13. IPS and IDS	
2.1.6.14. Symantec Endpoint Protection	
2.1.6.15. Able to integrate into Global Intelligence Network(GIN) data in security analysis	2.2.2.2 Able to integrate into Global Intelligence Network(GIN) data in security analysis
2.1.6.16. Daily Service Summary delivered by e-mail	2.2.2.3 Daily Service Summary delivered by e-mail
2.1.6.17. Online logs may be queried by customer via the SII	2.2.2.4 Online logs may be queried by customer via the SII
2.1.6.18. Compliance reporting must be available via SII	2.2.2.5 Compliance reporting must be available via SII
2.1.6.19. Must be able to access Secure Internet Interface	2.2.2.6 Must be able to access Secure Internet Interface
2.1.6.20. Operations manual must be available on the SII	2.2.2.7 Operations manual must be available on the SII
2.1.6.21. Change Management	

2.1.6.22. Management Standard Changes (Includes a single, low-risk configuration or policy change using SII standard change request templates. For endpoints, includes basic administrative tasks on the Management Console) 2.1.6.23. Unlimited request for minor changes 2.1.6.24. Significant Changes (Includes software changes or high-risk policy changes that interrupt device functionality. Includes Endpoint patch and maintenance updates to Management Console and Endpoint Protection Database): within 5 business day 2.1.6.25. Web Portal(Secure Internet Interface or SII) 2.1.6.26. Should have a secured two-factor authentication 2.1.6.27. Provide at most 5 registered VIP device per credentials 2.1.6.28. Should provide least 3 account/credential for GSIS personnel 2.1.6.29. Should be available 24 x 7 x 365 2.1.6.30. Able to generate custom and scheduled reports and can be downloaded and emailed as an attachment 2.1.6.31. Web chat feature for immediate communication to security analyst.	**2.2.3 Change Management** 2.2.3.1 Management Standard Changes (Includes a single, low-risk configuration or policy change using SII standard change request templates. For endpoints, includes basic administrative tasks on the Management Console) 2.2.3.2 Unlimited request for minor changes 2.2.3.3 Significant Changes (Includes software changes or high-risk policy changes that interrupt device functionality. Includes Endpoint patch and maintenance updates to Management Console and Endpoint Protection Database): within 5 business day **2.2.4 Web Portal(Secure Internet Interface or SII)** 2.2.4.1 Should have a secured two-factor authentication 2.2.4.2 Provide at most 5 registered VIP device per credentials 2.2.4.3 Should provide least 3 account/credential for GSIS personnel 2.2.4.4 Should be available 24 x 7 x 365 2.2.4.5 Able to generate custom and scheduled reports and can be downloaded and emailed as an attachment 2.2.4.6 Web chat feature for immediate communication to security analyst.

B. New Procurement Schedule

Procurement Activity	From	To
Submission of Bids	04 May 2015, 10:00AM	08 May 2015, 10:00AM
Opening of Bids	04 May 2015, 10:30AM	08 May 2015, 10:30AM

For the guidance and information of all concerned.

VP SALVACION P. MATE
Chairperson
GBAC for Infrastructure and Information Technology