SUPPLEMENTAL BID BULLETIN NO. 2023-12-002

Procurement of Cyber Security Platform Based on Machine Learning and AI (OSG PR No. 023-11-209)

TO ALL PROSPECTIVE BIDDERS:

Please be guided on the following revisions to the Terms of Reference:

Particulars	From	To
Qualification of Supplier	*The bidder shall submit a valid and current Certificate of Distributorship/Dealership/Resellers of the product being offered, issued by the principal or manufacturer of the product (if the bidder is not the manufacturer). If not issued by the manufacturer, they must also submit a certification/document linking the bidder to the manufacturer.*	*"The bidder must have completed, within the last five years from the submission date and receipt of at least one (1) single contract of a similar nature amounting to at least fifty percent (25%) of the ABC. For a similar contract, the bidder must have completed at least one (1) ICT subscription contract in the last five years."*
Technical Specifications		
1. Regarding Technology, **Item 1.3**	*After the initial learning period, the technology must automatically provide a complete audit trail of all subnets found in the network.*	*"By inputting just an IP, Domain, URL, or Port, it should provide a real-time view that traces the attack's origin and entry point, uncovers the attacker's trajectory, and delivers a thorough root-cause analysis"*
Item 1.4.2	*It should operate completely based on behavior, where technologies that make use of rules and/or signatures will not be allowed*	*"It should operate completely by combining both rule-based/signature, User and entity behavior analytics (UEBA), and Machine Learning"*
2. Regarding External Integrations and Reports **Item 2.0.1**	*The entire deployment summary indicating the total number of devices, the total number of subnets, and processed media bandwidth*	*"The entire deployment summary indicating either of the following: the total number of devices, the total number of subnets, or processed media bandwidth"*
Item 2.2.1	*a. SIEM and SOAR*	*"a. SIEM or SOAR"*
Item 2.2.2	*b. Ticketing System and Case Management*	*"b. A Ticketing System or Case Management is preferred but not required"*
Item 2.3	*Have the capability to connect to TAXII servers and import STIX XML files*	*"Have the capability to connect to TAXII servers or import XML files"*
Item 2.5	*The technology must have its own mobile app available in both GooglePlay and AppleStore to enable remote management of incidents via mobile phones*	*"The technology must have a web-based platform that monitors the security alerts and tasks of the systems within the coverage of the platform."*
3. Regarding Architecture	*It must support a complete and scalable architecture through the licensing of additional components*	*"It must support a complete and scalable architecture wherein its licensing is independent on several*

Item 3.0	*required to integrate with the various digital environments, including on-premises, cloud, and hybrids, if the contractor wishes to acquire them in the future, supporting at least:*	*endpoints and through the integration with the various digital environments, supporting either of the following:"*
Item 3.0.1	*a. IaaS - AWS, Azure, GCP*	*"a. IaaS - AWS, Azure or GCP"*
Item 3.0.2	*b. SaaS - AWS, Azure, M365, GCP, Google Workspace, Zoom, Box, Dropbox*	*"b. SaaS – such as AWS, Azure, M365, GCP, Google Workspace, Zoom, Box, and Dropbox is preferred but not required"*
Item 3.0.3	*c. Email - Office 365, Gmail, Exchange*	*"c. Email – such as Office 365, Gmail, Exchange is preferred but not required"*
Item 3.0.6	*f. containers*	*"f. containers are preferred but not required."*
Item 3.0.7	*g. Off VPN Mobile Workforce*	*"g. Off VPN Mobile Workforce or on-premises assets"*
Item 3.4	*A cloud-based Master appliance will be deployed in either AWS or Azure environment in Southeast Asia Region.*	*"A cloud-based Master appliance that can be deployed in any on-premises equipment or public cloud environment located in the country"*
Item 3.5	*Cloud Master appliance must support the analysis of 300 IP devices (license for 300 IP devices)*	*"Cloud Master appliance must support 3GB Traffic Throughput without any restriction on the number of endpoints"*
Item 3.6.4	*Virtual Appliances capturing the span traffic from the virtual environment must support 7 VMWare Physical Host, hosting 37 VM Servers.*	*"Virtual or physical appliance capturing the span traffic from the virtual environment must support 7 VMWare Physical Host, hosting 37 VM Servers via network switches"*
4. Services **Item 4.1.2**	*Fully triaged alerts must be encrypted using a shared secret key and emailed to a named distribution list within the organization. The alert should be provided with the intelligence ascertained to take immediate action.*	*"Alerts must be communicated to a named distribution list through the following: instant messaging, Phone, and Email. The notification should include results of analysis, proof of event (IoCs) as well as recommendation for remediation."*

Attached is the revised Terms of Reference.

For your guidance.

Makati City, 13 December 2023.

ASG SHARON E. MILLAN-DECANO
Chairperson

SSS AILEEN E. DALWATAN
Vice Chairperson

SSS CHERYL ANGELINE M. ROQUE-JAVIER
Member

SSII LEANNE MAUREEN S. APOLINAR
Member

ASIII ALANNA GAYLE ASHLEY B. KHIO
Member

ASIII EMILE JUSTIN D. CEBRIAN
Member

DIR. BERNADETTE M. LIM
Member