Republic of the Philippines
Office of the Solicitor General
134 Amorsolo St. Legaspi Village, Makati City

Technical Working Group for
Information and Communications Technology

please Gla,
for appropriate
action
11/14/23

TERMS OF REFERENCE

Supply and Delivery of Third-Party Risk Management Solution

Background:

In an increasingly interconnected and digital business environment, the reliance on third-party vendors, suppliers, and service providers has become integral to the operations of modern organizations. These external relationships offer numerous benefits, such as cost efficiencies, specialized expertise, and access to global markets. However, they also introduce a new set of challenges and risks, particularly in the realm of cybersecurity and data protection.

The Case Management Service recognizes the critical importance of effectively managing third-party risks to safeguard our operations, protect sensitive data, and maintain the trust of our stakeholders. As a result, procuring a comprehensive third-party risk management solution has become a strategic imperative for our organization.

Objective:

The primary aim of this procurement initiative is to acquire a third-party risk management solution to enhance our cybersecurity posture and protect our digital assets, data, and infrastructure from evolving cyber threats.

It also aims to improve risk mitigation, compliance requirements, data protection, and operational continuity by addressing security issues detected by the solution. In addition, the said solution can also assist in determining whether our current and future partners adhere to the standards of cyber security principles.

Terms:

1. *Scope*. – Supply and delivery of third-party risk management service.

2. *ABC*. - The Approved Budget for the Contract (ABC) is **One Million and Eight Hundred Thousand Pesos (₱1,800,000.00)**, including all government taxes, charges, and other standard fees.

ICT SUBSCRIPTION			
ITEM	QTY	UNIT COST	TOTAL
10 Slots + 1 Self (Monitoring for Self + up to 10 entities)	1	1,800,000.00	1,800,000.00
		TOTAL	₱ 1,800,000.00

3. *Payment.* - The supplier shall be paid in full, subject to deduction of applicable taxes, upon the issuance by the OSG of the corresponding Certificate of Acceptance. All bid prices shall be considered as fixed prices, and, therefore, not subject to price escalation during contract implementation.

4. *Delivery and Training:*

a. All items should be delivered within 30 days of receipt of the Notice to Proceed.

b. Provide training demonstration covering essential items for correct use and day-to-day administration upon delivery and deployment.

c. Deployment and training demonstration must be done during business hours.

d. Training demonstration must begin upon deployment within ten (10) days of solution delivery and must be coordinated with CMS. The CMS will provide certification for delivery and training completion.

e. Product guides, materials, and documentation should be available online.

5. *Schedule of Payment.* - To guarantee the performance by the winning bidder of its obligations under the contract, it shall post a performance security before the signing of the contract. The performance security shall be in an amount not less than the required percentage of the total contract price in any of the following forms and accordance with the following schedule:

Form of Performance Security	Amount of Performance Security (Not less than the required % of the Total Contract Price)	Statement of Compliance
a) Cash or cashier's/ manager's check issued by a Universal of Commercial Bank.	5%	

b) Bank draft/ guarantee or irrevocable letter of credit issued by a Universal or Commercial Bank; *however,* it shall be confirmed or authenticated by a Universal or Commercial Bank if issued by a foreign bank.	5%	
c) Surety bond callable upon demand issued by a surety or insurance company duly certified by the Insurance Commission as authorized to issue such security.	30%	
TERMS OF PAYMENT		**Statement of Compliance**
Supplier agrees to be paid based on a progressive billing scheme as follows:		
• Within thirty (30) days from completion of the delivery and issuance of the Inspection and Acceptance Report by the OSG and submission of all other required documents - 95% of the contract price. • One (1) year from the issuance of the Inspection and Acceptance Report by the OSG - 5% of the contract price.		

All bid prices shall be considered as fixed prices, and therefore not subject to price escalation during contract implementation.

6. *Qualifications of the Supplier:*

a. The bidder must have completed, within the last three years from the date of submission and receipt of at least one (1) single contract of similar nature amounting to at least fifty percent (50%) of the ABC, or the prospective bidder should have completed at least two (2) similar contracts, and the aggregate contract amounts should be equivalent to at least fifty percent (50%) of the ABC, and the largest of these similar contracts must be equivalent to at least half of the fifty percent (50%) of the ABC as required.

For this purpose, similar contract shall refer to procurement contract of ICT software subscription, and/or other similar contracts.

b. 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, must also submit a certification/document linking the bidder to the manufacturer.

c. During contract implementation, the bidder/supplier must remain an authorized distributor, reseller, or partner to maintain said License Software. Suppose the bidder/supplier cannot maintain its distributor, reseller, or partnership agreement with the Manufacturer/Principal. In that case, this may serve as a ground/reason for terminating its contract with OSG.

7. Applicable provisions of the Government Procurement Reform Act (RA No. 9184) and its Revised Implementing Rules and Regulations (RIRR) shall form part of the Terms of Reference.

Technical Specifications:

ITEM	SPECIFICATIONS	COMPLIANCE
Specific Requirements for Third-Party Risk Management Service		
Warranty and After-Sales Requirements	- 1-Year Warranty - To assure that manufacturing defects shall be corrected by the Supplier, a warranty shall be required from the Supplier as provided under Section 62.1 of the 2016 revised IRR of RA No. 9184. - The Procuring Entity shall promptly notify the Supplier in writing of any claims arising under this warranty. Upon receipt of such notice, the Supplier shall, repair or replace the defective Goods or parts thereof without cost to the Procuring Entity, pursuant to the Generic Procurement Manual.	
	- Original or downloaded from the internet technical brochure/datasheet or other forms of manufacturer's un-amended sales literature, unconditional statements of specification and compliance issued by the manufacturer, samples, independent test data, etc.	
	- The Bidder shall submit: i) Certificate or Distributorship/Dealership Agreement by the Manufacturer with the distributor or dealer; and ii) Certificate or Contract/Dealership Agreement between the distributor/dealer and the bidder.	
	- Certification that the supplier shall issue a Warranty Certificate	
Contract Similar to the Project	- **ICT Subscription** - Completed within **five (5) years** prior to the deadline for the submission and receipt of bids	

10 Slots + 1 Self (Monitoring for Self and Up to 10 Entities)		
ITEM	SPECIFICATIONS	COMPLIANCE
Ratings Evaluation Requirements Criteria		
	The solution should be able to provide security ratings of an organization that is highly accurate	

	and reliable from an outside in security perspective. The ratings should be created and updated automatically through software automation. The ratings should be shown as scores and be updated daily as new security issues are detected.	
	The scores should have a published algorithm and have a direct correlation to possible cyber breaches/risks. There should be a documented whitepaper with 3rd party validation on the scoring methodology.	
	The solutions' ratings/scores should publish its scoring methodology and algorithm publicly so that organizations can understand how they are being scored by the solution and validate the scores appropriately for the organization's remediation actions.	
	The solution should be widely adopted and in use by existing suppliers. Organizations should be able to see which suppliers are actively engaged and not engaged in the platform.	
	The solution should be easy to use and navigate so that all our stakeholders, technical or non-technical, can use it without formal training. However, formal training and Executive Briefings should be provided as part of standard customer service.	
	The solution should be able to fill multiple use cases of Cyber Reputation Management, Merger & Acquisitions, Vendor Due Diligence, Regulatory/Compliance, Vendor Risk Management, and Executive Level Reporting.	
	The solution should be able to provide a company tree of all subsidiaries and provide independent scoring for each of the subsidiaries. The score should be available to view without consuming additional licenses.	
Response Time of Solution and Ease to Scale		
	The solution should be able to rate and monitor your entire global supply chain. Both small, large and new companies should already be in the ratings platform to derive meaningful timely value.	
	In the event there is an unscored organization in the ratings platform, the solution should rapidly be able to produce a new rating under 20 minutes.	
	The solution should have the ability to be flexible in its licensing model. The ability to monitor and un-monitor organizations at will allowing the customer to bring organizations in and out of the platform without adversely impacting their licensing.	

	The solution should provide both risk matrix categorization and the ability to put vendors into different folders.	
Ratings/Scores Features		
	The solution's data should be presented in a manner that is easy to review and drill specifically into the data.	
	The solution's scoring should update its score daily as new security issues are detected by the ratings solution. New security issues detected should be visible and prioritized in the platform daily.	
	The solution should be able to generate an improvement plan on how to mitigate risk and improve the rating. The score improvement plan should clearly show the forecasted change when the specific issues are resolved.	
	The solution should be capable on describing a security issue, when it detects one. It should provide information on why it's a risk and what the recommendations are to fix the risk. The solution should also disclose the full IP details and a timestamp of when this issue was last observed.	
	The solution should be capable on looking at an organization's digital assets. It should be easily able to see all the IPs that belongs to an organization. Full IP details should be disclosed with sources for attribution.	
	The solution should also have an interface in the platform to self-correct the digital footprint in the event the IP attribution is incorrect. An interface should allow an organization to self-correct its digital footprint by requesting IPs to be added or removed.	
	The solution should be capable to create a customized rating or scorecard specifically targeting a part/subsidiary/department of a large organization by using filters such as IP ranges, domains, sub-domains and geographic location.	
	The solution should provide a compliance mapping to conduct a gap analysis of commonly used frameworks such as CMMC, GDPR, HIPPA, ISO 27001, NIST, NERC, NYDFS, PCI, SIG (Core, Full, Lite).	
	The Solution should have map external findings back to SIG (Core, Full, Lite).	
	The solution should have the ability to upload a custom assessment and map its external findings to the related issue.	
	The solution should allow for vendor detection of 4th parties.	

	The solution should have configurable alerts & notifications. Alerts should be configurable based on score change, risk factor change, new issues being detected, and new breaches being detected, etc. Notifications should be configurable to alert individuals or teams.	
Remediation of Issues Features		
	When fixing a detected security issue, the solution should provide an interface for submitting the items that have been fixed for review to the ratings provider. When submitting the item for review, there should be notification sent back to the submitter for tracking purposes.	
	During the remediation process, the submitter should receive an email confirmation if the issues have been resolved or declined. The solution should provide a dashboard showing all vendor invitations (accepted, declined) and the vendor is actively working through the issues.	
	The Solution should update within 72 hours after the remediation activity occurs.	
	When contesting false positive, the solution should provide an interface for submitting detected security issues that are believed to be false positives. If false positives do occur and are accepted by the ratings provider, they should be removed from the card within 72 hours.	
	Must include product training and demonstration on deployment, configuration, administration, maintenance, and basic troubleshooting	
Generation of Reports		
	The solution should provide a variety of reports on a company's security posture, including summary reports (simplified view) and detailed reports (all detected security issues with full IP details).	
	The solution should allow for side-by-side comparison reporting of various organizations while providing performance trends overtime.	
	The solution should provide board friendly reports for average supply scores, monitored organizations, engaged organizations, risk remediation performance & findings, and breaches for your own organization and your vendors.	
	The solution should provide board friendly reports for average supply scores, monitored organizations, engaged organizations, risk remediation performance & findings, and breaches for your own organization and your vendors.	
Inviting other Vendors/Suppliers/Organizations Features		

	The solution should allow for access on visibility to a vendor, supplier or other organizations. The invited organization should have the same full access capability.	
	The solution should provide a dashboard to track invited vendors/supplier/organization that have accepted the invitation and are remediating security issues.	
	The solution should have visibility into remediation activities being conducted by 3rd party vendors/suppliers/organizations.	
	When inviting a vendor/supplier/organization, a designated contact should be provided in the situation that vendor is active is using the same platform.	
Integration of 3rd party tools (SIEM, RMM, PSA, etc)		
	The solution should provide an extensive Marketplace for Integrations, API and Developer Hubs.	
	The library to integrate with a SIEM, Ticketing Systems, Productivity Systems and GRC Solutions.	
	The API should allow for building a custom integration, if necessary, with access to a well-documented API with code examples in multiple languages such as Python and JavaScript.	
	The platform should have a named customer success manager assigned to the customer. The customer success manager is responsible for onboarding your team, leading the development of your customer success plan, schedule regular cadence of status meetings (and working sessions as needed), working as an extension of your team to onboard vendors, validation of your IP footprint, coordinate roadmap reviews and provide your feedback on product enhancement to the product team as part of the license fee.	
	The service should offer an Executive Business Review on a regular basis to remain on track with company goals and objectives.	
Licensing		
	The solution should stay have continuous monitoring license that always provides deep level access and remediation.	
	There should be no alterations or variations of the term continuous monitoring.	
	The solution should have the ability to swap monitored companies when it is no longer applicable to continuously monitor.	
Questionnaire Capabilities		

	The solution should provide an integrated questionnaire management solution for 3rd party risk assessment questionnaires.	
	The solution should have the ability to map detected vulnerabilities and finding back to pre-built and custom questionnaires.	
	The solution should have the ability to map detected vulnerabilities and finding back to pre-built and custom questionnaires.	

Technical Working Group for ICT Subscriptions

DIR IV EDUARDO ALEJANDRO O. SANTOS

DIR IV EDITHA R. BUENDIA

SS II OMAR T. GABRIELES

ITO II CEDRIC S. DELA CRUZ

SAO JOY Y. CHUA

CMT III JESUS NINO CHUA

AO IV RAY CHARLIE V. ALEGRE

Approved/Disapproved:

MENARDO I. GUEVARRA
Solicitor General

Certified Funds Available:

BERNADETTE M. LIM
Dir IV - FMS