CREDIT INFORMATION CORPORATION
6F Exchange Corner Building
107 V. A. Rufino Street corner Esteban St.,
Legaspi Village, Makati City 1229
(02) 8236-5900 | www.creditinfo.gov.ph

Bids and Awards Committee

SUBJECT : **Bid Bulletin No. 1**

PROJECT No. : **2021-CIMS(015)-PB-036**

PROJECT : **Renewal of Managed Security Services**

DATE : **September 20, 2021**

This Bid Bulletin is hereby issued for the information and guidance of all prospective bidders. It shall form an integral part of the bidding documents issued earlier relative to above project.

1. Section I. Invitation to Bid

Provision	Original Provision	Provision, as amended
Item 9, page 9	**"**Bid opening shall be on *September 27, 2021; 1:00 P.M.* at Credit Information Corporation,6F Exchange Corner Building, 107 V.A. Rufino Street corner Esteban St. Legaspi Village, Makati City and through video conferencing or webcasting via *Webex Meeting.* Bids will be opened inthe presence of the bidders' representatives who choose to attend the activity. Bidders may witness the opening of the bids via Webex meeting or in person. One (1) representative per bidder will be allowed entry to the venue provided. …"	**"**Bid opening shall be on *September 27, 2021; 1:00 P.M.* at Credit Information Corporation,6FExchange Corner Building, 107 V.A. Rufino Street corner Esteban St. Legaspi Village, Makati City and through video conferencing or webcasting via *Webex Meeting* ***or Zoom Meeting***. Bids will be opened in the presence of the bidders' representatives who choose to attend the activity. Bidders may witness the opening of the bids via *Webex Meeting* ***or Zoom meeting*** or in person. One (1) representative per bidder will be allowed entry to the venue provided. …"

2. Section VII. Technical Specifications

Provision	Original Provision	Provision, as amended
Item 6.2. Technical Requirements, Item 2. Security Monitoring, Item (a.2) Log Sources, page 38	"… 2. Log sources includes: 1) Firewall/IDS 2) Network monitoring solutions 3) End-Point protection management server 4) Active Directory Servers 5) Web Application Server logs 6) Database Audit vault and DB Firewall logs …"	"… 2. Log sources includes: 1) Firewall/IDS ***= 6*** 2) Network Monitoring Solutions = ***1 (Network Security Logging, Analysis, and Reporting), 8 Switches, 3 PAM, 3 DLP, 1 WAF/CDN*** 3) End-Point Protection Management Servers ***= 3*** 4) Active Directory Servers ***= 7*** 5) Web Application Server logs ***= 14, 1 GSuite*** 6) Database Audit Vault and DB Firewall Logs ***= 2, 1 DB in DR Site*** …"

3. Attached as **Annex "C**" is the list of clarified issues raised by prospective bidders.

All other provisions not herein modified shall remain in full force and effect.

For your information and guidance.

Digitally signed
by Bautista Maria
Bernadette Bilbao

MARIA BERNADETTE B. BAUTISTA
BAC Chairperson

ANNEX C

CLARIFIED ISSUES

Provision	Query/ Clarification/ Request	Response
Section VII, Technical Specifications, Item 6.2. Technical Requirements, Item 2. Security Monitoring, Item (a.2)	Can the bidder request for a full inventory or complete list of the actual log sources that will be included during the onboarding including its quantity?	Refer to Bid Bulletin No. 1
Section VII. Technical Specifications, Item 6.2. Technical Requirements, Item 2. Security Monitoring, Item (a.2)	What is the total number of endpoints covered by the requirement?	140 Endpoints
Section VII. Technical Specifications, Item 6.2. Technical Requirements, Item 1. Service Provider Capability, Item (i)	Is the Service Provider's platform should be industry recognized limited to only Gartner and Forrester?	Only these two (2) research companies will be considered.
Section I. Invitation to Bid, Item Nos. 7 and 9	requests for an extension of submission for this bid	Submission and opening of bids shall proceed as scheduled.
1. Service Provider Capability d) The Service Provider should support any SIEM and should be platform agnostic.	Will the Service provider install/setup a new SIEM or CIC has an existing SIEM and this will be used by the Service Provider?	The SP should use their own or adopt the Solution used by the existing provider.
	If the Service provider will use the existing SIEM of CIC, will the service provider be allowed to assess the reliability and integrity of the existing SIEM?	The SP should use their own or adopt the Solution used by the existing provider.
	If the Service provider will use the existing SIEM of CIC, will then the license, warranty and support be the responsibility of CIC to ensure it is valid for the duration of the Service Provider contract?	License will be part of the contract agreement.
	If the service provider will use the existing SIEM of CIC, will then in the event of increase in storage capacity of the Log collector and Database of the SIEM be the responsibility of CIC?	This will be part of the contract agreement that must be considered and evaluated by the SP in their cost proposal.
2. Security Monitoring a) Log collection and transport 9. The Service Provider should have financial sector professionals to support monitoring of IT	What is Financial Sector Professional? Please expound	These are Security Analysts that have background supporting SOC operations in Financial Sector.

enabled controls for monitoring.		
2. Security Monitoring b) Monitoring, correlation and classification of security events 1. The Service Provider shall monitor system logs, security events, vulnerability data, host network intrusions and file integrity data.	Does CIC have a host network intrusion system? if NONE, Will the MSSP include the Host Network Intrusion system as part of its Service?	Network IPS is provided by CIC's Managed Firewall Service Provider. Host IPS is part of EndPoint Protection Solution, which are registered as log sources.
	Does CIC have a File integrity system? If NONE, will the MSSP include the File Integrity System as part of its Service?	The MSSP should provide a file integrity system.
	Does CIC have an existing firewall and endpoint protection solution?	Fortinet & Symantec EndPoint
	How many assets to monitor (firewall, end points, applications, servers)?	Refer to Bid Bulletin No. 1
5. Privileged Access Management a) The proposed solution must be deployable on-premise, hybrid, and provided as a cloud offering.	Does this mean that CIC does not currently have a PAM Solutions (Privileged Access Management) and Service Provider is expected to provide the PAM Solutions as part of its Service?	The existing PAM will not be renewed; the SP is required to provide a new PAM solution as part and additional log source of the managed security service.
6. Vulnerability Assessment b) Test web applications against OWASP top 10.	How many web applications to test?	Eleven web applications will be tested.
	How frequent of the test?	The requirement is semi-annual, however, better if the SP is able to perform the VA more frequently.
6. Vulnerability Assessment d) The Service Provider should execute non-disruptive attack-simulation to determine weaknesses of target information	Will penetration testing be needed?	Only VA is being required.
7. Knowledge Transfer b) Develop incident response playbooks and conduct table-top exercises	Does CIC have existing playbooks and INFOSEC policies?	This refers to new incident response to new threats or threats that the CIC CIRT has no playbook yet. CIC has InfoSec policies.