CREDIT INFORMATION CORPORATION
6F Exchange Corner Building
107 V. A. Rufino Street corner Esteban St.,
Legaspi Village, Makati City 1229
(02) 8-236-5900 | www.creditinfo.gov.ph

Bids and Awards Committee

SUBJECT	:	**Bid Bulletin No. 2**
PROJECT No.	:	**2020-CIMS(008)-PB-001**
PROJECT	:	**Procurement of Managed Security Services**
DATE	:	**April 8, 2020**

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.

I. Invitation to Bid, Item No. 2 and 7, on pages 3-4, and Bid Data Sheet ITB Clause 21 on page 36 of the Bidding Documents is hereby amended, to wit:

The deadline of submission and opening of bids is on ***May 6, 2020, 2:30 P.M.***;

II. Bid Data Sheet, ITB Clause 5.4, paragraph 2 on page 34 of the Bidding Documents is hereby clarified to wit:

For this purpose, similar contracts shall refer to any contracts involving Managed Security Services or ***Managed Services specific to security***.

III. Section VII. Technical Specifications on pages 62-67 of the Bidding Documents is hereby amended in the attached Annex A of this Bid Bulletin.

.

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

For your information and guidance.

Signed

MILCAH CAPUNDAG

BAC Chairperson

Annex A

Detailed Technical Specifications

Item No.	TERMS	Statement of Compliance ("Comply" or "Not Comply")	Proof of Compliance
SECTION 1: SERVICE PROVIDER CAPABILITY			
1.1	24x7 Security Operations and Response;		
1.2	Manage own local or global Security Operation Center (SOC);		
1.3	SOC is housed in a data center grade facility compliant (certified) to industry best practices such as:		
1.3.1	ISO 27001:2013 Information Security Management System (ISMS)		
~~1.3.2~~	Deleted: ~~ISO 22301:2012 Business Continuity Management System (BCMS)~~	-	-
1.3.2	Other Information Security Certifications		
1.4	The Service Provider should have DR for the primary SOC.		
1.5	Assign a service delivery manager to CIC as point of contact of the project;		
1.5.1	Deliver manager must have one or more of the following CISSP, CISM, ITIL-F, PMP, and Prince2;		
1.5.2	Service Delivery Manager must have more than three (3) years experience as service delivery manager.		
1.6	Must assign at least one (1) dedicated security analyst to monitor CIC account;		
1.6.1	Security analysts must have one or more of the following CEH, CISSP, GCIH, ITIL-F, or any equivalent security certifications.		
1.7	The Service Provider should have more than 5 years experience in providing managed security services.		
1.8	The service provider should support any SIEM and should be platform agnostic		
1.9	Service provider should have Cyber Security Advisory services to enable consultative support during monitoring;		
1.10	Service provider must have a security operations center for local monitoring and local team for incident response;		

1.11	If the service of non-local incident responders will be necessary, the service provider shall shoulder their expenses;		
SECTION 2: SECURITY MONITORING			
2.1	**Log collection and transport**		
2.1.1	The service provider shall collect and store log data from different sources in the CIC network;		
2.1.2	The service provider must ingest logs from the following CIC devices/log-sources: 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.		
2.1.3	The service provider shall assist in the setup and configuration of existing log management and correlation facility to achieve Service Level Agreement;		
2.1.4	The service provider shall design and setup secure connectivity from CIC to service provider's Security Operation Center (SOC) for log transfer;		
2.1.5	The service provider must be able to capture real-time log data from monitored hosts and devices in the CIC infrastructure;		
2.1.6	The service provider must ensure security of captured data from disclosure to dis-interested parties;		
2.1.7	The service provider must ensure availability of online log and events up to three (3) months within their facility ;		
2.1.8	The service provider must ensure availability of offline log and events up to twelve (12) months within their facility;		
2.1.9	Support for logging and monitoring of business applications.		
2.1.10	The service provider should have financial sector professionals to support monitoring of IT enabled controls for monitoring.		
2.2	**Monitoring, correlation and classification of security events:**		
2.2.1	The service provider shall monitor system logs and security events;		
2.2.2	The service provider shall ensure logging facility receives needed data to achieve agreed service levels;		
2.2.3	The service provider shall apply correlation and classification policies to SEIM facility;		
2.2.4	The service provider using captured data and policies shall correlate and classify security events;		

2.2.5	The service provider shall likewise ensure the confidentiality of security events;		
2.2.6	The service provider shall ensure access to these correlated and classified events to CIC security team;		
2.2.7	The service provider should support compliance to ISO 27001, Data Privacy Act and/or BSP c982 requirements.		
2.3	**Incident Notification:**		
2.3.1	The service provider shall rate the risks of security incidents and provide notification to the CIC via SMS, Email, or Phone;		
2.3.2	The service provider shall provide expert assessment (technical deep dive) of security incidents to CIC;		
2.3.3	The service provider shall create a ticket of each security incident in CIC's help-desk system for appropriate action by the CIC;		
2.3.4	The service provider shall also alert CIC's nominated point of contact as security incidents are detected.		
2.3.5	The service provider shall rate security incidents based on or similar to the following risk rating matrix: Urgency/Impact High Med. Low Very Low < 2 Hrs P1 P2 P2 P3 2-12 Hrs P2 P2 P3 P4 12-24 Hrs P2 P3 P3 P4 > 24 Hrs P3 P3 P4 P4 Impact: Severity of the security incident to CIC's critical assets; Urgency: How soon the security incident must be addressed;		
2.3.6	Change requests (Time to complete an approved written change request from CIC; excludes CIC controlled activities): 5 Business Days		
2.3.7	Incident Rating Time (Time to rate a Security Incident): < 60 Minutes		
2.3.8	Method to notify CIC of P1 Security Incidents: SMS plus Phone call		
2.3.9	Method to notify CIC of P2 Security Incidents: SMS or Email		
2.3.10	Method to notify CIC of P3 Security Incidents: Email		
2.3.11	Method to notify CIC of P4 Security Incidents: Email		
2.3.12	Time agreed to report a P1 Security Incident: 15 Minutes		
2.3.13	Time agreed to report a P2 Security Incident: 30 Minutes		

2.3.14	Time agreed to report a P3 Security Incident: NA		
2.3.15	Time agreed to report a P4 Security Incident: NA		
2.3.16	Monthly monitoring service management and preparation of monthly service reports		
SECTION 3: THREAT DETECTION			
3.01	Full 24x7 threat monitoring by skilled security analysts, including targeted threat hunting to validate potential threats or validate spread across the network;		
3.02	Proactive threat hunting as needed to validate zero-day threats and to understand the breadth and depth of an attack;		
3.03	Detailed, in-depth understanding of the attack, providing with actionable insights about where the attacker went, what they did and how many devices where affected;		
3.04	Disrupts future attacks by an understanding of root cause to address any potential policy gaps;		
3.05	Provides actionable list of hosts affected and best practices advice and assistance with incident response and remediation activities;		
3.06	Provide threat advisory to the CIC on emerging threats in the industry;		
3.07	Submit regular detection reports on a weekly, monthly, and quarterly basis;		
3.08	The service provider's Threat Intelligence Platform (TIP) must have the capability to collect intelligence from multiple sources and automatically enrich the platform; threat intelligence sources must be relevant to CIC's environment, e.g. banking & finance, credit bureau, financial fraud, etc,		
3.09	The platform categorizes intelligence to help perform analytics on threats, recognize tactics, techniques, and procedures (TTPs), and understand relationships through modeling and visualizations;		
3.10	The platform provide action by supporting various integration via Application Program Interfaces (APIs) and email notifications;		
3.11	The platform is actively collaborating with other members of trusted treat intelligence community (provide list).		
3.12	The platform provides integration with log management and security solutions of the CIC;		
3.13	The Service provider should provide vulnerability advisory based on the assets of the CIC.		
3.14	The Service provider should provide monthly threat breafings (presentation) on current global and local cyber security threat.		
SECTION 4: INCIDENT RESPONSE			
4.01	Review of the CIC's Security Incident Response		

	Plan;		
4.04	Provide technical assistance to the CIC CSIRT during breach without additional cost to CIC.		
4.05	Provide network/firewall/web application breach response;		
4.06	Identification and cleansing or containment of malicious code, malware, spyware, and system-file hacks;		
4.07	Root cause analysis to identify the intrusion vector and provide mitigating procedures to address network and system vulnerabilities;		
4.08	Identify indicators of compromise and scan network to search for other laterally infected systems;		
4.09	The service provider should provide insider threat investigation if needed;		
4.10	The service provider should provide employee misconduct investigations if needed;		
4.11	The service provider should provide incident and investigation reports;		
4.12	The service provider should have in-house Cyber security forensic specialist to support advanced investigation. Must be supported by certification or training (recent);		
SECTION 5: VULNERABILITY ASSESSMENT			
5.1	The service provider should conduct semi-annual vulnerability assessment to identify potential threats and vulnerabilities that may be visible from external network;		
5.2	Test web applications againts OWASP top 10;		
5.3	The following public-facing web sites must be covered by the tests. 1) www.creditinfo.gov.ph 2) cisportal.creditinfo.gov.ph 3) ftp.creditinfo.com.ph 4) ftp-test.creditinfo.com.ph 5) online.creditinfo.com.ph 6) online-test.creditinfo.com.ph 7) a2a.creditinfo.com.ph 8) a2a-test.creditinfo.com.ph 9) mk1.creditinfo.com.ph 10) cb1.creditinfo.com.ph 11) mk2.creditinfo.com.ph		
5.4	The service provider should execute non-disruptive attack-simulation to determine weaknesses of target information systems; and		
5.5	The service provider should identify the risk level where CIC is exposed to so that appropriate counter measures can be developed and applied.		
5.6	The service provider must recommend solutions to discovered issues;		

5.7	The service provider must monitor remediation of identified risks;		
SECTION 6: KNOWLEDGE/TECHNOLOGY TRANSFER			
6.1	The service provider should provide training on leading an implementation of an ISMS from an accredited PECB/BSI training providers for a minimum of four participants.		
6.2	Conduct an incident response readiness training or incident response exercises to CIC Cyber Security Incident Response Team (CSIRT);		
6.3	Develop incident response playbooks and conduct table-top exercises on the following: 1. Widespread malware incident 2. Data breach of CIS 3. Phishing attacks 4. Web defacement 5. Ransomeware incident		