



*Bids and Awards Committee*

**RESPONSE TO CLARIFICATIONS FOR INFORMATION OF ALL PROSPECTIVE BIDDERS**

Project No.: **2022-CIMS(021)-PB-0041**

Project Title: **Procurement of Managed Security Services**


<b>Provision</b>	<b>Query/ Clarification/ Request</b>	<b>Response</b>
Section VII. Technical Specifications	Kindly provide estimated EPS needed for approx. 50 devices.	An average of 82.43 EPS daily with a peak of 130.79 EPS.
Section VII. Technical Specifications	May we request to please help to provide list of your IT Devices, Application & Security devices.	See <b>Annex A</b> for the list of the security, network and application devices.
Technical Document and Section VII. Technical Specifications	Under Service Provider: a) Duly notarized statement that the Service Provider has been in business of providing Managed Security Services for at least five (5) years prior to the deadline for the submission of bids.	
	a) IF JVA, will you consider different years of Service? (ICS more than 5yrs in the Service + JVA Partner 3yrs in Services)	We refer you to Sec. 23 of the IRR of RA 9184.  The submission of technical and financial eligibility documents by any of the joint venture partners constitutes compliance: Provided, that the partner responsible to submit the NFCC shall likewise submit the Statement of all of its ongoing contracts and Audited Financial Statements
	b) Can we request to lower the number of years can we make it at least 1 year in offering Managed Services.	We value the Service Provider experience on providing this service. Hence what is in the terms will be our baseline
Section VII. Technical Specifications	Under Service Provider: b-2) Other Information Security Certifications  What are the other Information Security Certifications do you consider? Please Specify	ISO 22301:2012 Business Continuity Management System (BCMS), PCI DSS, Cyber Essentials

Provision	Query/ Clarification/ Request	Response
Section VII. Technical Specifications	Security Analyst a) Alongside with the 24/7 SOC Analysts, the Service Provider shall assign at least two (2) Security Analysts to the CIC project to monitor CIC account and must be engaged during onboarding and incident response activities. They must be permanent employees of the Service Provider for at least one and half (1 1/2) years. (Provide Cert. of Employment, updated curriculum vitae & related certifications).  For Clarification, SOC 3(Personnel) Analyst?	Two security analysts must be assigned and be available to monitor CIC events (24x7)
Section VII. Technical Specifications	Incident Response k) The Service Provider should have in-house Cyber security forensic specialist to support advanced investigation. Must be supported by certification or training (recent).  What are the certification accepted by CIC?	Please refer to this document: <a href="https://public.cyber.mil/cw/cwmp/dod-approved-8570-baseline-certifications">https://public.cyber.mil/cw/cwmp/dod-approved-8570-baseline-certifications</a>
Section VII. Technical Specifications	Knowledge/Technology Transfer c) Computer Based Training in Information Security for two (2) personnel and Information Security Management training from ISACA for one (1) personnel.  For Confirmation, Is this purely training only, No certification needed?	Training and Certification to validate personnel capability after training interventions.
Eligibility Requirements	For the SLCC requirements, will you consider Security related project?	Projects relating to information security projects (e.g. managed firewall, Vulnerability Management, Digital Forensics, etc.) as managed service and supported by helpdesk service

Please note that the provisions of the Bidding Documents are not modified and shall remain in full force and effect. This is NOT a Supplemental/Bid Bulletin

Very truly yours,

FOR THE BIDS AND AWARDS COMMITTEE

  
**MARIA LOURDES L. RIFAREAL**  
 BAC Chairperson

## ANNEX A

<b>1. Security Devices</b>				
<b>No.</b>	<b>Device</b>	<b>Brand</b>	<b>Device</b>	<b>Number of Devices</b>
1	Firewall	Fortinet / WAF / Database Firewall		8
2	IDS/IPS	Fortinet		
3	VPN devices	Fortinet		
4	Anti-Virus	Symantec		2
5	Proxy			
6	Remote Access Server			
7	NAC			
<b>2. Network, Servers &amp; Other Devices</b>				
<b>No.</b>	<b>Device</b>	<b>Brand</b>	<b>Device</b>	<b>Number of Devices</b>
1	Routers			
2	Switches	Fortinet/HP/Meraki		8
3	AD/ DC			7
4	Critical Servers		PAM/DLP	2
5	Desktops			100
6	Other Devices		Audit Vault / Access Points / Analyzer	4
<b>3. Applications</b>				
<b>No.</b>	<b>Device</b>	<b>Name of Application</b>	<b>Operating System</b>	<b>Number of Servers</b>
1	Authentication Server		Microsoft	7
2	Messaging	Google		1
3	Database Server	Oracle		3
4	Web Server		Microsoft	4
5	Network Management			
6	ERP			
7	Custom Application			
8	Web Applications		Microsoft	3
9	Email Gateway		Linux	1