REQUEST FOR QUOTATION

Republic of the Philippines
SOCIAL SECURITY SYSTEM
East Avenue, Diliman, Quezon City

2021-0006

SEALED QUOTATION FORM

January 22, 2021
Date

PHILGEPS REF. NO. : 7427335
DATE POSTED : 01-23-21
POSTED BY : ERIKA

Sir / Madam:

Please furnish us with your quotation on or before **January 27, 2021 @ 10:00AM** for the following items:

No.	QTY	PARTICULARS	Unit Cost	Total Cost
1	3 Years	**Subscription of Secure Socket Layer (SSL) Certificates with the following requirements:** A. Subscription for Website Security On-line Services - Extended Validation (EV) Secure Sockets Layer (SSL) Certificates for Five (5) named Domains B. Subscription for Website Security On-line Services - Organization Validated (OV) Wildcard Secure Sockets Layer (SSL) Certificates C. Subscription for Website Security On-line Services - Intranet Secure Sockets Layer (SSL) Certificates ***(Please accomplish the attached Terms of Reference-Statement of Compliance)*** **TOTAL ABC = ₱ 700,000.00** PMO – Memo dated 01/22/2021 received by PPMD on 01/22/2021 with Request # 2021-0015 APP FY 2021, #3 January (1st Update) - Secure Socket Layer (SSL) Subscription with 3-year validity		₱_____

Delivery Terms: **Five (5) Calendar Days from receipt of approved Job Order / Purchase Order.**

Payment Terms: **Government Terms (Payment is upon delivery of items / services & submission of billing documents)**

Price validity : **Three (3) Months**

NOTE/S: 1.) **For canvass with an ABC of P 100,000.00 and above**, the winning bidder is required to post a Performance Bond from receipt of Notice of Award equivalent to 5% Cash (Goods & Consulting Services) & 10% Cash (Infrastructure), Cashier's / Manager's Check, Bank Guarantee / Draft or 30% Surety Bond callable upon demand, of the contract price.

2.) Supplier is required to indicate his PhilGeps Registration Number on the canvass form.

3.) SSS shall withhold the applicable taxes from the amount payable in accordance with the BIR regulations.

4.) Alternative offer is not allowed.

5.) Quantity is subject to change but not to exceed of the approved PO/JO

6.) For further clarifications, you may contact Mr. Noel Manalo or Ms. Jennifer Barot / PMO at 8920-6401 local 5581 / 5584 or email at manalong@sss.gov.ph / barotjm@sss.gov.ph.

7.) Please submit the accomplished Request for Quotation (RFQ) Form before the closing date at PPMD 2nd flr. SSS Main Bldg., East Ave., Quezon City.Submit in Sealed Envelope address to Ms. VIOLETA V. JAVAR – Acting Head, Procurement Planning & Management Department and indicate the RFQ Form number, company name, name of company representative, business address and contact details.

This is to certify that my Company is updated in the payment of contributions and loans to SSS, and conformed with the above terms & conditions, and the data / quotation indicated are valid.

_____
Owner/Company Representative
(Sign over Printed Name)

Reminder : Price quotation should be made with extra care taking into account the specification and unit of quantity to avoid errors. The offeror binds himself to this quotation.

Please indicate below your Business Name, Address and Telephone Number and Date Received.
Your Business SSS No. _____
PhilGeps Registration No. _____
T I N no. _____
Date Received : _____
_____
(Business Name)
_____
(Address & Telephone No.)
_____
(E-mail Address)

Very Truly Yours,

VIOLETA V. JAVAR
Acting Head
Procurement Planning & Management Department
Tel No. 8920-6401 loc 5504-5507/5549
Fax No. 7435-9861
E-mail Address: bansilea@sss.gov.ph; ppmd@sss.gov.ph

/ccm/

TERMS OF REFERENCE

Secure Socket Layer (SSL)

ITEM	SPECIFICATION	STATEMENT OF COMPLIANCE
A. Subscription for Website Security On-Line Services - Extended Validation (EV) Secure Sockets Layer (SSL) Certificates for Five (5) named Domains		
1.	**Technical Specifications**	
1.1.	**General specifications**	
1.1.1	Must have a signature algorithm strength of SHA-256 with ECC option	
1.1.2	Trust Level should be Extended Validation	
1.1.3	Must have an encryption strength of 2048	
1.1.4	Must support Cryptographic protocol version of TLS 1.2	
1.1.5	Must be able to provide security for both www.domain.com and domain.com (without the www)	
1.1.6	Must support HTTPS with padlock display on browsers	
1.1.7	Must provide for Certificates that supports SAN options	
1.1.8	Must be able to perform secured Browser to Server and Server to Server authentication	
1.1.9	Allow display of verified Domain Name and Organization Name on certificate	
1.1.10	Support unlimited SSL server licensing within certificate validity period	
1.1.11	Must provide Three (3)-Year Subscription Plan	
1.1.12	Must provide 13-month validity certificate per year	
1.1.13	Must have an issuance speed of One (1) – Five (5) calendar days	
1.1.14	Must allow unlimited re-issuance of certificate/s for different / replacements servers	
1.1.15	Must provide for clickable secure site seal	
1.1.16	Must support activation of Green Address Bar and Organization Name should be displayed in the Browser	
1.1.17	Must have Root certificate that is readily available on all major browsers	

ITEM	SPECIFICATION	STATEMENT OF COMPLIANCE
1.1.18	Must have a Free Certificate Inventory Tool (CIT) to locate all SSL Certificates on internal and public networks regardless of issuing CA	
1.1.19	Must provide Free SSL and Website Security Checker with evaluation reports	
1.1.20	Must provide free management portal to manage purchased certificate with free feature to set unlimited number of user administrator	
1.1.21	Must be universally compatible with browsers and devices	
1.1.22	Must be able to provide alerts/notifications for expiration of certificates	
1.1.23	Must provide Online support page as reference on how to generate CSR and install certificate	
1.1.24	Must provide free additional thirty (30) calendar days on top of the expiration date of certificate for every renewal	
1.1.25	Underwritten warranty must NOT be lower than US$ 1.5M *(Proof should be submitted)*	
1.2.	**Trust Service Principles and Criteria for Certification Authorities**	
1.2.1.	Certificate Provider should be a Public Certification Authority *(Proof should be submitted)*	
1.2.2.	Certificate Provider should be a member of CA Browser Forum *(Proof should be submitted)*	
2.	**Service Support Requirements**	
2.1.	Must have local technical support team.	
2.2.	Local support should be via phone and email through a ticketing system	
3.	**Maintenance Services Response time**	
3.1.	Must provide the SSS with a hotline contact number for immediate reporting of need for services	
4.	OTHER REQUIREMENTS	
	1) The winning supplier shall provide the following: a. Procedure on Support problem escalation within five (5) calendar days upon receipt of Approved PO/JO	

ITEM	SPECIFICATION	STATEMENT OF COMPLIANCE
B. Subscription for Website Security On-Line Services - Organization Validated (OV) Wildcard Secure Sockets Layer (SSL) Certificates		
1.	**Technical Specifications**	
1.1.	**General specifications**	
1.1.1	Must have a signature algorithm strength of SHA-256 with ECC option	
1.1.2	Trust Level should be Organization Validated	
1.1.3	Must have an encryption strength of 2048	
1.1.4	Must support Cryptographic protocol version of TLS 1.2	
1.1.5	Must be able to provide security for both www.domain.com and domain.com (without the www)	
1.1.6	Must support HTTPS with padlock display on browsers	
1.1.7	Must provide for Certificates that supports SAN options	
1.1.8	Must be able to perform secured Browser to Server and Server to Server authentication	
1.1.9	Allow display of verified Domain Name and Organization Name on certificate	
1.1.10	Support unlimited SSL server licensing within certificate validity period	
1.1.11	Must provide Three (3)-Year Subscription Plan	
1.1.12	Must provide 13-month validity certificate per year	
1.1.13	Must have an issuance speed of One (1) – Five (5) calendar days	
1.1.14	Must allow unlimited re-issuance of certificate/s for different / replacements servers	
1.1.15	Must provide for clickable secure site seal	
1.1.16	Must have Root certificate that is readily available on all major browsers	
1.1.17	Must have a Free Certificate Inventory Tool (CIT) to locate all SSL Certificates on internal and public networks regardless of issuing CA	
1.1.18	Must provide Free SSL and Website Security Checker with evaluation reports	

13

ITEM	SPECIFICATION	STATEMENT OF COMPLIANCE
1.1.19	Must provide free management portal to manage purchased certificate with free feature to set unlimited number of user administrator	
1.1.20	Must be universally compatible with browsers and devices	
1.1.21	Must be able to provide alerts/notifications for expiration of certificates	
1.1.22	Must provide Online support page as reference on how to generate CSR and install certificate	
1.1.23	Must provide free additional thirty (30) calendar days on top of the expiration date of certificate for every renewal	
1.1.24	Underwritten warranty must NOT be lower than US$ 1.5M *(Proof should be submitted)*	
1.2.	**Trust Service Principles and Criteria for Certification Authorities**	
1.2.3.	Certificate Provider should be a Public Certification Authority *(Proof should be submitted)*	
1.2.4.	Certificate Provider should be a member of CA Browser Forum *(Proof should be submitted)*	
2.	**Service Support Requirements**	
2.1.	Must have local technical support team.	
2.2.	Local support should be via phone and email through a ticketing system	
3.	**Maintenance Services Response time**	
3.1.	Must provide the SSS with a hotline contact number for immediate reporting of need for services	
4.	OTHER REQUIREMENTS	
	1) The winning supplier shall provide the following: b. Procedure on Support problem escalation within five (5) calendar days upon receipt of Approved PO/JO	

ITEM	SPECIFICATION	STATEMENT OF COMPLIANCE
C. Subscription for Website Security On-Line Services – Intranet Secure Sockets Layer (SSL) Certificates		
1.	**Technical Specifications**	
1.1.	**General specifications**	
1.1.1	Should be vetted/verified within an Organization Validated Profile	
1.1.2	Browser should display HTTPS with Padlock	
1.1.3	Certificate Validity is 3 Years	
1.1.4	Issuance speed is One (1) – Three (3) calendar days	
1.1.5	Signature algorithm strength is SHA-256	
1.1.6	Certificate should be 2048-bit encryption strength	
1.1.7	Secures internal hostname or private IP address	
1.1.8	Unlimited SSL server licensing within certificate validity period	
1.1.9	Unlimited reissuance to different servers/replacement for the lifetime of the certificate	
1.1.10	Should have a free management portal to manage purchased certificate with free feature to set unlimited number of user administrator	
1.1.11	Should have a Free Certificate Inventory Tool (CIT) to locate all SSL Certificates on internal and public networks regardless of issuing CA	
1.1.12	There should be alerts/notifications for expiration of certificates	
1.1.13	Should have free additional thirty (30) calendar days on top of the expiration date of certificate for every renewal	
1.1.14	Root certificate and Intermediate Certificate should be available	
1.1.15	Online support page should be available for reference on how to generate CSR and install certificate	
1.2.	**Trust Service Principles and Criteria for Certification Authorities**	
1.2.5.	Certificate Provider should be a Public Certification Authority. (A proof should be submitted upon submission of quote)	

15

ITEM	SPECIFICATION	STATEMENT OF COMPLIANCE
1.2.6.	Certificate Provider should be a member of CA Browser Forum. (A proof should be submitted upon submission of quote)	
2.	**Service Support Requirements**	
2.1.	Vendor should have local technical support team	
2.2.	Local support should be via phone and email through a ticketing system	

PREPARED BY:

_____

Signature Over Printed Name
(Authorized Representative)

COMPANY NAME : _____

ADDRESS : _____

CONTACT NUMBER : _____

16