TERMS OF REFERENCE

ONE (1) LOT SECURE SOCKETS LAYER (SSL) CERTIFICATE SERVICES FOR THE GOVERNANCE COMMISSION FOR GOCCs (GCG) COVERING THE PERIOD OF 01 JULY 2021 TO 31 DECEMBER 2021

1. BACKGROUND AND RATIONALE

1.1 Secure Sockets Layer (SSL) protocol is the most popular protocol used in the Internet for facilitating secure communications through authentication, encryption, and decryption. It is a standard technology behind establishing an encrypted connection between a web server (host) and a web browser (client). This connection between the two makes sure that all the data passed between them remain private and intrinsic.

1.2 Moreover, to provide a higher degree of security assurance, server certificates such as Extended Validation (EV) and Organization Validation (OV) are used to increase the website's trust factor and authenticity. EV Certificates and OV Certificates are issued by Certificate Authorities (CA) only after confirming the physical and operational existence of the requesting entity through affirming its legal documents.

1.3 Thus, the Governance Commission for Government Owned or Controlled Corporations (GCG) wants to guarantee that the information being sent over the internet is secure as it passes through multiple computers until it finally reaches the destination server. The SSL certificate will work as an intermediary between GCG servers and the web browsers which transforms sensitive information into an encrypted format so that it can be sent over the internet without the risk of any data breach.

2. TECHNICAL SPECIFICATIONS

2.1 EXTENDED VALIDATION (EV) STANDARD REQUIREMENTS

2.1.1 The bidder must provide three (3) EV SSL certificate and satisfies the minimum requirements and specifications below.

2.1.2 Certificate Specifications:

2.1.2.1 Must have a Trust Level of Extended Validation (EV).

2.1.2.2 Must have an organization name displayed in the web browser.

2.1.2.3 Must have an Underwritten Warranty not be lower than One Million Five Hundred Thousand Dollars Only ($1,500,000.00).

2.1.3 Feature Specifications:

2.1.3.1 Must have a display of HTTPS (Secure Hyper Text Transfer Protocol) with padlock in web browsers.

2.1.3.2 Must have a clickable Secure Site Seal.

2.1.3.3 Must have a verified domain name.

2.1.3.4 Must have an organization name displayed in the certificate.

2.1.3.5 Must support Subject Alternative Name (SAN) options in the certificate.

2.1.3.6 Must have a signature algorithm strength of SHA-256 with Elliptic Curve Cryptography (ECC) option.

2.1.3.7 Must have a 2048-bit encryption strength in the certificate.

2.1.3.8 Must support Transport Layer Security (TLS) version 1.2 in the cryptographic protocol.

2.1.3.9 Must support both www.domain.com and domain.com (without the www).

2.1.3.10 Must have unlimited SSL server licensing within certificate validity period.

2.1.3.11 Must have unlimited reissuance to different servers/replacements.

2.1.3.12 Must support all major web browsers for the root certificate.

2.1.3.13 Must have browser to server and server to server authentication in the certificate.

2.1.3.14 Must have 3-10 calendar days vetting turn-around for organization details.

2.2 ORGANIZATION VALIDATION (OV) WILDCARD REQUIREMENTS

2.2.1 The bidder must provide one (1) OV Wildcard SSL certificate and satisfies the minimum requirements and specifications below.

2.2.2 Certificate Specifications:

2.2.2.1 Must have a Trust Level of Organization Validation (OV).

2.2.2.2 Must have the secure top-level domain name as well as its 1st level sub-domains for the certificate.

2.2.2.3 Must have an Underwritten Warranty not be lower than One Million Two Hundred Fifty Thousand Dollars Only ($1,250,000.00).

2.2.3 Feature Specifications:

2.2.3.1 Must have a display of HTTPS (Secure Hyper Text Transfer Protocol) with padlock in web browsers.

2.2.3.2 Must have a clickable Secure Site Seal.

2.2.3.3 Must have a verified domain name.

2.2.3.4 Must have an organization name displayed in the certificate.

2.2.3.5 Must support Subject Alternative Name (SAN) options in the certificate.

2.2.3.6 Must have a signature algorithm strength of SHA-256 with Elliptic Curve Cryptography (ECC) option.

2.2.3.7 Must have a 2048-bit encryption strength in the certificate.

2.2.3.8 Must support Transport Layer Security (TLS) version 1.2 in the cryptographic protocol.

2.2.3.9 Must support both www.domain.com and domain.com (without the www).

2.2.3.10 Must have unlimited SSL server licensing within certificate validity period.

2.2.3.11 Must have unlimited reissuance to different servers/replacements.

2.2.3.12 Must support all major web browsers for the root certificate.

2.2.3.13 Must have browser to server and server to server authentication in the certificate.

2.2.3.14 Must have 3-10 calendar days vetting turn-around for organization details.

2.3 CERTIFICATE PROVIDER REQUIREMENTS

2.3.1 The certificate provider for the abovementioned EV and OV Wildcard SSL should have the following qualifications below.

2.3.1.1 Must be a Global Pacific Certification Authority.

2.3.1.2 Must be a member of Certification Authority (CA) Browser Forum.

2.3.1.3 Must be a member of Online Trust Alliance.

2.3.1.4 Must have a local technical support team.

3. BUDGET REQUIREMENTS

3.1 The budget for One (1) Lot Secure Sockets Layer (SSL) Certificate Services for GCG covering the period 01 July 2021 to 31 December 2021 is One Hundred Thousand Pesos Only (₱100,000.00).

4. SCOPE OF WORK

The Winning Bidder (hereafter referred to as simply the "bidder") must:

4.1 perform the supply and delivery of the proposed SSL certificates;

4.2 provide comprehensive user manual or guidelines, and assistance for setting-up the proposed SSL certificates;

4.3 provide a management portal for the purchased certificates with a feature to set unlimited number of user administrator;

4.4 provide a Certificate Inventory Tool (CIT) to local all SSL certificates for internal and public networks regardless of the issuing Certificate Authority (CA);

4.5 provide a notification tool for SSL certificate expirations; and

4.6 provide an SSL and website security checker with evaluation reports.

5. TRAINING REQUIREMENTS

5.1 The bidder shall provide in-depth knowledge transfer on installation and management of SSL certificates to be conducted by a designated product expert.

6. SUPPORT AND MAINTENANCE

6.1 The bidder must provide full-time support and managed services as specified:

6.1.1 single point of contact for all concerns on the proposed SSL certificates;

6.1.2 two (2) hour response time upon receipt of call and four (4) hours for onsite support, if applicable; and

6.1.3 service desk support via telephone or email.

6.2 The bidder must provide the procedure on support and issue escalation.

7. CONFIDENTIALITY

7.1 Information or rights acquired and obtained from the GCG, including but not limited to any and all obligations prior to the termination or expiration hereof and provisions on confidentiality and proprietary rights, will remain in effect after termination of the services rendered to the GCG. Hence, the undertaking of the certificate provider not to disclose and to keep information confidential shall subsist even after the expiration or termination of its obligation to the GCG nor can the certificate provider, at any time, disclose items mentioned or enumerated in Section 7.2 or any information it acquires by virtue of the contract which the GCG deems confidential.

7.2 Records, documents, reports and relevant data, such as diagrams, plans, designs, estimates, specifications and other supporting records of materials complied and prepared in the courses of the performance of the services shall be absolute properties of GCG and shall not be used by the certificate provider for purposes not related to this agreement without prior written approval of GCG. Copies of such documents as required in this TOR shall be turned over to GCG upon completion of the project except that the certificate provider shall have the right to retain a copy of the same

8. DELIVERY AND IMPLEMENTATION SCHEDULE

8.1 The delivery of proposed SSL certificates must be completed within thirty (30) calendar days from the receipt of the Notice to Proceed.

8.2 The bidder shall be subjected to the evaluation by the end-user after the implementation of the project.