TERMS OF REFERENCE

PROCUREMENT OF APPLICATION SECURITY TESTING CONSULTANT FOR THE EXISTING GCG APPLICATIONS

1. INTRODUCTION

Since 2013, the Governance Commission for GOCCs (GCG) through its internal IT Team has successfully developed and implemented several web-based applications for organizational process improvements and digital public services. Some of these applications manage the submission of GOCCs' financial and non-financial information, performance evaluation of Appointive Directors and office automation tools such as for document management and resource reservation.

With the goal to provide secured web applications to GCG stakeholders, the Information and Communications Technology Group (ICTG) conducts various testing stages prior deployment to all its internally developed applications. However, with the rapidly evolving cyber-attacks that may pose a threat to the GCG's day-to-day operations, it has become paramount to implement additional layers of security testing protocols such as the Application Security Testing conducted by third-party provider to further increase the security of GCG applications.

Thus, the ICTG finds it best to procure an Application Security Testing Service for the existing or already deployed GCG web-based applications to identify possible loopholes in the code and even to the system architecture, which can be an entry point to any possible cyberattacks.

2. NEED FOR A SERVICE CONTRACT

The requirement to engage the services of an Application Security Testing Service Provider (SP) is due to the non-availability of an in-house expert that can work with the application security requirements of GCG Applications.

2.1 The engagement of an SP aims to meet the following objectives:

2.1.1 To have a better understanding on the potential vulnerabilities and security weaknesses of GCG Applications;

2.1.2 Identify areas within the GCG Applications that are most vulnerable to attacks;

2.1.3 Assess and evaluate the current security controls implemented; and

2.1.4 Detect gaps, inconsistencies, and redundancies in the implemented security controls.

3. EVALUATION CRITERIA

3.1 Technical Proposal – 80%

3.1.1 Applicable Experience of the Consultant – 50%

The Service Provider (SP) must possess the following qualifications:

a. Minimum of three (3) years of cumulative experience in conducting Application Security Testing services. SPs with less than three (3) years of experience shall automatically be disqualified. In addition, SPs

previously engaged by GCG who received unsatisfactory or negative feedback shall also be automatically disqualified; and

b. Successfully completed the same or similar to Application Security Testing services to at least five (5) clients.

3.1.2 Quality of the Personnel to be assigned – 40%

The SP must propose three (3) personnel to conduct the Application Security Testing activities. The proposed personnel must possess the following qualifications:

a. Bachelor's Degree or higher in Computer Engineering, Computer Science, Electrical Engineering, Information Systems, Information Technology, or a closely related Engineering or IT discipline; and

b. The SP must identify one (1) Project Lead and two (2) Application Security Testers. The three (3) proposed personnel must be certified in at least one (1) of the following certifications:

- Certified Information Systems Security Professional (CISSP);
- GIAC Web Application Penetration Tester (GWAPT); and
- Offensive Security Certified Professional (OSCP).

c. The Project Lead must have at least three (3) years of cumulative experience as a Project Lead for projects the same or similar to Application Security Testing services. The SP shall be automatically disqualified if their identified Project Lead has less than three (3) years of experience.

d. Each of the Application Security Testers must have at least two (2) years of cumulative experience as a Tester for projects the same or similar to Application Security Testing services. The SP shall be automatically disqualified if at least one (1) of their identified Application Security Testers has less than two (2) years of experience.

3.1.3 Plan of Approach and Methodology – 10%

The alignment of the bidders' plan of approach and methodology on each of the proposed Application Security Testing activities indicated in 6.1 of the TOR.

3.2 Financial Proposal – 20%

3.2.1 The budget proposal must be less than or equal to the approved budget for the contract of **Seven Hundred Thousand Pesos Only (P 700,000.00).**

4 REQUIRED DOCUMENTS TO BE SUBMITTED

4.1 In addition to the required eligibility documents, as required in Annex "H" for *Small Value Procurement (SVP)* of the Revised Implementing Rules and Regulations (IRR) of the Republic Act (R.A). No 9184, to be submitted, the SP shall also submit the following documents:

4.1.1 Curriculum Vitae[1] and relevant certifications of the three (3) personnel to be assigned.

4.1.2 List of completed government and private contracts similar or related to Application Security Testing projects. The list shall indicate for each contract the following:

a. Name and Address of the client;
b. Name of the contract;
c. Project Start Date; and
d. Project Completion Date.

5 SCOPE OF WORK

5.1 The list of GCG Applications for the project shall be discussed and agreed between the ICTG Project Team and the SP during the Project Kick-Off (Item 6.1.1 of the TOR). Each of the application shall be categorized according to its complexity. The testing period for all targeted applications must total to **SIXTY (60) WORKING DAYS ONLY**.

	COMPLEXITY	TESTING PERIOD (WORKING DAYS)	NO. OF TARGET APPLICATIONS
5.1.1	**Low** ▪ Mostly automated testing with manual validation; ▪ No user authentication; ▪ Static website with less than or equal to five (5) dynamic pages.	Five (5)	Two (2)
5.1.2	**Medium** ▪ Manual and automated testing; ▪ With user authentication; ▪ With two (2) to three (3) user roles; and ▪ Websites with five (5) to ten (10) dynamic pages.	Ten (10)	Two (2)
5.1.3	**High** ▪ Manual testing and validation; ▪ With user authentication; ▪ Websites with more than ten (10) dynamic pages; ▪ With more than three (3) user roles; and ▪ Has complex workflow and transactions.	Fifteen (15)	Two (2)

[1] Please see Annex A - Curriculum Vitae (CV) of the Application Security Testing Resource Personnel

6 SCHEDULE OF ACTIVITIES, TIMELINE, AND PAYMENT SCHEDULE

6.1 Payments shall be made every after completion of each milestones indicated below:

	MILESTONES	ESTIMATED TIMELINE (WORKING DAYS)	PAYMENT SCHEDULE (%)
6.1.1	**Project Kick-Off** 6.1.1.1 Documentation of the Approach and Methodology 6.1.1.2 Proposed Project Team 6.1.1.3 Documentation of the targeted GCG Applications to be tested 6.1.1.4 Proposed Project Timeline based on the targeted GCG Applications	20 working days from the receipt of the NTP	15%
6.1.2	**Application Security Testing** Phase I: Application Profiling 6.1.2.1 Documentation of the components and functionality of the targeted GCG Applications Phase II: Conduct of Application Security Testing 6.1.2.2 Documentation of detailed findings 6.1.2.3 Documentation of recommendations and proposed solutions 6.1.2.3 Documentation of recommendations and proposed solutions	60 working days from the acceptance of Item 6.1.1 of the TOR	70%
6.1.3	**Project Closure and Acceptance** 6.1.3.1 Presentation of the Technical and Executive Summary Report	20 working days from the acceptance of Item 6.1.2 of the TOR	15%

6.2 The Service Provider shall be rated by the end-user after the conduct of the project.

6.3 All required output/deliverables stated above shall be accompanied by working papers, schedules, and database of data or information. Any extension or modification in the deadline of reports shall be made only upon prior written approval of the Head of the Procuring Entity (HoPE).

6.4 All payments shall be subject to existing accounting and auditing rules and regulations applicable to GCG.

6.5 Processing and release of allotted payment schedule per item indicated above shall be made within twenty (20) working days after the acceptance of the submission of complete billing documents along with the approved deliverables.

6.6 GCG adopts the Expanded Modified Direct Payment Scheme (ExMDPS) as mode of payment to creditors/payees as per DBM Circular No. 2013-16. In this line, GCG uses Direct Payment Scheme (DPS) via bank debit system through issuance of List of Due and Demandable Accounts Payable - Authority to Debit Account (LDDAP-ADA) in the settlement of accounts payable due to creditors/payees. Section 5.9.2 of the DBM Circular noted that bank charges shall be borne/paid by the creditor/payee concerned, in this case, by the SERVICE PROVIDER, if their account is not maintained at Landbank.

7 ENGAGEMENT PERIOD

7.1 The GCG shall engage the services of the Application Security Testing Service Provider for an estimated period of one hundred (100) working days. The conduct of the project shall be undertaken during office hours or on a schedule as agreed upon by the parties, subject further to GCG's guidelines. Any amendment/modification of the work schedules shall be made only upon prior written approval of the HoPE, in which case, the engagement shall be correspondingly extended for such period called for by the amendment/modification under the same terms, with no additional cost on the part of GCG.

8 OTHER TERMS AND CONDITIONS

8.1 Any information or document obtained from GCG, including but not limited to 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 Service Provider not to disclose and to keep information confidential shall subsist even after the expiration or termination of its services to the GCG nor can the Service Provider, at any time, disclose that their services were engaged by the GCG for the Application Security Testing Project.

9 PROPRIETARY RIGHTS TO GCG

9.1 Records and other documents, reports, and relevant data, such as diagrams, plans, designs, estimates, specifications, and other supporting records of materials the HoPE compiled and prepared during the performance of the services, shall be exclusively owned by GCG, and shall not be used by the Service Provider for purposes not related to this agreement, without prior written approval of the HoPE.

ANNEX A

CURRICULUM VITAE (CV) OF APPLICATION SECURITY TESTING CONSULTANT

Proposed Position: _____ Name of Firm: _____

Name of Staff: _____ Years with Firm: _____

Profession: _____ Current Position in the Firm: _____

Date of Birth: _____ Nationality: _____ Contact Information: _____

QUALIFICATIONS: *(start from most recent)*

Education

[Summarize college/university and other specialized education, giving names of schools/institutions, dates attended, and degrees/certificates obtained using the matrix below]

School/Institution	Degree/Title	Inclusive Dates

Employment Record

[Starting with present position, list in reverse order every employment held by nominated staff. List all positions since graduation, giving dates, names of employing organizations, titles of positions held, and key responsibility. Indicate relevant work experience of staff in his/her nominated position.]

Position Title	Office and Location	Inclusive Dates	Key Responsibility

Projects Presently Being Undertaken

[Provide outline of projects presently being undertaken using the matrix below]

Project Title with Brief Description	Client	Position	Inclusive Dates	Summary of Duties and Responsibilities

Professional Certification

[Provide an outline of all professional certifications related to Application Security Testing from recognized certifying bodies using the matrix below]

Certificate Obtained	Certifying Body/Provider	Date of Conferment/ Registration	License/Professional Number	Validity Date

Certification:

I, *[full name of proposed professional staff],* certify that to the best of my knowledge and belief, these data correctly describe me, my qualifications, and my experience.

I also commit that I shall work for the project as *[nominated position]* once the firm is awarded the contract.

_____Date: _____
[Signature over printed name of nominated key staff]

_____Date: _____
[Signature over printed name of authorized representative of the firm]

SUBSCRIBED AND SWORN to before me this __ day of [month] [year] at [place of execution], Philippines. Affiant/s is/are personally known to me and was/were identified by me through competent evidence of identity as defined in the 2004 Rules on Notarial Practice (A.M. No. 02-8-13-SC). Affiant/s exhibited to me his/her [insert type of government identification card used], with his/her photograph and signature appearing thereon, with no. _____.

Witness my hand and seal this ___ day of [month] [year].

NAME OF NOTARY PUBLIC
Serial No. of Commission _____
Notary Public for _____ until _____
Roll of Attorneys No. _____
PTR No. __, [date issued], [place issued]
IBP No. __, [date issued], [place issued]
Doc. No. ___
Page No. ___
Book No. ___
Series of ____.