Support Services Sector

Information Security Office

Conduct of Third Party Vulnerability Assessment and Penetration Testing for CY 2020

Terms of Reference

June 2020

TABLE OF CONTENTS

PREPARED BY

Name	Position Title	Date Approved
Lindy Vivien Aldaba	**Officer III**	

REVIEWED AND APPROVED BY:

Name	Position Title	Date Approved
Jonathan C. Pineda	**Vice President & CISO**	

DOCUMENT HISTORY

Version	Primary Author (s)	Description/Changes	Issue Date
1.0	**Lindy Vivien Aldaba**	**1st Draft**	May 27, 2020

APPROVAL PAGE

Conduct of Third Party Vulnerability Assessment and Penetration Testing

Terms of Reference

Support Services Sector
Information Security Office

Prepared by:

Lindy Vivien S. Aldaba
Officer III
Information Security Office

Approved by:

Jonathan C. Pineda
Chief Information Security Officer
Information Security Office

A. BACKGROUND

A.1 PROJECT OVERVIEW/OBJECTIVE

The annual third party service is to check the vulnerabilities of GSIS external-facing systems and to test if these systems may be penetrated.

The service is required to have an independent assessment and conduct of non-destructive tests, giving the GSIS the actual security posture of our external-facing systems from a possible hacker's perspective. This would assist us in prioritizing the security requirements of the GSIS.

A.2 PROJECT SCOPE

The winning bidder must supply and deliver the following at **the GSIS**:

1. Provide external vulnerability and penetration tests for 21 resources/devices, including conduct of Red Team Simulation Attacks.
2. Provide the necessary tools and hardware to deliver the service.
3. To provide documentation, reports and a remediation/action plan to address the vulnerabilities discovered.

B. PROJECT ESTIMATES

B.1 APPROVED BUDGET COST

The ***Government Service Insurance System (GSIS)***, intends to apply the sum of ***Nine Hundred Eighty Eight Thousand Two Hundred Thirty Three Pesos (PhP 988,233.00)*** being the Approved Budget for the Contract (ABC) for the ***Conduct of Third Party Vulnerability Assessment and Penetration Testing for CY 2020.*** Bids received in excess of the ABC shall be automatically rejected at opening of financial proposals.

B.2 SOURCE OF FUNDS

The ABC authorized for the ***Conduct of Third Party Vulnerability Assessment and Penetration Testing*** project shall be sourced from the ***Retainers and Consultancy Fee of the Operating Expense budget of ISO for CY 2020***.

C. GENERAL SCOPE OF WORK/BID REQUIREMENT

The GSIS through ISO must select a bidder through small value procurement for the Conduct of Third Party Vulnerability Assessment and Penetration Testing for CY 2020

C.1 MINIMUM TECHNICAL REQUIREMENTS

1. Approach and methodology to be used shall be aligned to the GSIS' needs. Vendor should consider the business of the organization while planning the testing and vulnerabilities are prioritized in accordance with organization management and feedback. This includes any existing or planned compliances (in house, local regulatory and global).

2. The Plan and Methodology must be duly reviewed and accepted by Information Security Office prior to implementation.

3. Approach and methodology shall be derived from a team experienced in conducting VA and Penetration tests. These shall be based on a globally accepted framework.

4. Reporting shall provide industry based correlation of vulnerabilities.

5. Vendor team shall actively involve GSIS in the conduct of the VA/PT Services and immediately notify GSIS of any critical vulnerability even prior to the actual report issuance.

6. Tests shall be conducted on the production environment; therefore, no destructive tests shall be executed.

7. Penetration testing shall be confined to assessing whether the vulnerability could be exploited and in no circumstance shall the external perimeter be crossed.

8. Protocol sniffing activity shall be conducted to test for passwords sent in clear text over the network.

9. Findings and recommendations shall be kept classified and presented according to severity.

10. Report shall provide remediation suggestions duly prioritized and aligned to GSIS business. These should provide a practical, do-able and effective solution for remediation of the vulnerabilities discovered.

11. Report shall be finalized by the Vendor after validation with the GSIS ISO Team.

12. Based on the findings, the Vendor shall provide references and knowledge for configuration, and infrastructure best practices that will help the GSIS ISO team to be able to incorporate the same in the existing systems and raise the security state of the organization.

13. Follow-up assessments shall be carried out and shall focus on closure of the issues that were discovered.

C.2 IMPLEMENTATION STRATEGY/DEVELOPMENT SCHEDULE

The winning bidder shall complete the project **within seventy five (75) calendar days from the date specified in the Notice to Proceed (NTP).**

Item No	Description	Quantity	Total	Delivered / Completed
1	Pre-Assessment phase to define objectives and to finalize the scope of boundaries.	1	1	Within 15 CDs from receipt of Contract of Small Value Procurement (Purchase Order)
2	Assessment phase that comprises the **Vulnerability Assessment (via Black box and Gray Box Test), Penetration Testing (including Red Team Attack Simulation).** Service provider will have their own tools for tests that would be required to assess system vulnerability.	1	1	45 CDs from item 1
3	Post assessment that covers the reports and presentation of recommendation and action plans. VA/PT Report of the activities carried out and the findings of the Vulnerability Assessment, Penetration Testing. The following minimum details of the report shall	1	1	15 CDs from item 2

	be as follows: ▪ Management summary ▪ Scope of the VA/PT services ▪ Tools that have been used ▪ Dates & times of the actual tests on the systems ▪ Output of tests performed ▪ A list of all validated vulnerabilities with included recommendations on "how to fix" the vulnerabilities found ▪ A list of action points according to recommended priority.			

D. MODE OF PROCUREMENT

The GSIS through ISO shall select a bidder through ***Small Value Procurement*** for the ***Conduct of Third Party Vulnerability Assessment and Penetration Testing for CY 2020.***

E. PROJECT MANAGEMENT METHODOLOGY

The project shall be headed by the Information Security Office (ISO). The plan and methodology must be duly reviewed and accepted by the ISO prior to implementation. Should there be any disagreement ISO shall have the final decision on the matter.

F. PAYMENT SCHEDULE/MILESTONES

1. Full payment shall be made upon complete delivery and issuance of certificate of completion and final acceptance.

2. Payments shall be subject to applicable taxes.

3. The winning bidder must submit the following documents prior to issuance of GSIS of the Certificate of Final Acceptance and processing of payment:

    - VA/PT and Red Teaming Report
    - Certificate of Completion
    - Other documents required in this TOR

G. OTHER CONSIDERATIONS

F.1 ELIGIBILITY OF BIDDERS

1. The bidder shall submit project documentation such as but not limited to the following:

    1.1 VA/PT and Red Teaming Plan
    1.2 VA/PT and Red Teaming Methodology
    1.3 VA/PT and Red Teaming Reports including the following:
        1.3.1 Management summary
        1.3.2 Scope of the VA/PT and Red Teaming services
        1.3.3 Tools that have been used
        1.3.4 Dates & times of the actual tests on the systems
        1.3.5 Output of tests performed

1.3.6 A list of all identified vulnerabilities with included recommendations on "how to fix" the vulnerabilities found

1.3.7 A list of action points according to recommended priority

Failure to include the documents in the bid envelope is a ground for disqualification of the bidder.

2. The bidder must have available, qualified and experienced personnel who will provide services for Conduct of Third Party Vulnerability Assessment and Penetration Testing for CY 2020. **The bidder must include in their bid envelope the proof of compliance on the following requirements:**

2.1 Vendor must have at least five (5) years of experience in conducting VA/PT.

2.2 Vendor must provide an experienced Project Implementation Team.

2.2.1 The Project Manager should have a valid Certification in the field of Security.

2.2.2 The members of the implementation team should be Certified Ethical Hackers or Licensed Penetration Testers and should not have conducted the same service to the GSIS for the last two years.

2.3 Vendor shall have adequate number of qualified resources or a minimum of five (5) team members for onsite and/or remote services for continuous VA/PT Assessments.

2.4 The Project Implementation Team should be assigned up-to-the-end of the project. GSIS reserves the right to interview, approve and change personnel assignment of the Project Implementation Team.

2.5 Resume of the Project team including their certification must be submitted.

3. The bidder must warrant that the services to be delivered are suitable to the requirements stated herein with respect to the quality, capacity and purpose of the project.

4. The bidder must warrant against hidden defects all the deliverables in this project.

5. The winning bidder must warrant the merchantability of the product/service.

F. 2 OTHER RESPONSIBILITIES OF THE BIDDER/SERVICE PROVIDER

1. The bidder/service provider must complete all scheduled deliverables as stated in this document **at GSIS Home Office only**.

2. The bidder/service provider must bear all the expenses in the delivery and completion of the project.

3. The bidder/service provider is expected to conform to GSIS' office rules and regulations.

4. The bidder/service provider shall ensure the absolute confidentiality of all information, documents or records acquired in the course of or as an incident to this Project. It shall not use or disclose to any person, firm, or corporation any information hereto acquired for its benefits or to the detriment of GSIS.

5. The GSIS reserves the right to interview, approve, and change personnel assignment of the winning bidder.