

# **BIDDING DOCUMENTS FOR PENETRATION TESTING AND FORENSIC SOFTWARE**



Republic of the Philippines  
NATIONAL PRIVACY COMMISSION

**July 2021**

# Table of Contents

<b>Glossary of Acronyms, Terms, and Abbreviations .....</b>	<b>3</b>
<b>Section I. Invitation to Bid.....</b>	<b>6</b>
<b>Section II. Instructions to Bidders.....</b>	<b>9</b>
1. Scope of Bid .....	10
2. Funding Information.....	10
3. Bidding Requirements .....	10
4. Corrupt, Fraudulent, Collusive, and Coercive Practices .....	10
5. Eligible Bidders.....	10
6. Origin of Goods .....	11
7. Subcontracts .....	11
8. Pre-Bid Conference .....	11
9. Clarification and Amendment of Bidding Documents .....	11
10. Documents comprising the Bid: Eligibility and Technical Components .....	11
11. Documents comprising the Bid: Financial Component .....	12
12. Bid Prices .....	12
13. Bid and Payment Currencies .....	13
14. Bid Security .....	13
15. Sealing and Marking of Bids .....	13
16. Deadline for Submission of Bids .....	13
17. Opening and Preliminary Examination of Bids .....	13
18. Domestic Preference .....	14
19. Detailed Evaluation and Comparison of Bids .....	14
20. Post-Qualification .....	14
21. Signing of the Contract .....	15
<b>Section III. Bid Data Sheet .....</b>	<b>16</b>
<b>Section IV. General Conditions of Contract .....</b>	<b>18</b>
1. Scope of Contract .....	19
2. Advance Payment and Terms of Payment .....	19
3. Performance Security .....	19
4. Inspection and Tests .....	19
5. Warranty .....	20
6. Liability of the Supplier .....	20
<b>Section V. Special Conditions of Contract .....</b>	<b>21</b>
<b>Section VI. Schedule of Requirements .....</b>	<b>34</b>
<b>Section VII. Technical Specifications .....</b>	<b>35</b>
<b>Section VIII. Checklist of Technical and Financial Documents .....</b>	<b>45</b>

# *Glossary of Acronyms, Terms, and Abbreviations*

**ABC** – Approved Budget for the Contract.

**BAC** – Bids and Awards Committee.

**Bid** – A signed offer or proposal to undertake a contract submitted by a bidder in response to and in consonance with the requirements of the bidding documents. Also referred to as *Proposal* and *Tender*. (2016 revised IRR, Section 5[c])

**Bidder** – Refers to a contractor, manufacturer, supplier, distributor and/or consultant who submits a bid in response to the requirements of the Bidding Documents. (2016 revised IRR, Section 5[d])

**Bidding Documents** – The documents issued by the Procuring Entity as the bases for bids, furnishing all information necessary for a prospective bidder to prepare a bid for the Goods, Infrastructure Projects, and/or Consulting Services required by the Procuring Entity. (2016 revised IRR, Section 5[e])

**BIR** – Bureau of Internal Revenue.

**BSP** – Bangko Sentral ng Pilipinas.

**Consulting Services** – Refer to services for Infrastructure Projects and other types of projects or activities of the GOP requiring adequate external technical and professional expertise that are beyond the capability and/or capacity of the GOP to undertake such as, but not limited to: (i) advisory and review services; (ii) pre-investment or feasibility studies; (iii) design; (iv) construction supervision; (v) management and related services; and (vi) other technical services or special studies. (2016 revised IRR, Section 5[i])

**CDA** - Cooperative Development Authority.

**Contract** – Refers to the agreement entered into between the Procuring Entity and the Supplier or Manufacturer or Distributor or Service Provider for procurement of Goods and Services; Contractor for Procurement of Infrastructure Projects; or Consultant or Consulting Firm for Procurement of Consulting Services; as the case may be, as recorded in the Contract Form signed by the parties, including all attachments and appendices thereto and all documents incorporated by reference therein.

**CIF** – Cost Insurance and Freight.

**CIP** – Carriage and Insurance Paid.

**CPI** – Consumer Price Index.

**DDP** – Refers to the quoted price of the Goods, which means “delivered duty paid.”

**DTI** – Department of Trade and Industry.

**EXW** – Ex works.

**FCA** – “Free Carrier” shipping point.

**FOB** – “Free on Board” shipping point.

**Foreign-funded Procurement or Foreign-Assisted Project**– Refers to procurement whose funding source is from a foreign government, foreign or international financing institution as specified in the Treaty or International or Executive Agreement. (2016 revised IRR, Section 5[b]).

**Framework Agreement** – Refers to a written agreement between a procuring entity and a supplier or service provider that identifies the terms and conditions, under which specific purchases, otherwise known as “Call-Offs,” are made for the duration of the agreement. It is in the nature of an option contract between the procuring entity and the bidder(s) granting the procuring entity the option to either place an order for any of the goods or services identified in the Framework Agreement List or not buy at all, within a minimum period of one (1) year to a maximum period of three (3) years. (GPPB Resolution No. 27-2019)

**GFI** – Government Financial Institution.

**GOCC** – Government-owned and/or –controlled corporation.

**Goods** – Refer to all items, supplies, materials and general support services, except Consulting Services and Infrastructure Projects, which may be needed in the transaction of public businesses or in the pursuit of any government undertaking, project or activity, whether in the nature of equipment, furniture, stationery, materials for construction, or personal property of any kind, including non-personal or contractual services such as the repair and maintenance of equipment and furniture, as well as trucking, hauling, janitorial, security, and related or analogous services, as well as procurement of materials and supplies provided by the Procuring Entity for such services. The term “related” or “analogous services” shall include, but is not limited to, lease or purchase of office space, media advertisements, health maintenance services, and other services essential to the operation of the Procuring Entity. (2016 revised IRR, Section 5[r])

**GOP** – Government of the Philippines.

**GPPB** – Government Procurement Policy Board.

**INCOTERMS** – International Commercial Terms.

**Infrastructure Projects** – Include the construction, improvement, rehabilitation, demolition, repair, restoration or maintenance of roads and bridges, railways, airports, seaports, communication facilities, civil works components of information technology projects, irrigation, flood control and drainage, water supply, sanitation, sewerage and solid waste management systems, shore protection, energy/power and electrification facilities, national

buildings, school buildings, hospital buildings, and other related construction projects of the government. Also referred to as *civil works or works*. (2016 revised IRR, Section 5[u])

**LGUs** – Local Government Units.

**NFCC** – Net Financial Contracting Capacity.

**NGA** – National Government Agency.

**PhilGEPS** - Philippine Government Electronic Procurement System.

**Procurement Project** – refers to a specific or identified procurement covering goods, infrastructure project or consulting services. A Procurement Project shall be described, detailed, and scheduled in the Project Procurement Management Plan prepared by the agency which shall be consolidated in the procuring entity's Annual Procurement Plan. (GPPB Circular No. 06-2019 dated 17 July 2019)

**PSA** – Philippine Statistics Authority.

**SEC** – Securities and Exchange Commission.

**SLCC** – Single Largest Completed Contract.

**Supplier** – refers to a citizen, or any corporate body or commercial company duly organized and registered under the laws where it is established, habitually established in business and engaged in the manufacture or sale of the merchandise or performance of the general services covered by his bid. (Item 3.8 of GPPB Resolution No. 13-2019, dated 23 May 2019). Supplier as used in these Bidding Documents may likewise refer to a distributor, manufacturer, contractor, or consultant.

**UN** – United Nations.

## ***Section I. Invitation to Bid***



Republic of the Philippines  
NATIONAL PRIVACY COMMISSION

**INVITATION TO BID FOR THE PROCUREMENT OF  
PENETRATION TESTING AND FORENSIC SOFTWARE**

1. The National Privacy Commission, through the General Appropriations Act FY 2020 intends to apply the sum of *THREE MILLION THREE HUNDRED SIXTY-ONE THOUSAND PESOS (Php 3,361,000.00)* being the ABC to payments under the contract for the *procurement of Penetration Testing and Forensic Software (APP 2020-0082)*. Bids received in excess of the ABC shall be automatically rejected at bid opening.
2. The *National Privacy Commission* now invites bids for the above Procurement Project. Delivery of the Goods is required *within 30 working days from receipt of Purchase Order/Contract/Notice to Proceed*. Bidders should have completed, within *three (3) years* from the date of submission and receipt of bids, a contract similar to the Project. The description of an eligible bidder is contained in the Bidding Documents, particularly, in Section II (Instructions to Bidders).
3. Bidding will be conducted through open competitive bidding procedures using a non-discretionary “*pass/fail*” criterion as specified in the 2016 revised Implementing Rules and Regulations (IRR) of Republic Act (RA) No. 9184.
  - a. Bidding is restricted to Filipino citizens/sole proprietorships, partnerships, or organizations with at least sixty percent (60%) interest or outstanding capital stock belonging to citizens of the Philippines, and to citizens or organizations of a country the laws or regulations of which grant similar rights or privileges to Filipino citizens, pursuant to RA No. 5183.
4. Prospective Bidders may obtain further information from *National Privacy Commission* and inspect the Bidding Documents at the address given below during *Monday to Friday, 9:00 A.M. to 4:00 P.M. Due to alternative work arrangement being adopted, please set an appointment first with the NPC-BAC Secretariat through the email address given below.*

*For the processing of payment of the Bidding Documents, please be reminded to bring the following documents:*

- a. *Copy of Invitation to Bid;*
  - b. *Original or CTC of Letter of Intent;*
  - c. *Copy of company ID; and*
  - d. *If paying through check, it should be named to Bureau of Treasury*
5. A complete set of Bidding Documents may be acquired by interested Bidders on July 22, 2021 from the given address and website(s) below *and upon payment of the applicable fee for the Bidding Documents, pursuant to the latest Guidelines issued by the GPPB, in the amount of Php5,000.00*. The Procuring Entity shall allow the bidder to present its proof of payment for the fees *in person or through electronic means*.

6. The *National Privacy Commission* will hold a Pre-Bid Conference on *July 29, 2021, 02:00PM through video conferencing or webcasting via Microsoft Teams* which shall be open to prospective bidders.
7. Bids must be duly received by the BAC Secretariat through manual submission at the office address indicated below, on or before *August 12, 2021, 10:00AM*. Late bids shall not be accepted.
8. All Bids must be accompanied by a bid security in any of the acceptable forms and in the amount stated in **ITB** Clause 14.
9. Bid opening shall be on *August 12, 2021, 03:00PM* at the given address below and through *video conferencing or webcasting via Microsoft Teams*. Bids will be opened in the presence of the bidders' representatives who choose to attend the activity.
10. *If you wish to join the pre-bid conference and the bid opening through video conferencing or webcasting via Microsoft Teams, please coordinate with the NPC-BAC Secretariat through the e-mail address given below.*
11. The *National Privacy Commission* reserves the right to reject any and all bids, declare a failure of bidding, or not award the contract at any time prior to contract award in accordance with Sections 35.6 and 41 of the 2016 revised IRR of RA No. 9184, without thereby incurring any liability to the affected bidder or bidders.
12. For further information, please refer to:

***ATTY. KRISHNA AIRA TANA-CAGUIA***

*Bids and Awards Committee- Secretariat, Head  
East Banquet Hall, 5<sup>th</sup> floor, Delegation Building  
Philippine International Convention Center, Pasay City  
(02) 8234-2228 local 127  
bacsecretariat@privacy.gov.ph  
[www.privacy.gov.ph](http://www.privacy.gov.ph)*

*Note: Due to the alternative work arrangement being adopted by the National Privacy Commission, please communicate through the e-mail address provided.*

13. You may visit the following websites: For downloading of Bidding Documents:  
[www.privacy.gov.ph](http://www.privacy.gov.ph)

*July 17, 2021*

\_\_\_\_\_  
*sgd*  
***ATTY. MARIA THERESITA E. PATULA***  
*BAC, Chairperson*



## ***Section II. Instructions to Bidders***

## **1. Scope of Bid**

The Procuring Entity, *National Privacy Commission* wishes to receive Bids for the *procurement of Penetration Testing and Forensic Software* with identification number *APP 2020-0082*.

The Procurement Project (referred to herein as “Project”) is composed of *one (1) lot*, the details of which are described in Section VII (Technical Specifications).

## **2. Funding Information**

2.1. The GOP through the source of funding as indicated below for *General Appropriations Act FY 2020 (Continuing Appropriation)* in the amount of *THREE MILLION THREE HUNDRED SIXTY-ONE THOUSAND PESOS (Php 3,361,000.00)*.

2.2. The source of funding is *NGA, the General Appropriations Act or Special Appropriations*.

## **3. Bidding Requirements**

The Bidding for the Project shall be governed by all the provisions of RA No. 9184 and its 2016 revised IRR, including its Generic Procurement Manuals and associated policies, rules and regulations as the primary source thereof, while the herein clauses shall serve as the secondary source thereof.

Any amendments made to the IRR and other GPPB issuances shall be applicable only to the ongoing posting, advertisement, or **IB** by the BAC through the issuance of a supplemental or bid bulletin.

The Bidder, by the act of submitting its Bid, shall be deemed to have verified and accepted the general requirements of this Project, including other factors that may affect the cost, duration and execution or implementation of the contract, project, or work and examine all instructions, forms, terms, and project requirements in the Bidding Documents.

## **4. Corrupt, Fraudulent, Collusive, and Coercive Practices**

The Procuring Entity, as well as the Bidders and Suppliers, shall observe the highest standard of ethics during the procurement and execution of the contract. They or through an agent shall not engage in corrupt, fraudulent, collusive, coercive, and obstructive practices defined under Annex “I” of the 2016 revised IRR of RA No. 9184 or other integrity violations in competing for the Project.

## **5. Eligible Bidders**

5.1. Only Bids of Bidders found to be legally, technically, and financially capable will be evaluated.

- 5.2. Foreign ownership limited to those allowed under the rules may participate in this Project.
- 5.3. Pursuant to Section 23.4.1.3 of the 2016 revised IRR of RA No.9184, the Bidder shall have an SLCC that is at least one (1) contract similar to the Project the value of which, adjusted to current prices using the PSA's CPI, must be at least equivalent to:
  - a. For the procurement of Non-expendable Supplies and Services: The Bidder must have completed a single contract that is similar to this Project, equivalent to at least fifty percent (50%) of the ABC.
- 5.4. The Bidders shall comply with the eligibility criteria under Section 23.4.1 of the 2016 IRR of RA No. 9184.

## **6. Origin of Goods**

There is no restriction on the origin of goods other than those prohibited by a decision of the UN Security Council taken under Chapter VII of the Charter of the UN, subject to Domestic Preference requirements under **ITB** Clause 18.

## **7. Subcontracts**

- 7.1. Subcontracting is not allowed.

## **8. Pre-Bid Conference**

The Procuring Entity will hold a pre-bid conference for this Project on the specified date and time through videoconferencing/webcasting as indicated in paragraph 6 of the **IB**.

## **9. Clarification and Amendment of Bidding Documents**

Prospective bidders may request for clarification on and/or interpretation of any part of the Bidding Documents. Such requests must be in writing and received by the Procuring Entity, either at its given address or through electronic mail indicated in the **IB**, at least ten (10) calendar days before the deadline set for the submission and receipt of Bids.

## **10. Documents comprising the Bid: Eligibility and Technical Components**

- 10.1. The first envelope shall contain the eligibility and technical documents of the Bid as specified in **Section VIII (Checklist of Technical and Financial Documents)**.
- 10.2. The Bidder's SLCC as indicated in **ITB** Clause 5.3 should have been completed within *three (3)* prior to the deadline for the submission and receipt of bids.

- 10.3. If the eligibility requirements or statements, the bids, and all other documents for submission to the BAC are in foreign language other than English, it must be accompanied by a translation in English, which shall be authenticated by the appropriate Philippine foreign service establishment, post, or the equivalent office having jurisdiction over the foreign bidder's affairs in the Philippines. Similar to the required authentication above, for Contracting Parties to the Apostille Convention, only the translated documents shall be authenticated through an apostille pursuant to GPPB Resolution No. 13-2019 dated 23 May 2019. The English translation shall govern, for purposes of interpretation of the bid.

## **11. Documents comprising the Bid: Financial Component**

- 11.1. The second bid envelope shall contain the financial documents for the Bid as specified in **Section VIII (Checklist of Technical and Financial Documents)**.
- 11.2. If the Bidder claims preference as a Domestic Bidder or Domestic Entity, a certification issued by DTI shall be provided by the Bidder in accordance with Section 43.1.3 of the 2016 revised IRR of RA No. 9184.
- 11.3. Any bid exceeding the ABC indicated in paragraph 1 of the **IB** shall not be accepted.
- 11.4. For Foreign-funded Procurement, a ceiling may be applied to bid prices provided the conditions are met under Section 31.2 of the 2016 revised IRR of RA No. 9184.

## **12. Bid Prices**

- 12.1. Prices indicated on the Price Schedule shall be entered separately in the following manner:
  - a. For Goods offered from within the Procuring Entity's country:
    - i. The price of the Goods quoted EXW (ex-works, ex-factory, ex-warehouse, ex-showroom, or off-the-shelf, as applicable);
    - ii. The cost of all customs duties and sales and other taxes already paid or payable;
    - iii. The cost of transportation, insurance, and other costs incidental to delivery of the Goods to their final destination; and
    - iv. The price of other (incidental) services, if any, listed in e.
  - b. For Goods offered from abroad:
    - i. Unless otherwise stated in the **BDS**, the price of the Goods shall be quoted delivered duty paid (DDP) with the place of destination in the Philippines as specified in the **BDS**. In quoting the price, the Bidder shall be free to use transportation through carriers

registered in any eligible country. Similarly, the Bidder may obtain insurance services from any eligible source country.

- ii. The price of other (incidental) services, if any, as listed in **Section VII (Technical Specifications)**.

### **13. Bid and Payment Currencies**

13.1. For Goods that the Bidder will supply from outside the Philippines, the bid prices may be quoted in the local currency or tradeable currency accepted by the BSP at the discretion of the Bidder. However, for purposes of bid evaluation, Bids denominated in foreign currencies, shall be converted to Philippine currency based on the exchange rate as published in the BSP reference rate bulletin on the day of the bid opening.

13.2. Payment of the contract price shall be made in *Philippine Pesos*.

### **14. Bid Security**

14.1. The Bidder shall submit a Bid Securing Declaration or any form of Bid Security in the amount indicated in the **BDS**, which shall be not less than the percentage of the ABC in accordance with the schedule in the **BDS**.

14.2. The Bid and bid security shall be valid until *120 calendar days from the date of opening of bid, which is on August 12, 2021*. Any Bid not accompanied by an acceptable bid security shall be rejected by the Procuring Entity as non-responsive.

### **15. Sealing and Marking of Bids**

Each Bidder shall submit one copy of the first and second components of its Bid.

The Procuring Entity may request additional hard copies and/or electronic copies of the Bid. However, failure of the Bidders to comply with the said request shall not be a ground for disqualification.

If the Procuring Entity allows the submission of bids through online submission or any other electronic means, the Bidder shall submit an electronic copy of its Bid, which must be digitally signed. An electronic copy that cannot be opened or is corrupted shall be considered non-responsive and, thus, automatically disqualified.

### **16. Deadline for Submission of Bids**

16.1. The Bidders shall submit on the specified date and time and either at its physical address or through online submission as indicated in paragraph 7 of the **IB**.

### **17. Opening and Preliminary Examination of Bids**

- 17.1. The BAC shall open the Bids in public at the time, on the date, and at the place specified in paragraph 9 of the **IB**. The Bidders' representatives who are present shall sign a register evidencing their attendance. In case videoconferencing, webcasting or other similar technologies will be used, attendance of participants shall likewise be recorded by the BAC Secretariat.

In case the Bids cannot be opened as scheduled due to justifiable reasons, the rescheduling requirements under Section 29 of the 2016 revised IRR of RA No. 9184 shall prevail.

- 17.2. The preliminary examination of bids shall be governed by Section 30 of the 2016 revised IRR of RA No. 9184.

## **18. Domestic Preference**

- 18.1. The Procuring Entity will grant a margin of preference for the purpose of comparison of Bids in accordance with Section 43.1.2 of the 2016 revised IRR of RA No. 9184.

## **19. Detailed Evaluation and Comparison of Bids**

- 19.1. The Procuring BAC shall immediately conduct a detailed evaluation of all Bids rated "*passed*," using non-discretionary pass/fail criteria. The BAC shall consider the conditions in the evaluation of Bids under Section 32.2 of the 2016 revised IRR of RA No. 9184.
- 19.2. If the Project allows partial bids, bidders may submit a proposal on any of the lots or items, and evaluation will be undertaken on a per lot or item basis, as the case maybe. In this case, the Bid Security as required by **ITB** Clause 15 shall be submitted for each lot or item separately.
- 19.3. The descriptions of the lots or items shall be indicated in **Section VII (Technical Specifications)**, although the ABCs of these lots or items are indicated in the **BDS** for purposes of the NFCC computation pursuant to Section 23.4.2.6 of the 2016 revised IRR of RA No. 9184. The NFCC must be sufficient for the total of the ABCs for all the lots or items participated in by the prospective Bidder.
- 19.4. The Project shall be awarded as *one Project having several items that shall be awarded as one contract*.
- 19.5. Except for bidders submitting a committed Line of Credit from a Universal or Commercial Bank in lieu of its NFCC computation, all Bids must include the NFCC computation pursuant to Section 23.4.1.4 of the 2016 revised IRR of RA No. 9184, which must be sufficient for the total of the ABCs for all the lots or items participated in by the prospective Bidder. For bidders submitting the committed Line of Credit, it must be at least equal to ten percent (10%) of the ABCs for all the lots or items participated in by the prospective Bidder.

## **20. Post-Qualification**

- 20.1. Within a non-extendible period of five (5) calendar days from receipt by the Bidder of the notice from the BAC that it submitted the Lowest Calculated Bid, the Bidder shall submit its latest income and business tax returns filed and paid through the BIR Electronic Filing and Payment System (eFPS) and other appropriate licenses and permits required by law and stated in the **BDS**.

## **21. Signing of the Contract**

- 21.1. The documents required in Section 37.2 of the 2016 revised IRR of RA No. 9184 shall form part of the Contract. Additional Contract documents are indicated in the **BDS**.

## ***Section III. Bid Data Sheet***



# Bid Data Sheet

ITB Clause	
5.3	<p>For this purpose, contracts similar to the Project shall be:</p> <ul style="list-style-type: none"> <li>a. <i>Contracts for the supply of digital forensic software, penetration testing software, software for forensic laboratories, modern digital forensic equipment and applications such as computer forensic machines, cellular/mobile phone forensic tools, or latest versions of forensic and investigation software.</i></li> <li>b. completed within <b>three (3) years</b> prior to the deadline for the submission and receipt of bids.</li> </ul>
7.1	<i>Not applicable</i>
12	The price of the Goods shall be quoted DDP National Privacy Commission Office or the applicable International Commercial Terms (INCOTERMS) for this Project.
14.1	<p>The bid security shall be in the form of a Bid Securing Declaration, or any of the following forms and amounts:</p> <ul style="list-style-type: none"> <li>a. The amount of not less than <i>Php 67,220.00</i>, if bid security is in cash, cashier's/manager's check, bank draft/guarantee or irrevocable letter of credit; or</li> <li>b. The amount of not less than <i>Php 168,050.00</i>, if bid security is in Surety Bond.</li> </ul>
15	<b><i>Each bidder shall submit one (1) original and one (1) readable copies of the first (technical) and second (financial) components of its bid. Documents to be submitted shall be properly tabbed and labeled.</i></b>
19.3	<i>Not applicable</i>
20.2	<i>Not applicable</i>
21.2	<i>Not applicable</i>

## ***Section IV. General Conditions of Contract***

## 1. Scope of Contract

This Contract shall include all such items, although not specifically mentioned, that can be reasonably inferred as being required for its completion as if such items were expressly mentioned herein. All the provisions of RA No. 9184 and its 2016 revised IRR, including the Generic Procurement Manual, and associated issuances, constitute the primary source for the terms and conditions of the Contract, and thus, applicable in contract implementation. Herein clauses shall serve as the secondary source for the terms and conditions of the Contract.

This is without prejudice to Sections 74.1 and 74.2 of the 2016 revised IRR of RA No. 9184 allowing the GPPB to amend the IRR, which shall be applied to all procurement activities, the advertisement, posting, or invitation of which were issued after the effectivity of the said amendment.

Additional requirements for the completion of this Contract shall be provided in the **Special Conditions of Contract (SCC)**.

## 2. Advance Payment and Terms of Payment

2.1. Advance payment of the contract amount is provided under Annex “D” of the revised 2016 IRR of RA No. 9184.

2.2. The Procuring Entity is allowed to determine the terms of payment on the partial or staggered delivery of the Goods procured, provided such partial payment shall correspond to the value of the goods delivered and accepted in accordance with prevailing accounting and auditing rules and regulations. The terms of payment are indicated in the **SCC**.

## 3. Performance Security

Within ten (10) calendar days from receipt of the Notice of Award by the Bidder from the Procuring Entity but in no case later than prior to the signing of the Contract by both parties, the successful Bidder shall furnish the performance security in any of the forms prescribed in Section 39 of the 2016 revised IRR of RA No. 9184.

## 4. Inspection and Tests

The Procuring Entity or its representative shall have the right to inspect and/or to test the Goods to confirm their conformity to the Project specifications at no extra cost to the Procuring Entity in accordance with the Generic Procurement Manual. In addition to tests in the **SCC, Section IV (Technical Specifications)** shall specify what inspections and/or tests the Procuring Entity requires, and where they are to be conducted. The Procuring Entity shall notify the Supplier in writing, in a timely manner, of the identity of any representatives retained for these purposes.

All reasonable facilities and assistance for the inspection and testing of Goods, including access to drawings and production data, shall be provided by the Supplier to the authorized inspectors at no charge to the Procuring Entity.

## **5. Warranty**

- 5.1 In order to assure that manufacturing defects shall be corrected by the Supplier, a warranty shall be required from the Supplier as provided under Section 62.1 of the 2016 revised IRR of RA No. 9184.
- 5.2 The Procuring Entity shall promptly notify the Supplier in writing of any claims arising under this warranty. Upon receipt of such notice, the Supplier shall, repair or replace the defective Goods or parts thereof without cost to the Procuring Entity, pursuant to the Generic Procurement Manual.

## **6. Liability of the Supplier**

The Supplier's liability under this Contract shall be as provided by the laws of the Republic of the Philippines.

If the Supplier is a joint venture, all partners to the joint venture shall be jointly and severally liable to the Procuring Entity.

## ***Section V. Special Conditions of Contract***

# Special Conditions of Contract

GCC Clause								
1	<p style="text-align: center;"><b>1. TECHNICAL SPECIFICATIONS</b></p> <p style="text-align: center;"><b>I. PENETRATION TESTING PLATFORM</b></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #cccccc;"> <th style="text-align: center;">Qty.</th> <th style="text-align: center;">Item</th> <th style="text-align: center;">Specifications</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">1</td> <td style="text-align: center;">Penetration Testing Platform</td> <td> <p>The technical specifications of a license renewal to the Commissions' existing Penetration Testing Software License, <b>SHOULD MEET THE FOLLOWING SPECIFICATIONS:</b></p> <p><b>A.1.1 Installation, Deployment and Integration</b></p> <ul style="list-style-type: none"> <li>• Solution must be able to support installation on 64-bit Linux and Windows (64-bit).</li> <li>• Solution must have latest updates (e.g. exploit module) as frequent as on a weekly basis.</li> <li>• Solution must support offline activation and manual updates.</li> <li>• Solution must be able to perform full backup to prevent data loss and enable to easily migrate data.</li> </ul> <p><b>A.1.2 Administration</b></p> <ul style="list-style-type: none"> <li>• Solution must include web-based user interface through encrypted channels.</li> <li>• Solution must support command line console within.</li> <li>• Solution must allow API integration with other systems or be able to automate workflow.</li> <li>• Solution must be able to run jobs or tasks (e.g. scan, exploit) on schedule.</li> </ul> <p><b>A.1.3 Host Scan and Web Scan</b></p> <ul style="list-style-type: none"> <li>• Solution can conduct scans and discover the host's OS and running services.</li> <li>• Solution can support customized nmap command for scan.</li> <li>• Solution can support dry runs to show the scan information in task log only.</li> </ul> </td> </tr> </tbody> </table>		Qty.	Item	Specifications	1	Penetration Testing Platform	<p>The technical specifications of a license renewal to the Commissions' existing Penetration Testing Software License, <b>SHOULD MEET THE FOLLOWING SPECIFICATIONS:</b></p> <p><b>A.1.1 Installation, Deployment and Integration</b></p> <ul style="list-style-type: none"> <li>• Solution must be able to support installation on 64-bit Linux and Windows (64-bit).</li> <li>• Solution must have latest updates (e.g. exploit module) as frequent as on a weekly basis.</li> <li>• Solution must support offline activation and manual updates.</li> <li>• Solution must be able to perform full backup to prevent data loss and enable to easily migrate data.</li> </ul> <p><b>A.1.2 Administration</b></p> <ul style="list-style-type: none"> <li>• Solution must include web-based user interface through encrypted channels.</li> <li>• Solution must support command line console within.</li> <li>• Solution must allow API integration with other systems or be able to automate workflow.</li> <li>• Solution must be able to run jobs or tasks (e.g. scan, exploit) on schedule.</li> </ul> <p><b>A.1.3 Host Scan and Web Scan</b></p> <ul style="list-style-type: none"> <li>• Solution can conduct scans and discover the host's OS and running services.</li> <li>• Solution can support customized nmap command for scan.</li> <li>• Solution can support dry runs to show the scan information in task log only.</li> </ul>
Qty.	Item	Specifications						
1	Penetration Testing Platform	<p>The technical specifications of a license renewal to the Commissions' existing Penetration Testing Software License, <b>SHOULD MEET THE FOLLOWING SPECIFICATIONS:</b></p> <p><b>A.1.1 Installation, Deployment and Integration</b></p> <ul style="list-style-type: none"> <li>• Solution must be able to support installation on 64-bit Linux and Windows (64-bit).</li> <li>• Solution must have latest updates (e.g. exploit module) as frequent as on a weekly basis.</li> <li>• Solution must support offline activation and manual updates.</li> <li>• Solution must be able to perform full backup to prevent data loss and enable to easily migrate data.</li> </ul> <p><b>A.1.2 Administration</b></p> <ul style="list-style-type: none"> <li>• Solution must include web-based user interface through encrypted channels.</li> <li>• Solution must support command line console within.</li> <li>• Solution must allow API integration with other systems or be able to automate workflow.</li> <li>• Solution must be able to run jobs or tasks (e.g. scan, exploit) on schedule.</li> </ul> <p><b>A.1.3 Host Scan and Web Scan</b></p> <ul style="list-style-type: none"> <li>• Solution can conduct scans and discover the host's OS and running services.</li> <li>• Solution can support customized nmap command for scan.</li> <li>• Solution can support dry runs to show the scan information in task log only.</li> </ul>						

			<ul style="list-style-type: none"> <li>• Solution must be able to integrate with Nexpose to discover host's OS, running services and vulnerabilities via existing scan results or new scans.</li> <li>• Solution must support automatic tag by OS</li> <li>• Solution must support importing of scan result from external solutions including but not limited to: Nexpose, Metasploit, Foundstone, Microsoft, nCircle, NetSparker, Nessus, Qualys, Burp, Acunetix, AppScan, Nmap, Retina, Amap, Critical Watch, IP Address List, Libpcap, Spiceworks and Core Impact.</li> </ul> <p><b>A.1.4 System Exploitation</b></p> <ul style="list-style-type: none"> <li>• Solution must be able to apply exploits on individual IP or multiple IPs.</li> <li>• Solution can automatically select and apply exploit modules based on OS, service and vulnerability references.</li> <li>• Solution must have at least 6 reliability levels of exploit codes for automated exploitation.</li> <li>• Solution must support running individual exploit module manually from the user interface.</li> <li>• Solution must support dry run to show exploit information in task log only.</li> <li>• Solution must support replay of exploitation tasks.</li> <li>• Solution must support automation of common yet complicated security tests (Metamodules) that provide a more efficient way to get specific jobs done.</li> <li>• Solution must support the reuse of manually added or captured credentials within a project to validate specified credentials on additional hosts in the target network.</li> </ul> <p><b>A.1.5 Bruteforcing</b></p> <ul style="list-style-type: none"> <li>• Solution can support brute force testing on services including but not limited to AFP, SMB, Postgres, DB2, MySQL, MSSQL, HTTP, HTTPS, SSH, SSH PUBKEY, Telnet, FTP, POP3, VNC, SNMP, WinRM.</li> </ul>
--	--	--	--

			<ul style="list-style-type: none"> <li>• Solution can provide password references for factory default logins.</li> <li>• Solution can support customized credentials and dictionary import for brute force and or dictionary attack.</li> <li>• Solution can support credential mutation to create multiple permutations of a specified password, which enables building of a larger list based on a defined set of passwords.</li> </ul> <p><b>A.1.6 Post Exploitation Action and Evidence Collection</b></p> <ul style="list-style-type: none"> <li>• Solution must support exploitation payload types including but not limited to: “Meterpreter”, “Command Shell” and "Powershell".</li> <li>• Solution must support customized macros to run selected operations automatically after exploit.</li> <li>• Solution must support post exploitation actions including but not limited to collect system data (screen capture, password, system information), build a virtual desktop connection, access file system, search the file system, run a command shell, create proxy pivot, create VPN pivot.</li> <li>• Solution must support deploying of persistent listeners to allow exploited hosts to connect back to the penetration testing platform automatically.</li> </ul> <p><b>A.1.7 Social Engineering Campaign</b></p> <ul style="list-style-type: none"> <li>• Solution must support web campaign, Email campaign and USB campaign.</li> <li>• Solution must allow web campaign customized with http/https, IP address, port and path (e.g. <a href="https://www.abc.com:1234/abcd">https://www.abc.com:1234/abcd</a>).</li> <li>• Solution must support web content to be cloned from another web site (e.g. <a href="http://www.google.com">www.google.com</a>).</li> <li>• Solution must support web campaign that browser autopwn (apply all the appropriate exploit modules based on the browser version), specific browser exploit (e.g.</li> </ul>
--	--	--	---



			<p>MS11-050) and not do anything (just checking the connection from the users).</p> <ul style="list-style-type: none"> <li>• Solution must support email campaign content customization to include a specific URL or an agent attachment.</li> <li>• Solution must support USB campaign that generates an agent deployment .exe file.</li> </ul> <p><b>A.1.8 Web Application Exploitation</b></p> <ul style="list-style-type: none"> <li>• Solution must support web crawling on IPv4 and IPv6 web sites.</li> <li>• Solution must support web crawling applied on a web site (e.g. <a href="http://www.abc.com">http://www.abc.com</a>) or started from a specific point (e.g. <a href="http://www.abc.com/path/starthere/">http://www.abc.com/path/starthere/</a>).</li> <li>• Solution must support detection of vulnerable URLs and parameters such as SQL Injection and Cross Site Scripting.</li> </ul> <p><b>A.1.9 Report and Data Export</b></p> <ul style="list-style-type: none"> <li>• Solution must provide built-in standard reports and support customized report functionality.</li> <li>• Solution must provide at least 10 built-in standard reports.</li> <li>• Solution must support report formats including but not limited to PDF, Word, RTF and HTML.</li> <li>• Solution must support reports to be stored locally and sent to recipient by email after created.</li> <li>• Solution must be able to support data export which allows a zip archive of the project suitable for importing into another instance of the solution.</li> </ul> <p><b>A.1.10 Other Requirements</b></p> <ul style="list-style-type: none"> <li>• Bidder/Supplier should be authorized by the Manufacturer to negotiate, and/or to bid and/or to sell.</li> <li>• Software license must be compatible with the current penetration testing software for renewal for One (1) year.</li> <li>• Bidder/Supplier should have at least two (2) Government contracts in relation to Digital or</li> </ul>
--	--	--	--

		<p>Computer Forensics with satisfactory performance.</p> <ul style="list-style-type: none"> <li>• Supplier should provide a minimum of 1-2 days of hands-on training on the use, analysis, and administration of the software.</li> <li>• Delivery schedule: 30 working days from receipt of Purchase Order / Contract / Notice to Proceed</li> </ul>
--	--	---

**II. CLOUD ANALYZER SOFTWARE / MOBILE FORENSIC CLOUD ANALYSIS AND INVESTIGATION SOFTWARE**

<b>Qty.</b>	<b>Item</b>	<b>Specifications</b>
1	Cloud Analyzer Software / Mobile Forensic Cloud Analysis and Investigation Software	<p>The renewal of the Commission’s existing Cloud Analysis and Investigation Software License <b>SHOULD MEET THE FOLLOWING SPECIFICATIONS:</b></p> <ul style="list-style-type: none"> <li>• Software licenses must be compatible with the current mobile forensic cloud analyzer system software for renewal</li> <li>• Inclusive of One (1) Year Maintenance Systems</li> <li>• Software shall allow gathering user data from popular social media and cloud-based sources.</li> <li>• Able to collect and hash digital evidence from HTML-based web pages.</li> <li>• Can enable the user to view user search history and gather geo-location data.</li> <li>• Able to normalize and sort data into different formats</li> <li>• Can generate easy-to-read reports available in different formats like PDF for entire data sets or filtered information</li> <li>• Support reporting of extracted data from the cloud to a machine-readable format so it can be digested by other analysis systems.</li> <li>• Supplier should have a local partner to provide immediate post-sales support</li> <li>• Supplier should have Manufacturer’s Authorization to supply and support the renewal of the said license. Supplier should have at least Two (2) government contracts with satisfactory performance for the same product or digital forensic.</li> </ul> <p><b>Qualification Requirements</b></p>

		<ul style="list-style-type: none"> <li>• Direct contracting supplier must provide a price quotation or a pro-forma invoice together with the conditions of sale.</li> <li>• Must provide a certificate or proof being the duly authorized or sole distributor (provider) of the said Software(s).</li> <li>• Inclusive of One (1) Year Maintenance Systems per software as stipulated on Section (III)(A), unless explicitly stated.</li> <li>• Provider must provide basic training for all software subscriptions.</li> <li>• Supplier should have a local partner to provide immediate post-sales support.</li> <li>• Supplier should have Manufacturer's Authorization to supply and support the renewal of software licenses.</li> <li>• Supplier should have at least Two (2) government contracts with satisfactory performance for the software(s) stipulated on Section (III)(A).</li> <li>• Supplier should provide a minimum of 1-2 days of hands-on training on the use, analysis, and administration of the software.</li> <li>• Delivery schedule: 30 working days from receipt of Purchase Order / Contract / Notice to Proceed</li> </ul>
--	--	---

**III. DIGITAL FORENSIC INVESTIGATION SOFTWARE**

<b>Qty.</b>	<b>Item</b>	<b>Specifications</b>
1	Digital Forensic Investigation Software	<p>The renewal of the Commission's existing Digital Forensic Investigation Software License <b>SHOULD MEET THE FOLLOWING SPECIFICATIONS:</b></p> <p>Software licenses must be compatible with the current digital forensic investigation software for renewal</p> <p>Inclusive of One (1) Year Maintenance Systems</p> <p>Capable of acquiring data in a forensically sound manner using software accepted by courts worldwide.</p> <p>Capable of investigating and analyzing data from multiple platforms such as Windows,</p>

			<p>Linux, AIX, OS X, Solaris, and more—using a single tool.</p> <p>Capable of finding information despite attempt to hide, cloak, or delete data</p> <p>Capable of easily managing large volumes of computer evidence, viewing all relevant files, including deleted files, file slack, and unallocated space.</p> <p>Capable of creating exact duplicates of original data and verifying by hash and error check.</p> <p>Capable of transferring evidence files directly to law enforcement or legal representatives.</p> <p>Capable of providing review options that allow non-investigators, such as attorneys, to review evidence with ease.</p> <p>Capable of providing reporting options for quick report preparation.</p> <p>Supplier should have a local partner to provide immediate post-sales support</p> <p>Supplier should have Manufacturer’s Authorization to supply and support the renewal of the said license.</p> <p>Supplier should have at least Two (2) government contracts with satisfactory performance for the same product or digital forensic.</p> <p>Supplier should provide a minimum of 1-2 days of hands-on training on the use, analysis, and administration of the software.</p> <p>Delivery schedule: 30 working days from receipt of Purchase Order / Contract / Notice to Proceed</p>
<b>IV. MOBILE FORENSIC APPLICATION</b>			
<b>Qty.</b>	<b>Item</b>	<b>Specifications</b>	

	1	Mobile Forensic Application	<p>The renewal of the Commission’s existing Mobile Forensic Investigation Device License <b>SHOULD MEET THE FOLLOWING SPECIFICATIONS:</b></p> <p>Software licenses must be compatible with the current mobile forensic investigation device software for renewal</p> <p>Inclusive of One (1) Year Maintenance Systems</p> <p>One (1) Year support on mobile connector tips and cables</p> <p>Inclusive of decoding, analysis and report generation software license</p> <p>Capable of Bypassing pattern, password or PIN locks.</p> <p>Capable of extracting physical, file system, and logical data from smartphones, feature phones, tablets, players, GPS devices, SIM cards, smart watches, mass storage devices, drones and other devices with memory storage to access live, hidden and even deleted data.</p> <p>Capable of displaying and visualizing data in a unified format to build timelines and maps and more easily see relevant connections</p> <p>Can generate easy-to-read reports available in different formats like PDF for entire data sets or filtered information.</p> <p>Supplier should have a local partner to provide immediate post-sales support.</p> <p>Supplier should have Manufacturer’s Authorization to supply and support the renewal of the said license.</p> <p>Supplier should have at least Two (2) government contracts with satisfactory performance for the same product or digital forensic.</p>
--	---	-----------------------------	---

Supplier should provide a minimum of 1-2 days of hands-on training on the use, analysis, and administration of the software.

Delivery schedule: 30 working days from receipt of Purchase Order / Contract / Notice to Proceed

**V. SYSTEM VULNERABILITY ASSESSMENT SOFTWARE**

Qty.	Item	Specifications
1	System Vulnerability Assessment Software	<p>The renewal of the Commission’s existing Vulnerability Assessment Software <b>SHOULD MEET THE FOLLOWING SPECIFICATIONS:</b></p> <p>Software licenses must be compatible with the current vulnerability assessment software for renewal</p> <p>Inclusive of One (1) Year Maintenance Systems</p> <p>Capable of operating 100% on-premises. Scan results should always be available on premise. Describe the solution's architecture. Detail all components and modules required to deliver the complete solution.</p> <p>Must be offered as either Software Product or Software as a Service.</p> <p>Must support at least the below mentioned supported platforms as OS: Ubuntu Linux LTS, Microsoft Windows Server, Microsoft Windows and Red Hat Enterprise Linux Server</p> <p>Must have the capability to perform both internal and external scanning.</p> <p>Must include web-based management user interface over encrypted traffics. It must not be accessed in clear text.</p> <p>Must support having scan engine pooling with multiple engines grouped together to run any single scan to reduce and improve scanning time by load sharing.</p>

		<p>Supplier should have a local partner to provide immediate post-sales support.</p> <p>Supplier should have Manufacturer's Authorization to supply and support the renewal of the said license.</p> <p>Supplier should have at least Two (2) government contracts with satisfactory performance for the same product.</p> <p>Supplier should provide a minimum of 1-2 days of hands-on training on the use, analysis, and administration of the software.</p> <p>Delivery schedule: 30 working days from receipt of Purchase Order / Contract / Notice to Proceed</p>
--	--	--

**2. TRAINING**

A Training Plan shall be submitted which includes the course design and method of delivery, specific topics to be covered and the corresponding date and times for each topic. The plan must also indicate the recommended minimum qualifications of the participants.

Training shall be provided to at least twenty (20) selected personnel within thirty (30) days from the date of issuance of Certificate of User Acceptance or on the date and time as set by the National Privacy Commission for such purpose.

Proof of completion of required training to be conducted shall be the issuance of training certificates to the participants.

**3. DELIVERY AND DOCUMENTS –**

For purposes of the Contract, “EXW,” “FOB,” “FCA,” “CIF,” “CIP,” “DDP” and other trade terms used to describe the obligations of the parties shall have the meanings assigned to them by the current edition of INCOTERMS published by the International Chamber of Commerce, Paris. The Delivery terms of this Contract shall be as follows:

“The delivery terms applicable to this Contract are delivered *at the National Privacy Commission (East Banquet Hall, 5<sup>th</sup> floor, Delegation Building, Philippine International Convention Center, Pasay City)*. Risk and title will pass from the Supplier

to the Procuring Entity upon receipt and final acceptance of the Goods at their final destination.”

Delivery of the Goods shall be made by the Supplier in accordance with the terms specified in Section VI (Schedule of Requirements).

For purposes of this Clause the Procuring Entity’s Representative at the Project Site is *Mr. Walden Frederick Canlas*

#### **4. INCIDENTAL SERVICES –**

The Supplier is required to provide all of the following services, including additional services, if any, specified in Section VI. Schedule of Requirements:

- a. performance or supervision of on-site assembly and/or start-up of the supplied Goods;
- b. furnishing of tools required for assembly and/or maintenance of the supplied Goods;
- c. furnishing of a detailed operations and maintenance manual for each appropriate unit of the supplied Goods;
- d. performance or supervision or maintenance and/or repair of the supplied Goods, for a period of time agreed by the parties, provided that this service shall not relieve the Supplier of any warranty obligations under this Contract; and
- e. training of the Procuring Entity’s personnel, at the Supplier’s plant and/or on-site, in assembly, start-up, operation, maintenance, and/or repair of the supplied Goods.

The Contract price for the Goods shall include the prices charged by the Supplier for incidental services and shall not exceed the prevailing rates charged to other parties by the Supplier for similar services.

#### **5. TRANSPORTATION –**

Where the Supplier is required under Contract to deliver the Goods CIF, CIP, or DDP, transport of the Goods to the port of destination or such other named place of destination in the Philippines, as shall be specified in this Contract, shall be arranged and paid for by the Supplier, and the cost thereof shall be included in the Contract Price.

Where the Supplier is required under this Contract to transport the Goods to a specified place of destination within the Philippines, defined as the Project Site, transport to such place of destination in the Philippines, including insurance and storage, as shall be specified in this Contract, shall be arranged by the Supplier, and related costs shall be included in the contract price.



	<p>Where the Supplier is required under Contract to deliver the Goods CIF, CIP or DDP, Goods are to be transported on carriers of Philippine registry. In the event that no carrier of Philippine registry is available, Goods may be shipped by a carrier which is not of Philippine registry provided that the Supplier obtains and presents to the Procuring Entity certification to this effect from the nearest Philippine consulate to the port of dispatch. In the event that carriers of Philippine registry are available but their schedule delays the Supplier in its performance of this Contract the period from when the Goods were first ready for shipment and the actual date of shipment the period of delay will be considered force majeure.</p> <p>The Procuring Entity accepts no liability for the damage of Goods during transit other than those prescribed by INCOTERMS for DDP deliveries. In the case of Goods supplied from within the Philippines or supplied by domestic Suppliers risk and title will not be deemed to have passed to the Procuring Entity until their receipt and final acceptance at the final destination.</p>
2.2	<p>The terms of payment shall be as follows:</p> <p><i>Payment shall be made when the Service/Goods have been rendered or delivered in accordance with the signed contract and instructions and upon issuance of Inspection and Acceptance Report by the Inspection and Acceptance Committee and Certificate of Acceptance by the End-User.</i></p>
4	<p>The inspections and tests that will be conducted are:</p> <p><i>The inspections and tests will be conducted by the Inspection and Acceptance Committee of the National Privacy Commission and the end-user.</i></p>

## *Section VI. Schedule of Requirements*

The delivery schedule expressed as weeks/months stipulates hereafter a delivery date which is the date of delivery to the project site.

Item Number	Description	Quantity	Total	Delivered, Weeks/Months
1	Penetration Testing Platform	1	1	30 working days from receipt of Purchase Order / Contract / Notice to Proceed
2	Cloud Analyzer Software / Mobile Forensic Cloud Analysis and Investigation Software	1	1	30 working days from receipt of Purchase Order / Contract / Notice to Proceed
3	Digital Forensic Investigation Software	1	1	30 working days from receipt of Purchase Order / Contract / Notice to Proceed
4	Mobile Forensic Application	1	1	30 working days from receipt of Purchase Order / Contract / Notice to Proceed
5	System Vulnerability Assessment Software	1	1	30 working days from receipt of Purchase Order / Contract / Notice to Proceed

*I hereby undertake to comply and deliver all the above requirements.*

\_\_\_\_\_  
**Company Name**

\_\_\_\_\_  
**Name and Signature of Authorized Representative**

\_\_\_\_\_  
**Date**

## ***Section VII. Technical Specifications***

# Technical Specifications

*[Bidders must state here either “Comply” or “Not Comply” against each of the individual parameters of each Specification stating the corresponding performance parameter of the equipment offered. Statements of “Comply” or “Not Comply” must be supported by evidence in a Bidders Bid and cross-referenced to that evidence. Evidence shall be in the form of manufacturer’s un-amended sales literature, unconditional statements of specification and compliance issued by the manufacturer, samples, independent test data etc., as appropriate. A statement that is not supported by evidence or is subsequently found to be contradicted by the evidence presented will render the Bid under evaluation liable for rejection. A statement either in the Bidder's statement of compliance or the supporting evidence that is found to be false either during Bid evaluation, post-qualification or the execution of the Contract may be regarded as fraudulent and render the Bidder or supplier liable for prosecution subject to the applicable laws and issuances.]*

Item	Specification	Statement of Compliance
1	<p><b>PENETRATION TESTING PLATFORM</b></p> <p><b>A.1.1 Installation, Deployment and Integration</b></p> <ul style="list-style-type: none"> <li>• Solution must be able to support installation on 64-bit Linux and Windows (64-bit).</li> <li>• Solution must have latest updates (e.g. exploit module) as frequent as on a weekly basis.</li> <li>• Solution must support offline activation and manual updates.</li> <li>• Solution must be able to perform full backup to prevent data loss and enable to easily migrate data.</li> </ul> <p><b>A.1.2 Administration</b></p> <ul style="list-style-type: none"> <li>• Solution must include web-based user interface through encrypted channels.</li> <li>• Solution must support command line console within.</li> <li>• Solution must allow API integration with other systems or be able to automate workflow.</li> <li>• Solution must be able to run jobs or tasks (e.g. scan, exploit) on schedule.</li> </ul> <p><b>A.1.3 Host Scan and Web Scan</b></p> <ul style="list-style-type: none"> <li>• Solution can conduct scans and discover the host's OS and running services.</li> </ul>	

- Solution can support customized nmap command for scan.
- Solution can support dry runs to show the scan information in task log only.
- Solution must be able to integrate with Nexpose to discover host's OS, running services and vulnerabilities via existing scan results or new scans.
- Solution must support automatic tag by OS
- Solution must support importing of scan result from external solutions including but not limited to: Nexpose, Metasploit, Foundstone, Microsoft, nCircle, NetSparker, Nessus, Qualys, Burp, Acunetix, AppScan, Nmap, Retina, Amap, Critical Watch, IP Address List, Libpcap, Spiceworks and Core Impact.

#### **A.1.4 System Exploitation**

- Solution must be able to apply exploits on individual IP or multiple IPs.
- Solution can automatically select and apply exploit modules based on OS, service and vulnerability references.
- Solution must have at least 6 reliability levels of exploit codes for automated exploitation.
- Solution must support running individual exploit module manually from the user interface.
- Solution must support dry run to show exploit information in task log only.
- Solution must support replay of exploitation tasks.
- Solution must support automation of common yet complicated security tests (Metamodules) that provide a more efficient way to get specific jobs done.
- Solution must support the reuse of manually added or captured credentials within a project to validate specified credentials on additional hosts in the target network.

#### **A.1.5 Bruteforcing**

- Solution can support brute force testing on services including but not limited to AFP, SMB, Postgres, DB2, MySQL, MSSQL, HTTP, HTTPS, SSH, SSH PUBKEY, Telnet, FTP, POP3, VNC, SNMP, WinRM.

- Solution can provide password references for factory default logins.
- Solution can support customized credentials and dictionary import for brute force and or dictionary attack.
- Solution can support credential mutation to create multiple permutations of a specified password, which enables building of a larger list based on a defined set of passwords.

#### **A.1.6 Post Exploitation Action and Evidence Collection**

- Solution must support exploitation payload types including but not limited to: “Meterpreter”, “Command Shell” and "Powershell".
- Solution must support customized macros to run selected operations automatically after exploit.
- Solution must support post exploitation actions including but not limited to collect system data (screen capture, password, system information), build a virtual desktop connection, access file system, search the file system, run a command shell, create proxy pivot, create VPN pivot.
- Solution must support deploying of persistent listeners to allow exploited hosts to connect back to the penetration testing platform automatically.

#### **A.1.7 Social Engineering Campaign**

- Solution must support web campaign, Email campaign and USB campaign.
- Solution must allow web campaign customized with http/https, IP address, port and path (e.g. <https://www.abc.com:1234/abcd>).
- Solution must support web content to be cloned from another web site (e.g. [www.google.com](http://www.google.com)).
- Solution must support web campaign that browser autopwn (apply all the appropriate exploit modules based on the browser version), specific browser exploit (e.g. MS11-050) and not do anything (just checking the connection from the users).
- Solution must support email campaign content customization to include a specific URL or an agent attachment.
- Solution must support USB campaign that generates an agent deployment .exe file.

### **A.1.8 Web Application Exploitation**

- Solution must support web crawling on IPv4 and IPv6 web sites.
- Solution must support web crawling applied on a web site (e.g. <http://www.abc.com>) or started from a specific point (e.g. <http://www.abc.com/path/starthere/>).
- Solution must support detection of vulnerable URLs and parameters such as SQL Injection and Cross Site Scripting.

### **A.1.9 Report and Data Export**

- Solution must provide built-in standard reports and support customized report functionality.
- Solution must provide at least 10 built-in standard reports.
- Solution must support report formats including but not limited to PDF, Word, RTF and HTML.
- Solution must support reports to be stored locally and sent to recipient by email after created.
- Solution must be able to support data export which allows a zip archive of the project suitable for importing into another instance of the solution.

### **A.1.10 Other Requirements**

- Bidder/Supplier should be authorized by the Manufacturer to negotiate, and/or to bid and/or to sell.
- Software license must be compatible with the current penetration testing software for renewal for One (1) year.
- Bidder/Supplier should have at least two (2) Government contracts in relation to Digital or Computer Forensics with satisfactory performance.
- Supplier should provide a minimum of 1-2 days of hands-on training on the use, analysis, and administration of the software.
- Delivery schedule: 30 working days from receipt of Purchase Order / Contract / Notice to Proceed

2	<p><b>CLOUD ANALYZER SOFTWARE / MOBILE FORENSIC CLOUD ANALYSIS AND INVESTIGATION SOFTWARE</b></p> <p>The renewal of the Commission’s existing Cloud Analysis and Investigation Software License <b>SHOULD MEET THE FOLLOWING SPECIFICATIONS:</b></p> <ul style="list-style-type: none"> <li>• Software licenses must be compatible with the current mobile forensic cloud analyzer system software for renewal</li> <li>• Inclusive of One (1) Year Maintenance Systems</li> <li>• Software shall allow gathering user data from popular social media and cloud-based sources.</li> <li>• Able to collect and hash digital evidence from HTML-based web pages.</li> <li>• Can enable the user to view user search history and gather geo-location data.</li> <li>• Able to normalize and sort data into different formats</li> <li>• Can generate easy-to-read reports available in different formats like PDF for entire data sets or filtered information</li> <li>• Support reporting of extracted data from the cloud to a machine-readable format so it can be digested by other analysis systems.</li> <li>• Supplier should have a local partner to provide immediate post-sales support</li> <li>• Supplier should have Manufacturer’s Authorization to supply and support the renewal of the said license. Supplier should have at least Two (2) government contracts with satisfactory performance for the same product or digital forensic.</li> </ul> <p><b>Qualification Requirements</b></p> <ul style="list-style-type: none"> <li>• Direct contracting supplier must provide a price quotation or a pro-forma invoice together with the conditions of sale.</li> <li>• Must provide a certificate or proof being the duly authorized or sole distributor (provider) of the said Software(s).</li> <li>• Inclusive of One (1) Year Maintenance Systems per software as stipulated on Section (III)(A), unless explicitly stated.</li> <li>• Provider must provide basic training for all software subscriptions.</li> <li>• Supplier should have a local partner to provide immediate post-sales support.</li> </ul>	
---	---	--



	<ul style="list-style-type: none"> <li>• Supplier should have Manufacturer’s Authorization to supply and support the renewal of software licenses.</li> <li>• Supplier should have at least Two (2) government contracts with satisfactory performance for the software(s) stipulated on Section (III)(A).</li> <li>• Supplier should provide a minimum of 1-2 days of hands-on training on the use, analysis, and administration of the software.</li> <li>• Delivery schedule: 30 working days from receipt of Purchase Order / Contract / Notice to Proceed</li> </ul>	
3	<p><b>DIGITAL FORENSIC INVESTIGATION SOFTWARE</b></p> <p>The renewal of the Commission’s existing Digital Forensic Investigation Software License <b>SHOULD MEET THE FOLLOWING SPECIFICATIONS:</b></p> <p>Software licenses must be compatible with the current digital forensic investigation software for renewal</p> <p>Inclusive of One (1) Year Maintenance Systems</p> <p>Capable of acquiring data in a forensically sound manner using software accepted by courts worldwide.</p> <p>Capable of investigating and analyzing data from multiple platforms such as Windows, Linux, AIX, OS X, Solaris, and more—using a single tool.</p> <p>Capable of finding information despite attempt to hide, cloak, or delete data</p> <p>Capable of easily managing large volumes of computer evidence, viewing all relevant files, including deleted files, file slack, and unallocated space.</p> <p>Capable of creating exact duplicates of original data and verifying by hash and error check.</p> <p>Capable of transferring evidence files directly to law enforcement or legal representatives.</p> <p>Capable of providing review options that allow non-investigators, such as attorneys, to review evidence with ease.</p>	

	<p>Capable of providing reporting options for quick report preparation.</p> <p>Supplier should have a local partner to provide immediate post-sales support</p> <p>Supplier should have Manufacturer’s Authorization to supply and support the renewal of the said license.</p> <p>Supplier should have at least Two (2) government contracts with satisfactory performance for the same product or digital forensic.</p> <p>Supplier should provide a minimum of 1-2 days of hands-on training on the use, analysis, and administration of the software.</p> <p>Delivery schedule: 30 working days from receipt of Purchase Order / Contract / Notice to Proceed</p>	
4	<p><b>MOBILE FORENSIC APPLICATION</b></p> <p>The renewal of the Commission’s existing Mobile Forensic Investigation Device License <b>SHOULD MEET THE FOLLOWING SPECIFICATIONS:</b></p> <p>Software licenses must be compatible with the current mobile forensic investigation device software for renewal</p> <p>Inclusive of One (1) Year Maintenance Systems</p> <p>One (1) Year support on mobile connector tips and cables</p> <p>Inclusive of decoding, analysis and report generation software license</p> <p>Capable of Bypassing pattern, password or PIN locks.</p> <p>Capable of extracting physical, file system, and logical data from smartphones, feature phones, tablets, players, GPS devices, SIM cards, smart watches, mass storage devices, drones and other devices with memory storage to access live, hidden and even deleted data.</p> <p>Capable of displaying and visualizing data in a unified format to build timelines and maps and more easily see relevant connections</p>	

	<p>Can generate easy-to-read reports available in different formats like PDF for entire data sets or filtered information.</p> <p>Supplier should have a local partner to provide immediate post-sales support.</p> <p>Supplier should have Manufacturer’s Authorization to supply and support the renewal of the said license.</p> <p>Supplier should have at least Two (2) government contracts with satisfactory performance for the same product or digital forensic.</p> <p>Supplier should provide a minimum of 1-2 days of hands-on training on the use, analysis, and administration of the software.</p> <p>Delivery schedule: 30 working days from receipt of Purchase Order / Contract / Notice to Proceed</p>	
5	<p><b>SYSTEM VULNERABILITY ASSESSMENT SOFTWARE</b></p> <p>The renewal of the Commission’s existing Vulnerability Assessment Software <b>SHOULD MEET THE FOLLOWING SPECIFICATIONS:</b></p> <p>Software licenses must be compatible with the current vulnerability assessment software for renewal</p> <p>Inclusive of One (1) Year Maintenance Systems</p> <p>Capable of operating 100% on-premises. Scan results should always be available on premise. Describe the solution's architecture. Detail all components and modules required to deliver the complete solution.</p> <p>Must be offered as either Software Product or Software as a Service.</p> <p>Must support at least the below mentioned supported platforms as OS: Ubuntu Linux LTS, Microsoft Windows Server, Microsoft Windows and Red Hat Enterprise Linux Server</p> <p>Must have the capability to perform both internal and external scanning.</p>	

	<p>Must include web-based management user interface over encrypted traffics. It must not be accessed in clear text.</p> <p>Must support having scan engine pooling with multiple engines grouped together to run any single scan to reduce and improve scanning time by load sharing.</p> <p>Supplier should have a local partner to provide immediate post-sales support.</p> <p>Supplier should have Manufacturer's Authorization to supply and support the renewal of the said license.</p> <p>Supplier should have at least Two (2) government contracts with satisfactory performance for the same product.</p> <p>Supplier should provide a minimum of 1-2 days of hands-on training on the use, analysis, and administration of the software.</p> <p>Delivery schedule: 30 working days from receipt of Purchase Order / Contract / Notice to Proceed</p>	
--	--	--

*I hereby undertake to comply and deliver all the above requirements.*

\_\_\_\_\_

**Company Name**

\_\_\_\_\_

**Name and Signature of Authorized Representative**

\_\_\_\_\_

**Date**

***Section VIII. Checklist of Technical and  
Financial Documents***

# Checklist of Technical and Financial Documents

## I. TECHNICAL COMPONENT ENVELOPE

### *Class “A” Documents*

#### Legal Documents

- (a) Valid PhilGEPS Registration Certificate (Platinum Membership) (all pages);  
**or**
- (b) Registration certificate from Securities and Exchange Commission (SEC), Department of Trade and Industry (DTI) for sole proprietorship, or Cooperative Development Authority (CDA) for cooperatives or its equivalent document,  
**and**
- (c) Mayor’s or Business permit issued by the city or municipality where the principal place of business of the prospective bidder is located, or the equivalent document for Exclusive Economic Zones or Areas;  
**and**
- (d) Tax clearance per E.O. No. 398, s. 2005, as finally reviewed and approved by the Bureau of Internal Revenue (BIR).

#### Technical Documents

- (e) Statement of the prospective bidder of all its ongoing government and private contracts, including contracts awarded but not yet started, if any, whether similar or not similar in nature and complexity to the contract to be bid; **and**
- (f) Statement of the bidder’s Single Largest Completed Contract (SLCC) similar to the contract to be bid, except under conditions provided for in Sections 23.4.1.3 and 23.4.2.4 of the 2016 revised IRR of RA No. 9184, within the relevant period as provided in the Bidding Documents; **and**
- (g) Original copy of Bid Security. If in the form of a Surety Bond, submit also a certification issued by the Insurance Commission;  
**or**  
Original copy of Notarized Bid Securing Declaration (*see attached template*); **and**
- (h) Conformity with the Technical Specifications, which may include production/delivery schedule, manpower requirements, and/or after-sales/parts, if applicable; **and**
- (i) Original duly signed Omnibus Sworn Statement (OSS) (*see attached template*);  
**and** if applicable, Original Notarized Secretary’s Certificate in case of a corporation, partnership, or cooperative; or Original Special Power of Attorney of all members of the joint venture giving full power and authority to its officer to sign the OSS and do acts to represent the Bidder.

#### Financial Documents

- (j) The Supplier’s audited financial statements, showing, among others, the Supplier’s total and current assets and liabilities, stamped “received” by the BIR or its duly accredited and authorized institutions, for the preceding calendar year which should not be earlier than two (2) years from the date of bid submission; **and**

- (k) The prospective bidder's computation of Net Financial Contracting Capacity (NFCC);  
**OR**  
A committed Line of Credit from a Universal or Commercial Bank in lieu of its NFCC computation.

***Class "B" Documents***

- (l) If applicable, a duly signed joint venture agreement (JVA) in case the joint venture is already in existence;  
**OR**  
duly notarized statements from all the potential joint venture partners stating that they will enter into and abide by the provisions of the JVA in the instance that the bid is successful.

**II. FINANCIAL COMPONENT ENVELOPE**

- (m) Original of duly signed and accomplished Financial Bid Form; **and**  
 (n) Original of duly signed and accomplished Price Schedule(s).

**Other documentary requirements under RA No. 9184 (as applicable)**

- (o) *[For foreign bidders claiming by reason of their country's extension of reciprocal rights to Filipinos]* Certification from the relevant government office of their country stating that Filipinos are allowed to participate in government procurement activities for the same item or product.  
 (p) Certification from the DTI if the Bidder claims preference as a Domestic Bidder or Domestic Entity.





## **Bid Securing Declaration Form**

*[shall be submitted with the Bid if bidder opts to provide this form of bid security]*

---

REPUBLIC OF THE PHILIPPINES)  
CITY OF \_\_\_\_\_) S.S.

### **BID SECURING DECLARATION** **Project Identification No.: *[Insert number]***

To: *[Insert name and address of the Procuring Entity]*

I/We, the undersigned, declare that:

1. I/We understand that, according to your conditions, bids must be supported by a Bid Security, which may be in the form of a Bid Securing Declaration.
2. I/We accept that: (a) I/we will be automatically disqualified from bidding for any procurement contract with any procuring entity for a period of two (2) years upon receipt of your Blacklisting Order; and, (b) I/we will pay the applicable fine provided under Section 6 of the Guidelines on the Use of Bid Securing Declaration, within fifteen (15) days from receipt of the written demand by the procuring entity for the commission of acts resulting to the enforcement of the bid securing declaration under Sections 23.1(b), 34.2, 40.1 and 69.1, except 69.1(f), of the IRR of RA No. 9184; without prejudice to other legal action the government may undertake.
3. I/We understand that this Bid Securing Declaration shall cease to be valid on the following circumstances:
  - a. Upon expiration of the bid validity period, or any extension thereof pursuant to your request;
  - b. I am/we are declared ineligible or post-disqualified upon receipt of your notice to such effect, and (i) I/we failed to timely file a request for reconsideration or (ii) I/we filed a waiver to avail of said right; and
  - c. I am/we are declared the bidder with the Lowest Calculated Responsive Bid, and I/we have furnished the performance security and signed the Contract.

IN WITNESS WHEREOF, I/We have hereunto set my/our hand/s this \_\_\_\_ day of *[month]* *[year]* at *[place of execution]*.

*[Insert NAME OF BIDDER OR ITS AUTHORIZED  
REPRESENTATIVE]*

*[Insert signatory's legal capacity]*

Affiant

### **[Jurat]**

*[Format shall be based on the latest Rules on Notarial Practice]*

## Omnibus Sworn Statement (Revised)

*[shall be submitted with the Bid]*

---

REPUBLIC OF THE PHILIPPINES )  
CITY/MUNICIPALITY OF \_\_\_\_\_ ) S.S.

### AFFIDAVIT

I, [Name of Affiant], of legal age, [Civil Status], [Nationality], and residing at [Address of Affiant], after having been duly sworn in accordance with law, do hereby depose and state that:

1. *[Select one, delete the other:]*

*[If a sole proprietorship:]* I am the sole proprietor or authorized representative of [Name of Bidder] with office address at [address of Bidder];

*[If a partnership, corporation, cooperative, or joint venture:]* I am the duly authorized and designated representative of [Name of Bidder] with office address at [address of Bidder];

2. *[Select one, delete the other:]*

*[If a sole proprietorship:]* As the owner and sole proprietor, or authorized representative of [Name of Bidder], I have full power and authority to do, execute and perform any and all acts necessary to participate, submit the bid, and to sign and execute the ensuing contract for [Name of the Project] of the [Name of the Procuring Entity], as shown in the attached duly notarized Special Power of Attorney;

*[If a partnership, corporation, cooperative, or joint venture:]* I am granted full power and authority to do, execute and perform any and all acts necessary to participate, submit the bid, and to sign and execute the ensuing contract for [Name of the Project] of the [Name of the Procuring Entity], as shown in the attached [state title of attached document showing proof of authorization (e.g., duly notarized Secretary's Certificate, Board/Partnership Resolution, or Special Power of Attorney, whichever is applicable)];

3. [Name of Bidder] is not "blacklisted" or barred from bidding by the Government of the Philippines or any of its agencies, offices, corporations, or Local Government Units, foreign government/foreign or international financing institution whose blacklisting rules have been recognized by the Government Procurement Policy Board, **by itself or by relation, membership, association, affiliation, or controlling interest with another blacklisted person or entity as defined and provided for in the Uniform Guidelines on Blacklisting;**

4. Each of the documents submitted in satisfaction of the bidding requirements is an authentic copy of the original, complete, and all statements and information provided therein are true and correct;

5. [Name of Bidder] is authorizing the Head of the Procuring Entity or its duly authorized representative(s) to verify all the documents submitted;

6. *[Select one, delete the rest:]*

*[If a sole proprietorship:]* The owner or sole proprietor is not related to the Head of the Procuring Entity, members of the Bids and Awards Committee (BAC), the Technical

Working Group, and the BAC Secretariat, the head of the Project Management Office or the end-user unit, and the project consultants by consanguinity or affinity up to the third civil degree;

*[If a partnership or cooperative:]* None of the officers and members of *[Name of Bidder]* is related to the Head of the Procuring Entity, members of the Bids and Awards Committee (BAC), the Technical Working Group, and the BAC Secretariat, the head of the Project Management Office or the end-user unit, and the project consultants by consanguinity or affinity up to the third civil degree;

*[If a corporation or joint venture:]* None of the officers, directors, and controlling stockholders of *[Name of Bidder]* is related to the Head of the Procuring Entity, members of the Bids and Awards Committee (BAC), the Technical Working Group, and the BAC Secretariat, the head of the Project Management Office or the end-user unit, and the project consultants by consanguinity or affinity up to the third civil degree;

7. *[Name of Bidder]* complies with existing labor laws and standards; and
8. *[Name of Bidder]* is aware of and has undertaken the responsibilities as a Bidder in compliance with the Philippine Bidding Documents, which includes:
  - a. Carefully examining all of the Bidding Documents;
  - b. Acknowledging all conditions, local or otherwise, affecting the implementation of the Contract;
  - c. Making an estimate of the facilities available and needed for the contract to be bid, if any; and
  - d. Inquiring or securing Supplemental/Bid Bulletin(s) issued for the *[Name of the Project]*.
9. *[Name of Bidder]* did not give or pay directly or indirectly, any commission, amount, fee, or any form of consideration, pecuniary or otherwise, to any person or official, personnel or representative of the government in relation to any procurement project or activity.
10. **In case advance payment was made or given, failure to perform or deliver any of the obligations and undertakings in the contract shall be sufficient grounds to constitute criminal liability for Swindling (Estafa) or the commission of fraud with unfaithfulness or abuse of confidence through misappropriating or converting any payment received by a person or entity under an obligation involving the duty to deliver certain goods or services, to the prejudice of the public and the government of the Philippines pursuant to Article 315 of Act No. 3815 s. 1930, as amended, or the Revised Penal Code.**

IN WITNESS WHEREOF, I have hereunto set my hand this \_\_\_ day of \_\_\_, 20\_\_ at \_\_\_\_\_, Philippines.

*[Insert NAME OF BIDDER OR ITS AUTHORIZED REPRESENTATIVE]*

*[Insert signatory's legal capacity]*

Affiant

**[Jurat]**

*[Format shall be based on the latest Rules on Notarial Practice]*