PhilGEPS
Philippine Government Electronic Procurement System
Central Portal for Philippine Government Procurement Oppurtunities

Help

# Bid Notice Abstract

## Request for Quotation (RFQ)

| | |
|---|---|
| **Reference Number** | 10400226 |
| **Procuring Entity** | MARITIME INDUSTRY AUTHORITY (MARINA) |
| **Title** | PROCUREMENT OF IT SECURITY SOLUTIONS |
| **Area of Delivery** | Metro Manila |

| | |
|---|---|
| **Solicitation Number:** | 2023-11-542 |
| **Trade Agreement:** | Implementing Rules and Regulations |
| **Procurement Mode:** | Negotiated Procurement - Small Value Procurement (Sec. 53.9) |
| **Classification:** | Goods - General Support Services |
| **Category:** | Information Technology |
| **Approved Budget for the Contract:** | PHP 1,000,000.00 |
| **Delivery Period:** | 30 Day/s |
| **Client Agency:** | |
| **Contact Person:** | ATTY. SHARON L. DE CHAVEZ - ALEDO<br>The BAC Chairperson<br>c/o BAC Office,10th Floor,MARINA Bldg.<br>A. Bonifacio Drive cor. 20th Street,<br>Port Area<br>Manila<br>Metro Manila<br>Philippines 1018<br>63-2-85246518<br><br>bacsec@marina.gov.ph |

| | |
|---|---|
| **Status** | **Pending** |
| **Associated Components** | 1 |
| **Bid Supplements** | 0 |
| **Document Request List** | 0 |
| **Date Published** | 07/12/2023 |
| **Last Updated / Time** | 06/12/2023 13:22 PM |
| **Closing Date / Time** | 11/12/2023 12:00 PM |

**Description**

PROCUREMENT OF IT SECURITY SOLUTIONS

Please see attached files or you may visit https://marina.gov.ph/small-value-procurement/

All submission in response to the RFQ shall be in hard copy with fresh signature only. Submission in electronic copies shall not be entertained.

| | |
|---|---|
| **Created by** | ATTY. SHARON L. DE CHAVEZ - ALEDO |
| **Date Created** | 06/12/2023 |

The PhilGEPS team is not responsible for any typographical errors or misinformation presented in the system. PhilGEPS only displays information provided for by its clients, and any queries regarding the postings should be directed to the contact person/s of the concerned party.

REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF TRANSPORTATION
MARITIME INDUSTRY AUTHORITY

## REQUEST FOR QUOTATION

DATE: __________

*Name of Company :* ______________________________

*Address :* ______________________________

*Business Permit Number :* ______________________________

*Company TIN :* ______________________________

*PhilGEPS Registration Number (required):* ______________________

*Name of Representative & Designation :* ______________________

The **Maritime Industry Authority (MARINA)** through its Bids and Awards Committee (BAC), intends to procure **IT SECURITY SOLUTIONS** in accordance with Section 53.9 (Small Value Procurement) of the 2016 Revised Implementing Rules and Regulations of Republic Act No. 9184. The Approved Budget for the Contract (ABC) is ***One Million Pesos (P1,000,000.00)***. The period for the performance of the obligations shall not go beyond of the appropriations for this Procurement Project.

Please quote your **best offer** for the item/s described herein, **subject to the Terms and Conditions** provided at the last page of this Request for Quotation (RFQ). Submit your quotation duly signed by your representative **not later than** 11 **December 2023** at the MARINA BAC Office located at 10th Floor MARINA Building, Bonifacio Drive cor., 20th Street, Port Area, Manila, Philippines.

A copy of the following are required to be submitted along with your signed quotation/proposal:

- Valid Business/Mayor's Permit
- Valid PhilGEPS Registration
- Latest Income/ Business Tax Return
- Notarized Omnibus Sworn Statement (with SPA or Secretary Certificate, whichever is applicable)
- Proof of at least two (2) experience in supplying IT Security related projects.
- Proof of at least two (2) Client Satisfactory Certificates related to IT Security.

For any clarification, you may contact Ms. Ellerie Torrente or Ms. Kristen Nicole Velasco at telephone no. **(+632) 8524-6518** or email address at **bacsec@marina.gov.ph**

**ATTY. SHARON D. ALEDO**
BAC Chairperson

## INSTRUCTIONS:

**(1)** Accomplish this RFQ correctly and accurately.
**(2)** Do not alter the content of this form in any way.
**(3)** All technical specifications are mandatory. Failure to comply with any of the mandatory requirements will disqualify your quotation.
**(4)** Failure to follow these instructions will disqualify your entire quotation.

Supplier's must state here either "**Comply**" or **any equivalent term** in the column "Supplier's Statement of Compliance" against each of the individual parameters of each specification. Please quote your **best offer** for the item/s below. Please do not leave any blank items. Indicate "**0**" if item being offered is for free.

After having carefully read and accepted the Terms and Conditions in the Request for Quotation, hereunder is our quotation for the item/s as follows:

## *PROCUREMENT OF IT SECURITY SOLUTION*

| Item No. | Description/Technical Specifications | | Supplier's Statement of Compliance | Unit Cost (VAT inclusive) | Total Cost (VAT inclusive) |
|---|---|---|---|---|---|
| | **FEATURES** | | | | |
| | Zero Day | Should be able to protect against zero-day vulnerability | | | |
| | OWASP Top 10 | Should be able to protect against the OWASP top 10 | | | |
| | Detection Speed | Should be able to defend and take action within milliseconds | | | |
| | Solution type | The solution should have a **memory based sensor** which should protect the server. It should not be just a host based agent. | | | |
| | Input Validation for Just-In-Time compiled web applications | Should be able to compare the user input to the output produced by various compilers (SQL, XML, OS, Java, etc.) in the application in **real time**. | | | |
| | Control Flow monitoring of pre-compiled applications | Should be able to look into the application flow at **runtime** and Control the application Flow Integrity for the binary code. | | | |
| | Stateful Analysis | Should be able to do Stateful processing of HTTP Pipeline in case of interpreted code. | | | |
| | White Listing Model | The whitelisting model should be based on developer intent and should not be based on a tedious learning model. | | | |

| | | | | | |
|---|---|---|---|---|---|
| | Air Gapped Compatibility | Should be a fit for a deployment in an Air Gapped environment with at least the below features<br>a) Should not send any information outside the network premises for sandboxing or what so ever.<br>b) Should be able to work without any signature updates. The protection capabilities should not be compromised in the process.<br>Once Installed all the native protection capabilities of the solution should be fully functional without connecting to the internet. Please mention in detail if there are any exceptions to this. | | | |
| | Preemptive Patching | Should be able to protect unpatched Windows Linux OS & third party Application & its processes against unknown and zero day attacks without the need any for any signatures of any form. All attacks should be terminated within milliseconds | | | |
| | Security for web Layer attacks / Interpreted code | • Should be able to protect against serialization and de-serialization attacks for Java and other interpreters.<br>• Should be able to report patterns used as payloads by the attacker and a correlated information on query executed at the application/database layer<br>• Should be able to capture session id, user id, ip details from the http stream during the attack.<br>• Should be able to provide on demand logs for analysis of attack at every layer - webserver, application and database layer<br>• Should be able to provide customization feature such that for attacks detected by the solution which got undetected by other security solutions in the network it should be able to provide signatures as a feedback loop. | | | |

|  |  |  |  |  |  |
|---|---|---|---|---|---|
|  | Deep memory visibility into Applications at run time | • Should be able to detect runtime flaws like Buffer errors that can lead to remote code exploitation of victim machine<br>• Detect attacks even when network or application behavioral or heuristic signatures fail to detect attacks<br>• Produces near zero false positives<br>• Provides SIEM with high confidence IOCs that help analysts establish detailed forensics<br>• Reduces dwell time of attackers to milliseconds |  |  |  |
|  | Protection against zero days. | Prevent malware (even those that have no signatures in industry standard reputation gateways like Virus Total, Reversing Labs etc.) from getting started |  |  |  |
|  | Protection on various Platforms | Protects in-premise, cloud or hybrid applications running on bare metal or VMs equally well |  |  |  |
|  | Host based Security | • Should be able to monitor running processes<br>• Should be able to provide customization feature such that for attacks detected by the solution which got undetected by other security solutions in the network it should be able to provide malicious file hash so that it serves as a feedback loop and makes the other security solutions smarter.<br>• Should monitor and protect the file system for important OS and application files on server based on automated and continuous baselining of known good files. |  |  |  |
|  | **NOTIFICATION AND LOGGING** |  |  |  |  |
|  | Syslog Server | Should be able to send logs to the syslog server |  |  |  |
|  | SMS notification | Should be able to send notification via sms at near real time about the attacks and threats |  |  |  |
|  | Email Notification | Should be able to send notification about the attacks and threats via email |  |  |  |

| | | | | | |
|---|---|---|---|---|---|
| | Reporting & Logging | Should be able log evidence on non-writeable media directly like worm drive so that bad actors are not able to delete logs and hence not able to defeat forensic investigations | | | |
| | Compliance Reporting | Compliance reporting - User, IP, URL etc. should be able to report at least the below transaction on which attack occurs<br>(i) User<br>(ii) IP<br>(iii) URL<br>(iv) Process<br>(vi) PID<br>(vii) original application memory address<br>(viii) memory address pointer changed based on attack | | | |
| | **MANAGEABILITY** | | | | |
| | GUI | Should have a single GUI to manage the entire solution | | | |
| | Integrations | Should have the provision to leverage existing security infra with minimal customization | | | |
| | Complied Code | Should be able to protect against compiled code of 1st and 3rd party applications without requiring the source code | | | |
| | Interpreted Code | Should be able to protect against interpreted code of 1st and 3rd party applications without requiring the source code | | | |
| | Memory Attacks | Should be able to protect all the server application processes from process memory attacks without requiring the source code. | | | |
| | False Positive | • Should have 100% true positive and negligible to zero false positive<br>• The solution should be able to differentiate between a threat and an attack without raising false alarms | | | |
| | **SCALABILITY** | | | | |
| | Sizing | should be able to protect up to X number of servers in the datacenter | | | |
| | Ease of Deployment | Should be easy to deploy | | | |

| | | | | | |
|---|---|---|---|---|---|
| | Ease of Manageability | Once Deployed and configured for an application it should not require professional help to manage and configure day to day policies | | | |
| | **SUPPORTED APPLICATIONS FOR INSTRUMENTATION** | | | | |
| | Memory based File-less attack | • Should be able to instrument and protect any java or .net framework based applications without causing any disruption to the normal working of the application and in specific the below.<br>• Should be able to protect IIS, Apache etc. servers | | | |
| | | Should have options to customize actions based on custom scripts written by user and by default have at least the below actions parameters<br>a) Process ID<br>b) Thread ID<br>c) Attacker IP<br>d) Attacker Port<br>e) Script | | | |
| | **III. Warranty**<br>The warranty shall be for a period of One (1) year. | | | | |
| | **Support**<br>- The Bidder shall provide daily 8 by 5 phone, email, and remote support with critical level onsite assistance<br>- The Bidder must have access to high-level of support via the principal for critical level concerns<br>- The Bidder must provide professional implementation services<br>- The Bidder must provide a monthly health check during the subscription period to ensure that the product is properly working | | | | |

Signature over Printed Name

Position/Designation

Office Telephone No.

Fax/Mobile No.

Email Address/es

# SCHEDULE OF REQUIREMENTS

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

| Item No. | Description | Delivery Schedule | Supplier's Statement of Compliance |
|---|---|---|---|
| 1 LOT | **PROCUREMENT OF IT SECURITY SOLUTION** | Thirty (30) Working Days upon Receipt of Purchase Order/Notice to Proceed. | |
| | a. Valid Business/Mayor's Permit<br>b. Valid PhilGEPS Registration<br>c. Latest Income/ Business Tax Return<br>d. Notarized Omnibus Sworn Statement (with SPA or Secretary Certificate, whichever is applicable)<br>e. Proof of at least two (2) experience in supplying IT Security related projects.<br>f. Proof of at least two (2) Client Satisfactory Certificates related to IT Security. | **Required to be submitted along with your signed quotation/ proposal** | |

Signature over Printed Name

Position/Designation

Office Telephone No.

Fax/Mobile No.

Email Address/es

| **FINANCIAL OFFER** | |
|---|---|
| **Approved Budget for the Contract** | **Total Offered Quotation** |
| **One Million Pesos**<br>**(P1,000,000.00)** | In words: ____________________<br>________________________________<br>________________________________<br>________________________________<br>In figures: ____________________<br>________________________________<br>________________________________<br>________________________________ |

| | |
|---|---|
| ***Terms of Payment:*** | Payment shall be made thirty (30) days upon the receipt of the Billing Statement and on a Bank-to-Bank basis.<br>In case of Automatic Debit Arrangement (ADA) through Land Bank of the Philippines (LBP) facilities, or other Commercial Banks, the applicable bank charges shall be for the account of the supplier. The supplier shall submit bank details together with billing statement/ invoice for ready reference. |
| Banking Institution: | |
| Account Number: | |
| Account Name: | |
| Branch: | |

____________________________
Signature over Printed Name

____________________________
Position/Designation

____________________________
Office Telephone No.

____________________________
Fax/Mobile No.

____________________________
Email Address/es

## TERMS AND CONDITIONS:

1. Bidders shall provide correct and accurate information required in this form.

2. Price quotation/s must be valid for a period of *thirty (30) calendar days* from the date of submission.

3. Price quotation, denominated in Philippine peso, shall include all taxes, duties and/or other charges payable relative to the items described in the RFQ.

4. Quotations exceeding the Approved Budget for the Contract shall be rejected.

5. **All submission in response to the RFQ shall be in hard copy with fresh signature only. Submission in electronic copies shall not be entertained.**

6. Award of contract shall be made to lowest calculated and responsive quotation (for goods and infrastructure) or, the highest rated offer (for consulting services) which complies with the minimum technical specifications and other terms and conditions stated herein.

7. Any interlineations, erasures or overwriting shall be valid only if they are signed or initialed by you or any of your duly authorized representative/s.

8. The item/s shall be delivered according to the requirements specified in the Technical Specifications.

9. The MARINA shall have the right to inspect and/or to test the goods to confirm their conformity to the technical specifications.

10. In case two or more bidders are determined to have submitted the Lowest Calculated Quotation/Lowest Calculated and Responsive Quotation, the MARINA-BAC shall adopt and employ "draw lots" as the tie-breaking method to finally determine the single winning provider in accordance with GPPB Circular 06-2005.

11. **Payment shall be processed after delivery and upon the submission of the required supporting documents, in accordance with existing accounting rules and regulations. Please note that the corresponding bank transfer fee, if any, shall be chargeable to the supplier's account.**

12. Liquidated damages equivalent to one tenth of one percent (0.1%) of value of the goods not delivered within the prescribed delivery period shall be imposed per day of delay. The MARINA shall rescind the contract once the cumulative amount of liquidated damages reaches ten percent (10%) of the amount of the contract without prejudice to other courses of action and remedies open to it.

______________________________
Signature over Printed Name

______________________________
Position/Designation

## TERMS OF REFERENCE
## IT SECURITY SOLUTION

### I. Background

The Maritime Industry Authority (MARINA) was created on 01 June 1974 as an attached Agency to the Office of the President (OP) with the issuance of Presidential Decree No. 474, otherwise known as the Maritime Industry Decree of 1974, to integrate the development, promotion and regulation of the maritime industry in the country and the creation of the Ministry (now Department) of Transportation (DOTr) by virtue of Executive Order No. 546, the MARINA was attached to the DOTr for policy and program coordination on 23 July 1979.By virtue of Republic Act No. 10635, the Maritime Industry Authority (MARINA) is established as the "Single Maritime Administration" responsible for the implementation and enforcement of the 1978 International Convention on Standards of Training, Certification and Watchkeeping for Seafarers, as amended, and International Agreements or Covenants related thereto.

The day-to-day operation of the Maritime Industry Authority's Standards Training, Certification and Seafarer Watchkeeping (STCW) depends on the reliability of IT equipment. Consider the accessibility of the online system for MARINA-STCW offices and stakeholders with little or no downtime.

### II. Objective

Gain assured runtime protection with the continuity to defend against evolving threats and known and unknown attacks automatically.

### III. Approved Budget Contract

The supplier shall bid for all items described in this Terms of reference, which shall not exceed the Approved Budget Contract (ABC) in the amount of One Million Pesos (1,000,000.00), inclusive of all applicable government charges.

### IV. Technical Specifications

| FEATURES | |
|---|---|
| Zero Day | Should be able to protect against zero-day vulnerability |
| OWASP Top 10 | Should be able to protect against the OWASP top 10 |
| Detection Speed | Should be able to defend and take action within milliseconds |
| Solution type | The solution should have a **memory-based sensor** which should protect the server. It should not be just a host-based agent. |
| Input Validation for Just-In-Time compiled web applications | Should be able to compare the user input to the output produced by various compilers (SQL, XML, OS, Java etc) in the application in **real time**. |

| | |
|---|---|
| Control Flow monitoring of pre-compiled applications | Should be able to look into the application flow at **runtime** and Control the application Flow Integrity for the binary code. |
| Stateful Analysis | Should be able to do Stateful processing of HTTP Pipeline in case of interpreted code. |
| White Listing Model | The whitelisting model should be based on developer intent and should not be based on a tedious learning model. |
| Air Gapped Compatibility | Should be a fit for a deployment in an Air Gapped environment with at least the below features<br>a) Should not send any information outside the network premises for sandboxing or what so ever.<br>B) Should be able to work without any signature updates. The protection capabilities should not be compromised in the process.<br>Once Installed all the native protection capabilities of the solution should be fully functional without connecting to the internet. Please mention in detail if there are any exceptions to this. |
| Preemptive Patching | Should be able to protect unpatched Windows Linux OS & third party Application & its processes against unknown and zero day attacks without the need any for any signatures of any form. All attacks should be terminated within milliseconds |
| Security for web Layer attacks / Interpreted code | • Should be able to protect against serialization and de-serialization attacks for Java and other interpreters.<br>• Should be able to report patterns used as payloads by the attacker and a correlated information on query executed at the application/database layer<br>• Should be able to capture session id, user id, ip details from the http stream during the attack.<br>• Should be able to provide on demand logs for analysis of attack at every layer - webserver, application and database layer<br>• Should be able to provide customization feature such that for attacks detected by the solution which got undetected by other security solutions in the network it should be able to provide signatures as a feedback loop. |
| Deep memory visibility into Applications at run time | • Should be able to detect runtime flaws like Buffer errors that can lead to remote code exploitation of victim machine<br>• Detect attacks even when network or application behavioral or heuristic signatures fail to detect attacks<br>• Produces near zero false positives |

| | |
|---|---|
| | - Provides SIEM with high confidence IOCs that help analysts establish detailed forensics<br>- Reduces dwell time of attackers to milliseconds |
| Protection against zero days. | Prevent malware (even those that have no signatures in industry standard reputation gateways like Virus Total, Reversing Labs etc.) from getting started |
| Protection on various Platforms | Protects in-premise, cloud or hybrid applications running on bare metal or VMs equally well |
| Host based Security | - Should be able to monitor running processes<br>- Should be able to provide customization feature such that for attacks detected by the solution which got undetected by other security solutions in the network it should be able to provide malicious file hash so that it serves as a feedback loop and makes the other security solutions smarter.<br>- Should monitor and protect the file system for important OS and application files on server based on automated and continuous baselining of known good files. |
| **NOTIFICATION AND LOGGING** | |
| Syslog Server | Should be able to send logs to the syslog server |
| SMS notification | Should be able to send notification via SMS at near real-time about the attacks and threats |
| Email Notification | Should be able to send notification about the attacks and threats via email |
| Reporting & Logging | Should be able log evidence on non-writeable media directly like worm drive so that bad actors are not able to delete logs and hence not able to defeat forensic investigations |
| Compliance Reporting | Compliance reporting - User, IP, URL etc. should be able to report at least the below transaction on which attack occurs<br>(i) User<br>(ii) IP<br>(iii) URL<br>(iv) Process<br>(vi) PID<br>(vii) original application memory address<br>(viii) memory address pointer changed based on attack |
| **MANAGEABILITY** | |
| GUI | Should have a single GUI to manage the entire solution |
| Integrations | Should have the provision to leverage existing security infra with minimal customization |

| | |
|---|---|
| Complied Code | Should be able to protect against compiled code of 1st and 3rd party applications without requiring the source code |
| Interpreted Code | Should be able to protect against interpreted code of 1st and 3rd party applications without requiring the source code |
| Memory Attacks | Should be able to protect all the server application processes from process memory attacks without requiring the source code. |
| False Positive | • Should have 100% true positive and negligible to zero false positive<br>• The solution should be able to differentiate between a threat and an attack without raising false alarms |
| **SCALABILITY** | |
| Sizing | should be able to protect up to X number of servers in the datacenter |
| Ease of Deployment | Should be easy to deploy |
| Ease of Manageability | Once Deployed and configured for an application it should not require professional help to manage and configure day to day policies |
| **SUPPORTED APPLICATIONS FOR INSTRUMENTATION** | |
| Memory based File-less attack | • Should be able to instrument and protect any java or .net framework based applications without causing any disruption to the normal working of the application and in specific the below.<br>• Should be able to protect IIS , Apache etc. servers |
| | Should have options to customize actions based on custom scripts written by user and by default have at least the below actions parameters<br>a) Process ID<br>b) Thread ID<br>c) Attacker IP<br>d) Attacker Port<br>e) Script |

## IV. Warranty

The warranty shall be for a period of One (1) year.

## V. Support

- The Bidder shall provide daily 8 by 5 phone, email, and remote support with critical level onsite assistance
- The Bidder must have access to high-level of support via the principal for critical level concerns

- The Bidder must provide professional implementation services
- The Bidder must provide a monthly health check during the subscription period to ensure that the product is properly working

## VI. Delivery

- Thirty (30) Working Days upon Receipt of Purchase Order/Notice to Proceed.

## VII. Qualification of the Supplier

- The Bidder must have at least two (2) experience in supplying IT Security related projects.
- The bidder should submit at least two (2) Client Satisfactory Certificates related to IT Security.

## VIII. Payment

- The payment can be made one-time fee annually upon issuance of the Billing Statement on a Bank-to-Bank basis. Automatic Debit Arrangement (ADA) through Land Bank of the Philippines (LBP) facilities, for other Commercial Bank, applicable bank charges shall be for the account of supplier. The supplier shall submit bank details together with billing statement/ invoice for ready reference.

**Prepared by:**

**DALMACIO L. GONZALES JR.**
Chief, ICTMD

**Recommending Approval:**

**SAMUEL L. BATALLA**
Executive Director,
STCW Office

**Reviewed by:**

FOR:
**JOHN E. GUARDAYA** 30 NOV 2023
Head, TWG for IT

30 nov
**Atty. SHARON D. ALEDO**
Chairperson, MARINA BAC

**APPROVED / ~~DISAPPROVED~~:**

**Atty. HERNANI N. FABIA**
Administrator

**Version 1 – October 13, 2023**

ASD NO.: 09-00
Initial Issue Date: 09-14-2023
Revision Date: 00

BAGONG PILIPINAS

MARINA

REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF TRANSPORTATION
MARITIME INDUSTRY AUTHORITY

# PURCHASE REQUEST

| | | |
|---|---|---|
| Office: **STCW OFFICE** | PR No.: | 2023-11-542 |
| Division/Section: **ICTMD** | SAI No.: | NOV 2 1 2023 |
| Date Request: | | |

| Item No. | Unit | Item Description | Quantity | Unit Cost | Total Cost |
|---|---|---|---|---|---|
| | LOT | **IT SECURITY SOLUTION** | 1 | 1,000,000.00 | 1,000,000.00 |
| | | | | | |
| ************ | ********* | ********************************** | *************** | ***************** | ****************** |
| | | | | | **1,000,000.00** |

WITH SUPPLEMENTAL TO PPMP
FY: 2023
MELLANIE T. BALIN 11/20/23
Chief, Administrative Officer

**Requisitioning Officer**

| | |
|---|---|
| Signature: | |
| Printed Name: | **SAMUEL L. BATALLA** |
| Designation | Executive Director<br>STCW Office |

Purpose:
To safeguard our organization's information technology (IT) infrastructure, data, and assets from various cyber threats and attacks. IT security solutions are implemented to ensure the confidentiality, integrity, and availability of sensitive information, as well as to protect against unauthorized access, data breaches, and other malicious activities.

**CERTIFICATION**

☑ FUNDS AVAILABLE
□ NO FUNDS AVAILABLE

**Atty. MARIVIC S. RAMOS**
Chief, Budget Division

□ Approved □ Disapproved

**PR Approver**

| | |
|---|---|
| Signature: | |
| Printed Name: | **Atty. HERNANI N. FABIA** |
| Designation | Administrator 11/22/23 |

***Note:***

## 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. **<u>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.</u>**

**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

*<u>[Jurat]</u>*
*[Format shall be based on the latest Rules on Notarial Practice]*