DOST-ASTI Bids and Awards Committee
REQUEST FOR QUOTATION

Kind of Procurement Activity:	Negotiated Procurement:Small-value Procurement		
Deadline of Submission of Bids:	Sep-20-2019, 2:00 PM		
RFQ No.:	19-09-2699	**Date:**	September-16-2019
PR No.:	GAA-19-08-8268	**Date:**	August-08-2019

The Department of Science and Technology (DOST) - Advanced Science and Technology Institute (ASTI), through its Bids and Awards Committee (BAC), intends to procure the item/s listed below. As such, suppliers, contractors, or distributors are invited to submit their quotation/s duly signed by authorized representative. Prospective bidder/s who will submit a proposal with the single/lowest calculated and responsive quotation shall be selected. Guidelines on the format and eligibility documents are listed at the box below the item/s to be procured.

Quotations may be sent via **a)** electronic mail at bac-sec@asti.dost.gov.ph, **b)** fax message, or **c)** delivering documents to the BAC Secretariat. For further inquiries, you may contact +63 2 249-8500 local 1206/1212 or +63 2 426-7423.

Thank you.

Respectfully,

PAUL JOHN M. SERRANO
Chairperson, BAC-2

NO.	TECHNICAL SPECIFICATIONS	QTY	UNIT	UNIT PRICE(Php)	TOTAL PRICE(Php)
1	**Cybersecurity Audit and Enhancement Services** charged to SAR with AIS project Contractor must provide the following services: a. Forensics and Incident Response - Contractor shall analyze past incident/s within the GRS and determine the root cause and associated timeline - Activities shall include, but are not limited to, the following: a.1. Log Analysis a.2. File System Analysis a.3. Full Disk Forensics a.4. Malware Analysis a.5. Timeline Generation b. Risk Assessment - Contractor shall assess the existing network infrastructure setup and create recommendations based on the needs of DOST-ASTI - Contractor shall also utilize the CIS Top 20 Critical Security Controls - Scope of work shall include, but are not limited to, the following: b.1. Identification - Identify individuals or roles who are associated with the relevant confidential/important data intended to be secure.	1	lot	900000.00	900,000.00

- Identify assets (hardware and software, both authorized and unauthorized) to develop baseline inventories.
- Review current documentation and policies for vulnerabilities and concurrence with industry best practices.
- Identify procedures that relate to the storage or transfer of confidential/important data.
- Identify statutory/regulatory compliance requirements (confidentiality, privacy, security).
- Identify core competencies & mission-critical business functions.

b.2. Comprehensive Assessment

- Interview those subjects identified previously to evaluate the strength of the Clients current controls.
- Evaluate items below to ensure security controls for data confidentiality, data integrity and data availability.

i. Workstation OS Deployment Guides
ii. Server OS Deployment Guides
iii. Network Segmentaiton
iv. Firewall Configuration
v. Remote Access
vi. External Exposure
vii. Eggress Traffic Policies
viii. Network Monitoring Capabilities
ix. Patching Strategies
x. Credential/Account Management

b.3. Report and Presentation

- Provide a detailed comprehensive security assessment report consisting of all findings identified above and recommended solutions.
- Provide a presentation to the client of the security assessment Project including detailed project recommended solutions.
- Provide a report for information sharing with other state/municipal entities for lessons learned/grouped remediation efforts.
- Provide a gap analysis of current state to anticipated future state.

Qualifications

The contractor must have at least one (1) staff/personnel with the following qualifications, as evidenced by their resume/CV:

- must have at least 10-year experience in IT security
- must have at least a Masters degree in Computer Science or other related fields
- must have at least 4 or more of the following certifications:

a. GCIH - GIAC Certified Incident Handler
b. GCIA - GIAC Certified Intrusion Analyst
c. GCDA - GIAC Certified Detection Analyst
d. GMON - GIAC Continous Monitoring Certification
e. GCFA - GIAC Certified Forensics Analyst
f. GSE - GIAC Security Expert

- must have the following certifications:

a. CISA - ISACA Certified Information Systems Auditor
b. CISM - ISCA Certified Information Systems Manager

Notes:

	- Should there be discrepancies with this document and the attached terms of reference (TOR), the TOR shall prevail - Price inclusive of government fees, taxes and duties - Progress payment: a. 15% to be paid upon submission of a project plan based on kickoff meeting with DOST-ASTI b. 35% to be paid upon submission of the vulnerability assessment report summarizing all security, risks, threats and vulnerabilities c. 35% to be paid upon submission of the recommended solutions report d. 15% to be paid upon submission of the compiled final report and presentation to DOST-ASTI				

TOTAL APPROVED BUDGET FOR THE CONTRACT:	**Php 900,000.00**

GUIDELINES

A. Submission of Quotations

1. Quotation/s shall include the Request for Quotation and/or the Purchase Request Number as state above;
2. Pictures or brand/model names or numbers, if applicable, should be specified in the quotation/s; and
3. Quotation/s must be signed by the company's duly authorized representative.

B. Eligibiliy Requirements

Pursuant to Annex "H" or Consolidated Guidelines for the Alternative Methods of Procurement of the 2016 Implementing Rules and Regulations (IRR) of Republic Act (RA) No. 9184, as amended by Government Procurement Policy Board Resolution No. 21-2017 dated 30 May 2017, the following documents shall be submitted except for Repeat Order, Shopping under Section 52.1(a), and Negotiated Procurement under Sections 53.1 (Two-Failed Biddings), and 53.5 (Agency-to-Agency):

For Procurement of Goods

1. Upon submission of quotation

   ✓ PhilGEPS Platinum Membership Certificate including Annex "A". If not available, the following alternate documents may be submitted:
   - PhilGEPS Registration Number
   - Mayor's Permit
     - For individuals/professionals engaged under Section 53.6, 53.7 and 53.9 of the 2016 IRR of RA No. 9184, only the Bureau of Internal Revenue (BIR) Certificate of Registration shall be submitted in lieu of the Mayor's Permit.

2. Upon issuance of Notice of Award (NOA)

   ✓ Omnibus Sworn Statement
   - Applicable only for bidders who have submitted their quotation on item/s with a total Approved Budget for the Contract (ABC) of above Php50,000.00.

   ✓ Income/Business Tax Return
   - Applicable only for: **a)** bidders who have submitted their quotation on item/s with a total ABC of above Php500,000.00; and **b)** bidders for Lease of Real Property and Venue (except for government agencies as lessors).

For Procurement of Infrastructure

1. The requirements for Goods with the same submission indicated therein; and
2. Valid Philippine Contractors Accreditation Board License.

For Procurement of Consulting Services

1. The requirements for Goods with the same submission indicated therein; and
2. Valid Professional Regulation Commission License or Curriculum Vitae.

NOTE: For new suppliers, submit a BIR Certificate of Registration for accounting purposes.

C. Terms and Conditions

1. Additional requirements, if necessary, may be requested by the BAC depending on the item to be bid;
2. For all kinds of procurement, the bidder who passed the bid evaluation, shall submit a duly notarized Omnibus Sworn Statement upon issuance of NOA, unless otherwise provided;
3. All transactions are subject to creditable withholding tax and final Value Added Tax or percentage tax per revenue regulation/s of the BIR;
4. A penalty of one-tenth of one percent (0.001) of the total value of the undelivered goods/services shall be charged as liquidated damages for every day of delay of the delivery; and
5. The DOST-ASTI reserves the right to accept or reject any proposal, to annul the bidding process, and to reject all proposals at any time prior to contract award, without thereby incurring any liability to the affected proponent or proponents.

Term Sheet
Cybersecurity Audit and Enhancement Services
PR No. GAA-19-08-8268

I. Rationale

DOST-Advanced Science and Technology Institute is implementing the *Synthetic Aperture Radar and Automatic Identification System for Innovative Terrestrial Monitoring and Maritime Surveillance* project (SAR with AIS) to improve terrestrial monitoring and maritime surveillance of high priority areas using satellite images. It can also be used for applications such as disaster risk reduction, forestry, agriculture, land cover mapping and land use classification, among many others.

As the SAR with AIS project's primary stakeholders are from the security sector, it is crucial to secure the ground receiving station's network infrastructure as their data may be deemed confidential for national defense and intelligence.

This is a supplemental document for the procurement of Cybersecurity Audit and Enhancement Services. Should there be discrepancies with the specifications under the Purchase Request (PR) and this Terms of Reference (TOR), the TOR shall prevail.

II. Scope of Work

Contractor must provide the following services:

a. Forensics and Incident Response

- Contractor shall analyze past incident/s within the GRS and determine the root cause and associated timeline
- Activities shall include, but are not limited to, the following:
    - a.1. Log Analysis
    - a.2. File System Analysis
    - a.3. Full Disk Forensics
    - a.3.1. Includes forensic analysis for at least one 4TB HDD
    - a.4. Malware Analysis
    - a.5. Timeline Generation

b. Risk Assessment

- Contractor shall assess the existing network infrastructure setup and create recommendations based on the needs of DOST-ASTI
- Contractor shall also utilize the CIS Top 20 Critical Security Controls
- Scope of work shall include, but are not limited to, the following:
    - b.1. Identification
        - Identify individuals or roles who are associated with the relevant confidential/important data intended to be secure.
        - Identify assets (hardware and software, both authorized and unauthorized) to develop baseline inventories.
        - Review current documentation and policies for vulnerabilities and concurrence with industry best practices.
        - Identify procedures that relate to the storage or transfer of confidential/important data.
        - Identify statutory/regulatory compliance requirements (confidentiality, privacy, security).
        - Identify core competencies & mission-critical business functions.
    - b.2. Comprehensive Assessment

- Interview those subjects identified previously to evaluate the strength of the Clients current controls.
- Evaluate items below to ensure security controls for data confidentiality, data integrity and data availability.

i. Workstation OS Deployment Guides
ii. Server OS Deployment Guides
iii. Network Segmentaiton
iv. Firewall Configuration
v. Remote Access
vi. External Exposure
vii. Eggress Traffic Policies
viii. Network Monitoring Capabilities
ix. Patching Strategies
x. Credential/Account Management

b.3. Report and Presentation
- Provide a detailed comprehensive security assessment report consisting of all findings identified above and recommended solutions.
- Provide a presentation to the client of the security assessment Project including detailed project recommended solutions.
- Provide a report for information sharing with other state/municipal entities for lessons learned/grouped remediation efforts.
- Provide a gap analysis of current state to anticipated future state.

III. Qualifications

The contractor must have at least one (1) staff/personnel with the following qualifications, as evidenced by their resume/CV:
- must have at least 10-year experience in IT security
- must have at least a Masters degree in Computer Science or other related fields
- must have at least 4 or more of the following certifications:

a. GCIH – GIAC Certified Incident Handler
b. GCIA – GIAC Certified Intrusion Analyst
c. GCDA – GIAC Certified Detection Analyst
d. GMON – GIAC Continous Monitoring Certification
e. GCFA – GIAC Certified Forensics Analyst
f. GSE – GIAC Security Expert

- must have the following certifications:

a. CISA – ISACA Certified Information Systems Auditor
b. CISM – ISCA Certified Information Systems Manager

IV. Payment and Duration:

- Price inclusive of government fees, taxes and duties
- Progress payment:

a. 15% to be paid upon submission of a project plan based on kickoff meeting with DOST-ASTI
b. 35% to be paid upon submission and acceptance of the vulnerability assessment report summarizing all security, risks, threats and vulnerabilities
c. 35% to be paid upon submission and acceptance of the recommended solutions report
d. 15% to be paid upon submission and acceptance of the compiled final report and presentation to DOST-ASTI

- Duration: The Contractor should be able to turnover all deliverables on or before 30 November 2019