Republic of the Philippines
Office of the Solicitor General
134 Amorsolo St. Legaspi Village, Makati City

Technical Working Group for
Information and Communications Technology

# TERMS OF REFERENCE

## PROCUREMENT OF CYBER SECURITY PLATFORM FOR CYBER-DEFENSE BASED ON MACHINE LEARNING AND AI

**Background:**

The Office of the Solicitor General is developing its capabilities in providing a **Cyber Security Platform for Cyber-Defense based on Machine Learning and AI**.

As the Office of the Solicitor General's ICT infrastructure and systems continue to expand, there is a greater need to be able to have a **CYBER SECURITY PLATFORM** which is a self-learning platform and has an adaptive approach that uses proven **Artificial Intelligence** to learn about the environment in which it finds itself and detect and respond to deviations from normal activity.

**Objective:**

The Office of the Solicitor General requires a **CYBER SECURITY PLATFORM** capable of identifying and containing any anomalous threats in the network in real time through Machine Learning and Artificial Intelligence.

To meet its objective, the Office of the Solicitor General seeks to acquire a comprehensive **CYBER SECURITY PLATFORM FOR CYBER-DEFENSE BASED ON MACHINE LEARNING AND AI**.

**Terms:**

1. *Scope.* - Supply and delivery of Cyber Security Platform for Cyber-Defense Based on Machine Learning and AI

2. *ABC.* - The Approved Budget for the Contract (ABC) is **Three Million and Five Hundred Thousand Pesos (₱3,500,000.00)**, inclusive of all government taxes, charges and other standard fees.

| ICT SUBSCRIPTION | | | |
|---|---|---|---|
| ITEM | QTY | UNIT COST | TOTAL |
| CYBER SECURITY PLATFORM FOR CYBER-DEFENSE BASED | 1 | 3,500,000.00 | 3,500,000.00 |

| | | | |
|---|---|---|---|
| **ON MACHINE LEARNING AND AI** | | | |
| | | **TOTAL** | **₱ 3,500,000.00** |

3. *Delivery and Training*:

a. All items should be delivered within 30 days of receipt of the Notice to Proceed.

b. Provide training covering essential items for correct use and day-to-day administration.

c. Training materials, product guides, and documentation should be available online.

d. Must be done during business hours

e. The course outline should be presented.

f. Training must begin upon deployment within ten (10) days of solution delivery and must be coordinated with CMS. The CMS will provide certification for delivery and training completion.

4. *Schedule of Payment*. - To guarantee the performance by the winning bidder of its obligations under the contract, it shall post a performance security before the signing of the contract. The performance security shall be in an amount not less than the required percentage of the total contract price in any of the following forms and in accordance with the following schedule:

| Form of Performance Security | Amount of Performance Security (Not less than the required % of the Total Contract Price) | Statement of Compliance |
|---|---|---|
| a) Cash or cashier's/ manager's check issued by a Universal of Commercial Bank. | 5% | |
| b) Bank draft/ guarantee or irrevocable letter of credit issued by a Universal or Commercial Bank; *however*, it shall be confirmed or authenticated by a Universal or Commercial Bank if issued by a foreign bank. | 5% | |
| c) Surety bond callable upon demand issued by a surety or insurance company duly certified by the Insurance Commission as authorized to issue such security. | 30% | |

| TERMS OF PAYMENT | Statement of Compliance |
|---|---|
| Supplier agrees to be paid based on a progressive billing scheme as follows: | |
| • Within thirty (30) days from completion of the delivery and issuance of the Inspection and Acceptance Report by the OSG and submission of all other required documents - 95% of the contract price.<br>• One (1) year from the issuance of the Inspection and Acceptance Report by the OSG - 5% of the contract price. | |

**All bid prices shall be considered as fixed prices, and therefore not subject to price escalation during contract implementation.**

5. *Qualifications of the Supplier*:

a. The bidder must have completed, within the last three years from the date of submission and receipt of at least one (1) single contract of similar nature amounting to at least fifty percent (50%) of the ABC, or the prospective bidder should have completed at least two (2) similar contracts, and the aggregate contract amounts should be equivalent to at least fifty percent (50%) of the ABC, and the largest of these similar contracts must be equivalent to at least half of the fifty percent (50%) of the ABC as required.

b. The bidder shall submit a valid and current Certificate of Distributorship/Dealership/ Resellers of the product being offered, issued by the principal or manufacturer of the product (if the bidder is not the manufacturer). If not issued by the manufacturer, must also submit a certification/document linking the bidder to the manufacturer.

c. During contract implementation, the bidder/supplier must remain an authorized distributor, reseller, or partner to maintain said License Software. Suppose the bidder/supplier cannot maintain its distributor, reseller, or partnership agreement with the Manufacturer/Principal. In that case, this may serve as a ground/reason for the termination of its contract with OSG.

d. Must have at least one certified personnel for the project implementation, with certification.

6. Applicable provisions of the Government Procurement Reform Act (RA No. 9184) and its Revised Implementing Rules and Regulations (RIRR) shall form part of the Terms of Reference.

## Technical Specifications:

| ITEM | SPECIFICATIONS | COMPLIANCE |
|---|---|---|
| **1. REGARDING TECHNOLOGY** | | |
| 1.1 | – It must use algorithms of artificial intelligence as well as techniques of unsupervised machine learning. | |
| 1.2 | – After the initial learning period, the technology must automatically provide a complete audit trail of all devices in the environment, pre-sorting at least the device type, hostname, mac address, and the first and last time the device was seen on the network. | |
| 1.3 | – After the initial learning period, the technology must automatically provide a complete audit trail of all subnets found in the network. | |
| 1.4 | – It must be a self-learning platform with an adaptive approach that uses proven artificial intelligence to learn about the environment in which it finds itself and detect and respond to deviations from normal activity. | |
| 1.4.1 | – a. the network's learnings must be adaptive and dynamic enough to suit any changes in the environment's behavior | |
| 1.4.2 | – b. it should operate completely based on behavior, where technologies that make use of rules and/or signatures will not be allowed | |
| 1.4.3 | – c. it should not need to share data with a global security cloud to get its security intelligence | |
| 1.5 | – It must be able to take autonomous action to contain in-progress threats, giving the security team time to investigate and remediate as needed. The autonomous response must: | |
| 1.5.1 | – a. relies on an understanding of normal activity and being able to interrupt the unusual activity only surgically | |
| 1.5.2 | – b. takes proportionate action in real-time - from connection-specific interruptions through to full device quarantines either directly or via integrations with firewalls and/or Network Access Controls | |
| 1.6 | – It should have an automated investigation that continuously investigates 100% of threats and surfaces only the most relevant incidents. | |

| | | |
|---|---|---|
| | Automatically writes reports that put teams in a position to take action. | |
| 1.7 | – It must have a Threat Dashboard for a simplified overview of real-time threats that is simple and intuitive and that enables at least: | |
| 1.7.1 | – a. an immediate understanding of breaches with a description of what those breaches mean | |
| 1.7.2 | – b. a recommendation for the action that could be taken | |
| 1.7.3 | – c. filtering for breaches more critical as well as for devices more critical | |
| 1.7.4 | – d. a complete breach detailing device data, connection logs, and device history | |
| 1.7.5 | – e. a possibility of opening a more detailed investigation of the logs and connections with the topology plotted in 3D | |
| 1.8 | – It must have a user interface to visualize threats in 3D and plot the map of any connection made by the internal devices in real time. | |
| 1.9 | – It must have a feature capable of enabling retrospective analysis of the incident's logs, returning the connection in seconds, minutes, hours, or days before a certain anomaly has been identified. | |
| 1.10 | – It must automatically group devices into groups and clusters by their behavior similarity. | |
| 1.11 | – It must provide simple and fast filters to enable the analysis of violations by at least Users, Devices, and types of breach. | |
| 1.12 | – It must have a detailed analysis of all the traffic received in the device, and the last time the main protocols were seen, among them, HTTP, HTTPS, FTP, LDAP, SMTP, SSH, SMB, POP3, NTLM, IMAP, Kerberos, among others. | |
| **2. REGARDING EXTERNAL INTEGRATIONS AND REPORTS** | | |
| 2.0 | – It should have the automatic creation of executive reports covering at least one overview of the following: | |
| 2.0.1 | – a. the entire deployment summary indicating the total number of devices, the total number of subnets, and processed media bandwidth | |
| 2.0.2 | – b. a summary of breaches per attack phase | |
| 2.0.3 | – c. a Devices breach summary | |

| | | |
|---|---|---|
| 2.0.4 | – d. a Top devices summary breaching high-priority conditions | |
| 2.0.5 | – e. a summary of the most frequent breaches to main compliance items such as misuse of USB, google drive, outbound RDP, and external SQL, among others | |
| 2.0.6 | – f. a Top devices summary that most breaches the compliance conditions generating risk to the organization | |
| 2.1 | – It should have AI-driven investigation Reports showing post-triage security incidents and correlated model-breaches | |
| 2.2 | – The system must be OPEN API, supporting integrations with other security elements: | |
| 2.2.1 | – a. SIEM and SOAR | |
| 2.2.2 | – b. Ticketing System and Case Management | |
| 2.2.3 | – c. Endpoints | |
| 2.2.4 | – d. VPN and Zero-Trust Technologies | |
| 2.2.5 | – e. Asset and Inventory Management | |
| 2.2.6 | – f. Firewalls | |
| 2.3 | – Have the capability to connect to TAXII servers and import STIX XML filers | |
| 2.4 | – Able to integrate to LDAP for authentication and LDAP enrichment | |
| 2.5 | – The technology must have its own mobile app available in both GooglePlay and AppleStore to enable remote management of incidents via mobile phones | |
| **3. REGARDING ARCHITECTURE** | | |
| 3.0 | – It must support a complete and scalable architecture through the licensing of additional components required to integrate with the various digital environments, including on-premises, cloud, and hybrids, if the contractor wishes to acquire them in the future, supporting at least: | |
| 3.0.1 | – a. IaaS - AWS, Azure, GCP | |
| 3.0.2 | – b. SaaS - AWS, Azure, M365, GCP, Google Workspace, Zoom, Box, Dropbox | |
| 3.0.3 | – c. Email - Office 365, Gmail, Exchange | |
| 3.0.4 | – d. IoT devices | |
| 3.0.5 | – e. Virtual Environment (virtual machines) | |
| 3.0.6 | – f. containers | |
| 3.0.7 | – g. Off VPN Mobile Workforce | |
| 3.0.8 | – h. 1600 IP Devices (future expansion) | |

| | | |
|---|---|---|
| 3.1 | – It must support a distributed architecture with components working in the MASTER-PROBEs architecture, where all data analysis and correlation are performed locally. Only metadata is forwarded to the central site for centralized administration, not to burden the network. | |
| 3.2 | – It must consume and analyze raw data (raw packets) through port mirroring (SPAN) or through the use of a TAP. | |
| 3.3 | – It will not be accepted if it only uses partial analysis of the packages using sflow, jflow, netflow, among others. | |
| 3.4 | – A cloud-based Master appliance will be deployed in either AWS or Azure environment in Southeast Asia Region. | |
| 3.5 | – Cloud Master appliance must support the analysis of 300 IP devices (license for 300 IP devices) | |
| 3.6 | – The virtual appliances will act as a probe to capture the network span traffic from the core switch and the virtual switches in the virtual environment. | |
| 3.6.1 | – Probe communication to the Master is encrypted via SSL. | |
| 3.6.2 | – Ingested network traffic is processed and sent to the Master; the size of data transferred across the network must be approximately 1-4% of the incoming SPAN bandwidth. | |
| 3.6.3 | – Virtual Appliance that will capture the network span traffic from the core switch must have the following hardware specification - 32 CPUs, 128Gb RAM, 800GB RAM, and at least three physical NICs. | |
| 3.6.4 | – Virtual Appliances capturing the span traffic from the virtual environment must support 7 VMWare Physical Host, hosting 37 VM Servers. | |
| **4. SERVICES** | | |
| 4.0 | – 24/7 Rapid feedback and expert remediation advice from Cyber Analysts | |
| 4.1 | Around-the-clock coverage of high-fidelity incidents, which are strong indicators of an emerging attack identified within the environment | |
| 4.1.1 | Immediately contact the team in the event of an attack via email and/or SMS or telephone call, | |

| | | |
|---|---|---|
| | depending on the preferred messaging delivery methods in the SOC contact list. | |
| 4.1.2 | Fully triaged alerts must be encrypted using a shared secret key and emailed to a named distribution list within the organization. The alert should be provided with the intelligence ascertained to take immediate action. | |
| **5. SUPPORT AND ASSISTANCE** | | |
| 5.0 | Must have an online portal available for client access by providing at least the following: | |
| 5.0.1 | a. two-factor authentication | |
| 5.0.2 | b. pre-scheduled periodic training sessions | |
| 5.0.3 | c. Training videos | |
| 5.0.4 | d. a complete library of solution documents, product guides as well as specific fields where the latest product updates and release notes can easily be validated | |
| 5.0.5 | e. contains a specific feature for opening support tickets, enabling fast, simple opening and case details. All ticket updates must be in the system, forwarded via email, and have a complete call history track. | |
| 5.0.6 | d. it must have fields about Cyber Threats and publications of security experts about current threats. | |
| 5.1 | It must provide helpdesk/diagnostic and remote support for issues. | |
| 5.2 | Must have automatic software update with the option to update manually | |
| 5.3 | Hardware support should provide all parts and materials necessary to keep the hardware in good operating condition. | |
| 5.4 | Health checks and diagnostics | |

## Technical Working Group for ICT Subscriptions

DIR IV EDUARDO ALEJANDRO O. SANTOS

DIR IV EDITHA R. BUENDIA

SS II OMAR E. GABRIELES

ASII MIGUEL MARTIN A. BUENAVENTURA
(RESIGNED)

ASII JONATHAN A. PABILLORE
(STUDY LEAVE)

ITO II CEDRIC S. DELA CRUZ

SAO JOY Y. CHUA

CMT III JESUS NIÑO CHUA

AO IV RAY CHARLIE V. ALEGRE

**Approved/Disapproved**:

**MENARDO I. GUEVARRA**
Solicitor General

Certified Funds Available:

**BERNADETTE M. LIM**
Dir IV - FMS