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 BASED ON AI/MACHINE LEARNING AND UTILIZE HUMAN INTELLIGENCE

Background:

The Office of the Solicitor General is expanding its capabilities to provide a **Cyber Security Platform based on AI/Machine Learning and Human Intelligence**.

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 and human intelligence for the analysis and verification.

Objective:

The Office of the Solicitor General requires expanding its **Cyber Security Platform**, which can identify and contain 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 based on AI/Machine Learning and Human Intelligence**.

Terms:

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

2. *ABC.* - The Approved Budget for the Contract (ABC) is **Fifteen Million Pesos (₱15,000,000.00)**, including all government taxes, charges, and other standard fees.

ICT SUBSCRIPTION			
ITEM	**QTY**	**UNIT COST**	**TOTAL**
CYBER SECURITY PLATFORM BASED ON MACHINE LEARNING, ARTIFICIAL AND HUMAN INTELLIGENCE (SIEM, SOAR, NSM, EDR, THREAT INTELLIGENCE, INCIDENT RESPONSE, SECURITY OPTIMIZING/ MONITORING, AND THREAT HUNTING/ANALYSIS)	1	15,000,000.00	15,000,000.00
		TOTAL	**₱ 15,000,000.00**

3. *Deliverables and Training*:

a. A cloud-based Security Operation Center (SOC) platform that includes SIEM, SOAR, NSM, EDR, Threat Intelligence, Incident Response, Security Optimizing/Monitoring, and Threat Hunting/Analysis, including onboarding.

b. 24 x 7 Managed Security Operation Center Service.

c. All items should be delivered within 30 days of receipt of the Notice to Proceed or before anniversary date of existing contract.

d. Provide training covering essential items for correct use and day-to-day administration. Training materials, product guides, and documentation should be available online. Must be done during business hours, and the course outline should be presented.

e. Training must begin upon deployment within ten (15) 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 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. • 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/supplier must have satisfactorily completed, within the last three years from the date of submission and receipt of at least one (1) single contract of a similar nature amounting to at least fifty percent (50%) of the ABC.

      For this purpose, the purchase ICT subscription for cybersecurity shall be referred to as a similar contract.

   b. The bidder/supplier 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. The bidder/supplier must maintain its status as an authorized distributor, reseller, or partner with the manufacturer/principal

for the duration of the contract. Failure to maintain such status is a ground for the OSG to terminate the said contract.

d. The principal of the offered solution must have a local office and a local agent in the Philippines to ensure compliance with local laws and regulations. Additionally, direct local engineers should be employed to oversee the implementation of technical services, ensuring adherence to local standards and project specifications.

e. The bidder must have at least one (1) certified engineer who can support the solution.

f. The financial proposal shall include all costs necessary for the supplier to fulfill its obligation to deliver and deploy the cybersecurity platform (software, hardware, etc.).

6. Applicable provisions of the New Government Procurement Act (RA No. 12009) and its Implementing Rules and Regulations (IRR) shall form part of the Terms of Reference.

Technical Specifications:

	Specification	Compliance
I	**GENERAL REQUIREMENTS**	
	The Vendor commits to ensuring compatibility of technology platforms, aligning with the current state of information technology applications of the ***Office of the Solicitor General (OSG)***.	
	The Vendor has international certificates/ certifications for information security monitoring services: • The service provider has achieved Externally Validated certification for the Information Security Monitoring Center (SOC) service of the CREST organization (https://www.crest-approved.org/). • The service provider has achieved information security assurance certification according to ISO/IEC 27001 for information security operation, monitoring, and incident handling (SOC).	
	The Managed Security Operations Center (MSOC) must be a consolidated platform that shall serve as the central framework for integrating Security Information and Event Management (SIEM), Security Orchestration Automation and Response (SOAR), Network Security Monitoring (NSM), Endpoint Detection and Response (EDR), and Threat Intelligence into a unified and cohesive ecosystem.	
	The MSOC should cover OSG's network infrastructure, including but not limited to: • Two (2) core switches and one (1) distribution switch • Forty (40) virtual machine servers; a combination of Linux and Windows OS • Three (3) network firewalls; 2 are in high availability	
	The MSOC can integrate other security solutions, including but not limited to: • Existing endpoint protection for servers and PCs/Workstations • Vulnerability and Patch Management	
II	**INFORMATION SECURITY MONITORING SOFTWARE SOLUTIONS**	
1	**Security Information & Event Management**	

	The SIEM should provide a centralized location for gathering and organizing data from any existing security control, IT, and productivity tools using pre-built integrations that are easy to use and do not incur additional costs for integrating new security tools.	
	The solution must be able to collect data from multiple sites using distributed sensors/data collectors.	
	Collects information security logs from various sources (such as servers, devices, applications) via syslog, API, JDBC, WMI, or through agents.	
	The solution must be able to collect data without limiting the type and number of devices to collect from.	
	The solution can integrate threat intelligence and telemetry data from multiple sources with security analytics to contextualize and correlate security alerts.	
	The solution must include UEBA natively to analyze traffic and produce security status and event information on individual users, as well as monitor network assets and analyze their behavior to detect threats.	
	The system removes redundant data, normalizes, and classifies in a common format optimized for analysis.	
	The system also allows for storing the original log for 90 days for later investigation & tracing.	
	Delivers a friendly search interface and user-defined search terms, similar to human language.	
	With the write actions on the interface, users can easily expand or narrow the search terms, making it convenient and fast to search events and alerts during monitoring and investigation.	
	Provides a data storage system that is indexed and backed up to carefully preserve all data, serving the investigation and tracing process in case of problems.	
	The storage system can be customized according to the size of the customer's system.	
	Provides a real-time alert monitoring interface; the alerts are prioritized depending on the severity of the attack type as well as the target being attacked.	
	The entire process from collecting & processing logs to analyzing and issuing alerts must be optimized, shorten the time from problem detection to alert notification should be within 1 minute only for a system size of approximately 1.5K EPS.	
	Provides nearly 1000 rules to detect anomalies in the system.	
	Users can customize and add new policies depending on the demand of the agency	

	The solution provides an intuitive, user-friendly administration interface, rich in information and customizable according to the actual needs of customers.	
	The interface also supports log source management, allowing new devices and applications to be added to the system to ensure instant monitoring.	
	Log source management should allow users to easily add new applications or devices to the system, ensuring continuous monitoring of the organization's system.	
	Has the capability to auto update new versions, new policies, and new knowledge, and must be updated automatically to monitor the customer's system completely.	
	Has a built-in normalizer for more than 100 common types of applications and devices.	
	The system provides an interface for adding normalizers easily, especially to the new types of applications and devices.	
	Capable of collecting all data from systems located in the IT infrastructure, such as operating systems, applications, endpoint protections, endpoint detection and response, network devices, security devices such as Firewall, Proxy, IPS/IDS, user access, or the organization's IT system administrator.	
	Capable of analyzing system collected from Data Source, where data is normalized, smoothed, classified, and correlated analysis in many dimensions to detect signs and unusual behavior appearing in the system.	
	Has a Front-End system that interacts with users, helps users operate, monitor, and handle alerts, violations, or search and investigate information from the system.	
	The SIEM tool must ensure compatibility with the existing technology platforms, aligning with the current state of information technology applications of OSG.	
	Can monitor and detect signs of attacks, such as signs of connection to the malware control server (C&C)	
	Can monitor signs of malware spread in the system	
	Can monitor and detect abnormal signs on the endpoint layer	
	Can detect signs of intrusion on the endpoint layer	
	Can monitor and detect network layer attacks	
	Generates a periodic report	

	An open-source SIEM platform is strictly prohibited.	
	The product must have the following international certifications/certificates: - CREST (SOC) - ISO27001 - SOC2 Certification	
2	**Network Security Monitoring**	
	The Solution has DPI technology that is applied to extract packets, analyze, and detect anomalies in the network, along with common protocol decoders and automated malware analysis technology on the HyperVisor platform (Sandboxing). The solution provides a new, optimal, and fully automated malware detection platform.	
	The solution is integrated with a code detecting various abnormal behavior groups on network layers and constantly being updated to be able to detect the latest attack signs, including abnormal behavior groups such as Network Scan, Trojan Activities, Shellcode Detect, Web Application Attack, Suspicious Login, etc.	
	The solution is combined with a code correlating abnormal signs during the investigation of APT attacks to link the smallest events on network layers and detecting potential attack signs disguised under queries to servers.	
	The system can detect various types of attacks commonly known as APT (Advanced Persistent Threats). These attacks often cause serious damage to organizations for a long time without being detected.	
	The solution can monitor network traffic in real-time and analyze packets to issue alerts about attacks, scanning, and mining vulnerabilities of applications and services targeting IT systems of governing units. NSM is deployed simply and quickly without any influence on services and applications in network infrastructure types based on signatures to advanced, disguised, and hidden attacks, such as APT.	
	The solution includes a number of outstanding features in terms of cyber-attack detection: • Detecting attacks scanning passwords in the network. • Detecting denial-of-service attack signs. • Detecting attack signs and scanning vulnerabilities. • Detecting web application attack signs (SQL Injection, XSS, etc.). • Detecting APTs.	

	• Detecting signs of scanning network information. • Detecting signs of mining services	
	The solution provides a set of tools assisting administrators and experts with in-depth investigation, review, and analysis of cyber incidents, including: • Reviewing connections related to a cyber-attack sign. • Reviewing connections related to an address and a computer within the network. • Supporting the regeneration of connections and queries within network in the form of PCAP to serve in-depth investigation and analysis	
3	**Security Orchestration, Automation & Response**	
	Allows separate security tools to work smoothly together to improve productivity in complex security processes. In addition to supporting many popular tools and playbooks.	
	Provides customization capabilities to integrate security technologies and develop playbooks according to the organization's needs.	
	Provides the ability to automate a sequence of actions already defined in playbooks in seconds, instead of hours when done manually.	
	Provides an intuitive interface for users to build playbooks by using the existing support interface or creating new playbooks in Python language.	
	Keeps track of all information during investigation, response, and synthesis, in order to provide analysts with a single centralized administration interface.	
	The management of information includes: • Operational coordination: Team members can easily interact on specific issues in each case to quickly make decisions or assign work to the right person. • Cybersecurity threat intelligence management: With integration with cybersecurity intelligence platforms, SOAR manages and delivers incident-related threat intelligence proactively and intuitively for analysts, helping to optimize analysis and incident response. • Support for investigation and tracing: SOAR provides users with the most convenient and optimal toolkit for investigation and tracing of cyber-attacks.	

	Supports tools to extract specialized reports and dashboards for all 3 user groups of the organization: Analyst, SOC Manager, and Chief Information Security Officer (CISO). All events and actions are stored to help the organization measure the effectiveness of the SOC operation team from many different perspectives.	
4	**Endpoint Detection & Response**	
	Comprehensive and proactive malware protection There is a mechanism that allows the agent component to actively monitor in kernel mode, capture events when malware enters, and destroy automatically and immediately.	
	Behavior Monitoring by Filter Driver The Filter Driver technology can monitor behavior related to File, Process, Memory, Registry, and Network on personal computers and servers. Suspicious behavior will be pushed to the centralized analysis backend components.	
	Centralized Analysis This solution applies various technologies, such as anomaly detection according to IOC/IOAs, behavioral modeling, and chaining relationships between suspected objects and highlighting anomalies and malware that have never been known in the world anomalies and malware that have never been known in the world.	
	Real-time reporting Cybersecurity situation is visually displayed on the whole system and on each user's machine.	
	Fast and Proactive Incident Response Provides the detection and analysis of anomalies on the console and an in-depth Forensic function on endpoints. As soon as the anomaly is verified, the function provides extensive malware removal tools.	
	Multi-platform support The solution supports the following platforms: Windows, Linux, macOS	
	Friendly Admin Interface The design of the control interface is optimized so that the operating team can easily monitor the system without performing multiple operations.	
	Cybersecurity Policy Support The Information Security policies are supported, such as: Control peripheral devices and Security Helpdesk to reduce the risk of malware infection.	

	Smooth Operation The design is lightweight, and the system is completely transparent.	
	Integration with Third-party Solutions This solution integrates with third-party knowledge sources such as Threat Intelligence, Advanced Malware Analysis, SOAR, and SIEM.	
III	**INFORMATION SECURITY MONITORING SERVICE**	
1	**24/7/365 Network Security Monitoring Service (Managed Security Services)**	
	Monitor and detect signs of network attacks, such as signs of connection to the malware control server (C&C), signs of widespread malware spread in the system. Monitor and detect abnormal signs on the Endpoint layer in the customer's system; Detect signs of intrusion on the Endpoint layer; Monitor and detect network layer attacks.	
	Respond to incidents 24/7: When detecting an intrusion attack, conduct an investigation, isolate the attacked area from the network system, then implement professional measures, review, and respond throughout the network to respond, handle, and prevent escalation and expansion of the infection.	
	Periodic information security report: periodic report on the information security monitoring situation during the service provision process.	
	Optimize the information security monitoring process by updating the monitoring rule set according to new attack techniques, and optimizing the monitoring rule set that generates many false alarms.	
	The personnel organization model includes the following roles: - 24/7 monitoring personnel (Tier 1) - Critical incident handling personnel (Tier 3) - Monitoring rule optimization personnel (Content Analysis) - Threat analysis and threat analysis personnel (Threat Analysis) - SOC management personnel (SOC Manager)	
	Tier 1 Staff: Monitor online 24/7, handle all warnings as instructed.	
	Tier 3 Staff: Receive escalation incidents from Tier 2 for more in-depth processing and rewrite the processing instruction for similar incidents to guide and train Tier 2.	
	Content Analysis Staff: Improve and optimize the system's processing capacity.	

	Threat Analysis Staff: Review, analyze, and update knowledge of new risks to the system.	
	SOC Manager Staff Administer the system; test and evaluate the system's performance ratio.	
IV	**Eligibility**	
	The proposed solution and services must be entirely developed in-house by the provider, offering MSOC, including SIEM, SOAR, NSM, EDR, and Threat Intelligence, without relying on any third-party solutions.	
	The service provider must hold a certificate demonstrating their participation and ranking in well-known hacking competitions such as Pwn2Own and ROOTCON.	
	The proposed services/solutions must be certified by CREST for SOC.	
	The proposed services/solutions must be certified by AICPA as SOC2 compliant.	

Technical Working Group for ICT Subscriptions

SSS JOEL N. VILLASERAN

DIR IV EDUARDO ALEJANDRO O. SANTOS

SSII OMAR T. GABRIELES

ITO III JAYVIE NEIL MALICK S. MALICDEM

ITO II CEDRIC S. DELA CRUZ

CMT III JESUS NIÑO CHUA

AO IV RAY CHARLIE V. ALEGRE

Approved/Disapproved:

DARLENE MARIE B. BERBERABE
Solicitor General

Certified Funds Available:
UNDER NEP 2026

ASG SAMANTHA P. CAMITAN
OIC - FMS