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 expanding its capabilities to provide 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 expanding its **CYBER SECURITY PLATFORM**, which is 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 **Eleven Million Pesos (₱11,000,000.00)**, including all government taxes, charges, and other standard fees.

ICT SUBSCRIPTION			
ITEM	QTY	UNIT COST	TOTAL
CYBER SECURITY PLATFORM FOR CYBER-DEFENSE BASED	1	11,000,000.00	11,000,000.00

ON MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE (850 XDR Endpoints)			
		TOTAL	**₱ 11,000,000.00**

3. *Deliverables and Training*:

a. A cloud-based Security Operation Center (SOC) platform that includes asset management, vulnerability assessment, threat intelligence, AI engines, and security orchestration, automation, and response (SOAR), as well as 850 Extended Detection and Response (XDR) endpoint licenses including onboarding.

b. 24 x 7 Managed Detection and Response Service for endpoints.

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

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 (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 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. • 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 (25%) 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 partnership 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 solutions must have ISO certifications of the following:

      - ISO 20000-1 IT Service Management System
      - ISO 9001 Quality Management Systems
      - ISO 27001 Information Security Management

e. 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.

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

g. 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 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. TECHNOLOGY: EXTENDED DETECTION AND RESPONSE (XDR)		
1.1	– It must leverage generative artificial intelligence (AI) and machine learning.	
1.2	– The technology must leverage big data analytics and generalization capabilities, allowing it to analyze vast amounts of data and detect new and unseen threats, significantly improving detection accuracy.	
1.3	– It should have a cloud-based security operation center (SOC) platform offering asset management, vulnerability assessment, threat intelligence, signatures, User and entity behavior analytics (UEBA), AI engines, correlation analysis, investigation, alert triage, security orchestration, automation, and response (SOAR), and flexible reporting.	
1.4	– It must provide comprehensive visibility into the organization's security landscape through passive and active traffic monitoring and by ingesting data from various platform components.	
1.5	– It must provide a simplified and detailed visual presentation of the entire attack chain - allowing the OSG to monitor the entire detection and elimination process from the comfort of a single, detailed dashboard. This will give the OSG full transparency and a holistic view of its security infrastructure.	
1.5.1	– The dashboard shall include the overall security system, management of pending issues, trends in security incidents, status of automated incident responses, and trends of assets at risk.	
1.5.2	– The solution shall have a display screen showcasing all data sources linked to the XDR platform, facilitating navigation to the pertinent log search page. It intuitively presents the reduction ratio from logs to security alerts and from security alerts to security incidents.	
1.5.3	– The dashboard must highlight the status of key security indicators, the protection status of core assets, and an overview of threats and intelligent countermeasures.	

1.5.4	– The solution must enable the users to customize the dashboard page to suit the OSG's requirements.	
1.5.5	– It must support a comprehensive display and detailed information on security incidents. It should be dynamically displayed based on various parameters such as threat level priority, threat descriptions, affected assets, data source, and the status of the security incident.	
1.5.6	– It must support customizable display formats for security incident pages, enabling the generation of various types of incident pages.	
1.6	– It must comprehensively display security incident details, including the file path, the created process, the security engine that detected the incident, mapping to MITRE ATT&CK techniques and procedures, and more.	
1.7	– It must support the automatic association of historical security incidents and alerts related to compromised host events or successful attacks, aiding the OSG's personnel in determining the root cause.	
1.8	– The solution shall streamline the management of historical alerts by arranging their basic information in chronological order.	
1.9	– The solution must correlate multiple security alerts during incidents, providing original network and endpoint alert data. It should associate the data with original logs for comprehensive security analysis.	
1.10	– The solution must support a granular, multi-tiered response handling mechanism, leveraging threat and attack surface entities.	
1.11	– The solution must support aggregation of alert lists from network, endpoint, and third-party devices. It should present a holistic view of security alert details, including alert description, severity, characterization, attack result, last detected date and time, and data source.	
1.12	– The solution must support categorizing security incidents into five event types: directed attacks, virus events, automated attacks, risk exposures, and uncharacterized threats. This feature should allow for efficient	

	screening of security incidents with a single click through different qualitative types.	
1.13	– The solution must support classifying security alerts into categories: targeted attacks, attack-defense exercises, internal tests, regulatory notifications, viruses, scanner attacks, vulnerability risks, business irregularities, and other threats.	
1.14	– The solution must support data ingestion from third-party security tools. This includes, but is not limited to, the following capabilities:	
1.14.1	– The solution can collect related logs from third-party devices by adding data sources.	
1.14.2	– The solution provides at least two data transfer protocols/formats to third-party devices, including Syslog and Kafka.	
1.14.3	– The solution provides at least 800 rules to parse third-party device logs.	
1.15	– The solution should have pre-built SOAR playbook policies. It should allow users to create new playbooks on the same page. Users can customize the threat response and execution workflow flexibly through a drag-and-drop interface. This enables automatic threat analysis, judgment, and response execution.	
1.16	– The solution must be integrated with existing network and endpoint security tools, including Firewalls, Endpoint security solutions, and Threat Intelligence, to rapidly respond and mitigate threats.	
1.17	– The solution must support the customization of SOAR playbook policies. This includes a built-in node library that supports automated task nodes, filter nodes, manual intervention, and marking nodes. It also supports various elements such as actions, scripts, filters, decisions, approvals, and input via a drag-and-drop interface to form a complete event-handling process script.	
1.18	– The solution must support the configuration of notification policies. It must support notifications via Instant Messaging (IM) and	

	email. Furthermore, it should allow for customizing different notification methods and templates based on various notification requirements.	
1.19	– The solution must display the applications connected to the Security Orchestration, Automation, and Response (SOAR).	
1.20	– The solution must support the integration capabilities of security experts, threat intelligence, and community immunity. This allows the system to intelligently respond to key threats in security incidents and security alerts. It must intercept external attacks in stages and automatically contain compromised entities.	
1.21	– The solution must support host isolation incident action by integrating with existing endpoint security solutions.	
1.22	– The solution will provide a comprehensive list of asset details, including but not limited to:	
1.22.1	– Multi-dimensional asset filtering capabilities, including filters for asset type, tag, importance level, asset status, source device, operating system, latest online time, first discovery time, and fuzzy search (search algorithm that matches pattern).	
1.22.2	– The ability to view asset lists by asset group or business group.	
1.22.3	– The functionality to manually add assets or import assets/asset groups from files, as well as the ability to export asset groups.	
1.22.4	– The option to customize the display of fields in the list.	
1.22.5	– The support for custom asset tags, internal and external IP ranges, and Internet unit IPs.	
1.23	– The solution must support editing owner information for effective asset management.	

1.24	– The solution must display the correlation analysis with the third-party data integrated into the XDR platform to better visualize the ingested data quality and provide enhanced visualization of the ingested data quality.	
1.25	– The solution must support customization of Indicator of Attack (IOA) and Indicator of Compromise (IOC) security alert rules. Users must define these rules by adding different attributes based on the OSG's specific needs. The OSG must have the option to define our own severity levels, provide rule descriptions, map the rules to MITRE ATT&CK techniques, and more.	
1.26	– The solution must support the customization of security incident rules. It must be able to define various aspects of these rules, including the rule name, indicator content, applicable host, and severity, and add our own remarks.	
1.27	– The solution must include an integrated ticketing system to streamline incident management and allow for seamless tracking and resolution of incidents directly within the XDR platform.	
1.28	– The solution shall offer pre-built security reports with the flexibility to customize new reports using a drag-and-drop interface. This feature lets users generate detailed security reports quickly and easily, leveraging pre-built templates. Additionally, it must have an intuitive drag-and-drop interface that allows users to create custom reports tailored to specific needs enhancing reporting flexibility.	
1.29	– The solution must offer comprehensive endpoint detection capabilities for at least 850 Endpoints of the OSG, including but not limited to:	
1.29.1	– Supports the generation of security alerts from security logs reported by Endpoint security solution.	
1.29.2	– Incidents will be automatically generated for high-severity security alerts.	
1.29.3	– Allows for manual generation of new security incidents or association of old security incidents with security alerts	

	from Managed Security Service platforms in a 1-to-1 or many-to-one relationship.	
1.29.4	– A whitelist filtering function is incorporated for security incidents generated by security operations software.	
1.29.5	– The solution maintains an alert reduction rate of 90%, supports the same process tree alert update mechanism, merges identical antivirus alerts, and includes a filtering function for antivirus alerts deemed to be of no value.	
2. NETWORK SECURITY SENSOR		
2.0	– The solution must capture network traffic of at least 3GB throughput of the agency and push it to the XDR Platform for analysis.	
2.1	– The solution must capture the network traffic logs within the OSG. All these network traffic logs will be pushed to the XDR Platform for in-depth analysis.	
2.2	– The solution must detect leakage of sensitive information defined based on specified file types and keywords.	
2.3	– The solution must detect attacks based on vulnerabilities, web-based and botnet.	
2.4	– The solution must detect abnormal traffic at standard ports running with non-standard protocols.	
2.5	– The solution must be able to correlate with the offered XDR Platform. It must support TLS certificate importation for encrypted data transmission.	
2.6	– The solution must create the rules to identify unauthorized access.	
3. MANAGED DETECTION AND RESPONSE SERVICES (MDR)		
3.0	– The service shall be able to collect and analyze alerts and logs from existing endpoint security solutions and the proposed XDR platform.	
3.1	– These services must combine technology and human expertise in performing cyber threat hunting, monitoring, and response.	

3.2	– The proposed solution must be able to provide 24x7 managed security services to detect and respond to cyberattacks targeting the server farm.	
3.3	– The proposed solution shall combine asset information gathered with tools with information gathered manually from end users to ensure a complete and comprehensive inventory of in-scope assets.	
3.4	– The proposed solution must include sharing the latest security/threat notifications, including the latest vulnerabilities and viruses.	
3.5	– The security/threat notification must be relevant to the monitored environment and not just a list of all the latest vulnerabilities and viruses.	
3.6	– The proposed solution shall leverage a combination of technology (i.e., big data analysis, threat intelligence, AI/ML) and security expertise to discover, detect, and analyze security events and threats.	
3.7	– The proposed solution must leverage real-time analysis of abnormal traffic, attack logs, and virus logs through desensitization and aggregation of massive data to discover security events.	
3.8	– The service must include a customer portal allowing customers to download previously generated reports. Report types should include weekly reports and monthly reports.	
3.9	– The service platform must support configuring security rules/use cases using complex event processing techniques.	
3.10	– The service must include creating customized use cases based on the end users' actual environment.	
3.11	– It must provide a dedicated MDR Platform to showcase the different security events happening within the OSG's network along with its current remediation stage	
3.12	– It shall provide the following security services: ▪ Threat Analysis and Identification ▪ Threat Response and Mitigation ▪ Security Device Management ▪ Asset Discovery Tracking ▪ Daily Communication with Security Experts	

4. DELIVERY AND DEPLOYMENT		
4.1	– All items should be delivered and deployed within 30 days of receipt of the Notice to Proceed.	
4.2	– Provide training covering essential items for correct use and day-to-day administration within ten (10) days upon deployment.	
4.3	– Training materials, product guides, and documentation should be available online	
4.4	– Deployment must be done during business hours	
4.5	– The course outline should be presented.	
5. SUPPORT AND SERVICES		
	For support and services, the bidder must have the following:	
5.1	– Unlimited corrective maintenance/ repair services within the warranty period	
5.2	– Twenty-four (24) hours by seven (7) days (Monday to Sunday) technical support and must meet the following response and resolution time: ▪ Critical incidents <30 minutes ▪ Critical threats <60 minutes ▪ Root cause analysis for all support cases filed.	
5.3	– The bidder must provide full documentation for the Activity Plan on installing patches and upgrades and Root Cause Analysis of incidents encountered.	
5.4	– The bidder must provide onsite support for installing and deploying software patches and version upgrades.	
5.5	– The bidder must provide a procedure for support and problem escalation	

Technical Working Group for ICT Subscriptions

SSS JOEL N. VILLASERAN

DIR IV EDUARDO ALEJANDRO O. SANTOS

ITO III JAYVIE NEIL MALICK S. MALICDEM

ITO II CEDRIC S. DELA CRUZ

SAO JOY Y. CHUA

CMT III JESUS NIÑO CHUA

AO IV RAY CHARLIE V. ALEGRE

Approved/Disapproved:	Certified Funds Available:
MENARDO I. GUEVARRA Solicitor General	**BERNADETTE M. LIM** Dir IV - FMS