ASTI-FM 03-11
REV 0/2 APR 2018

DOST-ASTI Bids and Awards Committee
Invitation to Bid (Public Bidding)

ITB No:	19-03-2319	**Date:**	March-08-2019
PR No:	CoARE-18-12-7071	**Date:**	December-11-2018
Source of Funds:			
Total ABC:	Php 1,750,000.00		
Time, Date & Venue of Pre-bid Conference:	March 21, 2019, 1:30 PM at DOST-ASTI		
Time and Date of Submission of Bids:	April 02, 2019, 12:00 PM		
Time, Date & Venue of Opening Bids:	April 02, 2019, 1:30 PM at DOST-ASTI		
Date of availability of Complete Set of Documents:	March 13, 2019		
Deadline of Potential Bidder's Clarifications:	March 23, 2019		
Deadline of ASTI's Supplemental Bid Bulletin:	March 26, 2019		
Delivery Schedule:			

The Advanced Science and Technology Institute (ASTI), through its Bids and Awards Committee (BAC), hereby invites all interested bidders to submit their bids for the item(s) listed below. Guidelines regarding the format, eligibility, technical and financial documents needed are described in the Instruction to Bidders of the Philippine Bidding Documents

Bidding will be conducted through open competitive bidding procedures using a non discretionary "pass/fail" criterion as specified in the 2016 R-IRR of RA 9184.

A complete set of Bidding Documents may be purchased by interested bidders upon payment of a fee for the Bidding Documents. It is also downloadable for free of charge at DOST-ASTI's website - ***www.asti.dost.gov.ph***

For further inquiries, contact ASTI's BAC Secretariat via email at ***bac-sec@asti.dost.gov.ph***. Interested bidders may also call the number - (632)-426-7423 and look for ASTI's BAC Secretariat.

Respectfully,

PEDRITO B. MANGAHAS
Chairperson, BAC-1

NO.	TECHNICAL SPECIFICATIONS	QTY	UNIT	UNIT PRICE(Php)	TOTAL PRICE(Php)
1	**Lease of Intrusion Detection System Appliance** No. Functional Description 1.0 General Specs 1.1 The proposed solution should be able to inspect the multi-protocol sessions to detect and flag the suspicious activity including suspicious file downloads through the web, the suspicious mail attachment and internal infections. 1.2 The proposed solution should support the native CEF,LEEF format for SIEM log integration 1.4 Proposed Anti-APT solution should perform advanced network detection and analysis of the enterprise's internal network 1.5 Upon detection of the threat, the proposed solution should be able to perform behavior analysis for advance detection 1.6 Proposed solution should have event detection capabilities that should include malware type, severity,	1	lot	1750000.00	1,750,000.00

	source and destination of attack. 1.7 Solution should provide risk based alerts or logs to help prioritize remediation effort 1.8 Solution should be deployed on premise along with on premise sandboxing capability 1.9 The proposed solution should be able to store Real payload of the detected threats 1.10 The proposed solution should be able to store packet captures (PCAP) of all Malicious communications detected by sandbox 1.11 The proposed soluton should use OS Sandboxes for detecting zeroday malwares, This should not be a CPU or chip based function 1.12 Solution should have ability to interrupt malicious communication 1.13 Solution should have no limitation in terms of supported users and limitation should be accounted in terms of only bandwidth 1.14 The proposed solution should be able to support XFF (X-Forwarded-For) to identify the IP Address of a host in a proxy/NAT environment. 1.15 Solution should be able to integrate with its own threat intelligence portal for further investigation, understanding and remediation an attack. 1.16 Solution deployment should cause limited interruption to the current network environment. 1.18 The proposed solution should allow Customer name to gain visibility to the internal networks and flag detected threats immediately 1.19 The proposed solution should have the ability to support out-of-band detection 1.20 The proposed solution should be able to detect (lateral moments) movement of the attacker without the need of installing agents on endpoint/server machines 1.21 The proposed solution should not have any port based limitation and should support all ports. 1.22 The proposed solution should support at least 100+ protocols for inspection. 1.23 The proposed solution should support to monitor traffic from multiple segments like WAN, DMZ, Server Farm, Wi-Fi network, MPLS links etc. simultaneously on a single appliance. 1.24 The Proposed solution should be able to support up to 5 network segments on a single appliance. 1.25 The proposed solution should be able to detect any suspicious communication within and outside of Customer's network 1.26 The Proposed solution should be able to detect communications to known command and control centers 1.27 The proposed solution should be able to detect reputation of url being accessed 1.28 The proposed solution should be able to identify and help Customer to understand the severity and stage of each attack 1.29 The proposed solution should have built in capabilities to add exceptions for detections 1.30 The proposed solution should have capabilities to configure files, IP, URLs and Domains to Black list or white list					

	1.31 The proposed solution should support Multiple protocols for inspection. Example :- HTTP, FTP, SMTP, SNMP, IM ,IRC,DNS and P2P protocols Internal direction :SMB ,Database protocol (MySQL, MSSQL, Oracle) on a single device 1.32 The proposed solution should have an built-in document vulnerabilities detection engine to assure analysis precision and analysis efficiency 1.33 The Proposed solution should have a Co-relation engine to automatically co-relate across multiple protocol, multiple sessions and volume traffic analysis. 1.34 The Proposed solution must provide a web service interface/API for customer to customize their own system integration 1.35 The Proposed solution must have capabilities to correlate the detections on the device itself. 1.36 The Proposed solution should support remote packet capturing to pass the Kerberos traffic from the remote location for analysis 1.37 The Proposed solution should monitor Inter-VM traffic on a Port Mirror Session. 1.38 The Proposed solution should provide correlated threat data such as: IP addresses, DNS domain names, URLs, Filenames, Process names, Windows Registry entries, File hashes, Malware detections and Malware families through a portal 1.42 The proposed solution should be able to run atleast 4 parallel sandboxes for analysis of payload 1.43 The proposed solution should have option allow sandbox instances to use a proxy for internet access. The Proposed solution should support for analysis of embedded URLs in PDFs The Proposed solution should support IPv6 environments, Should be able to tap into IPv6 network streams, perform analysis, and output IPv6-based network detection results. 2.0 Malware Analysis 2.1 Solution should have multiple built-in virtual execution environments within single appliance to simulate the file activities and find malicious behaviors for advanced threat detection. Solution should be able to provide detection details including the CVE-ID, HTTP referer and Targeted Attack campaign name 2.2 The proposed solution should be able to provide customizable sandbox to fulfill Customer's environments and needs. 2.3 Sandbox must supports multiple operating systems and for both 32-bits and 64-bits OS 2.4 Solution must have the capability to analyze large files. Must be able to support more than 40MB file size 2.5 Sandbox must have the ability to simulate the entire threat behavior. i.e. honeynet and honeypot framework 2.6 The Proposed solution should support windows XP, Windows 7, Windows 8,Windows 10, Microsoft 2003 and Microsoft 2008 operating environments for Sandboxing this requirement should be based on virtual execution and should not be a Hardware or chip based function. 2.7 The proposed solution should have gray ware					

	detection capabilities. 2.8 The proposed solution should be able to detect any malicious communication within and out side of Customer's network. 2.9 The proposed solution must provide a web service interface/API for Customer to customize their own system integration. 2.10 The Proposed solution should be able to detect Network Attacks and Exploits. 2.11 The proposed solution should have capability to scale out the detection when the bandwidth/increase increase in future 2.13 Solution must be capable of performing multiple file format analysis which includes but not limited to the following: LNK, Microsoft objects, pdf, exe files, compressed files, .chm, .swf, .jpg, .dll, .sys, .com and .hwp 2.14 The proposed solution should have an built-in document vulnerabilities detection engine to assure analysis precision and analysis efficiency. 2.15 The proposed solution must provide the capability to exportable network packet files and encrypted suspicious files for further investigation. 2.16 The proposed solution have the capability to performs tracking and analysis of virus downloads and suspicious files 2.17 The proposed solution should support exporting of analysis results such as C&C server IP and malicious domain listing 2.18 The proposed solution should have capabilities to scan inside password protected Archives 2.19 The Proposed solution should have capabilities to detect Malwares and Spywares on windows and non windows platforms 2.20 The proposed solution should have option to configure unrestrcited internet for Sandboxes 2.21 The proposed solution should have capabilities to configure files, IP, URLs and Domains to Black list or white list 2.22 The proposed solution must have capabilities to detect Mac, Linux and mobile malwares 2.23 The proposed solution should have capability to include User-defined and context-derived passwords for protected archives 2.24 The proposed solution should have capabilities to configure separate notifications to the administrator or individuals based on specific events like, Sandbox detection, Black List and license events etc. 2.25 The Proposed solution should be able to detect known malwares before sending suspicious files to Sandbox for analysis 2.26 The Proposed solution should be able to corelate local APT attacks with Golbal historical APT attacks.. 2.27 The Proposed solution should support atleast 1 Gbps of throughput 2.28 The Proposed solution should have two (2) x 1TB Hard disks 2.29 The Proposed solution should support atleast 5x10/100/1000 Ethernet Interfaces 2.30 The Proposed solution should have capability to detect attacker behaviour within the network like (hash					

	dumping, Hash Validation, Data Extraction from Database servers, DNS queries to suspicious or known C&C Servers, etc..) 2.31 The Proposed solution should be able to detect malicious and suspicious behaviors during non office hours 2.32 The Proposed solution should have on box correlation of threats 2.33 The Proposed solution should support open Web Services API for 3rd party or scripting integration 2.34 The Proposed solution should support Manual submission for analysis 2.35 The Proposed solution should be able toIdentify suspicious embedded object in document file like OLE & Macro extraction, Shellcode & exploit matching 2.36 The Proposed solution should be able to Detect malicious or malformed file Zero-day detection and Scripting embedded 2.37 The proposed solution should be able to detect and alert if file has suspicious attributes like True-file type, File extension & Naming trick The proposed solution should support Microsoft Office 2016 application for Office file analysis in sandbox images 3.0 Report 3.1 The proposed solution should have an intuitive Dashboard that offers real time threat visibility 3.2 The proposed solution should provide reports with (but not limited to) HTML/CSV/PDF formats 3.3 The proposed solution should provide an intuitive Dashboard that offers real time threat visibility and attack characteristics. 3.4 review detection details based on predefined smart filters 3.5 The proposed solution should be able to schedule reports and also provide the flexibility to generate on-demand reports in daily/weekly/monthly/yearly or specific range (by day and time) 3.6 The proposed solution should support logging of important parameters like Source IP, Destination IP, ports, protocol, Domain, time stamp etc. of the attacks sessions. 3.7 The proposed solution should have the flexibility to provides customizable dashboard. 3.8 The proposed solution should have the option to provide Investigative dashboard that is capable of displaying correlated graphical data that is based on link-graph, geo-map, chart , tree-map/pivot table. 3.9 The proposed solution should be able to provide in-depth reporting including the level of risk, static scanning results, sandbox assessment, network activity analysis, and a source tracking information. 3.10 The proposed solution must be able to provide intelligence portal for malware information, threat profile and containment remediation recommendations where applicable 3.12 The proposed solution should have capabilities to configure separate notifications to the administrator or individuals based on specific events like, Sandbox detection, Black List and license events etc. 3.13 The Proposed solution should be able to					

	generate out of box reports to highlight Infections, C&C behavior, Lateral Moment, Asset and data discovery and data Exfiltration 3.14 The proposed solution should have the ability to programmatically output sandbox detections in OpenIOC format 3.15 The Proposed solution should be able to determine overall host vulnerability levels by mapping threats to threat lifecycle rules 3.16 The Proposed solution should be able to provide details of prevalence, maturity of a given file 4.0 Authentication Administration and Configuration Requirement 4.1 The proposed solution shall support Local Password authentication schemes 4.2 The proposed solution shall support Remote administration using SSH/HTTPS 4.3 The proposed solution shall support CLI, GUI/Web based Administration Console. 5 SUPPORT 5.1 Vendor shall provide daily 8 by 5 phone, email, and remote support with critical level onsite assistance 5.2 Vendor must have access to high-level of support via the principal for critical level concerns 5.3 Vendor must provide professional implementation services 5.4 Vendor must provide an annual health check to ensure that the product is properly working 5.5 Vendor must provide pro-active Threat Management - giving the PROCURING ENTITY alerts must there be any malware threat detected in other parts of the world that may pose a problem for the PROCURING ENTITY. 6.0 RECOGNITION 6.1 Must be an Industry Recognition for Breach Detection and Performance				
TOTAL APPROVED BUDGET FOR THE CONTRACT (ABC):					**Php 1,750,000.00**

RESERVATION CLAUSE

The Advanced Science and Technology Institute 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.