ASTI-FM 03-10
REV 3/13 January 2020

DOST-ASTI Bids and Awards Committee
REQUEST FOR QUOTATION

Kind of Procurement Activity:	Negotiated Procurement:Small-value Procurement		
Deadline of Submission of Bids:	May-27-2020, 2:00 PM		
RFQ No.:	20-04-3121	**Date:**	May-22-2020
PR No.:	GAA-20-04-9885	**Date:**	April-15-2020

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,

Pedrito B. Mangahas
2020.05.22 14:10:50
+08'00'

PEDRITO B. MANGAHAS
Chairperson, BAC-1

NO.	TECHNICAL SPECIFICATIONS	QTY	UNIT	UNIT PRICE(Php)	TOTAL PRICE(Php)
1	**Lease of Intrusion Detection System** I. General Specs 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, suspicious mail attachments and internal infections. 2. The proposed solution should support the native CEF, LEEF format for SIEM log integration. 3. Proposed anti-APT solution should perform advanced network detection and analysis of the enterprise's internal network. 4. Upon detection of the threat, the proposed solution should be able to perform behavior analysis for advance detection. 5. Proposed solution should have event detection capabilities that should include malware type, severity, source and destination of attack. 6. Solution should provide risk-based alerts or logs to help prioritize remediation effort. 7. Solution should be deployed on premise along with on-premise sandboxing capability. 8. The proposed solution should be able to store real payload of the detected threats. 9. The proposed solution should be able to store packet captures (PCAP) of all malicious communications	1	lot	795000.00	795,000.00

Postal Address : ASTI Bldg., U.P Technology Park Complex, C.P. Garcia Ave., Diliman, Quezon City 1101
Website : www.asti.dost.gov.ph
Email : info@asti.dost.gov.ph
Tel No. : +632 8249-8500 +632 8426-9755
Fax No. : +632 8426-9764

	detected by sandbox. 10. The proposed solution should use OS sandboxes for detecting zero-day malwares. This should not be a CPU or chip-based function. 11. Solution should have the ability to interrupt malicious communication 12. Solution should have no limitation in terms of supported users and limitation should be accounted in terms of bandwidth only 13. 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. 14. Solution should be able to integrate with its own threat intelligence portal for further investigation, understanding and remediation an attack. 15. Solution deployment should cause limited interruption to the current network environment. 16. The proposed solution should allow the customer to gain visibility to the internal networks and flag detected threats immediately. 17. The proposed solution should have the ability to support out-of-band detection 18. The proposed solution should be able to detect lateral movements of the attacker without the need of installing agents on endpoint/server machines 19. The proposed solution should not have any port-based limitation and should support all ports. 20. The proposed solution should support at least 100+ protocols for inspection. 21. The proposed solution should be able to monitor traffic from multiple segments like WAN, DMZ, Server Farm, Wi-Fi network, MPLS links etc. simultaneously on a single appliance. 22. The proposed solution should be able to support up to 5 network segments on a single appliance. 23. The proposed solution should be able to detect any suspicious communication within and outside of customer's network. 24. The proposed solution should be able to detect communications to known command and control centers. 25. The proposed solution should be able to detect reputation of URLs being accessed. 26. The proposed solution should be able to identify and help the customer to understand the severity and stage of each attack. 27. The proposed solution should have built-in capabilities to add exceptions for detections. 28. The proposed solution should have capabilities to configure files, IP, URLs and Domains to black list or white list 29. The proposed solution should support multiple protocols for inspection. a. Example: HTTP, FTP, SMTP, SNMP, IM, IRC,DNS and P2P protocols b. Internal direction: SMB, Database protocol (MySQL, MSSQL, Oracle) on a single device 30. The proposed solution should have a built-in document vulnerabilities detection engine to assure analysis precision and analysis efficiency. 31. The proposed solution should have a correlation engine to automatically correlate across multiple					

protocols, multiple sessions and volume traffic analysis.
32. The proposed solution must provide a web service interface/API for customer to customize their own system integration.
33. The proposed solution must have capabilities to correlate the detections on the device itself.
34. The proposed solution should support remote packet capturing to pass Kerberos traffic from remote locations for analysis
35. The proposed solution should monitor Inter-VM traffic on a Port Mirror Session.
36. 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.
37. The proposed solution should be able to run at least 4 parallel sandboxes for analysis of payload
38. The proposed solution should have an option to allow sandbox instances to use a proxy for internet access.
39. The proposed solution should have support for analysis of embedded URLs in PDFs
40. The proposed solution should support IPv6 environments, and be able to tap into IPv6 network streams, perform analysis, and output IPv6-based network detection results.

II. Malware Analysis
1. The proposed solution should have multiple built-in virtual execution environments within a single appliance to simulate file activities and find malicious behaviors for advanced threat detection. The solution should be able to provide detection details including the CVE-ID, HTTP referrer and targeted attack campaign name
2. The proposed solution should be able to provide customizable sandbox to fulfill customer's environments and needs.
3. The sandbox must support multiple operating systems and for both 32-bits and 64-bits OS
4. Solution must have the capability to analyze large files. Must be able to support more than 40MB file size
5. Sandbox must have the ability to simulate the entire threat behavior. i.e. honeynet and honeypot framework
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.
7. The proposed solution should have grayware detection capabilities.
8. The proposed solution should be able to detect any malicious communication within and outside of customer's network.
9. The proposed solution must provide a web service interface/API for customer to customize their own system integration.

	10. The proposed solution should be able to detect network attacks and exploits. 11. The proposed solution should have the capability to scale out the detection when the bandwidth increases in the future. 12. 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 13. The proposed solution should have a built-in document vulnerabilities detection engine to assure analysis precision and analysis efficiency. 14. The proposed solution must provide the capability to export network packet files and encrypted suspicious files for further investigation. 15. The proposed solution has the capability to performs tracking and analysis of virus downloads and suspicious files. 16. The proposed solution should support exporting of analysis results such as C&C server IP and malicious domain listing 17. The proposed solution should have capabilities to scan inside password protected archives 18. The proposed solution should have capabilities to detect malwares and spywares on Windows and non-Windows platforms 19. The proposed solution should have an option to configure unrestricted Internet for sandboxes 20. The proposed solution should have capabilities to configure files, IP, URLs and Domains to blacklist or white list 21. The proposed solution must have capabilities to detect Mac, Linux and mobile malwares 22. The proposed solution should have capability to include user-defined and context-derived passwords for protected archives 23. The proposed solution should have capabilities to configure separate notifications to the administrator or individuals based on specific events like, Sandbox detection, blacklist and license events etc. 24. The proposed solution should be able to detect known malwares before sending suspicious files to sandbox for analysis 25. The proposed solution should be able to correlate local APT attacks with Global historical APT attacks. 26. The proposed solution should support at least 1 Gbps of throughput 27. The proposed solution should have two (2) x 1TB Hard disks 28. The proposed solution should support at least 5x10/100/1000 Ethernet Interfaces 29. The proposed solution should have capability to detect attacker behavior within the network like (hash dumping, Hash Validation, Data Extraction from Database servers, DNS queries to suspicious or known C&C Servers, etc.) 30. The proposed solution should be able to detect malicious and suspicious behaviors during non- office hours 31. The proposed solution should have on box				

	correlation of threats 32. The proposed solution should support open Web Services API for 3rd party or scripting integration 33. The proposed solution should support manual submission for analysis 34. The proposed solution should be able to identify suspicious embedded objects in document files like OLE & Macro extraction, Shellcode & exploit matching 35. The proposed solution should be able to detect malicious or malformed files, zero-day detection and embedded scripting. 36. 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. III. Reporting 1. The proposed solution should have an intuitive dashboard that offers real time threat visibility 2. The proposed solution should provide reports with (but not limited to) HTML/CSV/PDF formats 3. The proposed solution should provide an intuitive dashboard that offers real time threat visibility and attack characteristics. 4. Review detection details based on predefined smart filters 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) 6. The proposed solution should support logging of important parameters like Source IP, Destination IP, ports, protocol, Domain, time stamp etc. of the attack's sessions. 7. The proposed solution should have the flexibility to provide customizable dashboard. 8. The proposed solution should have the option to provide an investigative dashboard that can display correlated graphical data based on link-graph, geo-map, chart, tree-map/pivot table. 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. 10. The proposed solution must be able to provide intelligence portal for malware information, threat profile and containment remediation recommendations where applicable 11. The proposed solution should have capabilities to configure separate notifications to the administrator or individuals based on specific events like, sandbox detection, blacklist and license events etc. 12. The proposed solution should be able to generate out of box reports to highlight Infections, C&C behavior, lateral movement, asset and data discovery and data exfiltration 13. The proposed solution should have the ability to programmatically output sandbox detections in OpenIOC format					

14. The proposed solution should be able to determine overall host vulnerability levels by mapping threats to threat lifecycle rules
15. The proposed solution should be able to provide details of prevalence, maturity of a given file

IV. Authentication Administration and Configuration Requirement
1. The proposed solution shall support local password authentication schemes
2. The proposed solution shall support remote administration using SSH/HTTPS
3. The proposed solution shall support CLI, GUI/Web based Administration Console.

V. SUPPORT
1. Vendor shall provide daily 8 by 5 phone, email, and remote support with critical level onsite assistance
2. Vendor must have access to high-level of support via the principal for critical level concerns
3. Vendor must provide professional implementation services
4. Vendor must provide an annual health check to ensure that the product is properly working
5. Vendor must provide pro-active Threat Management - giving the PROCURING ENTITY alerts should there be any malware threat detected in other parts of the world that may pose a problem for the PROCURING ENTITY.

VI. OTHERS
1. The license renewal should start upon expiration of the existing license on June 20, 2020.
2. The lease period is from June 21, 2020 to December 31, 2020.
3. The winning bidder is required to conduct a requirements analysis for the configuration of the whole setup within 30 calendar days after issuance of Notice to Proceed. The bidder must submit complete documentation of the entire work plan, resource (hw/sw) requirements, manpower requirements, network design, course syllabus (for knowledge transfer) etc.
4. The winning bidder is required to deliver the solution to an ASTI-designated data center within 45 calendar days after issuance of Notice to Proceed. The bidder is also required to deploy and configure the device within 65 calendar days after Notice to Proceed.
5. The winning bidder may be required to conduct knowledge transfer for the solution delivered for at most 3 people. The total number of training days should not exceed 3. All costs related to the training will be shouldered by the winning bidder. These include but not limited to, lease of venue, meals, transportation of participants to and from the training venue, trainer fees, etc. ASTI may, at its discretion, prefer to conduct the training in its office premises. In

	that case, the lease of venue may be waived. The training must be conducted within ninety (90) calendar days from implementation acceptance. 6. At the end of the implementation phase, the winning bidder must submit a comprehensive documentation on the final setup. The documentation should include a network / logical diagram, configuration settings, and all manuals. 5. Payment will be made every quarter after acceptance.				
	TOTAL APPROVED BUDGET FOR THE CONTRACT:				**Php 795,000.00**

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.

ASTI-FM 03-09
REV 1/13 January 2020

Department: Knowledge Management Division	PR No. GAA-20-04-9885	Date: 2020-04-15
Section: MIS	SAI No.	Date:

Item No	Item Description	Quantity	Unit	Unit Cost	Total Amount
1	**Lease of Intrusion Detection System** I. General Specs 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, suspicious mail attachments and internal infections. 2. The proposed solution should support the native CEF, LEEF format for SIEM log integration. 3. Proposed anti-APT solution should perform advanced network detection and analysis of the enterprise's internal network. 4. Upon detection of the threat, the proposed solution should be able to perform behavior analysis for advance detection. 5. Proposed solution should have event detection capabilities that should include malware type, severity, source and destination of attack. 6. Solution should provide risk-based alerts or logs to help prioritize remediation effort. 7. Solution should be deployed on premise along with on-premise sandboxing capability. 8. The proposed solution should be able to store real payload of the detected threats. 9. The proposed solution should be able to store packet captures (PCAP) of all malicious communications detected by sandbox. 10. The proposed solution should use OS sandboxes for detecting zero-day malwares. This should not be a CPU or chip-based function. 11. Solution should have the ability to interrupt malicious communication 12. Solution should have no limitation in terms of supported users and limitation should be accounted in terms of bandwidth only 13. 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. 14. Solution should be able to integrate with its own threat intelligence portal for further investigation, understanding and remediation an attack. 15. Solution deployment should cause limited interruption to the current network environment. 16. The proposed solution should allow the customer to gain visibility to the internal networks and flag detected threats immediately. 17. The proposed solution should have the ability to support out-of-band detection 18. The proposed solution should be able to detect lateral movements of the attacker without the need of installing agents on endpoint/server machines 19. The proposed solution should not have any port-based limitation and should support all ports. 20. The proposed solution should support at least 100+ protocols for inspection. 21. The proposed solution should be able to monitor traffic from multiple segments like WAN, DMZ, Server Farm, Wi-Fi network,	1	lot	795,000.00	795,000.00

Postal Address : ASTI Bldg., U.P Technology Park Complex, C.P. Garcia Ave., Diliman, Quezon City 1101
Website : www.asti.dost.gov.ph
Email : info@asti.dost.gov.ph
Tel No. : +632 8249-8500, +632 8426-9755
Fax No. : +632 8426-9764

	MPLS links etc. simultaneously on a single appliance. 22. The proposed solution should be able to support up to 5 network segments on a single appliance. 23. The proposed solution should be able to detect any suspicious communication within and outside of customer's network. 24. The proposed solution should be able to detect communications to known command and control centers. 25. The proposed solution should be able to detect reputation of URLs being accessed. 26. The proposed solution should be able to identify and help the customer to understand the severity and stage of each attack. 27. The proposed solution should have built-in capabilities to add exceptions for detections. 28. The proposed solution should have capabilities to configure files, IP, URLs and Domains to black list or white list 29. The proposed solution should support multiple protocols for inspection. a. Example: HTTP, FTP, SMTP, SNMP, IM, IRC,DNS and P2P protocols b. Internal direction: SMB, Database protocol (MySQL, MSSQL, Oracle) on a single device 30. The proposed solution should have a built-in document vulnerabilities detection engine to assure analysis precision and analysis efficiency. 31. The proposed solution should have a correlation engine to automatically correlate across multiple protocols, multiple sessions and volume traffic analysis. 32. The proposed solution must provide a web service interface/API for customer to customize their own system integration. 33. The proposed solution must have capabilities to correlate the detections on the device itself. 34. The proposed solution should support remote packet capturing to pass Kerberos traffic from remote locations for analysis 35. The proposed solution should monitor Inter-VM traffic on a Port Mirror Session. 36. 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. 37. The proposed solution should be able to run at least 4 parallel sandboxes for analysis of payload 38. The proposed solution should have an option to allow sandbox instances to use a proxy for internet access. 39. The proposed solution should have support for analysis of embedded URLs in PDFs 40. The proposed solution should support IPv6 environments, and be able to tap into IPv6 network streams, perform analysis, and output IPv6-based network detection results. II. Malware Analysis 1. The proposed solution should have multiple built-in virtual execution environments within a single appliance to simulate file activities and find malicious behaviors for advanced threat detection. The solution should be able to provide detection details including the CVE-ID, HTTP referrer and targeted attack campaign name 2. The proposed solution should be able to provide customizable sandbox to fulfill customer's environments and needs. 3. The sandbox must support multiple operating systems and for both 32-bits and 64-bits OS 4. Solution must have the capability to analyze large files. Must be able to support more than 40MB file size 5. Sandbox must have the ability to simulate the entire threat behavior. i.e. honeynet and honeypot framework					

	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. 7. The proposed solution should have grayware detection capabilities. 8. The proposed solution should be able to detect any malicious communication within and outside of customer's network. 9. The proposed solution must provide a web service interface/API for customer to customize their own system integration. 10. The proposed solution should be able to detect network attacks and exploits. 11. The proposed solution should have the capability to scale out the detection when the bandwidth increases in the future. 12. 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 13. The proposed solution should have a built-in document vulnerabilities detection engine to assure analysis precision and analysis efficiency. 14. The proposed solution must provide the capability to export network packet files and encrypted suspicious files for further investigation. 15. The proposed solution has the capability to performs tracking and analysis of virus downloads and suspicious files. 16. The proposed solution should support exporting of analysis results such as C&C server IP and malicious domain listing 17. The proposed solution should have capabilities to scan inside password protected archives 18. The proposed solution should have capabilities to detect malwares and spywares on Windows and non-Windows platforms 19. The proposed solution should have an option to configure unrestricted Internet for sandboxes 20. The proposed solution should have capabilities to configure files, IP, URLs and Domains to blacklist or white list 21. The proposed solution must have capabilities to detect Mac, Linux and mobile malwares 22. The proposed solution should have capability to include user-defined and context-derived passwords for protected archives 23. The proposed solution should have capabilities to configure separate notifications to the administrator or individuals based on specific events like, Sandbox detection, blacklist and license events etc. 24. The proposed solution should be able to detect known malwares before sending suspicious files to sandbox for analysis 25. The proposed solution should be able to correlate local APT attacks with Global historical APT attacks. 26. The proposed solution should support at least 1 Gbps of throughput 27. The proposed solution should have two (2) x 1TB Hard disks 28. The proposed solution should support at least 5x10/100/1000 Ethernet Interfaces 29. The proposed solution should have capability to detect attacker behavior within the network like (hash dumping, Hash Validation, Data Extraction from Database servers, DNS queries to suspicious or known C&C Servers, etc.) 30. The proposed solution should be able to detect malicious and suspicious behaviors during non- office hours 31. The proposed solution should have on box correlation of threats 32. The proposed solution should support open Web Services API for 3rd party or scripting integration					

33. The proposed solution should support manual submission for analysis
34. The proposed solution should be able to identify suspicious embedded objects in document files like OLE & Macro extraction, Shellcode & exploit matching
35. The proposed solution should be able to detect malicious or malformed files, zero-day detection and embedded scripting.
36. 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.

III. Reporting
1. The proposed solution should have an intuitive dashboard that offers real time threat visibility
2. The proposed solution should provide reports with (but not limited to) HTML/CSV/PDF formats
3. The proposed solution should provide an intuitive dashboard that offers real time threat visibility and attack characteristics.
4. Review detection details based on predefined smart filters
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)
6. The proposed solution should support logging of important parameters like Source IP, Destination IP, ports, protocol, Domain, time stamp etc. of the attack's sessions.
7. The proposed solution should have the flexibility to provide customizable dashboard.
8. The proposed solution should have the option to provide an investigative dashboard that can display correlated graphical data based on link-graph, geo-map, chart, tree-map/pivot table.
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.
10. The proposed solution must be able to provide intelligence portal for malware information, threat profile and containment remediation recommendations where applicable
11. The proposed solution should have capabilities to configure separate notifications to the administrator or individuals based on specific events like, sandbox detection, blacklist and license events etc.
12. The proposed solution should be able to generate out of box reports to highlight Infections, C&C behavior, lateral movement, asset and data discovery and data exfiltration
13. The proposed solution should have the ability to programmatically output sandbox detections in OpenIOC format
14. The proposed solution should be able to determine overall host vulnerability levels by mapping threats to threat lifecycle rules
15. The proposed solution should be able to provide details of prevalence, maturity of a given file

IV. Authentication Administration and Configuration Requirement
1. The proposed solution shall support local password authentication schemes
2. The proposed solution shall support remote administration using SSH/HTTPS
3. The proposed solution shall support CLI, GUI/Web based Administration Console.

V. SUPPORT
1. Vendor shall provide daily 8 by 5 phone, email, and remote

	support with critical level onsite assistance 2. Vendor must have access to high-level of support via the principal for critical level concerns 3. Vendor must provide professional implementation services 4. Vendor must provide an annual health check to ensure that the product is properly working 5. Vendor must provide pro-active Threat Management - giving the PROCURING ENTITY alerts should there be any malware threat detected in other parts of the world that may pose a problem for the PROCURING ENTITY. VI. OTHERS 1. The license renewal should start upon expiration of the existing license on June 20, 2020. 2. The lease period is from June 21, 2020 to December 31, 2020. 3. The winning bidder is required to conduct a requirements analysis for the configuration of the whole setup within 30 calendar days after issuance of Notice to Proceed. The bidder must submit complete documentation of the entire work plan, resource (hw/sw) requirements, manpower requirements, network design, course syllabus (for knowledge transfer) etc. 4. The winning bidder is required to deliver the solution to an ASTI-designated data center within 45 calendar days after issuance of Notice to Proceed. The bidder is also required to deploy and configure the device within 65 calendar days after Notice to Proceed. 5. The winning bidder may be required to conduct knowledge transfer for the solution delivered for at most 3 people. The total number of training days should not exceed 3. All costs related to the training will be shouldered by the winning bidder. These include but not limited to, lease of venue, meals, transportation of participants to and from the training venue, trainer fees, etc. ASTI may, at its discretion, prefer to conduct the training in its office premises. In that case, the lease of venue may be waived. The training must be conducted within ninety (90) calendar days from implementation acceptance. 6. At the end of the implementation phase, the winning bidder must submit a comprehensive documentation on the final setup. The documentation should include a network / logical diagram, configuration settings, and all manuals. 5. Payment will be made every quarter after acceptance.				
				TOTAL	**795,000.00**

Purpose: Lease of Intrusion Detection System to be used in ASTI's local network

Charge To:

■ ASTI-GAA ❑ GIA/Contract Research:

❑ MOOE ❑ MOOE
❑ CO ❑ CO

Mode of Procurement: (Please check one)

❑ Alternative Mode ❑ Public Bidding ❑ Cash Advance

	Requested by:	Approved by:
Signature:	Digitally signed by Rene Mendoza Date: 2020.04.15 16:00:51 +08'00'	Digitally signed by ALVIN E. RETAMAR Date: 2020.04.21 12:26:28 +08'00'
Printed Name:	Rene Mendoza	Alvin Retamar
Designation:	Chief Science Research Specialist	Chief Science Research Specialist

Republic of the Philippines
Department of Science and Technology
ADVANCED SCIENCE AND TECHNOLOGY INSTITUTE

CANVASS SHEET

Item No.	Description	Qty.	Unit	Price Quotations (₱)[1]					
				CT Link		Supplier 2		Supplier 3	
				Unit Price	Total	Unit Price	Total	Unit Price	Total
1	**Lease of Intrusion Detection System**	**1**	**lot**	**795,000.00**	**795,000.00**				
	Delivery Terms	**45**	**days**						
	Payment Terms								
	Delivery Terms								
	Payment Terms								

Put a check (✓) what is applicable.

____✓____ One (1) price quotation was received in preparation for the above procurement transaction/s.

_____ Two (2) price quotations were received in preparation for the above procurement transaction/s.

_____ Three (3) price quotations were received in preparation for the above procurement transaction/s.

Attached is/are the proposal/s acquired from the supplier/s.

Canvassed By:

Khatlyn Rabago
SRS II

Noted By:

RENE C. MENDOZA
Division Chief

Digitally signed by Rene Mendoza
Date: 2020.04.15 15:59:48 +08'00'

1 Prices are inclusive of taxes and other charges.

Department of Science and Technology

Advanced Science and Technology Institute

C.P. Garcia Ave., U.P. Technopark, U.P. Campus, Diliman, Quezon City 1101

Annual Procurement Plan for 2020

APP-2020-NCSE-011 (SUPPLEMENTAL)

Code		Procurement Program/Activity/Project	PMO/ End-User	Mode of Procurement	Schedule for Each Procurement Activity				Source of Fund	Estimated Budget (PhP)			Remarks (Brief Description of Program/Activity/ Project)
					Advertisment / Posting of IB/REI	Submission/ Opening of Bids	Notice of Award	Contract Signing		Total	MOOE	CO	
50203220 02	11	Technical Book: The Elements of Computing Systems, second edition: Building a Modern Computer from First Principles (2nd Edition, Hardbound) by Noam Nisan, Shimon Schocken; 2nd Edition (Novemner, 2020); The MIT Press;ISBN-10:0262640686 ISBN-13:978-0262640688	CSD	NP-53.9 Small Value Procurement	2nd Quarter of 2020				GOP	5,005.00	5,005.00	0.00	Gul.ai
50203220 02	11	Techical Book: Practical Quantum Computing for Developers: Programming Quantum Rigs in the Cloud using Python, Quantum Assembly Language and IBM QExperience (First Edition, Paperback); Author: Vladimir Silva; Edition: 1st Edition, December 13, 2018; Publisher: Apress; ISBN: ISBN-10:1484242173 ISBN-13:978-1484242179	CSD	NP-53.9 Small Value Procurement	2nd Quarter of 2020				GOP	2,000.00	2,000.00	0.00	Gul.ai
50203220 02	11	Technical Book: Quantum Computing for Developers (First Edition, Paperback); Author: Johan Vos; Edition: 1st Edition May 2020; Publisher: Manning Publication; ISBN: ISBN-10:1617296325 ISBN-13: 978-1617296321	CSD	NP-53.9 Small Value Procurement	2nd Quarter of 2020				GOP	3,600.00	3,600.00	0.00	Gul.ai
50203220 02	11	Technical Book: Mastering Quantum Computing with IBM QX: Explore the world of quantum computing using the Quantum Composer and Qiskit (First Edition, Paperback); Author:Christine Corbelt Moran; Edition: 1st Edition January 31, 2019; Publication: Packet Publishing; ISBN: ISBN-10:1789136431 ISBN-13:978-1789136432	CSD	NP-53.9 Small Value Procurement	2nd Quarter of 2020				GOP	3,300.00	3,300.00	0.00	Gul.ai
50203220 02	11	Technical Book: Problems and Solutions in Quantum Computing and Quantum Information (4th Edition, Hardbound); Author:Willi-Hans Steeb, Yorick Hardy; Edition: 4th Edition April 26, 2018; Publication: World Scientific; ISBN: ISBN-10:9813238402 ISBN-13: 978-9813238404	CSD	NP-53.9 Small Value Procurement	2nd Quarter of 2020				GOP	6,450.00	6,450.00	0.00	Gul.ai
50203220 02	11	Technical Book: Programming Quantum Computers: Essential Algorithms and Code Samples (1st Edition, Paperback); Author: Eric R. Johnston, Nic Harrigan, Mercedes Gimeno-Segovia; Edition: 1st Edition July 23, 2019; Publication: O'Reilly Media; ISBN: ISBN-13:978-1492039686 ISBN-10: 1492039683	CSD	NP-53.9 Small Value Procurement	2nd Quarter of 2020				GOP	2,860.00	2,860.00	0.00	Gul.ai
50203220 02	11	Technical Book: Quantum Computing: An Applied Approach (1st Edition, Hardbound); Author: Jack D. Hidary; Edition: 1st Edition August 30, 2019; Publication: Springer; ISBN-10:3030239217 ISBN-13:978-3030239213	CSD	NP-53.9 Small Value Procurement	2nd Quarter of 2020				GOP	2,200.00	2,200.00	0.00	Gul.ai
50203220 02	11	Technical Book: No-Nonsense Quantum Mechanics: A Student-Friendly Introduction (Second Edition, Paperback); Author: Jakob Schwichtenberg; Edition: 2nd Edition December 1, 2018; Publication: Independently Published; ISBN-10:1790455383 ISBN-13:978-1790455386	CSD	NP-53.9 Small Value Procurement	2nd Quarter of 2020				GOP	2,100.00	2,100.00	0.00	Gul.ai
50203220 02	11	Technical Book: Mathematics of Quantum Computing: An Introduction (First Edition, Hardbound); Author: Wolfgang Scherer; Edition: 1st Edition November13, 2019; Publication: Springer; ISBN-10:303012357X ISBN-13:978-3030123574	CSD	NP-53.9 Small Value Procurement	2nd Quarter of 2020				GOP	10,010.00	10,010.00	0.00	Gul.ai
50203220 02	11	Technical Book: Foundations of Deep Reinforcement Learning: Theory and Practice in Python (Addison-Wesley Data & Analytics Series) (First Edition, Paperback); Author: Laura Graesser, Wah Loon Keng; Edition: 1st Edition December 15, 2019; Publication: Addison-Wesley Data and Analytics Series; ISBN-13: 978-0135172384 ISBN-10:0135172381	CSD	NP-53.9 Small Value Procurement	2nd Quarter of 2020				GOP	2,359.00	2,359.00	0.00	Gul.ai
50203220 02	11	Technical Book: The Design and Analysis of Computer Experiments (Springer Series in Statistics) (Second edition, Hardbound); Editor: Thomas J.Santner, Brian J. Williams, William I. Notz; Edition 2nd Edition, 2018 Edition January 09, 2019; Publication: Springer; ISBN-10149398845X ISBN-13:978-1493988457	CSD	NP-53.9 Small Value Procurement	2nd Quarter of 2020				GOP	7,250.00	7,250.00	0.00	Gul.ai
50203220 02	11	Technical Book: Hands-On Data Science for Marketing: Improve your marketing strategies with machine learning using Python and R; Editor: Yoon Hyup Hwang; Edition: 1st Edition March 2019; Publication: Packt Publishing; ISBN-13:978-1789346343 ISBN-101789346347	CSD	NP-53.9 Small Value Procurement	2nd Quarter of 2020				GOP	3,250.00	3,250.00	0.00	Gul.ai
50203220 02	11	Technical Book: A Guide to Algorithm Design: Paradigms, Methods, and Complexity Analysis; Editor: Anne Benoit, Yves Robert, Frederic Vivien; Edition 2013, Hardcover; Publication: CRC Press; 1st edition (August 27, 2013); ISBN-13: 978-1439825648 ISBN-10:1439825645	CSD	NP-53.9 Small Value Procurement	2nd Quarter of 2020				GOP	6,578.00	6,578.00	0.00	Gul.ai
50212030 00	11	Extension of Security Services for Eight (8) months (01 May 2020 - December 31, 2020)	FAD	Extension of Contract for General Support Services	2nd - 4th Quarter of 2020				GOP	1,366,454.48	1,366,454.48	0.00	
50299070 99	11	Lease of Intrusion Detection System The lease period is from June 21, 2020 to Dec. 31, 2020	KMD	NP-53.9 Small Value Procurement	2nd Quarter of 2020				GOP	795,000.00	795,000.00	0.00	
50204020 00	11	Data Center Electricity Expense for 1 month	SSED	Renewal of WETI	2nd Quarter of 2020				GOP	200,000.00	200,000.00	0.00	SAGAP

50211990 00	11	Fabrication of electronic panel graphic overlay Size: 4.9in x 2.0in Material: GE 8B35-112 Lexan film 0.25mm Overlay finish: Matt Screen Color : 5 Protective Film: 3M 3K04 Embossed buttons: 4 Rear adhesive: 3M Quantity: 50pcs Delivery: 2 weeks upon receipt of Notice to Proceed Manufacturing drawings will be provided by end-user upon request Price is inclusive of government fees, taxes and duties	SSED	NP-53.9 Small Value Procurement	2nd Quarter of 2020	GOP	9,000.00	9,000.00	0.00	Optimization
50211990 00	11	PCB Fabrication of tuner and demodulator boards Number of Designs: 6 Layers: 2,4	SSED	NP-53.9 Small Value Procurement	2nd Quarter of 2020	GOP	60,000.00	60,000.00	0.00	RuralSync
50207020 02	11	ISDB-T Receiver Eval Board Evaluation Board for ISDB-T Receiver Tuner Features: ATSC/QAM, DVB-T2/T/C2/C, ISDB-T/C, DTMB	SSED	NP-53.9 Small Value Procurement	2nd Quarter of 2020	GOP	55,488.00	55,488.00	0.00	RuralSync
50203990 00	11	1.00mm copper plate 100mm x 100mm x 1.00mm Pure Copper Metal Sheet	SSED	NP-53.9 Small Value Procurement	2nd Quarter of 2020	GOP	3,840.00	3,840.00	0.00	RuralSync
50203990 00	11	1.00mm copper plate 100mm x 100mm x 1.00mm Pure Copper Metal Sheet	SSED	NP-53.9 Small Value Procurement	2nd Quarter of 2020	GOP	1,680.00	1,680.00	0.00	RuralSync
50203990 00	11	ISDB-T Tuner IC ATSC/QAM, DVB-T2/T/C2/C, ISDB-T/C, DTMB 1.7 MHz, 6 MHz, 7 MHz, 8 MHz, and 10 MHz channel bandwidths	SSED	NP-53.9 Small Value Procurement	2nd Quarter of 2020	GOP	1,246.95	1,246.95	0.00	RuralSync
50213050 03	11	2.5-inch SATA III 1 Terabyte Internal SSD SATA 6 Gb/s Interface, compatible with SATA 3 Gb/s & SATA 1.5 Gb/s	SSED	NP-53.9 Small Value Procurement	2nd Quarter of 2020	GOP	30,000.00	30,000.00	0.00	SAR with AIS
50604050 03	11	Downconverter	SSED	Competitive Bidding	2nd Quarter of 2020	GOP	1,500,000.00	0.00	1,500,000.00	Grasped
50604050 03	11	Spectrum Analyzer	SSED	Competitive Bidding	2nd Quarter of 2020	GOP	5,500,000.00	0.00	5,500,000.00	Grasped
50205030 00	11	Local Transport to Court of Appeals CDO - City Tourism Office, City Hall Complex, CDO for 8 months	SSED	Competitive Bidding	2nd - 4th Quarter of 2020	GOP	315,000.00	315,000.00	0.00	Innovate
						TOTAL	**9,894,671.43**	**2,894,671.43**	**7,000,000.00**	

Prepared and Consolidated By:

CHERALINE A. BORJA
Member, Bids and Awards Committee Secretariat

Recommending Approval:

Pedrito B. Mangahas
2020.05.14 17:02:23 +08'00'

PEDRITO B. MANGAHAS
Chairperson, Bids and Awards Committee - 1

PAUL JOHN M. SERRANO
Chairperson, Bids and Awards Committee - 2

Approved By:

Digitally signed by ALVIN E. RETAMAR
Date: 2020.05.14 22:14:39 +08'00'

ALVIN E. RETAMAR
Officer-in-Charge, DOST-ASTI