



Republic of the Philippines
DEPARTMENT OF THE INTERIOR AND LOCAL GOVERNMENT
BUREAU OF JAIL MANAGEMENT AND PENOLOGY
NATIONAL HEADQUARTERS

144 Mindanao Avenue, Quezon City
Trunk lines: (+632)927-6383 • 927-5505
Email Address: chief@bjmp.gov.ph Website: www.bjmp.gov.ph

BIDS AND AWARDS COMMITTEE
Bid Bulletin No. 1

**SUPPLY, DELIVERY, INSTALLATION AND CONFIGURATION OF END POINT
SECURITY SOLUTION**
G-2020-025

This Bid Bulletin No. 1 is being issued to further clarify, modify and amend items/specifications in the bidding documents in response to clarification from prospective bidder and to confirm key issues addressed during the Pre-bid Conference on October 19, 2020 for the aforementioned project.

FROM	TO
Invitation to Bid 9. Bid opening shall be on November 3, 2020 at 2:30 PM via ZOOM (Meeting ID: 963 4019 5074 and Password 533115). Bids will be opened in the presence of the bidders' representatives who choose to attend the activity	Invitation to Bid 9. Bid opening shall be on November 3, 2020 at 2:30 PM via ZOOM (<u>Meeting ID: 978 1502 1226 and Password 546026</u>). Bids will be opened in the presence of the bidders' representatives who choose to attend the activity
Technical Specifications 1.1.a Must have a unified/single console and dashboard for central management of all components, such as, advanced endpoint protection, web gateway, server security, mobile control and so on. 1.1.e Must be able to support installation of endpoint agents on the following operating systems, such as: Microsoft Windows 8/10 (32 and 64 bits); Windows Server 2008 and up, Mac OS, IOS, Android, Linux OS, Ubuntu and Later editions	Technical Specifications 1.1.a Must have a unified/single console and dashboard for central management of all components, such as, advanced endpoint protection, <u>web security and control</u> , and server security. 1.1.e Must be able to support installation of endpoint agents on the following operating systems, such as: Microsoft Windows 8/10 (32 and 64 bits); <u>at least Windows Server 2008 R2</u> , Mac OS, Linux OS, Ubuntu and Later editions
1.1.h. Must have a file reputation database covering at least twenty (20) countries world-wide with multi endpoint sensor/spam traps and at least 1TB / files proceed a week	1.1.h. Must have the ability to monitor servers system critical files and registry keys, provides default rules in monitoring changes to critical system files and add monitoring of multi-locations/exclusions from its database via policy
1.1.i. Must provide management capabilities for policy establishment and configuration through thick client, secured web based console or its equivalent	1.1.i. Must provide management capabilities for policy establishment and configuration through <u>thin</u> client, secured web based console or its equivalent.
1.1.n. Must be able to assign policy based on location, multiple criteria using Boolean operators (AND OR), applying	1.1.n. Must be able to <u>support policy assignment based on users or device</u> . Applying all protection technologies such


all protection technologies (Antivirus, Proactive Threat Protection, Network Threat Protection, Device and application control, content updates and ETC.).	as Antivirus, Proactive Threat or Network Protection, Device control and Application control.
1.1.p. NO PROVISION	1.1.p Must have the capability to manage, monitor or stop local administrative users or malicious processes to disable the endpoint protection for system protection or controls, users change configuration, login/access and registry monitoring.
1.2.f Must be able to turn on tracer than can identify the source of network based virus infection	1.2.f Must be able to turn on tracer than can identify the source of network based virus infection <u>or have a root-cause analysis to detect communications between endpoint computers and servers involved in botnet or other malware attacks or its equivalent solution.</u>
1.4.b. Must supports host-based firewall that defines the source base on IP Address or Application name	1.4.b. Must support host-based firewall that defines the source base on IP Address or Application name <u>or has the ability to monitor and configure the endpoint operating system's native client firewall system.</u>
1.9. Messaging Gateway Security and Control	1.9. <u>Supports</u> Messaging Gateway Security and Control <u>either in solution offered or related services</u> (Optional)
3.1 Protected Application Whitelisting	3.1 Protected Application Whitelisting <u>or the Must have the capability to detect, allow/block applications based on BJMP's list of allowed/blocked applications.</u>
3.2 System Controls	Remove
3.3 System User Configuration Changes – must be able to monitor user account (creation, change, deletion, locked), users access rights and management	Remove
3.4 System Login Activity and Access Monitor – must be able to monitor login/off of users and failed logins	Remove
3.5 System Hardening Monitor - Detects changes to various registry keys that are critical to the security of the operating system	Remove
3.6 System File and Directory Monitor – must able to monitors system -critical file/directory additions, deletions, changes, access attempts, as well as file share volume creation and /deletion	Remove
3.7 System Registry Monitor	Remove
NO PROVISION	<u>3.8 The solution must be capable of protecting attacks to the security of the operating system</u>
4. Must have functionalities and features for Data Loss/Leak Prevention, such as, fingerprinting, filtering and encryption.	4. Must have <u>any of</u> functionalities and features for Data Loss/Leak Prevention, such as, fingerprinting, filtering, encryption, <u>monitor and restrict the transfer of files</u>

	<u>containing sensitive data, prevent a user from sending file containing sensitive data outside the organization network.</u>
5. Must support patch management and IT inventory solution or its equivalent solution	5. Must support <u>integration with third-party</u> Patch Management and IT Inventory solutions or it's equivalent solution
6. Other Requirement Bidders should have experienced Project Manager (PM) and certified technical personnel for the implementation of the proposed solution: Must have at least One (1) Certified Information Security Officer or Manager who will work closely with the Project Management in the deployment of the solution.	6. Other Requirement Bidders should have experienced Project Manager (PM) and certified technical personnel for the implementation of the proposed solution: Must have at least one (1) Certified Information Security Officer or Manager, Certified Solutions Architects or its equivalent of the solution/brand being offered who will work closely with the Project Management in the deployment of the solution.
8. Warranty Period / Coverage of Warranty 3 years warranty, updated and support of the solution being offered; Must provide 24 x 7 phone and e-mail technical support; Must provide 8 x 5 phone, email, remote & On-site support; The Bidder must provide a procedure on support and problem escalation	<u>8. Warranty and Support</u> <ol style="list-style-type: none"> 1. The bidder must provide 3 years warranty, updates and support of the offered. 2. Must provide 24 x 7 phone and e-mail technical support. 3. Must provide 8 x 5 phone, email, remote, & On-site support 4. The Bidder must provide a procedure on support and problem escalation
Additional Requirement	9. Must support integration with the existing firewall equipment to create a more coordinated end-to-end security solution.
Additional Requirement	10. Shall be capable of server lock down, whitelisting of current applications and prevent unauthorized applications from running.
Additional Requirement	<u>11. Bidders Qualification</u> <ol style="list-style-type: none"> 1. The bidder must have at least four (4) certified in-house engineers of the solution offered. 2. The solution being offered must belong to Gartner's Leader's quadrant for Endpoint Protection Platform 2019. 3. The bidder must provide a Certification from Manufacturer as Certified and Authorized Partner of the solution being offered.

This Bid Bulletin No. 1 shall form part of the Bidding Documents. Any provision in the issued Bid Documents inconsistent herewith is hereby amended, modified and superseded accordingly.

Issued this 27th day of October 2020 at BJMP National Headquarters, 144 Mindanao Ave., Quezon City.



DENNIS U ROCAMORA, CESE
Jail Chief Superintendent 
Deputy Chief for Operations of the Jail Bureau
Chairperson, BJMP-NHQ BAC