Republic of the Philippines
Department of Agriculture
Bureau of Fisheries and Aquatic Resources
BIDS AND AWARDS COMMITTEE OFFICE
2/F Fisheries Building Complex BPI Compound Brgy. Vasra, Q.C.
website: www.bfar.da.gov.ph e-mail: bfarbac2018@gmail.com

SUPPLEMENTAL BID BULLETIN 01
August 20, 2021

SUBJECT: Bid Reference No: 2021-22
RENEWAL OF BFAR CYBER SECURITY LICENSE

This Supplemental Bid Bulletin No. 01 is issued to all participating bidders to clarify, amend and/or modify certain provisions and requirements set forth under the above-entitled procurement project:

Technical Specifications

FROM

Description	Quantity	Unit
RENEWAL OF 500 LICENSES OF EXISTING CYBERSECURITY SOULITON OF THE BUREAU OF FISHERIES AND AQUATIC RESOURCES	**1**	**Lot**
A. Modules/Features:		
1. Network Performance Monitoring		
1.1 Network scanning, detection of devices and TCP/IP services, web access with browser		
1.2 Interactive network maps, user maps, branches, intelligent maps, pop-up menu with definable own tools		
1.3 Simultaneous work of multiple administrators, management of administrator authorizations, administrator access log		
1.4 Response time and correctness, packets received/lost statistics (PING, SMB, HTTP, POP3, SNMP, IMAP, SQL, etc.)		
1.5 WMI counters: CPU load, memory usage, disk usage, network traffic, etc.		
1.6 Windows actions: service status change (start, stop, restart), event log entries		
1.7 SNMP v1/2/3 counters: network traffic, temperature, humidity, power supply voltage, toner level, etc.		
1.8 Security improved by adding the AES, DES and 3DES encryption for SNMPv3 protocol		
1.9 Routers and switches: port mapping		
1.10 Notifications (on desktop, by e-mail, by SMS) and repair actions (program launch, computer restart, etc.)		

1.11 Indicate the work station where a given activity has been performed		
2. Device and Equipment Inventory		
2.1 List of applications and Windows updates on single workstation (registry)		
2.2 List of applications and Windows updates on single workstation (disks scan)		
2.3 Overview of workstation hardware		
2.4 Details of workstation hardware (model, motherboard, CPU, memory, disk drives, adapters, etc.)		
2.5 Hardware and software inventory audit		
2.6 Hardware and software change history		
2.7 Fixed Assets: IT assets register database (defining own fixed asset types, their attributes and values, attachments, data import from CSV file)		
2.8 List of Inventory on Android devices		
2.9 Key reading for the latest MS Office suites		
2.10 Info about the number of found occurrences added to the table filtering mechanism, with the option of temporary toggling the filter on/off		
2.11 File manager functionality added in remote access		
2.12 Export to PDF/TXT/XLS/XML/HTML file formats in the Devices tab in the list of devices and agent		
3. User Activity Monitoring		
3.1 Detailed work time (activity/break start and end time)		
3.2 Faster blocking of the launched applications - the applications are blocked during the attempted launch		
3.3 Visited web pages (number of page visits, with headers, number and duration of visits		
3.4 Blocking web pages		
3.5 Printouts: audit (per printer, user, computer), printing costs		
3.6 Static remote view of user desktop (without access)		
3.7 Screenshots (user work history “screen by screen”)		
3.8 User activity overview		
3.9 General information on user activity		
3.10 Detailed work time monitoring		
3.11 Application usage monitoring		
3.12 Visited web sites (duration and number of visits)		
3.13 Printing costs and auditing		
3.14 Network traffic generated by the user		
3.15 Alarm configuration window from the “device/performance/ services and meters” window		

3.16 Report form of the user data sheet, including information about current settings for individual users		
3.17 Optimization of file transfer in File Manager Remote removal of user files		
4. Help Desk / Ticketing System		
4.1 Trouble ticket database		
4.2 Creating and managing trouble tickets (assigning to administrators with e-mail notification)		
4.3 Remote access to machines (an employee and administrator can see the same screen) with possible request for consent from the use		
4.4 Agent and offline scanner for Linux Ubuntu, offline scanner for Mac OSX		
4.5 Information on merging the issue in HelpDesk		
4.6 File manager functionality in remote access		
4.7 File manager functionality in the console and in the device details dialog box		
4.8 Functionality of Windows process		
4.9 File manager functionality in remote access		
4.10 Configuring custom fields related to the selected trouble ticket category		
4.11 Automatic clearing of the conversation history in the chat feature		
4.12 Chat window notification: about a message being written in the current conversation, about the reading of the last message in the current conversation		
4.13 Option of displaying knowledge database articles as a list		
4.14 Agent menu with notification settings and counters		
4.15 Agent notifications about chat messages and files, and about comments to the tickets		
4.16 Remote Command Execution tab in the Windows section of the device details dialog box		
5. Data Guard		
5.1 List of devices currently connected to the network		
5.2 Identification of devices on the basis of their serial numbers		
5.3 Defining access rights to selected data media		
5.4 History of operations performed on the devices		
5.5 Access rights created on the device and Active Directory level		
5.6 Removal of outdated or non-existent media (e.g. USB) “authorized medium” attribute and modification of the alarm for “external” device connected		
5.7 Report form of the user data sheet, including information about current settings for individual users		
B. Management of Admin Authorization		
• Access to application server from a console in a local network		
• Simultaneous work of multiple administrators		

• Varied access rights for different system users		
• View of information from a web browser		
• Reminders for the administrator in the case of a change in the user's key data and settings		
• Rights to disable/ de-install the nVision agent		
• Administrator name in the notifications in the remote access		

TO

Description	**Quantity**	**Unit**
Renewal of 500 Licenses of existing Cybersecurity Solution of the Bureau of Fisheries and Aquatic Resources		
MINIMUM CONFIGURATION SPECIFICATION		
A. Malware Execution Control • Not signature based • Must have predictive analysis • Autonomous • Pre-execution • Rejects unwanted programs (PUPs	**1**	**lot**
B. Device Control • Provides control over use of USB mass storage devices • Helps prevent the exfiltration of data through removable media		
C. Application Control • Device binary lockdown for fixed function devices • Prevents bad binaries. • Prevents modification of any binary, even good ones. • Allows for change windows		
D. Script Control • Stops unauthorized PowerShell and Active Scripts • Stops risky VBA macro methods, weaponized docs, and file less attacks		
E. Memory Protection • Stops exploitation • Halts process injection • Blocks privilege escalations		
F. Minimum System requirements • Windows XP SP3 and newer / Windows Server 2003 and newer • Mac OS X 10.9 and latest version • MEMORY: 2GB Ram or Higher • Hard Disk Space: 300 MB of disk space • Additional requirements: .NET 3.5 (SP1) and Internet Access for authentication and registration		

G. The Endpoint Protection Solution (EPS) shall meet all of the following requirements: • The EPS shall employ algorithmic code analysis to identify malicious software prior to execution • The EPS shall not permit software identified as malicious to execute • The EPS shall provide protection against execution of malicious software, memory attacks and control malicious scripts • The EPS must be installed on Servers and Desktops/Laptops • The EPS must be recognized by Microsoft as Antivirus • The EPS must provide detailed information on the treats which are blocked • The EPS shall identify and block action by both malicious executable code as well as malicious scripts or commands • The EPS shall detect and prevent unauthorized or malicious code changes to programs running in system memory • The EPS shall function equally well on both Internet-connected and air gapped networks		
• The EPS shall NOT require an Internet or network connection to function at maximum efficiency The EPS shall NOT require frequent updates of any on-premise component • The EPS shall NOT rely on a database of signatures or hashes to identify malicious software • The EPS shall NOT rely on behavior or heuristic analysis to identify malicious software • The EPS shall NOT rely on "whitelists" of known good software to permit or deny execution • The EPS shall NOT rely on "sandboxing" to contain malicious software		
H. The EPS shall include the following: • Agent software to be installed on each endpoints • Access to the could-based agent management console • Remote assistance with implementation and configuration • Ongoing support, upgrades and maintenance for a period of 12 months		
I. Configuration management • Solution should configure the information system to provide only essential capabilities and restrict the use of unnecessary services.		
J. Incident Handling/Information Correlation • The solution should enable the capability to correlate information and individual incident responses to achieve organization wide perspective on incident awareness and response across all threat vectors.		

K. Incident Monitoring• The solution should provide automated reporting mechanisms to report on security incidents such as abnormal user or application behavior, known attacks, and violations of corporate policy.		
L. Intelligence and Visibility • *The solution should allow for near real-time visibility into files as they move across the environment reducing the time required to detect and thwart attacks.*		
M. Technology Integration • The solution should seamlessly integrate with existing and future technology.		

****nothing follows****

All other portions of the Bidding Documents affected by these amendments shall be made to conform the same.

Amendments/inclusions/clarifications made herein shall be considered an integral part of the Bidding Documents.

The changes made in the Philippine Bidding Documents (6th Edition, July 2020) are deemed integrated in terms and conditions for this project.
For further inquiries, please coordinate/call the Bids and Awards Committee Secretariat at Tel. No. 8332-4661 or bac.eps@bfar.da.gov.ph.

Please be guided accordingly.

ORIGINAL SIGNED
ATTY. DEMOSTHENES R. ESCOTO
Chairman, Bids and Awards Committee