



REPUBLIKA NG PILIPINAS  
KAGAWARAN NG PANANALAPI  
**KAWANIHAN NG INGATANG-YAMAN**  
(BUREAU OF THE TREASURY)  
INTRAMUROS, MANILA 1002

*Funding the Republic*

**INVITATION TO APPLY FOR ELIGIBILITY AND TO BID**

The Bureau of the Treasury (BTr), through the Bids and Awards Committee (BAC), invites suppliers to apply for eligibility and to bid for the hereunder project:

- Name of Project : **Supply of Controller Based Wireless Solution and Messaging Security System**
- Location : **Bureau of the Treasury  
Palacio del Gobernador  
Intramuros, Manila**
- Brief Description : **The goods to be purchased shall include the following:**
- a. 1 Unit Wireless Switch Controller**
  - b. 15 Units 802.11a and 802.11b/g Managed Access Points**
  - c. 1 Unit Power Over Ethernet Switch**
  - d. 1 Unit Secure IP/MAC Address Management and Layer 2 Network Access Control Solution**
  - e. 1 Unit Messaging Security System**
- Approved Budget for the Contract (ABC) : **Php3,600,000.00**

Details of technical specifications of each component goods mentioned herein shall be as indicated in the attached Annex "A".

Prospective bidders should have the experience in supplying the goods within the last 3 years with an amount of at least 50% of the proposed goods for bidding and **must at least meet the minimum requirements** of the goods to be procured as stated in the bidding documents.

The Eligibility Check/ Screening as well as the Preliminary Examination of Bids shall use non-discretionary "pass/fail" criteria.

The Approved Budget for the Contract (ABC) is understood to be inclusive of all applicable taxes, e.g. VAT.

All particulars relative to Eligibility Statement and Screening, Bid Security, Performance Security, Pre-Bidding Conference, Evaluation of Bids, Post-Qualification and Award of Contract shall be governed by pertinent provisions of R.A. 9184 and its Implementing Rules and Regulations.

The complete schedule of activities is listed, as follows:

<b>Activities</b>	<b>Schedule</b>
1. Issuance of Bidding Documents (upon payment of non-refundable amount of P3,600.00)	November 23, 2007, Office of BAC Secretariat, Rm. 409, Palacio del Gobernador, Intramuros, Manila
2. Pre-Bid Conference	November 28, 2007, 9:00 AM, Conference Rm. Of DTOP Gisela F. Lood, Rm. 401
3. Opening of Bids	December 11, 2007, 9:00 AM
4. Bid Evaluation & Post Qualification	December 12-19,2007
5. Notice of Award	December 20, 2007

Other terms and conditions in relation hereto are as indicated in the Terms of Reference, Instructions to Bidders and Bid Data Sheet.

The BTr BAC reserves the right to reject documents which do not comply with the requirements and reject any and all bids, annul the bidding process, or not award the contract, without thereby incurring any liability to the affected bidder or bidders.

The BAC assumes no responsibility whatsoever to compensate or indemnify bidders for expenses incurred in the preparation of the bid.

**ATTY. WILLIAM A. BELUSO, JR.**  
Acting Chairperson, BAC

For inquiries, pls. call:  
MS. MYRNA C. DELA CRUZ  
BAC Secretariat  
Tel. No. 5228122 loc. 410; Telefax No. 5273082

## **TECHNICAL SPECIFICATIONS**

### **Controller Based Wireless Solution and Messaging Security System**

#### **A. 1 unit - Wireless Switch Controller**

##### **A.1. Port Configuration**

- Must have at least one Ethernet port and serial console port.

##### **A.2. Access Point Support**

- Must be able to support at least 15 fit/managed access points

##### **A.3. Encryption**

- WPA, WPA2, AES, WEP encryption, TKIP

##### **A.4. Wireless Networking**

- Supports at least 32 WLANs;
- Multiple ESSID and BSSID traffic segmentation;
- VLAN to ESSID mapping;
- auto assignment of VLANs (on RADIUS authentication);
- power save protocol polling;
- pre-emptive roaming; congestion control;
- Layer 2 and Layer 3 deployment of Access Points
- Layer 3 Mobility (inter-subnet roaming);
- Support for FMC (Fixed Mobile Convergence) for seamless hand-off of Voice over Wi-Fi to the mobile network;
- 802.11n ready.

##### **A.5. Packet Forwarding**

- 802.1D, 802.1Q, 802.3 bridging, Proxy ARP; IP packet steering-redirection

##### **A.6. Management**

- Web Interface Management, CLI via telnet, SSH or serial;
- Secure Web-based GUI (SSL);
- SNMP v1/v2/v3;
- SNMP traps -40+ user configurable options;
- Syslog;
- TFTP Client;
- SNTP;
- DHCP client/server/relay, switch auto-configuration and firmware updates with DHCP options;
- multiple user roles for switch access;
- Syslogs

##### **A.7. Filtering**

- L2/3/4 stateful packet analysis; network address translation (NAT)

##### **A.8. Authentication**

- ACLs;PSK;802.1x/EAP-TLS, TTLS, PEAP, Kerberos Integrated AAA/RADIUS server with native support for EAP-TTLS and EAP-PEAP (includes a built-in username/password database;
- supports LDAP

##### **A.9. IPSec VPN gateway (support for up to 100 tunnels)**

- Supports DES, 3DES and AES encryption

A.10. Secure guest access (Hotspot provisioning)

- Local Web-based authentication;
- URL redirection for user login;
- customizable login/welcome pages;
- support for external authentication/billing systems

A.11. RADIUS Support

- User-based VLANs;
- MAC-based authentication;
- User-based QoS;
- Local-based authentication;
- Allowed ESSIDs

A.12. RF priority/Wireless QoS

- 802.11 traffic prioritization and precedence;
- WMM-power save with admission control;
- Layer1-4 packet classification;
- 802.1p VLAN priority;
- DiffServ/TOS;

A.13. System Resiliency and Redundancy

- Active/Standby, Active/Active and 1:Many redundancy with access port and MU load balancing;
- self healing;
- Must support license aggregation between switch members of the redundancy groups.

A.14. Other Requirements:

Training

- Administration and Configuration Training for 3 persons

Warranty and Support

- 3 years – labor, parts and on-site support
- 8 x 5 with Advance Hardware Replacement

**B. 15 units - 802.11a and 802.11b/g MANAGED ACCESS POINTS**

B.1. Dual-band operation

- Must support both 802.11a and 802.11b/g 802.1x supplicant
- Allows authentication to a RADIUS server to enable an 802.1x-protected Ethernet port 802.11h
- Enables worldwide operation through support for standard-based dynamic frequency selection and power control 802.11i
- Support for IEEE standards-based security protocols for strong Encryption (AES, TKIP), Authentication and Key Management (802.1x-EAP) 802.3af
- Simplifies and reduces total cost of installation through support of standards-based Power-over-Ethernet (PoE)

B.2. Antennas

- Omni directional antennas must be integrated.

B.3. Mounting

- The AP must support ceiling and wall mounting and must have a provision for Kensington locks (or equivalent).

B.4. Compatibility Requirement

- For full compatibility with the wireless controller, the Access Points must be the same brand as the wireless controller.

B.5. Warranty and Support

- 3 years – labor, parts and on-site support
- 8 x 5 with Advance Hardware Replacement

## C. 1 unit – Power Over Ethernet SWITCH

### C.1. Port Configuration

- 24 PORT 10/100 Base-T + 2 Gigabit Port

### C.2. Ethernet (Copper or Fiber)

- Supports IEEE 802.3af standards

### C.3. VLAN

- Supports IEEE 802.1Q VLANS

### C.4. QoS

- Must provide classification, marking, rate policing, and IEEE 802.1p and Diffserv queuing based on IEEE 802.1p bits or Diffserv markings in the packet.

### C.5. Must have:

- IEEE 802.1d Spanning Tree;
- Multiple Spanning Tree IEEE 802.1s;
- Rapid Spanning Tree IEEE 802.1w;
- Link Aggregation IEEE 802.3ad;
- IGMP Snooping;
- IEEE 802.1x;
- Port Mirroring;
- Security Filtering or Access Control Lists;
- Flow control IEEE 802.3x;
- CLI/Web/Menu based.
- DHCP client/BootP, TFTP, Telnet

### C.6. Compatibility Requirement

- For full compatibility with the wireless controller, the PoE Switch must be the same brand as the wireless controller.

### C.7. Other Requirements:

#### Training

- Administration and Configuration Training for 3 persons

#### Warranty and Support

- 3 years – labor, parts and on-site support
- 8 x 5 with Advance Hardware Replacement

#### Structured Cabling System for Managed APs and Switch

- The Wireless LAN solution must be controller-based and must allow central management of Access Points.
- The Vendor shall include the cabling requirements for the WLAN deployment. Three Access Points must be installed on the following floors: Second, Third, Fourth and Sixth Floor. Two Access Points on the Ground Floor.
- All Access Points must be designed to terminate to a single PoE switch on the fourth floor. One spare unit of the Access Point must be included in the solution as well as an extra pair of UTP cable on each floor for future expansion.
- Category 5e UTP Cable 4-Pair
- RJ45 Patch Cords
- Roughing-Ins and Consumables
- Labor and Engineering

## **D. 1 unit - SECURE IP/MAC ADDRESS MANAGEMENT AND LAYER 2 NETWORK ACCESS CONTROL SOLUTION**

### D.1. IP/MAC Address Management Layer 2 Network Access Control

- The solution must be appliance-based.
- The solution must be able to monitor and manage an aggregate of 500 IP/MAC Addresses from four (4) physically-segmented networks
- It must support both wired and wireless environments
- It must provide network based blocking of IP/MAC Addresses that are unauthorized to connect to the network.
- It must be able to operate in the following environments: static IP, dynamic IP and mixed TCP/IP environments.
- It must provide automatic detection and prevention of IP conflicts.
- It must be able to detect IP and Layer 2 related events such as IP Change, New MAC, IP Conflict and etc. in real-time and save these logs in a database system. Event alerts via email must be provided for critical IP related events.
- It must be able to support the creation of groups and categorize users into their physical or logical groups for easy management.
- Deployment must be transparent to the existing network and seamless without requiring network reconfiguration nor upgrade.
- It must provide layer 2 network access control without requiring users to login using ID and password.
- It must allow automatic IP/MAC resource monitoring. Resource monitoring should include automatic discovery/detection, display and update on IP, MAC, hostname, workgroup name, time and etc.
- It must allow creation/import of additional column descriptions (name of user of IP/MAC, designation, department, telephone number, email address, etc) for a more comprehensive monitoring.
- It must allow IP-MAC binding to prevent users from changing their IP addresses without the IT Manager's permission
- It must allow comprehensive and real-time IP/MAC inventory and logging.
- It must allow layer 2 level blocking and MAC authentication. Unregistered MAC addresses must instantly be blocked from the network or be provided with an optional temporary access.
- It must include DHCP services and must allow creation of two types of DHCP pools for (1) authorized pool for registered MAC addresses and (2) unauthorized pool for unregistered MAC addresses allowed for temporary access.
- It must automatically detect and block other DHCP servers existing in the same network.
- It must allow pre-defined/temporary network access periods for visitors.
- The solution must include all the required bundle of software and hardware necessary.
- The solution must be implemented without installing any agent program on PC or laptop clients.
- It must allow System Administrators to pro-actively manage IP/MAC Address that are expired or no longer active in the network for a defined number of days.
- It must allow System Administrators to control (block/close), from the management console, any physical port of the switches it discovers in the network.

### D.2. Other Requirements:

#### Training

- Administration and Configuration Training for 3 persons

#### Warranty and Support

- 1 year

#### Console, Management & Database Server

- at least Dual Core Xeon Pro 3040
- Dual Gigabit NIC
- 2GB Memory
- min 160GB HDD
- Combo Drive
- MS 2003 Server
- Suitable DB Software
- Proposed IP/MAC Address
- Rack mount server
- Rack mount Kit

## **E. 1 – unit MESSAGING SECURITY SYSTEM**

### **E.1. Hardware Requirements**

- Must provide one (1) unit of purpose-built appliance
- Minimum two (2) 10/100/1000 Ethernet Ports
- Must be able to support up to 10,000 concurrent SMTP sessions
- Can support up to 1,000 users
- Hardened and secured operating system

### **E.2. Software Requirements**

- Antivirus for e-mail (must be integrated in the appliance)
- Anti-spyware (must be integrated in the appliance)
- Anti-spam and Anti-phishing (must be integrated in the appliance)
- Advanced E-mail Content Filtering (must be integrated in the appliance)
- Quarantine Management (may not be integrated with the appliance)
- Operating System

### **E.3. Anti-Spam and Anti-Phishing Requirements**

- Must filter incoming and outgoing e-mails to keep exploits out and sensitive information in
- Maximum 1 in 1,000,000 false positive rates
- Must use at least the following methods: integrity analysis, content filtering, heuristic detection, black/white lists, Bayesian filtering, and self tuning
- Must be able to set filtering to include group-based policies, lexical e-mail scanning, and attachment content covering at least 300 e-mail attachment types
- Must be capable of configure and enforce policy and monitor the effectiveness of their security and anti-virus safeguards for comprehensive policy management and detailed graphical reporting
- Must have specific rules for identifying and blocking phishing attacks;
- Must Integrate with Open LDAP, Active Directory or other LDAP servers to identify invalid recipients
- Must control the maximum number of bounces per hour due to invalid email recipients according to sender's IP address/range, domain and email reputation
- Ability to perform SMTP session control and traffic rate limiting (down to per recipient) according to sender's IP address/range, domain or email reputation
- Must analyse each mail by at least the following layers : Connection layer, message header, subject, body including contents such as attachments, images, text
- Must support global white list and black list

### **E.4. Anti-Virus Requirements**

- Block 100% of known viruses
- Protect against zero-day attacks and unknown viruses
- Must filter all incoming and outgoing emails
- Must block malware from SMTP and Web Mails
- Must allow automatic updates of virus definition file
- Must scan/filter attachments and compressed files
- Must be able to send messages for processed infected files as cleaned, moved to quarantine or customized message

### **E.5. Advanced Content Filtering**

- Must identify keywords or phrases in email message headers, subject lines or message bodies
- Must filter different email encoding formats (MIME, UUE, XXE, base 64)
- Must filter different mail encoding formats
- Must block, quarantine, copy or redirect message which has triggered content filter rule
- Must easily identify from log file the rule that has caused content filtering to trigger
- Must block emails with too many file attachments, or attachments over a specific size
- Must filter into text of file attachments for 300 common file formats
- File attachment detection by true file type, file name, file extension and MIME type

**E.6. Management, Monitoring and Reporting Requirements**

- The proposed must have graphical monitoring of both incoming and outgoing email flow for last hour, last day, last week and last month
- Must provide detailed and summary statistical reports of messaging volume and categories.
- Centralized message tracking based on sender and/or recipient address/domain, subject, time period, message event for multiple appliances
- Reports can be generated based on date range
- Reports can be categorized based on recipient, policy, and attacker
- Must have real-time graphical monitoring system
- Must be able to send e-mail alerts for system problems
- Must include a quarantine manager that allows

**E.7. Policy Administration**

- Could support multiple domains per IP address or multiple domains using different IP address on single appliance
- Allows per user or user group policy
- Must allow Single View of all user policies for easier management
- Rate limit control by IP address, domain and sender's reputation
- Reverse DNS Domain Lookup and Policy Assignment
- Per Sender Policy settings on:
  - Maximum Messages per connection
  - Maximum Recipients per message
  - Maximum message size
  - Maximum Concurrent sessions per IP address
- Ability to quarantine, duplicate and quarantine, strip attachment, BCC or redirection of email to another host or another recipient, replacing the whole message or just attachment with predefined message notification template.
- LDAP routing, LDAP recipient address verification.
- Ability to control user name and password of quarantine areas so that some quarantine areas can only access by authorized personnel.
- Support both command line and GUI content filters to allow complex policy control requirements.

**E.8. Other Requirements:****Training**

- Administration and Configuration Training for 3 persons

**Warranty and Support**

- 3 years – labor, parts and on-site support

**F. OTHER VENDOR REQUIREMENTS**

- The vendor must submit a certification coming from the equipment manufacturer endorsing the vendor/supplier to bid, sell, support or maintain the proposed equipment.
- The vendor must submit a certification coming from the equipment manufacturer/ distributor and vendor/supplier that they will extend technical support to end-user directly for the product offered.
- The vendor must have a certified technical engineers (regular employee) on the product and brand being offered.
- The vendor must have an installed base with the same brand and product line. It should be an installation in the Philippines and by the Vendor/Supplier proposing the equipment with the same brand and product line.
- The vendor must be a certified partner for all of the equipment being offered.
- The vendor must have at least 10 yrs in the IT business.
- The vendor must submit a certification specifying the number of years of experience on the brand and product being offered.