Republic of the Philippines
Office of the Solicitor General
134 Amorsolo St., Legaspi Village, Makati City

Technical Working Group for
Information and Communications Technology

TERMS OF REFERENCE

Procurement of Internet Load Balancing, Bandwidth Management, and Aggregation Solution for OSG Main and Convergys One Buildings

Background:

The Office of the Solicitor General (OSG) depends on uninterrupted, high-performance internet access for all its Wide Area Network (WAN) critical operations. To ensure resilience, the OSG maintains multiple internet connections from various service providers. However, effectively combining these disparate links to prevent outages, manage traffic, and maximize total speed requires a specialized system.

To meet this need, the OSG is procuring a comprehensive **Internet Load Balancing, Bandwidth Management, and Aggregation Solution**. This integrated system will serve as the central gateway for all internet traffic. It will actively **load balance** requests across all available links to prevent bottlenecks, intelligently **manage bandwidth** to prioritize critical government functions, and **aggregate** the connections to create a single, faster, and more reliable data pipe. This will ensure operational continuity and optimal performance for the OSG's headquarters in Makati and its branch offices.

Objective:

This procurement aims to deploy a solution that achieves the following primary objectives, directly tied to its core functions:

- **Achieve Maximum Uptime through Load Balancing:** To dynamically distribute internet traffic across multiple ISP links, providing seamless, automatic failover that ensures continuous operation even if one or more links fail.
- **Optimize Performance with Bandwidth Management:** To guarantee the performance of essential applications (e.g., video conferencing, VoIP, secure databases) by implementing Quality of Service (QoS) policies that prioritize critical data over less important traffic.
- **Increase Throughput via Link Aggregation:** To combine the speeds of all active internet connections, creating a larger pool of available bandwidth for faster downloads, uploads, and overall improved user experience.
- **Simplify Network Operations:** To centralize the control, monitoring, and reporting of all internet links through a single, user-friendly management console.

Terms:

1. *Scope* - The scope of this project includes the supply, delivery, installation, configuration, and commissioning of a complete and integrated **Internet Load Balancing, Bandwidth Management, and Aggregation Solution**. The solution must cover both the OSG Head Office and Convergys One Office.

2. *ABC.* - The Approved Budget for the Contract (ABC) is **Three Million Pesos (₱3,000,000.00)** inclusive of all government taxes, charges, and other standard fees.

ICT EQUIPMENT			
ITEM	**QTY**	**UNIT COST**	**TOTAL**
Internet Load Balancing, Bandwidth Management, and Aggregation Solution for OSG Main and Convergys One Buildings	**1 Lot**	3,000,000.00	3,000,000.00
		TOTAL	**₱ 3,000,000.00**

3. *Payment.* - The supplier shall be paid in full, subject to deduction of applicable taxes and retention upon the issuance by the OSG of the corresponding Certificate of Inspection and Acceptance. All bid prices shall be considered as fixed prices, and therefore not subject to price escalation during contact implementation.

4. *Delivery.* Delivery shall be within forty-five (45) calendar days upon receipt of the Notice to Proceed. Delay in delivery shall be subject to a penalty equivalent to 1/10 of 1% of the cost of the undelivered item/s for every day of delay.

5. *Training.*

   a. The Supplier must provide the necessary comprehensive training/knowledge transfer program for the end users within ten days solution delivery.

   b. The training must be conducted during business hours and coordinated with CMS. The CMS will provide certification for delivery and training completion.

   c. The course outline, All training materials, product guides, and documentation should be available online.

6. *Qualifications of the Supplier:*

   a. The Bidder shall have an SLCC that is at least one (1) contract similar to the Project, the value of which, adjusted to current prices using the PSA's Consumer Price Index, must be equivalent to at least fifty percent (50%) of the ABC, completed within 5 years before the deadline for the submission and receipt of bids.

      For this purpose, a similar contract shall refer to the procurement contract of any ICT security device.

   b. The bidder must present a Client Satisfaction Certification for at least three (3) contracts with government agencies and/or private corporations with whom the bidder has previous or ongoing contract/s similar to this project.

   c. The bidder shall submit a valid and current Certificate of Distributorship/Dealership/Resellership of the product being offered, issued by the principal or manufacturer of the product (if the bidder is not the manufacturer). If not issued by the manufacturer, they must also submit a certification/document linking the bidder to the manufacturer.

   d. The bidder must attach a brochure of the brand being offered.

   e. The bidder must have a main office or satellite office within Regions III, IV, and NCR.

   f. The bidder shall submit documents relevant to the project, such as but not limited to the following:

      - Valid DTI or SEC Registration;
      - Valid and Current Mayor's Permit/Municipal License;
      - Valid and Current Business Permit;
      - Tax Clearance Certificate as finally reviewed and approved by BIR;
      - Statement of contracts completed, which are similar in nature to the contract to be bid.
      - Net Financial Contracting Capacity (NFCC) Computation

7. *Warranty/ Product Support Requirement*

The winning Bidder should provide a notarized undertaking that it will provide the warranty/after-sales support requirement, as follows:

a) Provide three (3) years of standard hardware warranty with 24x7 support services.
b) For technical assistance, the contact person would be designated by the provider and supported through email/online/phone for the entire standard support services.
c) Must provide eight (8) hours x five (5) days of technical support through unlimited phone, email, remote, and chat.
d) Must have a high priority level for the Support available eight (8) hours x five (5) days with unlimited phone, email, remote, and chat assistance.
e) Must provide technical support covering the following, but not limited to:
    - Online incident submission
    - Less than 4 hours response time upon receipt of the request from OSG.
    - Consulting services on related support and services

8. Applicable provisions of the New Government Procurement Act (RA No. 12009) and its Implementing Rules and Regulations (IRR) shall form part of the Terms of Reference.

Technical Specifications:

OSG MAIN		
Items	**Details/Particulars**	**Compliance**
1	**Architecture**	
a	Internet Load Balancing, Bandwidth Management, and Aggregation Solution should be a component-based appliance solution.	
b	Hardware should be green-compliant to ensure power consumption is lower.	
c	The data center unit should support 8 WAN links with 1 LAN port with 8Copper + 2Fiber/10G Port	
d	Should incorporate any combination of wired & wireless connections (IMA, Ethernet, Satellite, FRADS, Traditional Routers, DSL & Cable Modems, Wireless/4G/LTE, Microwave). Aggregate any combination of DS3, T1, E1, E3, DSL, Wireless, or Cable.	
e	The Central office / Main office appliance must provide the capability to load balance **3Gbps** of aggregated throughput. The same appliance must be upgradeable to up to 10Gbps with software re-licensing.	
f	The Operating System must be 64-bit.	
g	Should have a minimum of 16GB RAM.	
h	Should have a Data Storage capacity of 128GB SSD.	
j	Should have the capability to handle 5,000,000 sessions.	
k	Should have client session logging on syslog.	
l	Should have Session logging capability with Source IP, Destination IP, protocol, Source & Destination ports with NATed IP, ISP link, and date & time stamp.	
m	Must be a single integrated appliance for all the features mentioned.	
2	**Load Balancing Features**	
a	Should support 7 ISP links	
b	The solution must have DNS capability for inbound load balancing. All available WAN links must be active-active for inbound DNS resolution	
c	Selection of the shortest path to the destination based on load/hops/response time	
d	Should support static & dynamic outbound as well as inbound load balancing	
e	The solution must support DNS for resolving inbound DNS resolution to a healthy link and load balances Inbound traffic across multiple WAN links. When the link is down, it will not hand out the IP address associated with that link, and when that link is restored, that IP address will be handed out again. The solution must also have an option to assign a weight value to each link for DNS resolution.	
f	The solution must support the following load balancing algorithms:	

OSG MAIN		
Items	**Details/Particulars**	**Compliance**
	i Round Robin	
	ii Weighted Average	
	iii Fastest Route	
	iv Response Time	
	v Spillover - Traffic must be sent over the backup link only after at least 90% throughput of higher priority lines is reached.	
g	The appliance must support configurable health checks and time for failure to detect link status	
h	The solution must support continuous health checking or monitoring of link availability using ICMP, TCP/UDP protocols, and reliability and performance based on WAN parameters such as latency, packet loss, jitter, and available bandwidth.	
i	The hardware appliance should support DNS for resolving inbound URL resolution to a healthy link	
j	The Hardware appliance should provide client connection state details with TCP state, like syn_sent, established connections	
k	The hardware/appliance should have support for forwarding of dynamic routing protocol packets	
3	**Link Management Feature**	
a	The solution must be able to redirect traffic based on Source/Destination IP & port	
b	The solution must have an option to define the inbound/outbound Kbps limit of throughput of any given link	
c	The solution must provide details of the client routed to each link with IP & port details	
d	In case of link failure, the device should detect it in not more than 5 seconds	
e	The solution must be able to automatically load balance and fail over VoIP, VPN, and Thin Clients, even without duplicating the session to available links	
f	The solution must provide seamless failover of VoIP sessions without breaking or dropping the call	
g	The solution must support selective encryption so that data on MPLS lines is not encrypted, since it is on a private cloud	
h	The solution must encrypt site-to-site traffic over Internet lines. When traffic is being sent over MPLS, the solution must have the option to encrypt it or send the data as it is (unencrypted)	
h	The solution must have support for day and time-based Link Management policy scheduling	
i	WAN parameters such as latency, packet loss, jitter, and available bandwidth of the links should be considered while deciding on the health status of the link.	
4	**Redundancy**	

OSG MAIN		
Items	**Details/Particulars**	**Compliance**
a	The solution must support an open standard redundancy protocol	
b	The solution must support transparent & stateful failover between 2 devices using client table mirroring	
5	**QoS, Traffic Shaping & Bandwidth Management support**	
a	The same hardware or appliance must have bandwidth management support	
b	The solution must support optimized multiple-line QoS	
c	The solution must support bandwidth management based on any L3-L7 information on two or more lines	
d	Should support CBQ, WRR, and RED mechanisms for QoS	
e	Should support the minimum & maximum bandwidth allocation limit for traffic shaping	
f	Must support Two-Way bandwidth management	
g	The solution should support traffic classification based on layer-3 to layer-7 information	
h	The solution must have categories and application signatures to be able to classify & limit P2P bandwidth & protocols like Kazaa, Bit-Torrent, eDonkey, etc.	
i	The solution must have support for day and time-based bandwidth management policy scheduling	
j	The solution must support multiple LAN aliases with VLAN support and must be able to allocate bandwidth based on users, groups, and even applications	
k	Must have a list of Layer7 applications classified in separate categories to select from.	
6	**VPN Load Balancing and Redundancy**	
a	The same appliance must have IPSec/VPN support for gateway-to-gateway communication between the data center and remote site.	
b	The system must be able to load balance the VPN traffic between two locations across multiple WAN links of any service provider at each location.	
c	Solution must be able to support transparent failover of sessions from one path to the other between the two locations.	
d	Solution must support Routing decisions based on Path availability.	
e	The solution must be able to actively monitor the quality of all the paths between the two locations, such as latency, jitter, packet Loss, and so on.	
f	The solution must be able to support Routing decisions based on user-defined threshold values for each of the quality parameters of the Path. This must be based on WAN parameters such as latency, packet loss, jitter, and available bandwidth.	

OSG MAIN		
Items	**Details/Particulars**	**Compliance**
g	The solution must be able to use all available paths between two locations, even for a single session.	
h	The solution must support 2000 IPSec and GRE tunnels per appliance	
i	The solution must support a hybrid WAN which combines Internet/public lines (Broadband, DSL, LTE, etc.) and private lines (MPLS, leased lines, IPVPNs, point-to-point links, etc.)	
j	The solution must provide active-active link load balancing of hybrid networks for inter-site communication.	
k	Must have split tunneling support, wherein the public link can be used for site-to-site communication and the Internet simultaneously.	
l	The solution must support WAN-WAN routing. When the remote site's Internet is down, Internet-bound traffic must traverse the private link and connect to the data center for Internet access.	
7	**WAN Optimization**	
a	The same appliance must have an option to upgrade with a software license to optimize traffic between 2 locations through an add-on license.	
b	The solution supports WAN Optimization technology, such as compression, caching, and protocol optimization on multiple lines and hybrid WAN through an add-on license.	
8	**Server Load Balancing**	
a	The system must have an option to upgrade the software license to load balance the traffic between multiple servers in the LAN in the same appliance.	
b	The system must have an option to detect the status of a server and switch the traffic to other servers if a server is down.	
9	**Site Load Balancing for DC/DR**	
a	The system must have an option to detect if a site is down and fail over to the other system at the DR site.	
b	When both sites are active, the system should be able to distribute the load between both DC and DR sites.	
10	**High Availability**	
a	The Hardware appliance must support high availability with a cluster feature for Stateful failover.	
b	Ensures the availability and performance of applications with a single point of management for ease of maintenance.	
c	Must have a dedicated fast failover cable to detect backup device failure less than 500ms.	
11	**Security**	
a	The solution should protect against DoS-based attacks from the Internet side.	

OSG MAIN		
Items	**Details/Particulars**	**Compliance**
b	The solution must protect against network-based attacks with an in-built firewall.	
c	Full stateful packet inspection firewall with a minimum of 100 ACL support without any performance degradation.	
d	Solution must support static NAT, static PAT, & dynamic NAT.	
e	The hardware appliance should support VLANs.	
f	The solution must have VPN redundancy or VPN switching without needing to restart sessions.	
g	The solution must restrict access based on destination/source IP, ports, and domains/URLs.	
h	The solution must be able to do encryption of data packets on multiple lines.	
i	The solution must be FIPS 140-2 compliant.	
12	**ISP Health Monitoring**	
a	Shall provide an individual health check for each link.	
b	Should have a health check on any IP/Domains & Ports, etc.	
c	Should provide AND & OR mechanism between health checks.	
13	**Device Management & Reporting**	
a	The solution must have a GUI interface for configuration & reporting.	
b	Should provide HTTPS interface management.	
c	Should provide an SSH / CLI interface.	
d	The solution must support SNMP V2 and V3.	
e	The solution must support NetFlow v5 and v9 integration.	
f	The solution must support the ability to assign IP addresses and host configuration information to devices on the Local Area Network.	
g	The Hardware must be able to provide individual links' uptime relative to the appliance's uptime.	
h	The Hardware appliance must support native mailing and syslog (UDP and TCP) functions.	
i	The solution must be ready for multiple-site deployment, with an option to auto-configure VPN tunnels, QoS, web filters, and policy routing rules between the DC and multiple locations.	
j	The solution must have a centralized management console option for multi-site deployment, which allows users to manage all the devices from a single dashboard without the burden of logging into each unit individually.	
k	The same appliance or hardware must have the ability to integrate or enable controller/orchestrator functionalities in the DC appliance via a software license for multi-site deployment.	

OSG MAIN		
Items	**Details/Particulars**	**Compliance**
14	**DDoS Blocking**	
	Built-in services running on the unit are automatically safeguarded against DDoS attacks. A DDoS blocker provides an extra layer of security.	
15	**Web URL Filtration Services**	
a	The solution must provide the ability to restrict and log web access by various users and groups of users. The restriction should be based on URLs or application categories, add-on license.	
b	The solution must be able to block P2P applications such as torrent, block other applications that are not work-related, and add an on-license.	
c	The solution must be able to filter and apply business policies based on users, groups, subnets, URLs, applications, and add-on licenses.	
d	The solution must have time-based scheduling for filtering of websites or URLs, add-on license	
16	**Anti-Virus and Anti-Spam**	
a	The appliance can have an antivirus engine designed for detecting Trojans, viruses, malware, and other malicious threats through an add-on license.	
b	The appliance can have an anti-spam engine that uses a wide variety of local and network tests to identify spam signatures through an add-on license.	
17	**IDS/IPS**	
a	The appliance can monitor network traffic and alert administrators when potential hostile traffic is detected. It gathers and analyzes information from various areas within the network to identify possible security breaches, which include both external and internal threats. IPS / IDS can respond to malicious traffic by acting, such as blocking the user or source IP address from accessing the network. thru an add-on license	
18	**Awards & Recognition**	
a	Must have Gartner's Peer Insight or Equivalent.	
b	Must have SPARKS Matrix Quadrant Knowledge Solution or Equivalent.	
c	Must have Info-Tech Research Group Software Review or Equivalent.	
19	**Certification Standards**	
a	OEM should be an ISO-certified organization and must provide the ISO certification.	
b	OEM should have the patents for the WAN technology.	
c	OEM Should Have a 24/7 Toll-Free Number.	
d	OEM should have a local representative and have a technical support center along with a 24/7 toll-free number.	

OSG MAIN		
Items	**Details/Particulars**	**Compliance**
e	All the Technical Specs mentioned should be available in a single appliance.	
20	**Availability**	
a	45 to 60 Days Delivery Lead Time.	

CONVERGYS ONE OFFICE		
Items	**Details/Particulars**	**Compliance**
1	**Architecture**	
a	INTERNET LOAD BALANCING, BANDWIDTH MANAGEMENT, AND AGGREGATION SOLUTION should be a component-based appliance solution	
b	Hardware should be green-compliant to ensure power consumption is lower.	
c	The data center unit should support 8 WAN links with 1 LAN port with 8Copper + 2Fiber/10G Port	
d	Should incorporate any combination of wired & wireless connections (IMA, Ethernet, Satellite, FRADS, Traditional Routers, DSL & Cable Modems, Wireless/4G/LTE, Microwave). Aggregate any combination of DS3, T1, E1, E3, DSL, Wireless, or Cable.	
e	The Branch/Remote Office appliance must provide the capability to load balance **2Gbps** of aggregated throughput. The same appliance must be upgradeable to up to 10Gbps with software re-licensing.	
f	Operating System 64-Bit.	
g	Should have a minimum of 16GB RAM.	
h	Should have a data storage capacity of 128GB SSD	
j	Should have the capability to handle 5,000,000 sessions	
k	Should have client session logging on syslog	
l	Should have Session logging capability with Source IP, Destination IP, protocol, Source & Destination ports with NATed IP, ISP link, and date & time stamp	
m	Must be a single integrated appliance for all the features mentioned	
2	**Load Balancing Features**	
a	Should support 7 ISP links.	
b	The solution must have DNS capability for inbound load balancing. All available WAN links must be active-active for inbound DNS resolution.	
c	Selection of the shortest path to the destination based on load/hops/response time.	
d	Should support static & dynamic outbound as well as inbound load balancing.	
e	The solution must support DNS for resolving inbound DNS resolution to a healthy link and load balances Inbound traffic across multiple WAN links. When the link is down, it will not hand out the IP address associated with that link, and when that link is restored,	

CONVERGYS ONE OFFICE		
Items	**Details/Particulars**	**Compliance**
	that IP address will be handed out again. The solution must also have an option to assign a weight value to each link for DNS resolution.	
f	The solution must support the following load balancing algorithms:	
	i Round Robin	
	ii Weighted Average	
	iii Fastest Route	
	iv Response Time	
	v Spillover - Traffic must be sent over the backup link only after at least 90% throughput of higher priority lines is reached.	
g	The appliance must support configurable health checks and time for failure to detect link status.	
h	The solution must support continuous health checking or monitoring of link availability using ICMP, TCP/UDP protocols, and reliability and performance based on WAN parameters such as latency, packet loss, jitter, and available bandwidth.	
i	The Hardware appliance should support DNS for resolving inbound URL resolution to a healthy link.	
j	The Hardware appliance should provide client connection state details with TCP state, like syn_sent, established connections.	
k	The Hardware/appliance should have support for forwarding of dynamic routing protocol packets.	
3	**Link Management Feature**	
a	The solution must be able to redirect traffic based on Source/Destination IP & port.	
b	The solution must have an option to define the inbound/outbound Kbps limit of throughput of any given link.	
c	The solution must provide details of the client routed to each link with IP & port details.	
d	In case of link failure, the device should detect it in not more than 5 seconds.	
e	The solution must be able to automatically load balance and fail over VoIP, VPN, and Thin Clients, even without duplicating the session to available links.	
f	The solution must provide seamless failover of VoIP sessions without breaking or dropping the call.	
g	The solution must support selective encryption so that data on MPLS lines is not encrypted, since it is on a private cloud.	
h	The solution must encrypt site-to-site traffic over Internet lines. When traffic is being sent over MPLS, the solution must have the option to encrypt it or send the data as it is (unencrypted)	

CONVERGYS ONE OFFICE		
Items	**Details/Particulars**	**Compliance**
h	The solution must have support for day and time-based Link Management policy scheduling	
i	WAN parameters such as Latency, Packet Loss, Jitter, and available bandwidth of the links should be considered while deciding on the health status of the link.	
4	**Redundancy**	
a	The solution must support an open standard redundancy protocol.	
b	The solution must support transparent & stateful failover between 2 devices using client table mirroring.	
5	**QoS, Traffic Shaping & Bandwidth Management support**	
a	The same hardware or appliance must have bandwidth management support	
b	The solution must support optimized multiple-line QoS.	
c	The solution must support bandwidth management based on any L3-L7 information on two or more lines.	
d	Should support CBQ, WRR, and RED mechanisms for QoS.	
e	Should support the minimum & maximum bandwidth allocation limit for traffic shaping.	
f	Must support Two-Way bandwidth management	
g	The solution should support traffic classification on the basis of layer-3 to layer-7 information.	
h	The solution must have categories and application signatures to be able to classify & limit P2P bandwidth & protocols like Kazaa, Bit-Torrent, eDonkey, etc.	
i	The solution must have support for day and time-based Bandwidth Management policy scheduling.	
j	The solution must support multiple LAN aliases with VLAN support and must be able to allocate bandwidth based on users, groups, and even applications.	
k	Must have a list of Layer7 applications classified in separate categories to select from.	
6	**VPN Load Balancing and Redundancy**	
a	The same appliance must have IPSec/VPN support for gateway-to-gateway communication between the data center and the remote site.	
b	The system must be able to load balance the VPN traffic between two locations across multiple WAN links of any service provider at each location.	
c	Solution must be able to support transparent failover of sessions from one path to the other between the two locations.	
d	Solution must support Routing decisions based on Path availability.	

CONVERGYS ONE OFFICE		
Items	**Details/Particulars**	**Compliance**
e	The solution must be able to actively monitor the quality of all the Paths between the two locations, such as Latency, Jitter, Packet Loss, and so on.	
f	The solution must be able to support Routing decisions based on user-defined threshold values for each of the quality parameters of the Path. This must be based on WAN parameters such as latency, packet loss, jitter, and available bandwidth.	
g	The solution must be able to use all available paths between two locations, even for a single session.	
h	The solution must support 2000 IPSec and GRE tunnels per appliance.	
i	The solution must support a hybrid WAN which combines Internet/public lines (Broadband, DSL, LTE, etc.) and private lines (MPLS, leased lines, IPVPNs, point-to-point links, etc).	
j	The solution must provide active-active link load balancing of hybrid networks for inter-site communication.	
k	Must have split tunneling support, wherein the public link can be used for site-to-site communication and the Internet simultaneously.	
l	The solution must support WAN-WAN routing. When the remote site's Internet is down, Internet-bound traffic must traverse the private link and connect to the data center for Internet access.	
7	**WAN Optimization**	
a	The same appliance must have an option to upgrade with a software license to optimize traffic between 2 locations through an add-on license.	
b	The solution supports WAN Optimization technology such as compression, caching, and protocol optimization on multiple lines and hybrid WAN thru an add-on license.	
8	**Server Load Balancing**	
a	The system must have an option to upgrade the software license to load balance the traffic between multiple servers in the LAN in the same appliance.	
b	The system must have an option to detect the status of a server and switch the traffic to other servers if a server is down.	
9	**Site Load Balancing for DC/DR**	
a	The system must have an option to detect if a site is down and failover to the other system at the DR site.	
b	When both sites are active, the system should be able to distribute the load between both DC and DR sites.	
10	**High Availability**	
a	The Hardware appliance must support high availability with a cluster feature for Stateful failover.	

CONVERGYS ONE OFFICE		
Items	**Details/Particulars**	**Compliance**
b	Ensures the availability and performance of applications with a single point of management for ease of maintenance.	
c	Must have a dedicated fast failover cable to detect backup device failure less than 500ms.	
11	**Security**	
a	The solution should protect against DoS-based attacks from the Internet side.	
b	The solution must protect against network-based attacks with an in-built firewall.	
c	Full stateful packet inspection firewall with a minimum of 100 ACL support without any performance degradation.	
d	Solution must support Static NAT, Static PAT, & Dynamic NAT.	
e	The Hardware appliance should support VLANs.	
f	The solution must have VPN redundancy or VPN switching without needing to restart sessions.	
g	The solution must restrict access based on destination/source IP, ports, and domains/URLs.	
h	The solution must be able to do encryption of data packets on multiple lines.	
i	The solution must be FIPS 140-2 compliant.	
12	**ISP Health Monitoring**	
a	Shall provide an individual health check for each link.	
b	Should have a health check on any IP/Domains & Ports, etc.	
c	Should provide AND & OR mechanism between health checks.	
13	**Device Management & Reporting**	
a	The solution must have a GUI interface for configuration & reporting	
b	Should provide HTTPS interface management	
c	Should provide an SSH / CLI interface	
d	The solution must support SNMP V2 and V3	
e	The solution must support NetFlow v5 and v9 integration	
f	The solution must support the ability to assign IP addresses and host configuration information to devices on the Local Area Network.	
g	The Hardware must be able to provide individual links' uptime relative to the appliance's uptime.	
h	The Hardware appliance must support native mailing and syslog (UDP and TCP) functions	
i	The solution must be ready for multiple sites deployment that has an option to auto-configure VPN tunnels, QoS, web filters, policy routing rules between DC and multiple locations	

CONVERGYS ONE OFFICE		
Items	**Details/Particulars**	**Compliance**
j	The solution must have a centralized management console option for multi-site deployment, which allows users to manage all the devices from a single dashboard without the burden of logging into each unit individually	
k	The same appliance or hardware must have the ability to integrate or enable controller/orchestrator functionalities in the DC appliance via a software license for multi-site deployment	
14	**DDoS Blocking**	
	Built-in services running on the unit are automatically safeguarded against DDoS attacks. A DDoS blocker provides an extra layer of security.	
15	**Web URL Filtration Services**	
a	The solution must provide the ability to restrict and log web access by various users and groups of users. The restriction should be based on URLs or application categories, add-on license	
b	The solution must be able to block P2P applications such as torrent, block other applications that are not work-related, and add an on-license.	
c	The solution must be able to filter and apply business policies based on users, groups, subnets, URLs, applications, and add-on licenses.	
d	The solution must have time-based scheduling for filtering of websites or URLs, add-on license	
16	**Anti-Virus and Anti-Spam**	
a	The appliance is capable of having an antivirus engine designed for detecting Trojans, viruses, malware, and other malicious threats through an add-on license	
b	The appliance can have an anti-spam engine that uses a wide variety of local and network tests to identify spam signatures thru add-on license	
17	**IDS/IPS**	
a	The appliance can monitor network traffic and alert administrators when potential hostile traffic is detected. It gathers and analyzes information from various areas within the network to identify possible security breaches, which include both external and internal threats. IPS / IDS can respond to malicious traffic by taking action such as blocking the user or source IP address from accessing the network. thru an add-on license	
18	**Awards & Recognition**	
a	Gartner's Peer Insight or Equivalent	
b	SPARKS Matrix Quadrant Knowledge Solution or Equivalent	
c	Info-Tech Research Group Software Review or Equivalent	

CONVERGYS ONE OFFICE		
Items	**Details/Particulars**	**Compliance**
19	**Certification Standards**	
a	OEM should have an ISO-certified organization.	
b	OEM should have the patents for the WAN technology.	
c	OEM should have a 24x7 toll-free number	
d	OEM should have a local representative and have a technical support center along with 24 x 7 toll-free number	
e	All the technical specs mentioned should be available in a single appliance.	
20	**Availability**	
a	45 to 60 Days Delivery Lead Time	

Other Services		
ITEM	**SPECIFICATIONS**	**COMPLIANCE**
Support Service Requirement	The bidder must provide the following:	
	* Unlimited corrective maintenance/ repair services within the warranty period	
	* Eight (8) hours by five (5) days (Monday to Friday, 8:00 AM -5:00 PM) technical support, and must meet the following response and resolution time:	
	> Within one (1) hour for phone or email support	
	> Within two (2) hours of response time for on-site support	
	> Root cause analysis for all support cases filed.	
	The bidder must provide full documentation for the Activity Plan on installing patches and upgrades, and Root Cause Analysis of incidents encountered.	
	The bidder must provide on-site support for installing and deploying software patches and version upgrades.	
	The bidder must provide a procedure for support and problem escalation.	
	* Submission of Activity/Service Report within 5 calendar days	

Technical Working Group for ICT Equipment

ASG GILBERT U. MEDRANO

SSS CARLOS G. REYNES, JR.

DIR IV EDUARDO ALEJANDRO O. SANTOS

SS II OMAR T. GABRIELES

SS I PATRICK JOSEPH S. TAPALES

AS III MARIVI A. TUMAMBING

AS III GABRIEL ANTONIO D. ROBENIOL

ITO III JAYVIE NEIL MALICK S. MALICDEM

ITO III AMELITO V. DUCUT

COMPRO III AUGUSTUS MARK B. DICHOSO

AO II ANGELICA JEAN C. DE MESA

Approved/Disapproved:

DARLENE MARIE B. BERBERABE
Solicitor General

Certified Funds Available:

ASG SAMANTHA O. CAMITAN
OIC - FMS