คุณลักษณะเฉพาะของอุปกรณ์สำหรับระบบเครือข่ายสารสนเทศคมนาคม (MOTNET)

ผู้ยื่นข้อเสนอต้องจัดหาและติดตั้งอุปกรณ์สำหรับให้บริการระบบเครือข่ายสารสนเทศคมนาคม (MOTNET) โดยมีรายละเอียดและคุณลักษณะของอุปกรณ์ดังต่อไปนี้

๑) อุปกรณ์ Core Switch สำหรับเชื่อมโยงเครือข่ายติดตั้ง ณ สำนักงานปลัดกระทรวงคมนาคม จำนวน ๒ ชุด มีคุณสมบัติอย่างน้อย ดังนี้

๑.๑) เป็นอุปกรณ์ที่มีลักษณะเป็น Modular Chassis มีจำนวน Interface Slot ที่ไม่นับรวมกับช่องสำหรับแผงวงจรควบคุม (Routing Engine/Supervisor) อย่างน้อย ๖ slots และมี Redundant Power Supply อย่างน้อย ๒ ชุด

๑.๒) มีการติดตั้ง Management Module หรือ Main Processing Unit แยกออกจาก Routing Engine/Supervisor หรือ Switching Fabric โดยต้องติดตั้งบน Slot ที่ต่างกัน

๑.๓) อุปกรณ์ที่เสนอต้องมี Switching Capacity หรือ Forwarding Capacity หรือ Backplane Capacity รวมสูงสุดอย่างน้อย ๒.๔ Tbps

๑.๔) Interface Module ที่เสนอต้องสามารถทำงานระดับ Layer ๒ และ Layer ๓ ได้ทุก Module ที่เสนอ

๑.๕) มี Interface Module ที่ทำงานแบบ Wire-speed หรือ Non-blocking หรือ Line rate ทุกพอร์ต พร้อม Built-in หรือติดตั้ง Transceiver แบบ ๑๐G Base-SR LC Connector หรือดีกว่า จำนวนอย่างน้อย ๔ พอร์ต และแบบ ๑๐๐๐ Base-SX LC Connector จำนวนอย่างน้อย ๔ พอร์ต

๑.๖) มี Interface Module แบบ ๑๐/๑๐๐/๑๐๐๐ Base-Tx หรือ ๑๐๐๐ Base-T จำนวน ๔๘ พอร์ต

๑.๗) มีเทคโนโลยีแบบ Intelligent Resilient Framework (IRF) หรือ Virtual Chassis Ports (VCPs) หรือ Fabric Path ในการทำงานแบบ Virtualization ได้

๑.๘) สามารถรองรับ MAC address รวมได้ไม่น้อยกว่า ๕๐๐,๐๐๐ MAC address

๑.๙) สามารถทำงานแบบ VLAN ตามมาตรฐาน IEEE ๘๐๒.๑Q ได้ไม่น้อยกว่า ๔,๐๐๐ VLAN

๑.๑๐) มีความสามารถในการเชื่อมต่อและการเลือกเส้นทาง แบบ Resilience Packet Ring (RPR) หรือ Rapid Ring Protection Protocol (RRPP) หรือ MPLS Traffic Engineering (MPLS-TE) โดยตัวอุปกรณ์เองได้

๑.๑๑) มีพอร์ต Console พร้อมสาย Cable เพื่อต่อ Terminal สำหรับกำหนดค่าการทำงานของอุปกรณ์ และตรวจสอบระบบได้

๑.๑๒) สามารถทำ IPv๔ Routing แบบ RIP, OSPF, BGP๔ และ IS-IS ได้

๑.๑๓) สามารถทำ IPv๖ Routing แบบ BGP๔ for IPv๖ , IS-ISv๖ และ OSPFv๓ ได้

๑.๑๔) สามารถทำ MPLS Layer ๓ VPN และ VPLS ได้ทุก Interface Module ที่เสนอ

๑.๑๕) มีโปรโตคอล Network Time Protocol (NTP) หรือ Simple Network Time Protocol (SNTP)

๑.๑๖) สามารถทำ Quality of Service แบบ Weighted Round Robin (WRR) และ Weighted Random Early Detection (WRED) ได้เป็นอย่างน้อย

๑.๑๗) สามารถทำงาน High Availability แบบ Virtual Redundancy Routing Protocol (VRRP) ได้

๑.๑๘) สามารถตรวจสอบคุณภาพเส้นทางการรับส่งข้อมูลแบบ Network Quality Analyst (NQA) หรือ IP Service Level Agreements (IP SLA) หรือ Real-time Performance Monitoring (RPM) เพื่อตรวจสอบการให้บริการแบบ Jitter และ TCP ได้เป็นอย่างน้อย

๑.๑๙) มีคุณสมบัติ Bidirectional Forwarding Detection (BFD) ในการตรวจสอบการทำงานของ OSPF, BGP, IS-IS และ MPLS ได้

๑.๒๐) สามารถกำหนดความเร็วในการรับส่งข้อมูล (Bandwidth Shaping) แบบ Port-Based Rate Limiting และทำ Access Control List (ACL) ได้

๑.๒๑) สามารถจัดเก็บข้อมูลทางสถิติการใช้งานเครือข่ายแบบ NetFlow หรือ sFlow หรือ J-Flow ได้

๑.๒๒) มีฟังก์ชั่นที่สามารถป้องกันการโจมตี หรือบุกรุกด้วย DHCP Protection หรือ DHCP Snooping, ARP Protection และ IP Source Guard ได้เป็นอย่างน้อย

๑.๒๓) สามารถกำหนดสิทธิการเข้าบริหารจัดการอุปกรณ์แบบ Role based access control โดยสามารถกำหนดให้ผู้ดูแลระบบมีสิทธิในการทำงานที่แตกต่างกันได้

๑.๒๔) สามารถบริหารจัดการอุปกรณ์โดยใช้ SNMPv๓, Web Based และ CLI ได้

๑.๒๕) อุปกรณ์ได้รับการรับรองมาตรฐาน EN, FCC และ UL เป็นอย่างน้อย

๒) อุปกรณ์ Router ที่ใช้เชื่อมโยงเครือข่ายในส่วนกลาง จำนวน ๖ ชุด ติดตั้ง ณ สำนักงานปลัดกระทรวงคมนาคม กรมเจ้าท่า กรมการขนส่งทางบก กรมท่าอากาศยาน กรมทางหลวง และกรมทางหลวงชนบท มีคุณสมบัติอย่างน้อย ดังนี้

๒.๑) เป็นอุปกรณ์ที่สามารถจัดหาเส้นทางเพื่อส่งแพกเกตข้อมูลไปยังเครือข่ายปลายทางที่ต้องการตามมาตรฐานของ OSI Model ที่ Layer ๓

๒.๒) เป็นอุปกรณ์แบบ Hardware appliance ที่มี Throughput สำหรับการทำงานของ Firewall ไม่น้อยกว่า ๑๐ Gbps

๒.๓) สามารถรองรับ Concurrent sessions ได้ไม่น้อยกว่า ๑,๔๐๐,๐๐๐ session และสามารถสร้าง Connections per Sessions ได้ไม่น้อยกว่า ๕๕,๐๐๐ sessions/second

๒.๔) มีพอร์ตแบบ ๑GE RJ๔๕ จำนวนไม่น้อยกว่า ๑๔ พอร์ต

๒.๕) มีช่องสำหรับติดตั้ง Transceiver แบบ ๑ GE SFP ไม่น้อยกว่า ๘ ช่อง และช่องสำหรับติดตั้ง Transceiver แบบ ๑๐GE SFP+ ไม่น้อยกว่า ๒ ช่อง

๒.๖) สามารถใช้งาน IPsec VPN หรือ IPSec NAT Traversal และการเข้ารหัสแบบ ๓DES, AES ได้

๒.๗) มี Throughput สำหรับการทำงาน IPsec VPN ไม่น้อยกว่า ๑๐ Gbps

๒.๘) สามารถรองรับการทำ IEEE ๘๐๒.๑Q VLAN Tagging หรือดีกว่า

๒.๙) มีคุณสมบัติในการป้องกันการโจมตีแบบ Denial of Service (DoS) ทั้ง iPv๖ และ IPv๔ และสามารถกำหนด Threshold ความผิดปกติของ Traffic L๔ ได้แก่ TCP Sync Flood, UDP/ICMP/SCTP Flood, UDP/SCTP Scan, ICMP Sweep, TCP port scan, TCP/UDP/ICMP/SCTP session โดยสามารถเลือกเปิดการบันทึก log แยกตามทราฟฟิคแต่ละประเภทได้

๒.๑๐) สามารถรองรับการทำ Virtual routers หรือ Virtual Domain หรือดีกว่า

๒.๑๑) สามารถทำงานลักษณะ Transparent Mode เพื่อใช้งานกับเครือข่ายเดิมได้ โดยไม่ต้องแก้ไข IP Address ของ Network เดิม

๒.๑๒) สามารถใช้งาน Routing แบบ Static, Dynamic Routing และอุปกรณ์สนับสนุนโปรโตคอลแบบ OSPF, ISIS, BGP๔ และสามารถทำ NAT๔๖, NAT๖๔, IPv๖ ได้เป็นอย่างน้อย

๒.๑๓) มีคุณสมบัติ SD-WAN ที่สามารถควบคุม Application ใช้งานผ่าน WAN Link ตามค่า SLA ที่กำหนดจาก Latency, Jitter, Packet Loss ได้เป็นอย่างน้อย และสามารถทำ Fail-over Link ได้แบบอัตโนมัติ

๒.๑๔) สามารถกำหนดสิทธิ (User Authentication) แบบ ๘๐๒.๑X, RADIUS, Active Directory ได้เป็นอย่างน้อย

๒.๑๕) สามารถเก็บรายละเอียดและตรวจสอบการใช้งาน (Logging/Reporting) ได้แก่ Application และ Bandwidth Usage ได้เป็นอย่างน้อย

๒.๑๖) สามารถจัดการ Configure อุปกรณ์ผ่านทาง Command Line Interface (Telnet หรือ SSH) และ Web UI ได้

๒.๑๗) มีแหล่งจ่ายไฟฟ้าอย่างน้อยจำนวน ๒ ชุดเพื่อทำงานแบบ Redundant Power Supply

๓) อุปกรณ์ Router ที่ใช้เชื่อมโยงเครือข่ายในส่วนภูมิภาคติดตั้ง ณ หน่วยงานส่วนภูมิภาค จำนวน ๕๓๑ ชุด มีคุณสมบัติอย่างน้อย ดังนี้

๓.๑) เป็นอุปกรณ์ที่สามารถจัดหาเส้นทางเพื่อส่งแพกเกตข้อมูลไปยังเครือข่ายปลายทางที่ต้องการตามมาตรฐานของ OSI Model ที่ Layer ๓

๓.๒) เป็นอุปกรณ์แบบ Purpose-built Security Appliance ที่มี Throughput สำหรับการทำงานของ Firewall ไม่น้อยกว่า ๘๐๐ Mbps

๓.๓) สามารถรองรับ Concurrent session ได้ไม่น้อยกว่า ๖๐,๐๐๐ session สามารถสร้าง New Session ได้ไม่น้อยกว่า ๒,๒๐๐ Session/Second

๓.๔) มี Memory ไม่น้อยกว่า ๒ GB

๓.๕) มี interface แบบ ๑๐/๑๐๐ หรือดีกว่าอย่างน้อย ๕ พอร์ต

๓.๖) สามารถใช้งาน IPsec VPN หรือ IPSec NAT Traversal และการเข้ารหัสแบบ ๓DES, AES ได้

๓.๗) มี Throughput สำหรับการทำงาน VPN ไม่น้อยกว่า ๘๕ Mbps

๓.๘) สามารถรองรับการทำ IEEE ๘๐๒.๑Q VLAN Tagging ได้ไม่น้อยกว่า ๓ VLAN หรือดีกว่า

๓.๙) สามารถทำงานลักษณะ Transparent Mode เพื่อใช้งานกับเครือข่ายเดิมได้ โดยไม่ต้องแก้ไข IP Address ของ Network เดิม

๓.๑๐) สามารถใช้งาน Routing แบบ Static, Dynamic Routing และอุปกรณ์สนับสนุนโปรโตคอลแบบ RIPv๑, RIPv๒, OSPF และ BGP

๓.๑๑) มีความสามารถในการทำ Traffic Management แบบ Maximum Bandwidth และ Priority

๓.๑๒) มีระบบ IPS และ Antivirus ในตัว กรณีที่ไม่มี ต้องเสนออุปกรณ์ IPS และ Antivirus ภายนอกมาต่อเพิ่มเติม

๓.๑๓) สามารถกำหนดสิทธิในการเข้าถึงเครือข่าย (User Authentication) ได้แก่ ฐานข้อมูลภายใน, RADIUS, RSA SecurID, และ LDAP เป็นอย่างน้อย

๓.๑๔) สามารถเก็บรายละเอียดและตรวจสอบการใช้งาน (Logging/Monitoring) ได้แก่ Syslog , ส่ง E-mail แจ้ง, และ SNMP เป็นอย่างน้อย

๓.๑๕) สามารถจัดการ Configure อุปกรณ์ผ่านทาง Command Line Interface (Telnet หรือ SSH) และ Web UI (HTTP หรือ HTTPS)

๔) อุปกรณ์ HQ Switch สำหรับเชื่อมโยงเครือข่ายติดตั้ง ณ สำนักงานปลัดกระทรวงคมนาคม จำนวน ๒ ชุด มีคุณสมบัติอย่างน้อย ดังนี้

๔.๑) สามารถทำงานแบบ Layer ๓ Switching หรือดีกว่า และรองรับเทคโนโลยีแบบ Ethernet, Fast Ethernet และ Gigabit Ethernet

๔.๒) เป็นอุปกรณ์ที่มี Switching Capacity ไม่น้อยกว่า ๑๑๕ Gbps และสามารถส่งผ่านข้อมูลได้ไม่น้อยกว่า ๙๘ Mpbs

๔.๓) มีพอร์ตแบบ ๑๐/๑๐๐/๑๐๐๐ (RJ-๔๕) แบบ auto-sensing ไม่น้อยกว่า ๒๐ Port และพอร์ตแบบ ๑๐๐๐-BaseX ที่ จำนวนไม่น้อยกว่า ๔ Port

๔.๔) สามารถทำ Routing Protocol แบบ RIP, OSPF, ISIS, MPLS, VRF และ BGP ได้เป็นอย่างน้อย

๔.๕) สามารถทำงานร่วมกับ MPLS VPN ได้อย่างน้อย ๖๐ VPN

๔.๖) มีระบบป้องกันการโจมตีแบบ DoS Attack หรือดีกว่าได้เป็นอย่างน้อย

๔.๗) สามารถทำ Spanning Tree ตามมาตรฐาน IEEE ๘๐๒.๑d, IEEE ๘๐๒.๑s และ IEEE ๘๐๒.๑w ได้

๔.๘) รองรับจำนวน MAC Address ได้ไม่ต่ำกว่า ๓๒,๐๐๐ MAC Address

๔.๙) สามารถทำ Link Aggregation Control Protocol (LACP) ตามมาตรฐาน IEEE ๘๐๒.๓ad ได้

๔.๑๐) สามารถป้องกันในเรื่องของ Failover ได้ในลักษณะที่เป็น Sub-second Failover เมื่อมีการเชื่อมต่อระหว่างอุปกรณ์ Switch เป็นแบบ Ring

๔.๑๑) สนับสนุนการทำ Access Control List และ FTP หรือ TFTP ได้

๔.๑๒) รองรับการจัดการ Traffic หรือ Quality of Service ได้ตามมาตรฐาน IEEE ๘๐๒.๑p

๔.๑๓) สามารถทำ Port Mirroring ได้ทั้งแบบ Ingress และ Egress โดยที่จะต้องรองรับการทำ Mirrored ได้หลายพอร์ต เพื่อส่งไปยัง Destination Port ๑ พอร์ต (Many-to-One)

๔.๑๔) รองรับการจัดเก็บข้อมูลทางสถิติ การใช้งานเครือข่าย แบบ NetFlow หรือ sFlow หรือ jFlow ได้

๔.๑๕) สามารถรองรับมาตรฐานดังนี้ได้เป็นอย่างน้อย IEEE ๘๐๒.๑D (Spanning-Tree Protocol), IEEE ๘๐๒.๑Q (VLAN Tagging), IEEE ๘๐๒.๑x, IEEE ๘๐๒.๑p (Priority Queuing), IEEE ๘๐๒.๓x (Flow Control) , IGMP Snooping , IEEE ๘๐๒.๑s (Multiple Spanning Trees)

๔.๑๖) มี Console Interface เพื่อใช้งานในรูปแบบ Command-Line-Mode ได้

๔.๑๗) ผ่านการทดสอบจากสถาบัน ICES, CISPR, UL, EN และ FCC เป็นอย่างน้อย

๕) อุปกรณ์ Firewall สำหรับให้บริการระบบเครือข่ายติดตั้ง ณ สำนักงานปลัดกระทรวงคมนาคม จำนวน ๒ ชุด มีคุณสมบัติอย่างน้อย ดังนี้

๕.๑) เป็นอุปกรณ์ที่ออกแบบเฉพาะ (Appliance) เพื่อทำหน้าที่เป็น Application Firewall โดยมีโครงสร้างแบบ Rack mount สามารถติดตั้งในตู้เก็บอุปกรณ์ขนาดมาตรฐาน ๑๙ นิ้วได้

๕.๒) มีจุดเชื่อมต่อ Network แบบ ๑๐/๑๐๐/๑๐๐๐ จำนวนไม่น้อยกว่า ๘ จุด และแบบ ๑๐G (SFP+) จำนวนไม่น้อยกว่า ๔ จุด

๕.๓) มี Hard Disk แบบ Solid-State ขนาดไม่ต่ำกว่า ๒๔๐ GB

๕.๔) สามารถทำงานแบบ Application Firewall (Layer ๗) ได้ที่ Throughput ไม่น้อยกว่า ๕ Gbps

๕.๕) สามารถรองรับ Concurrent Connections อย่างน้อย ๒,๐๐๐,๐๐๐ Connections และรองรับจำนวน Connection ไม่น้อยกว่า ๙๐,๐๐๐ Connections per Seconds

๕.๖) สามารถทำงานแบบ IPSec VPN ได้ที่ Throughput ไม่น้อยกว่า ๒ Gbps

๕.๗) สามารถเข้ารหัส (Encryption) แบบ ๓DES, AES ๒๕๖ bit และรองรับการ Authentication แบบ MD๕, SHA ได้เป็นอย่างน้อย

๕.๘) สามารถใช้งาน Routing แบบ Dynamic Routing ได้แก่ OSPF, BGP, RIP v๑/๒, IGMP และ PIM ได้เป็นอย่างน้อย

๕.๙) สามารถตรวจจับ Virus โดยป้องกันการ Download ไฟล์ที่มี Malware และตรวจสอบไฟล์ที่มีการมีการย่อขนาดไฟล์ได้ เช่น zip, gzip, gz ,๗z, rar, และ tar เป็นอย่างน้อย

๕.๑๐) รูปแบบ IP Reputation Anti-spam, Content-based Anti-spam, Block/allow List Anti-spam ได้ โดยสามารถเสนออุปกรณ์อื่นเพิ่มเติมเพื่อทำงานเป็นไปตามข้อกำหนด

๕.๑๑) สามารถจัดการระบบผ่านทาง SSH, Application GUI หรือ Web-based และ Console ได้

๕.๑๒) อุปกรณ์มีแหล่งจ่ายไฟไม่น้อยกว่า ๒ หน่วยและสามารถทำงานแบบ Hot-Swappable ได้

๕.๑๓) ผลิตภัณฑ์ยี่ห้อที่นำเสนอต้องได้รับการรับรองมาตรฐานความปลอดภัย CB, UL, FCC, CE และ VCCI เป็นอย่างน้อย

๕.๑๔) ส่วนบริหารจัดการอุปกรณ์ Firewall สามารถบริหารจัดการอุปกรณ์ที่นำเสนอได้แบบรวมศูนย์ (Centralized Management Firewall) ในรูปแบบของ Hardware Appliance หรือเป็น Software สำหรับบริหารจัดการ Firewall ที่มีระบบปฏิบัติการแบบเฉพาะที่ทำการ Hardening เรียบร้อยแล้ว โดยมีคุณสมบัติเฉพาะอย่างน้อย ดังนี้

๕.๑๔.๑) มีกลไกในการตรวจสอบ Security Policy เพื่อให้ Security Policy ทั้งหมดใช้ร่วมงานกันได้ และไม่ซ้ำซ้อน

๕.๑๔.๒) สามารถใช้งานแบบ Indexed Search Logging ได้

๕.๑๔.๓) สามารถจัดการ Security Policy ต่าง ๆ และจัดเก็บ Log ได้ทั้งแบบ Real Time และตรวจสอบย้อนหลัง

๕.๑๔.๔) สามารถหาความสัมพันธ์ (Correlation) ของ Log ต่าง ๆ ที่จัดเก็บ พร้อมทั้งแสดงข้อมูลเป็นเหตุการณ์ (Event) ต่าง ๆ และแนวโน้มของเหตุการณ์ในลักษณะของ Timelines หรือ Charts หรือ Maps ได้ กรณีอุปกรณ์ไม่รองรับการทำงาน สามารถเสนออุปกรณ์อื่นเพิ่มเติมเพื่อทำงานเป็นไปตามข้อกำหนดเพื่อพร้อมใช้งานในอนาคต

๕.๑๔.๕) สามารถจัดทำรายงานแบบ Predefined Report ได้แก่ รายงานประเภท Threat Prevention Report, Application and URL Filtering Report และ User Activity Report ได้เป็นอย่างน้อย

๕.๑๔.๖) สามารถกำหนดช่วงเวลาที่ต้องการให้สร้างและแสดงผลรายงานได้ (Scheduled Report) และกำหนดให้ส่งรายงานผ่านทาง Email ได้เป็นอย่างน้อย

๕.๑๕) สามารถทำการตรวจสอบ Traffic ที่เข้ารหัส SSL ด้วยการทำ SSL Decryption หรือ SSL Inspection (ทั้งแบบ Inbound และ Outbound) รวมทั้งการทำ SSL Decryption Broker หรือ Decryption Port Mirroring ได้ หรือนำเสนอระบบเพิ่มเติมเพื่อให้อุปกรณ์ทำงานตามข้อกำหนดได้

๖) อุปกรณ์จัดเก็บข้อมูลจราจรบนเครือข่ายสำหรับให้บริการระบบเครือข่ายติดตั้ง ณ สำนักงานปลัดกระทรวงคมนาคม จำนวน ๑ ชุด มีคุณสมบัติอย่างน้อยดังนี้

๖.๑) เป็นอุปกรณ์ Appliance ที่ออกแบบเฉพาะสำหรับเก็บบันทึกข้อมูลทางด้านการรักษาความปลอดภัยเครือข่ายโดยทำหน้าที่เป็น Log Management โดยเฉพาะสามารถติดตั้งใน Rack มาตรฐาน ๑๙ นิ้วได้

๖.๒) หน่วยประมวลผล (Processor) ที่มีจำนวน Core ไม่ต่ำกว่า ๖ Core

๖.๓) มีหน่วยความจำหลัก (Memory) ขนาดไม่น้อยกว่า ๓๒ GB

๖.๔) มี Storage หรือ Hard Disk สำหรับจัดเก็บข้อมูล ขนาดความจุรวมไม่น้อยกว่า ๑.๕ TB (หลังจากการทำ RAID ๕)

๖.๕) มีอินเตอร์เฟสเพื่อเชื่อมต่อกับเครือข่ายแบบ ๑๐/๑๐๐/๑๐๐๐ Mbps แบบ Copper จำนวน ๔ พอร์ท

๖.๖) สามารถรองรับอุปกรณ์ที่จัดเก็บ log ได้ไม่จำกัดจำนวนอุปกรณ์

๖.๗) สามารถจัดเก็บ Raw Log ที่ได้จากอุปกรณ์ โดยรองรับปริมาณข้อมูลได้ไม่น้อยกว่า ๓๐ GB ต่อวัน หรือ ๑๐๐,๐๐๐ เหตุการณ์ต่อวินาที (Event per Second: EPS) และสามารถทำการส่งต่อ (Forwarding) log ไปยังอุปกรณ์ Log Server อื่นๆ หรืออุปกรณ์ SIEM ได้

๖.๘) สามารถบีบอัดข้อมูล เพื่อลดขนาด Log ที่จัดเก็บได้ ในอัตราส่วนไม่น้อยกว่า ๑๐ ต่อ ๑

๖.๙) สามารถย้ายและถ่ายโอนข้อมูลสำรอง (Archive Log) ไปยังหน่วยเก็บข้อมูลภายนอกโดยใช้ NAS หรือ SAN ได้

๖.๑๐) สามารถบริหารจัดการอุปกรณ์ผ่าน Web Browser และ CLI ได้

๖.๑๑) สามารถกำหนดสิทธิ์การใช้งานระบบของผู้ดูแลระบบแต่ละคนได้แตกต่างกัน (Role Base Access Control)

๖.๑๒) สามารถพิสูจน์ตัวตนของผู้ดูแลระบบบน Local system หรือ Radius Server ได้

๖.๑๓) อุปกรณ์เก็บ Log ที่เสนอต้องรองรับการเก็บข้อมูล Log จากอุปกรณ์ อย่างน้อย ๓๕๐ รูปแบบ (Format) และรองรับการพัฒนาให้ระบบรับข้อมูล (Log) ที่ไม่สนับสนุนหรือรองรับแต่เดิมได้

๖.๑๔) สามารถจัดรูปแบบของข้อมูล Log ที่แตกต่างกัน ซึ่งมาจากหลากหลายอุปกรณ์ ให้อยู่ในรูปแบบมาตรฐานเดียวกันได้

๖.๑๕) มีความสามารถในการรับ Log (Log Source) จาก Protocol อย่างน้อยดังนี้

- Syslog
- FTP (File Transfer Protocol)
- SFTP (Secure File Transfer Protocol)
- SNMP (Simple Network Management Protocol)
- ODBC/JDBC
- OPSEC

๖.๑๖) มีระบบตรวจสอบเพื่อยืนยันว่าข้อมูลที่เก็บบันทึกจะไม่มีการแก้ไขหรือเปลี่ยนแปลง (File Integrity) ด้วย Algorithm แบบ SHA-๑ หรือ SHA-๒๕๖ หรือดีกว่า

๖.๑๗) เป็นระบบ Log Management ที่รองรับการออกรายงานตามมาตรฐานต่างๆ ดังนี้ ISO/IEC, FISMA, SOX, PCI-DSS, NERC, HIPAA

๖.๑๘) สามารถทำการค้นหา log ได้หลายรูปแบบ เช่น ตาราง, แผนภูมิ ได้

๖.๑๙) มีรูปแบบรายงาน (Predefine Report) และสามารถสร้าง (Custom) รูปแบบรายงานได้เองและสามารถจัดส่งรายงานให้กับผู้ดูแลระบบตามช่วงเวลาได้

๖.๒๐) สามารถส่งออกรูปแบบรายงานในรูปแบบไฟล์ดังต่อไปนี้ PDF, HTML และ CSV ได้เป็นอย่างน้อย

๗) เครื่องคอมพิวเตอร์แม่ข่ายทำหน้าที่บริหารระบบเครือข่าย (Network Management) ติดตั้ง ณ สำนักงานปลัดกระทรวงคมนาคมจำนวน ๑ ชุด มีคุณสมบัติอย่างน้อย ดังนี้

๗.๑) มีหน่วยประมวลผลกลาง (CPU) แบบ ๘ แกนหลัก (๘ core) หรือดีกว่า สำหรับคอมพิวเตอร์แม่ข่าย (Server) โดยเฉพาะและมีความเร็วสัญญาณนาฬิกาพื้นฐานไม่น้อยกว่า ๒.๔ GHz จำนวนไม่น้อยกว่า ๒ หน่วย

๗.๒) มีหน่วยความจำหลัก (RAM) ชนิด ECC DDR๓ หรือดีกว่า มีขนาดไม่ต่ำกว่า ๑๖ GB

๗.๓) มีหน่วยจัดเก็บข้อมูล (Hard Drive) ชนิด SCSI หรือ SAS ที่มีความเร็วรอบไม่น้อยกว่า ๑๐,๐๐๐ รอบต่อนาทีหรือชนิด Solid State Drive หรือดีกว่า และขนาดความจุไม่น้อยกว่า ๓๐๐ GB จำนวนอย่างน้อย ๔ หน่วย

๗.๔) ระบบ NMS ทั้งหมดสามารถทำงานภายใต้ระบบปฏิบัติการ Windows server ได้

๗.๕) สามารถตรวจหา (Discover) อุปกรณ์ได้ไม่น้อยกว่า ๑๐๐๐ Sensor

๗.๖) สามารถสนับสนุนการใช้งาน Windows Management Instrumentation (WMI) ได้

๗.๗) สามารถตรวจสอบค้นหาและแสดงสถานะของเครือข่ายในลักษณะที่เป็น Automatic Discovery

๗.๘) สามารถใช้งานการตรวจสอบผ่าน NetFlow หรือ IPFIX หรือ sFlow หรือ jFlow โดยสามารถใช้งานร่วมกับอุปกรณ์ระบบเครือข่ายที่นำเสนอได้

๗.๙) ระบบจัดการและบริหารเครือข่ายต้องสามารถจัดการอุปกรณ์เครือข่ายใด ๆ ที่สนับสนุนการใช้งาน Simple Network Protocol (SNMP) และสามารถจัดการ Management Information Base (MIB) ได้

๗.๑๐) สามารถตั้งค่า Thresholds ของ Event ต่าง ๆ ได้

๗.๑๑) สามารถกำหนด Automatic Action หรือคำสั่งในการทำงานได้เมื่อเกิด Event ที่กำหนดให้มีการตรวจจับ หรือสามารถทำ Action เพื่อ Response ต่อเหตุการณ์ที่เกิดขึ้น

๗.๑๒) มี Event Subsystem ในการรวบรวม Event จากจุดต่างๆในเครือข่ายเพื่อบ่งชี้แนวโน้มของปัญหาที่อาจจะเกิดขึ้นได้ โดยมี Event Browser Filter เพื่อให้ผู้บริหารเครือข่ายสามารถตรวจดูเฉพาะ Critical Event เฉพาะจุดที่สนใจได้

๗.๑๓) สามารถลำดับความสำคัญของเหตุการณ์หรือ Event จะต้องถูกแสดงด้วยรหัสสีที่ต่างกัน

๗.๑๔) สามารถบริหารเครือข่ายได้จากระยะไกล ด้วย Web Browser โดยสามารถแสดงรายงานเป็นกราฟฟิกแบบ Web-based และเจาะลึกเพื่อดูรายละเอียดเพิ่มเติมได้ทันที (Hot-line Capability to Drill Down)

๗.๑๕) สามารถใช้กับ Web User Interface เพื่อให้ Network Administrator สามารถเข้าถึงระบบโดยผ่านทาง Web Browser ทั่วไปได้

๗.๑๖) รองรับการทำ Failover Cluster ได้

๗.๑๗) สามารถใช้งาน Client App สำหรับ Windows ได้

๗.๑๘) สามารถรองรับการใช้งานผ่าน Mobile Apps ได้

๗.๑๙) ผู้ยื่นข้อเสนอจะต้องรับผิดชอบค่าใช้จ่ายในการใช้งานโปรแกรมระบบ NMS ทั้งหมดตลอดอายุสัญญา