ขอบเขตของงาน (Terms of Reference: TOR)
ซื้อสำหรับโครงการทดแทนและเพิ่มประสิทธิภาพระบบรักษาความปลอดภัยเครือข่าย GFMIS

๑. ความเป็นมา

เนื่องจากอุปกรณ์ Firewall ที่ใช้งานอยู่ในปัจจุบันเริ่มใช้งานมาตั้งแต่ปี ๒๕๕๔ และอุปกรณ์เริ่มเสื่อมสภาพ อีกทั้งเจ้าของผลิตภัณฑ์ได้ยกเลิกการขาย และหยุดการผลิตอุปกรณ์ Firewall ดังกล่าว ประกอบกับจากการตรวจสอบและติดตามสถานการณ์ความปลอดภัยเครือข่าย GFMIS พบว่ามีผู้ไม่หวังดีและพยายามโจมตีระบบ GFMIS ซึ่งอาจจะส่งผลกระทบต่อผู้ใช้งานระบบ GFMIS ทั่วประเทศ ไม่สามารถใช้บริการได้อย่างต่อเนื่อง

๒. วัตถุประสงค์

เพื่อจัดซื้อและติดตั้งอุปกรณ์ Firewall จำนวน ๓ ชุด และอุปกรณ์บริหารจัดการ Firewall จำนวน ๑ ชุด ที่ศูนย์คอมพิวเตอร์หลัก และอุปกรณ์ Firewall จำนวน ๑ ชุด ศูนย์คอมพิวเตอร์สำรอง และอุปกรณ์ Firewall จำนวน ๑ ชุด ที่ศูนย์คอมพิวเตอร์กรมบัญชีกลาง เพื่อให้ระบบ GFMIS สามารถรองรับการเข้าใช้งานของส่วนราชการทั่วประเทศได้อย่างต่อเนื่อง, มีประสิทธิภาพ และสามารถป้องกันภัยคุมคามรูปแบบใหม่ได้

๓. คุณสมบัติของผู้ประสงค์จะเสนอราคา

๓.๑ ผู้เสนอราคาต้องเป็นผู้มีอาชีพขายพัสดุที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

๓.๒ ผู้เสนอราคาต้องไม่เป็นผู้ที่ถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานของทางราชการและได้แจ้งเวียนชื่อแล้ว หรือไม่เป็นผู้ที่ได้รับผลของการสั่งให้นิติบุคคลหรือบุคคลอื่นเป็นผู้ทิ้งงานตามระเบียบของทางราชการ

๓.๓ ผู้เสนอราคาต้องไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้เสนอราคารายอื่น ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรม

๓.๔ ผู้เสนอราคาต้องไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้เสนอราคาได้มีคำสั่งให้สละสิทธิ์และความคุ้มกันเช่นว่านั้น

๓.๕ ผู้เสนอราคาต้องไม่เป็นผู้ที่ถูกประเมินสิทธิผู้เสนอราคาในสถานะที่ห้ามเข้าเสนอราคาและห้ามทำสัญญาตามที่ กวพ.กำหนด

๓.๖ บุคคลหรือนิติบุคคลที่จะเข้าเป็นคู่สัญญาต้องไม่อยู่ในฐานะเป็นผู้ไม่แสดงบัญชีรายรับรายจ่ายหรือแสดงบัญชีรายรับรายจ่ายไม่ถูกต้องครบถ้วนในสาระสำคัญ

๓.๗ บุคคลหรือนิติบุคคลที่จะเข้าเป็นคู่สัญญากับหน่วยงานของรัฐซึ่งได้ดำเนินการจัดซื้อจัดจ้างด้วยระบบอิเล็กทรอนิกส์ (e-Government Procurement : e-GP) ต้องลงทะเบียนในระบบอิเล็กทรอนิกส์ของกรมบัญชีกลางที่เว็บไซต์ศูนย์ข้อมูลจัดซื้อจัดจ้างภาครัฐ

๓.๘ คู่สัญญาต้องรับจ่ายเงินผ่านบัญชีธนาคาร เว้นแต่การรับจ่ายเงินแต่ละครั้งซึ่งมีมูลค่าไม่เกินสามหมื่นบาทคู่สัญญาอาจรับจ่ายเป็นเงินสดก็ได้

๓.๙ ผู้เสนอราคาต้องเป็นเจ้าของลิขสิทธิ์หรือได้รับมอบอำนาจหรือตัวแทนจากเจ้าของลิขสิทธิ์โปรแกรม

๓.๑๐ ผู้เสนอราคาต้องเป็นนิติบุคคลตามกฎหมายที่จดทะเบียนในประเทศไทย โดยมีหลักฐานการจดทะเบียนซึ่งกรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์ออกให้หรือรับรองให้ไม่เกิน ๖ เดือน นับถึงวันที่ยื่นซอง

๔. แบบรูปรายการหรือคุณลักษณะเฉพาะ

ระบบคอมพิวเตอร์และอุปกรณ์ในโครงการทดแทนและเพิ่มประสิทธิภาพระบบรักษาความปลอดภัยเครือข่าย GFMIS ที่จะจัดซื้อครั้งนี้ จะต้องเป็นของแท้ ของใหม่ ไม่เคยใช้งานมาก่อน ไม่เป็นของเก่าเก็บ อยู่ในสภาพที่จะใช้งานได้ทันที และมีคุณลักษณะเฉพาะตรงตามที่กำหนดไว้ ดังรายละเอียดภาคผนวกที่ ๑ ถึง ๔

๕. ระยะเวลาดำเนินการ

ผู้ชนะการประกวดราคาจะต้องดำเนินการจัดส่งและติดตั้งอุปกรณ์ในโครงการทดแทนและเพิ่มประสิทธิภาพระบบรักษาความปลอดภัยเครือข่าย GFMIS ณ สถานที่ตามที่สำนักงานปลัดกระทรวงการคลังหรือคณะกรรมการตรวจรับพัสดุกำหนด และส่งมอบงานภายในระยะเวลา ๑๒๐ วัน นับถัดจากวันลงนามในสัญญา

๖. ระยะเวลาส่งมอบงาน

ส่งมอบพร้อมติดตั้งอุปกรณ์ Firewall ที่ศูนย์คอมพิวเตอร์หลักและศูนย์คอมพิวเตอร์สำรองระบบ GFMIS ภายใน ๑๒๐ วัน นับถัดจากวันลงนามในสัญญา

๗. เงื่อนไขการชำระเงิน

ชำระเงินในอัตราร้อยละ ๑๐๐ ของจำนวนเงินตามสัญญา เมื่อคณะกรรมการตรวจรับได้ตรวจรับการส่งมอบงานเรียบร้อยแล้ว

๘. วงเงินในการจัดหา

วงเงินในการจัดซื้อโครงการทดแทนและเพิ่มประสิทธิภาพระบบรักษาความปลอดภัยเครือข่าย GFMIS เป็นเงินทั้งสิ้น ๕,๓๓๐,๐๐๐ บาท (ห้าล้านสามแสนสามหมื่นบาทถ้วน) โดยเบิกจ่ายจากเงินกันไว้เบิกเหลื่อมปี ๒๕๕๙ และเงินงบประมาณประจำปี ๒๕๖๐

๙. หน่วยงานผู้รับผิดชอบดำเนินการ

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง

ภาคผนวก ๑

รายละเอียดคุณลักษณะเฉพาะของ

โครงการทดแทนและเพิ่มประสิทธิภาพระบบรักษาความปลอดภัยเครือข่าย GFMIS

ภาคผนวก ๑

รายละเอียดคุณลักษณะเฉพาะของ

โครงการทดแทนและเพิ่มประสิทธิภาพระบบรักษาความปลอดภัยเครือข่าย GFMIS

อุปกรณ์ที่จัดซื้อในโครงการทดแทนและเพิ่มประสิทธิภาพระบบรักษาความปลอดภัยเครือข่าย GFMIS ที่จะจัดซื้อครั้งนี้ จะต้องเป็นของแท้ ของใหม่ สามารถที่จะใช้งานได้ทันที และมีคุณลักษณะเฉพาะตรงตามที่กำหนดไว้ ดังมีรายละเอียด ดังนี้

๑. อุปกรณ์ Firewall สำหรับ GFMIS DC (Internal Zone) จำนวน ๒ ชุด มีคุณสมบัติอย่างน้อย ดังนี้

๑.๑ อุปกรณ์ที่เสนอต้องอยู่ Gartner Enterprise Network Firewall ในปี ๒๐๑๖ เป็นอย่างน้อย

๑.๒ ผลิตภัณฑ์จะต้องมีผลการทดสอบ(Test Methodology v๖.๐) ของ Next Generation Firewall จาก NSS LAB ปี ๒๐๑๖ โดยมีผล Security Effectiveness ไม่น้อยกว่า ๙๙%

๑.๓ อุปกรณ์ที่นำเสนอเป็น Appliance สามารถทำงานแบบ Next Generation Firewall (NGFW) ที่ใช้เทคโนโลยีแบบ Stateful Inspection และมี Firewall Throughput ไม่น้อยกว่า ๒๕ Gbps

๑.๔ สามารถรับ Concurrent Connections ได้อย่างน้อย ๓,๒๐๐,๐๐๐ Connections และรับจำนวน New Connection ได้ไม่น้อยกว่า ๑๘๕,๐๐๐ Connections per Seconds

๑.๕ สนับสนุนการทำ VLANs tagging อย่างน้อย ๑,๐๒๔ VLANs

๑.๖ สนับสนุนการทำงาน Link Aggregation ตามมาตรฐาน ๘๐๒.๓ad

๑.๗ มีพอร์ตแบบ ๑๐/๑๐๐/๑๐๐๐ Base-T จำนวนไม่น้อยกว่า ๘ พอร์ต และพอร์ตแบบ ๑๐GBase-F SFP+ จำนวนไม่น้อยกว่า ๔ พอร์ตพร้อมโมดูล

๑.๘ มี Harddisk ในตัวอุปกรณ์ขนาดไม่น้อยกว่า ๕๐๐ GB

๑.๙ มี VPN Throughput ไม่น้อยกว่า ๖.๕ Gbps และรองรับการทำงานแบบ IPSec VPN ได้ทั้งแบบ Site to site และ Client to Site

๑.๑๐ สามารถใช้งาน Clientless SSL VPN แบบ Remote Access ได้ไม่น้อยกว่า ๕ Concurrent Users

๑.๑๑ มี IPS throughput ไม่น้อยกว่า ๗.๘ Gbps โดยจะต้องมีพื้นฐานการทำงานในการป้องกันภัยคุกคามในลักษณะ Exploit signatures, Protocol anomalies, Application controls และ Behavior-based detection ได้เป็นอย่างน้อย

๑.๑๒ สามารถทำงานได้ทั้งแบบ IPv๔ , IPv๖ และทำงานได้พร้อมกันทั้ง IPv๔ และ IPv๖

๑.๑๓ สามารถทำ High Availability (HA) Cluster แบบ Active-Active ได้ (ไม่กระทบหรือไม่ต้องแก้ไขระบบ Network เดิมที่ใช้งานร่วมกันอยู่) โดยสามารถทำ Session Synchronization สำหรับ Firewall และ VPN ได้

๑.๑๔ สามารถทำงานในลักษณะ ISP Redundancy ได้ทั้งแบบ Primary/Backup และ Load Sharing

๑.๑๕ สามารถตรวจสอบและควบคุม Applications ได้อย่างน้อย ๒,๐๐๐ Applications

๑.๑๖ สามารถกำหนด Security Policy ตาม User, User Group ด้วยการ Integrate เข้ากับ Active Directory ได้โดยไม่ต้องติดตั้งซอฟแวร์ (Agent) เพิ่มเติมบน Domain Controller และเครื่องของผู้ใช้งาน รวมทั้งสามารถทำการ Authentication ผ่าน Browser ได้สำหรับผู้ใช้งานที่ไม่ได้อยู่ใน Domain ขององค์กร

๑.๑๗ สนับสนุนการตรวจสอบผู้ใช้ (Authentication) ดังนี้ Firewall password, RADIUS, TACACS และSecureID เป็นอย่างน้อย

๑.๑๘ สามารถบริหารจัดการ Bandwidth (QoS) ในแบบ Weighted Priorities, Guarantees และ Limit ได้

๑.๑๙ สามารถใช้งาน Routing แบบ Dynamic Routing ได้แก่ OSPF, BGP, RIP, IGMP v๒/๓ และ PIM ได้เป็นอย่างน้อย

๑.๒๐ สามารถตรวจจับ Virus ที่มาในรูปแบบของ SMTP, POP๓, HTTP และ FTP protocol ได้ รวมถึงสามารถป้องกันการโจมตีจาก BOT และ
สามารถ Update ฐานข้อมูลได้อย่างน้อย ๑ ปี

๑.๒๑ สามารถทำงานแบบ URL Filtering เพื่อเพิ่มความปลอดภัยในการใช้งาน Web site ได้ โดยมีการจัดประเภทของ Content แบบ Pre-defined category ไม่น้อยกว่า ๖๐ ประเภทและสามารถ Update ฐานข้อมูลได้อย่างน้อย ๑ ปี

๑.๒๒ สามารถทำงานในลักษณะแจ้งเตือนและสอบถามผู้ใช้งานได้ (User Check) ในแบบ Real time เพื่อเป็นการให้ข้อมูลและเก็บข้อมูลจากการสอบถามผู้ใช้งาน Application และ URLs ในแต่ละ Filtering Rule ได้หรือมี Response Page แจ้งเตือนผู้ใช้ในกรณีที่มีการกำหนดให้ block application, URL, Antivirus และ File blocking

๑.๒๓ สามารถทำงาน High Availability ทั้งแบบ Active/Active และ Active/Passive โดยสามารถทำ Session failover ในกรณีเกิด Device และ link failure

๑.๒๔ สามารถจัดการระบบผ่านทาง SSH, Web-based และ Console ได้

๑.๒๕ ผลิตภัณฑ์ยี่ห้อที่นำเสนอต้องได้รับการรับรองมาตรฐาน ICSA และ NSS Labs เป็นอย่างน้อย

๑.๒๖ ผลิตภัณฑ์ยี่ห้อที่นำเสนอต้องได้รับการรับรองมาตรฐานความปลอดภัย CB, UL, FCC, CE เป็นอย่างน้อย

๑.๒๗ บริษัทผู้นำเสนอจะต้องได้รับการแต่งตั้งอย่างเป็นทางการ จากเจ้าของผลิตภัณฑ์ หรือผู้แทนเจ้าของผลิตภัณฑ์ในประเทศไทย

๑.๒๘ เป็นผลิตภัณฑ์ที่ผู้ผลิตยังมิได้ประกาศภาวะสิ้นสุดการขายหรือสิ้นสุดอายุหรือสิ้นสุดการบริการ (End-of-Sale หรือ End-of-Life หรือ End-of-Service)โดยมีหนังสือรับรองจากเจ้าของผลิตภัณฑ์ หรือผู้แทนเจ้าของผลิตภัณฑ์ในประเทศไทย

๑.๒๙ อุปกรณ์ที่นำเสนอต้องไม่ใช่ผลิตภัณฑ์ยี่ห้อเดียวกันกับ Firewall ตัวอื่นๆ ใน GFMIS DC Network เพื่อเพิ่มความปลอดภัยในการทำงานโดยภาพรวมของเครือข่าย

๑.๓๐ อุปกรณ์ทั้งหมดต้องเป็นอุปกรณ์ใหม่ไม่เคยผ่านการใช้งานมาก่อน โดยมีหนังสือรับรองจากเจ้าของผลิตภัณฑ์ หรือผู้แทนเจ้าของผลิตภัณฑ์ในประเทศไทย และสามารถใช้งานร่วมกับอุปกรณ์เดิมได้

๒. อุปกรณ์บริหารจัดการ Firewall GFMIS DC จำนวน ๑ ชุด มีคุณลักษณะอย่างน้อยดังนี้

๒.๑ เป็น Hardware Appliance ที่ทำหน้าที่ในการบริหารจัดการอุปกรณ์ Next Generation Firewall จากส่วนกลาง

๒.๒ ระบบที่เสนอจะต้องมี Centralized Management พร้อมลิขสิทธิ์ถูกต้องตามกฎหมายในการบริหารและจัดการ Security Gateways ที่เสนอ อย่างน้อย ๑๐ Gateways

๒.๓ มี Storage ไม่น้อยกว่า ๒ TB

๒.๔ มี Network Interface ชนิด Copper GbE อย่างน้อย ๑ พอร์ต

๒.๕ สามารถเก็บ Log ของ Firewall/ VPN ได้

๒.๖ สามารถจัดการระบบผ่านทาง SSH, Web-based และ Console ได้

๒.๗ ผลิตภัณฑ์ยี่ห้อที่นำเสนอต้องได้รับการรับรองมาตรฐานความปลอดภัย CB หรือ UL หรือ FCC หรือ CE เป็นอย่างน้อย

๒.๘ สามารถตรวจสอบ Log ได้ทั้งแบบ Real Time และตรวจสอบย้อนหลังได้

๒.๙ สามารถแสดงเหตุการณ์โดยระบุเป็นประเทศที่แสดงบนแผนที่ได้

๒.๑๐ สามารถแสดงรายงานของเหตุการณ์ภัยคุกคามต่างๆได้ และสามารถ Export ในรูปแบบของ PDF File

๒.๑๑ เป็นผลิตภัณฑ์ที่ผู้ผลิตยังมิได้ประกาศภาวะสิ้นสุดการขายหรือสิ้นสุดอายุหรือสิ้นสุดการบริการ (End-of-Sale หรือ End-of-Life หรือ End-of-Service)โดยมีหนังสือรับรองจากเจ้าของผลิตภัณฑ์ หรือผู้แทนเจ้าของผลิตภัณฑ์ในประเทศไทย

๒.๑๒ บริษัทผู้นำเสนอจะต้องได้รับการแต่งตั้งอย่างเป็นทางการ จากเจ้าของผลิตภัณฑ์ หรือผู้แทนเจ้าของผลิตภัณฑ์ในประเทศไทย

๓. อุปกรณ์ Firewall สำหรับ GFMIS DC (PKI Zone) จำนวน ๑ ชุด มีคุณลักษณะอย่างน้อยดังนี้

๓.๑ เป็นอุปกรณ์ Firewall ชนิด Stateful Inspection แบบ Appliance

๓.๒ มี Firewall Throughput ไม่น้อยกว่า ๑.๘ Gbps โดยมีพอร์ตแบบ Gigabit Ethernet (๑๐/๑๐๐/๑๐๐๐) อย่างน้อย ๘ พอร์ต

๓.๓ สามารถรับการใช้งานได้พร้อมกัน ๒๕๐,๐๐๐ Concurrent Connection และรับNew connection ได้ไม่น้อยกว่า ๒๐,๐๐๐ connection/sec

๓.๔ สามารถทำงานแบบ ๓DES/AES VPN โดยมี Throughput สำหรับการทำงานของ VPN ไม่น้อยกว่า ๒๕๐ Mbps

๓.๕ รองรับ Firewall +IPS +Application Control Throughput ได้ไม่น้อยกว่า ๔๕๐ Mbps

๓.๖ สามารถเชื่อมต่อด้วย Mobile connect ได้

๓.๗ สามารถทำ Split Tunnel VPN ได้

๓.๘ สามารถทำ Network Address Translation (NAT) และ Port Address Translation (PAT) ได้

๓.๙ สามารถเก็บรายละเอียดและตรวจสอบการใช้งาน (Logging/Monitoring) โดยเก็บเป็น Syslog ได้

๓.๑๐ สามารถรับ Routing แบบ Dynamic ได้แก่ OSPF, RIP ได้เป็นอย่างน้อย และสามารถทำงานมาตรฐาน IPv ๖

๓.๑๑ มี DRAM ขนาดไม่น้อยกว่า ๘ GB และ Flash Memory ขนาดไม่น้อยกว่า ๘ GB

๓.๑๒ สามารถใช้งาน USB ๒.๐ ได้ไม่น้อยกว่า ๑ Ports

๓.๑๓ สามารถทำ Link Aggregation ตามมาตรฐาน IEEE๘๐๒.๓ad ได้

๓.๑๔ รองรับการใช้งานแบบ High Available (HA) แบบActive/ Standby และ Active/Active ได้

๓.๑๕ สามารถกำหนดสิทธิในการเข้าถึงเครือข่าย (User Authentication) โดยอ้างอิงฐานข้อมูลจาก Radius หรือ Tacacsได้

๓.๑๖ สามารถจัดการอุปกรณ์ โดยใช้ CLI และ GUI ได้

๓.๑๗ ผลิตภัณฑ์ยี่ห้อที่นำเสนอต้องได้รับการรับรองมาตรฐานความปลอดภัย UL, FCC, CE เป็นอย่างน้อย

๓.๑๘ อุปกรณ์สามารถติดตั้งบน Rack ๑๙” ได้

๓.๑๙ บริษัทผู้นำเสนอจะต้องได้รับการแต่งตั้งอย่างเป็นทางการ จากเจ้าของผลิตภัณฑ์ หรือผู้แทนเจ้าของผลิตภัณฑ์ในประเทศไทย

๓.๒๐ อุปกรณ์ที่นำเสนอต้องไม่ใช่ผลิตภัณฑ์ยี่ห้อเดียวกันกับ Firewall ตัวอื่นๆ ใน GFMIS DC Network เพื่อเพิ่มความปลอดภัยในการทำงานโดยภาพรวมของเครือข่าย

๓.๒๑ เป็นผลิตภัณฑ์ที่ผู้ผลิตยังมิได้ประกาศภาวะสิ้นสุดการขายหรือสิ้นสุดอายุหรือสิ้นสุดการบริการ (End-of-Sale หรือ End-of-Life หรือ End-of-Service) โดยมีหนังสือรับรองจากเจ้าของผลิตภัณฑ์ หรือผู้แทนเจ้าของผลิตภัณฑ์ในประเทศไทย

๓.๒๒ อุปกรณ์ทั้งหมดต้องเป็นอุปกรณ์ใหม่ไม่เคยผ่านการใช้งานมาก่อน โดยมีหนังสือรับรองจากเจ้าของผลิตภัณฑ์ หรือผู้แทนเจ้าของผลิตภัณฑ์ในประเทศไทย และสามารถใช้งานร่วมกับอุปกรณ์เดิมได้อย่างไม่มีปัญหา

๔. อุปกรณ์ Firewall สำหรับ GFMIS DR (PKI Zone) จำนวน ๑ ชุด มีคุณลักษณะอย่างน้อยดังนี้

๔.๑ เป็นอุปกรณ์ Firewall ชนิด Stateful Inspection แบบ Appliance

๔.๒ มี Firewall Throughput ไม่น้อยกว่า ๑.๘ Gbps โดยมีพอร์ตแบบ Gigabit Ethernet (๑๐/๑๐๐/๑๐๐๐) อย่างน้อย ๘ พอร์ต

๔.๓ สามารถรับการใช้งานได้พร้อมกัน ๒๕๐,๐๐๐ Concurrent Connection และรับNew connection ได้ไม่น้อยกว่า ๒๐,๐๐๐ connection/sec

๔.๔ สามารถทำงานแบบ ๓DES/AES VPN โดยมี Throughput สำหรับการทำงานของ VPN ไม่น้อยกว่า ๒๕๐ Mbps

๔.๕ รองรับ Firewall +IPS +Application Control Throughput ได้ไม่น้อยกว่า ๔๕๐ Mbps

๔.๖ สามารถเชื่อมต่อด้วย Mobile connect ได้

๔.๗ สามารถทำ Split Tunnel VPN ได้

๔.๘ สามารถทำ Network Address Translation (NAT) และ Port Address Translation (PAT) ได้

๔.๙ สามารถเก็บรายละเอียดและตรวจสอบการใช้งาน (Logging/Monitoring) โดยเก็บเป็น Syslog ได้

๔.๑๐ สามารถรับ Routing แบบ Dynamic ได้แก่ OSPF, RIP ได้เป็นอย่างน้อย และสามารถทำงานมาตรฐาน IPv ๖

๔.๑๑ มี DRAM ขนาดไม่น้อยกว่า ๘ GB และ Flash Memory ขนาดไม่น้อยกว่า ๘ GB

๔.๑๒ สามารถใช้งาน USB ๒.๐ ได้ไม่น้อยกว่า ๑ Ports

๔.๑๓ สามารถทำ Link Aggregation ตามมาตรฐาน IEEE๘๐๒.๓ad ได้

๔.๑๔ รองรับการใช้งานแบบ High Available (HA) แบบActive/ Standby และ Active/Active ได้

๔.๑๕ สามารถกำหนดสิทธิในการเข้าถึงเครือข่าย (User Authentication) โดยอ้างอิงฐานข้อมูลจาก Radius หรือ Tacacsได้

๔.๑๖ สามารถจัดการอุปกรณ์ โดยใช้ CLI และ GUI ได้

๔.๑๗ ผลิตภัณฑ์ยี่ห้อที่นำเสนอต้องได้รับการรับรองมาตรฐานความปลอดภัย UL, FCC, CE เป็นอย่างน้อย

๔.๑๘ อุปกรณ์สามารถติดตั้งบน Rack ๑๙” ได้

๔.๑๙ บริษัทผู้นำเสนอจะต้องได้รับการแต่งตั้งอย่างเป็นทางการ จากเจ้าของผลิตภัณฑ์ หรือผู้แทนเจ้าของผลิตภัณฑ์ในประเทศไทย

๔.๒๐ อุปกรณ์ที่นำเสนอต้องไม่ใช่ผลิตภัณฑ์ยี่ห้อเดียวกันกับ Firewall ตัวอื่นๆ ใน GFMIS DR Network เพื่อเพิ่มความปลอดภัยในการทำงานโดยภาพรวมของเครือข่าย

๔.๒๑ เป็นผลิตภัณฑ์ที่ผู้ผลิตยังมิได้ประกาศภาวะสิ้นสุดการขายหรือสิ้นสุดอายุหรือสิ้นสุดการบริการ (End-of-Sale หรือ End-of-Life หรือ End-of-Service) โดยมีหนังสือรับรองจากเจ้าของผลิตภัณฑ์ หรือผู้แทนเจ้าของผลิตภัณฑ์ในประเทศไทย

๔.๒๒ อุปกรณ์ทั้งหมดต้องเป็นอุปกรณ์ใหม่ไม่เคยผ่านการใช้งานมาก่อน โดยมีหนังสือรับรองจากเจ้าของผลิตภัณฑ์ หรือผู้แทนเจ้าของผลิตภัณฑ์ในประเทศไทย และสามารถใช้งานร่วมกับอุปกรณ์เดิมได้อย่างไม่มีปัญหา

๕. อุปกรณ์ Firewall สำหรับ GFMIS CGD จำนวน ๑ ชุด มีคุณลักษณะอย่างน้อยดังนี้

๕.๑ เป็นอุปกรณ์ Firewall ชนิด Stateful Inspection แบบ Appliance

๕.๒ มี Firewall Throughput ไม่น้อยกว่า ๑.๘ Gbps โดยมีพอร์ตแบบ Gigabit Ethernet (๑๐/๑๐๐/๑๐๐๐) อย่างน้อย ๘ พอร์ต

๕.๓ สามารถรับการใช้งานได้พร้อมกัน ๒๕๐,๐๐๐ Concurrent Connection และรับ New connection ได้ไม่น้อยกว่า ๒๐,๐๐๐ connection/sec

๕.๔ สามารถทำงานแบบ ๓DES/AES VPN โดยมี Throughput สำหรับการทำงานของ VPN ไม่น้อยกว่า ๒๕๐ Mbps

๕.๕ รองรับ Firewall +IPS +Application Control Throughput ได้ไม่น้อยกว่า ๔๕๐ Mbps

๕.๖ สามารถเชื่อมต่อด้วย Mobile connect ได้

๕.๗ สามารถทำ Split Tunnel VPN ได้

๕.๘ สามารถทำ Network Address Translation (NAT) และ Port Address Translation (PAT) ได้

๕.๙ สามารถเก็บรายละเอียดและตรวจสอบการใช้งาน (Logging/Monitoring) โดยเก็บเป็น Syslog ได้

๕.๑๐ สามารถรับ Routing แบบ Dynamic ได้แก่ OSPF, RIP ได้เป็นอย่างน้อย และสามารถทำงานมาตรฐาน IPv ๖

๕.๑๑ มี DRAM ขนาดไม่น้อยกว่า ๘ GB และ Flash Memory ขนาดไม่น้อยกว่า ๘ GB

๕.๑๒ สามารถใช้งาน USB ๒.๐ ได้ไม่น้อยกว่า ๑ Ports

๕.๑๓ สามารถทำ Link Aggregation ตามมาตรฐาน IEEE๘๐๒.๓ad ได้

๕.๑๔ รองรับการใช้งานแบบ High Available (HA) แบบActive/ Standby และ Active/Active ได้

๕.๑๕ สามารถกำหนดสิทธิในการเข้าถึงเครือข่าย (User Authentication) โดยอ้างอิงฐานข้อมูลจาก Radius หรือ Tacacsได้

๕.๑๖ สามารถจัดการอุปกรณ์ โดยใช้ CLI และ GUI ได้

๕.๑๗ ผลิตภัณฑ์ยี่ห้อที่นำเสนอต้องได้รับการรับรองมาตรฐานความปลอดภัย UL, FCC, CE เป็นอย่างน้อย

๕.๑๘ อุปกรณ์สามารถติดตั้งบน Rack ๑๙” ได้

๕.๑๙ บริษัทผู้นำเสนอจะต้องได้รับการแต่งตั้งอย่างเป็นทางการ จากเจ้าของผลิตภัณฑ์ หรือผู้แทนเจ้าของผลิตภัณฑ์ในประเทศไทย

๕.๒๐ อุปกรณ์ที่นำเสนอต้องไม่ใช่ผลิตภัณฑ์ยี่ห้อเดียวกันกับ Firewall ตัวอื่นๆ ใน GFMIS CGD Network เพื่อเพิ่มความปลอดภัยในการทำงานโดยภาพรวมของเครือข่าย

๕.๒๑ เป็นผลิตภัณฑ์ที่ผู้ผลิตยังมิได้ประกาศภาวะสิ้นสุดการขายหรือสิ้นสุดอายุหรือสิ้นสุดการบริการ (End-of-Sale หรือ End-of-Life หรือ End-of-Service) โดยมีหนังสือรับรองจากเจ้าของผลิตภัณฑ์ หรือผู้แทนเจ้าของผลิตภัณฑ์ในประเทศไทย

๕.๒๒ อุปกรณ์ทั้งหมดต้องเป็นอุปกรณ์ใหม่ไม่เคยผ่านการใช้งานมาก่อน โดยมีหนังสือรับรองจากเจ้าของผลิตภัณฑ์ หรือผู้แทนเจ้าของผลิตภัณฑ์ในประเทศไทย และสามารถใช้งานร่วมกับอุปกรณ์เดิมได้อย่างไม่มีปัญหา

ภาคผนวก ๒
รายละเอียดการติดตั้งและทดสอบ
โครงการทดแทนและเพิ่มประสิทธิภาพระบบรักษาความปลอดภัยเครือข่าย GFMIS

ภาคผนวก ๒
รายละเอียดการติดตั้งและทดสอบ

ผู้ชนะการประกวดราคาจะต้องทำการติดตั้งอุปกรณ์ทั้งหมดของโครงการทดแทนและเพิ่มประสิทธิภาพระบบรักษาความปลอดภัยเครือข่าย GFMIS โดยต้องทำตามข้อกำหนดอย่างน้อยดังนี้

๑. การติดตั้ง

๑.๑. ผู้ชนะการประกวดราคาต้องเสนอแผนการติดตั้งอุปกรณ์ Firewall ทั้งหมดในโครงการที่ศูนย์คอมพิวเตอร์หลัก และศูนย์คอมพิวเตอร์สำรอง หรือสถานที่ตามที่สำนักงานปลัดกระทรวงการคลังหรือคณะกรรมการตรวจรับพัสดุกำหนด

๑.๒. ผู้ชนะการประกวดราคาต้องเสนอบุคคลที่ดำเนินการติดตั้งอุปกรณ์ Firewall ทั้งหมดโดยจะต้องได้รับประกาศนียบัตรในระดับผู้เชี่ยวชาญด้านอุปกรณ์ Firewall จากเจ้าของผลิตภัณฑ์ หรือมีประสบการณ์การติดตั้งอุปกรณ์ Firewall เดียวกับงานที่ดำเนินการจัดซื้ออย่างน้อย ๑ โครงการ จำนวนไม่น้อยกว่า ๑ คน

๑.๓. ผู้ชนะการประกวดราคาต้องจัดทำแผนการติดตั้งอุปกรณ์ Firewall และนำเสนอให้กระทรวงการคลังพิจารณาก่อนดำเนินการติดตั้งภายใน ๓๐ วัน นับถัดจากวันลงนามในสัญญาฯ

๑.๔. ผู้ชนะการประกวดราคาต้องติดตั้งอุปกรณ์ Firewall ตามแผนที่นำเสนอกับกระทรวงการคลัง

๑.๕. ผู้ชนะการประกวดราคาต้องรับผิดชอบเดินสายไฟฟ้า เดินสายสัญญาณที่เชื่อมโยงระหว่างอุปกรณ์ที่ทำการติดตั้งเข้ากับอุปกรณ์เดิมที่มีอยู่ ทั้งในศูนย์คอมพิวเตอร์หลัก ศูนย์คอมพิวเตอร์สำรอง และกระทรวงการคลัง เพื่อให้สามารถใช้งานได้อย่างเพียงพอครบถ้วน

๑.๖. หากการติดตั้งอุปกรณ์ที่จัดซื้อในโครงการนี้มีผลกระทบต่อ Procedure ที่ใช้งานอยู่ปัจจุบัน ผู้ชนะการประกวดต้องเป็นผู้รับผิดชอบดำเนินการจัดทำหรือแก้ไข Procedure ดังกล่าวให้สามารถใช้งานได้ดีดังเดิม

๑.๗. ผู้ชนะการประกวดราคาต้องเป็นผู้รับผิดชอบค่าใช้จ่ายทั้งหมดที่เกิดขึ้นหากมีการติดตั้ง Software, Hardware เพิ่มเติมเพื่อให้ระบบงาน GFMIS สามารถใช้งานได้ดีดังเดิม

๒. การทดสอบ

ผู้ชนะการประกวดราคาต้องออกแบบ และวางแผนการทดสอบอุปกรณ์ทั้งหมด เพื่อให้มั่นใจว่าการติดตั้งเรียบร้อย สามารถทำงานได้สมบูรณ์ และพร้อมตรวจรับเพื่อนำไปใช้งานจริง โดยการทดสอบนั้นจะต้องครอบคลุมหัวข้อการทดสอบดังต่อไปนี้

๒.๑. ทดสอบการเชื่อมต่อวง Network ทุกระบบ ที่เชื่อมต่อกับ Firewall ที่ติดตั้งใหม่

๒.๒. ทดสอบการทำ High Available (HA) ของอุปกรณ์ Firewall แบบ Internal Zone

ภาคผนวก ๓

การฝึกอบรมและเอกสารต่าง ๆ

โครงการทดแทนและเพิ่มประสิทธิภาพระบบรักษาความปลอดภัยเครือข่าย GFMIS

ภาคผนวก ๓

การฝึกอบรมและเอกสารต่าง ๆ

ผู้ชนะการประกวดราคาจะต้องจัดให้มีการฝึกอบรมทั้งภาคทฤษฎีและภาคปฏิบัติให้กับบุคลากรด้านต่าง ๆ ของสำนักงานปลัดกระทรวงการคลัง และ/หรือผู้ที่ได้รับความเห็นชอบจากคณะกรรมการตรวจรับเพื่อรองรับการปฏิบัติงานได้อย่างมีประสิทธิภาพ โดยต้องทำตามข้อกำหนดอย่างน้อยดังนี้

๑. การฝึกอบรม

๑.๑ ผู้ชนะการประกวดราคา จะต้องเสนอแผนการฝึกอบรมให้คณะกรรมการตรวจรับเห็นชอบและดำเนินการฝึกอบรมตามที่ได้รับเห็นชอบ

๑.๒ ผู้ชนะการประกวดราคา ต้องเสนอแผนการฝึกอบรมบุคลากรโดยระบุรายละเอียดอย่างน้อยดังนี้

๑.๒.๑ ประสบการณ์การทำงานของผู้สอน

๑.๒.๒ หลักสูตร (Curriculum) และแผนการสอน (Course Outline)

๑.๒.๓ ระดับผู้เข้ารับการอบรม

๑.๒.๔ จำนวนผู้เข้ารับการอบรม

๑.๒.๕ ระยะเวลาที่ดำเนินการฝึกอบรม

๑.๒.๖ ช่วงเวลาที่จะทำการฝึกอบรม

๑.๒.๗ สถานที่ที่ทำการฝึกอบรม

๑.๓ ผู้สอนจะต้องมีความรู้, ความเชี่ยวชาญและความชำนาญในหลักสูตรฝึกอบรม

๑.๔ ผู้ชนะการประกวดต้องจัดเตรียม Software, Hardware, หนังสือและเอกสารประกอบการฝึกอบรมตามหลักสูตรฝึกอบรมให้เพียงพอกับผู้เข้าฝึกอบรม

๑.๕ ผู้ชนะการประกวดราคา ต้องเป็นผู้ออกค่าใช้จ่ายในการฝึกอบรมทั้งหมด ซึ่งประกอบด้วยหลักสูตรอย่างน้อยดังต่อไปนี้

หัวข้อฝึกอบรม	บุคคลเข้ารับการฝึกอบรม	จำนวนคน (อย่างน้อย)	ระยะเวลา (อย่างน้อย)
หลักสูตรอุปกณ์ Firewall สำหรับ Internal Zone	ผู้ดูแลระบบ	๓	๓ วัน
หลักสูตร อุปกณ์ Firewall สำหรับ BOT และ PKI Zone	ผู้ดูแลระบบ	๓	๒ วัน

๒. เอกสารต่าง ๆ

๒.๑ ผู้ชนะการประกวดราคาต้องจัดทำคู่มือและเอกสาร โดยเนื้อหาและรูปแบบจะต้องได้รับการเห็นชอบจากคณะกรรมการตรวจรับก่อน และส่งมอบในรูปแบบเอกสารจำนวน ๑ ชุด และสำเนาในรูปแบบอิเล็กทรอนิกส์ลงใน Thumb Drive จำนวน ๕ ชุด

๒.๒ ผู้ชนะการประกวดราคาต้องจัดทำรายงานผลการทดสอบ ตามภาคผนวก ๒

๒.๓ ผู้ชนะการประกวดราคาต้องจัดทำเอกสารรายการอุปกรณ์ และสิทธิ์การใช้งาน ที่ส่งมอบพร้อมรายละเอียดโดยสังเขป

๒.๔ ผู้ชนะการประกวดราคาต้องจัดทำวิธีการและแผนการบำรุงรักษา Preventive Maintenance ตลอดระยะเวลารับประกัน

ภาคผนวก ๔
รายละเอียดการบริการบำรุงรักษาและซ่อมแซมแก้ไข
โครงการทดแทนและเพิ่มประสิทธิภาพระบบรักษาความปลอดภัยเครือข่าย GFMIS

ภาคผนวก ๔

รายละเอียดการบริการบำรุงรักษาและซ่อมแซมแก้ไข

ผู้ชนะการประกวดราคา ต้องบริการบำรุงรักษา ซ่อมแซม แก้ไข หรือเปลี่ยนแทนอุปกรณ์ในโครงการนี้ นับตั้งแต่ตรวจรับอุปกรณ์งวดสุดท้ายเสร็จสมบูรณ์ เป็นระยะเวลารับประกัน ๑ ปี โดยต้องปฏิบัติตามเงื่อนไขดังต่อไปนี้

๑. การบริการและการสนับสนุน

ผู้ชนะการประกวดราคาต้องบริการบำรุงรักษา ซ่อมแซม แก้ไข เปลี่ยนแทนอุปกรณ์ในโครงการนี้ พร้อมทั้งสนับสนุนและให้คำปรึกษาแนะนำเกี่ยวกับการใช้งานอุปกรณ์ที่เสนอทั้งหมดภายหลังการติดตั้ง นับตั้งแต่ตรวจรับอุปกรณ์งวดสุดท้ายเสร็จสมบูรณ์ เป็นระยะเวลารับประกัน ๑ ปี

๒. การบำรุงรักษาและซ่อมแซมแก้ไข

ผู้ชนะการประกวดราคา มีหน้าที่บำรุงรักษาและซ่อมแซมแก้ไขอุปกรณ์ในโครงการ ไม่ว่าจะติดตั้ง ณ สถานที่ใด ๆ ตามที่กำหนดในสัญญาให้อยู่ในสภาพใช้งานได้ดีอยู่เสมอตลอดระยะเวลารับประกันด้วยค่าใช้จ่ายของผู้ชนะการประกวดราคา หากอุปกรณ์บกพร่องหรือใช้งานไม่ได้ และความชำรุดนั้นมิได้เกิดจากความผิดของสำนักงานปลัดกระทรวงการคลัง ผู้ชนะการประกวดราคาต้องจัดการซ่อมแซมแก้ไขให้อยู่ในสภาพดีได้ดังเดิม โดยไม่คิดค่าใช้จ่ายใดๆ จากสำนักงานปลัดกระทรวงการคลัง ทั้งนี้ต้องเริ่มจัดการซ่อมแซมแก้ไขหลังจากที่ได้รับแจ้งจากสำนักงานปลัดกระทรวงการคลังหรือผู้ที่ได้รับมอบหมายจากสำนักงานปลัดกระทรวงการคลัง ดังนี้

๒.๑. สำหรับอุปกรณ์ Firewall สำหรับ Internal Zone และอุปกรณ์บริหารจัดการ Firewall Internal Zone

หากบกพร่องหรือใช้งานไม่ได้ ไม่ว่าจะติดตั้งอยู่ ณ สถานที่ใดตามที่กำหนดในสัญญา ความชำรุดนี้มิได้เกิดจากความผิดของสำนักงานปลัดกระทรวงการคลัง ผู้ชนะการประกวดราคาต้องเริ่มจัดการซ่อมแซมแก้ไขให้อยู่ในสภาพดีได้ดังเดิม โดยไม่คิดค่าใช้จ่าย ใดๆ จากสำนักงานปลัดกระทรวงการคลัง ทั้งนี้ต้องเริ่มจัดการซ่อมแซมแก้ไขหลังจากที่ได้รับแจ้งจากสำนักงานปลัดกระทรวงการคลังหรือผู้ที่ได้รับมอบหมายจากสำนักงานปลัดกระทรวงการคลังภายใน ๔ ชั่วโมง หากไม่สามารถเริ่มจัดการซ่อมแซมแก้ไขภายในเวลาดังกล่าว ผู้ชนะการประกวดราคาต้องถูกปรับ ในอัตราชั่วโมงละ ๒,๐๐๐ บาท (สองพันบาทถ้วน) เศษของชั่วโมงนับเป็น ๑ ชั่วโมง

ถ้าการซ่อมแซมแก้ไขไม่แล้วเสร็จภายใน ๑๒ ชั่วโมง นับแต่เริ่มทำการซ่อมแซมแก้ไข ผู้ชนะการประกวดราคา ต้องนำอุปกรณ์ หรือเครื่องสำรองที่มีประสิทธิภาพทัดเทียมกันมาให้ใช้แทนไปจนกว่าจะซ่อมแซมแล้วเสร็จสมบูรณ์ หากไม่สามารถนำอุปกรณ์ หรือเครื่องสำรองมาใช้แทนได้ ผู้ชนะการประกวดราคาต้องถูกปรับ ในอัตราชั่วโมงละ ๑๐,๐๐๐ บาท (หนึ่งหมื่นบาทถ้วน) นับตั้งแต่ชั่วโมงที่ ๑๒ เป็นต้นไป เศษของชั่วโมงนับเป็น ๑ ชั่วโมง

๒.๒. สำหรับอุปกรณ์ Firewall สำหรับ BOT และ PKI Zone

หากบกพร่องหรือใช้งานไม่ได้ ไม่ว่าจะติดตั้งอยู่ ณ สถานที่ใดตามที่กำหนดในสัญญา ความชำรุดนี้มิได้เกิดจากความผิดของสำนักงานปลัดกระทรวงการคลัง ผู้ชนะการประกวดราคาต้องเริ่มจัดการซ่อมแซมแก้ไขให้อยู่ในสภาพดีได้ดังเดิม โดยไม่คิดค่าใช้จ่าย ใดๆ จากสำนักงานปลัดกระทรวงการคลัง ทั้งนี้ต้องเริ่ม

จัดการซ่อมแซมแก้ไขหลังจากที่ได้รับแจ้งจากสำนักงานปลัดกระทรวงการคลังหรือผู้ที่ได้รับมอบหมายจากสำนักงานปลัดกระทรวงการคลังภายใน ๔ ชั่วโมง หากไม่สามารถเริ่มจัดการซ่อมแซมแก้ไขภายในเวลาดังกล่าว ผู้ชนะการประกวดราคาต้องถูกปรับ ในอัตราชั่วโมงละ ๑,๐๐๐ บาท (หนึ่งพันบาทถ้วน) เศษของชั่วโมงนับเป็น ๑ ชั่วโมง

ถ้าการซ่อมแซมแก้ไขไม่แล้วเสร็จภายใน ๑๒ ชั่วโมง นับแต่เริ่มทำการซ่อมแซมแก้ไข ผู้ชนะการประกวดราคา ต้องนำอุปกรณ์ หรือเครื่องสำรองที่มีประสิทธิภาพทัดเทียมกันมาให้ใช้แทนไปจนกว่าจะซ่อมแซมแล้วเสร็จสมบูรณ์ หากไม่สามารถนำอุปกรณ์ หรือเครื่องสำรองมาใช้แทนได้ ผู้ชนะการประกวดราคาต้องถูกปรับ ในอัตราชั่วโมงละ ๕,๐๐๐ บาท (ห้าพันบาทถ้วน) นับตั้งแต่ชั่วโมงที่ ๑๒ เป็นต้นไป เศษของชั่วโมงนับเป็น ๑ ชั่วโมง

๓. การบำรุงรักษาแบบป้องกัน (Preventive Maintenance)

ผู้ชนะการประกวดราคาต้องทำการบำรุงรักษา (Preventive Maintenance) ต้องบำรุงรักษา (Preventive Maintenance) อย่างน้อย ๓ เดือนต่อ ๑ ครั้ง นับจากวันตรวจรับงวดสุดท้ายเสร็จสมบูรณ์ เพื่อให้อุปกรณ์อยู่ในสภาพที่ใช้งานได้อย่างมีประสิทธิภาพตลอดเวลา หากผู้ชนะการประกวดราคาไม่สามารถทำการบำรุงรักษา (Preventive Maintenance) ได้ ผู้ชนะการประกวดราคาต้องถูกปรับในอัตรา ๑๐,๐๐๐ บาท (หนึ่งหมื่นบาทถ้วน) ต่อครั้ง ต่ออุปกรณ์