ขอบเขตของงาน (Terms of Reference : TOR)
โครงการจัดหาอุปกรณ์ระบบรักษาความมั่นคงปลอดภัยสารสนเทศ
และอุปกรณ์เครื่องข่ายเพื่อทดแทนของเดิม ด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding)

๑. หลักการและเหตุผล

สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ (สคร.) มีอุปกรณ์ระบบเครือข่ายสื่อสารและอุปกรณ์ระบบรักษาความมั่นคงปลอดภัยสารสนเทศ ซึ่งติดตั้งใช้งานมาตั้งแต่ปี พ.ศ. ๒๕๕๘ ให้บริการป้องกันและรักษาความมั่นคงปลอดภัยระบบงานสารสนเทศทั้งหมดของ สคร. ซึ่งมีสภาพเก่าเนื่องจากมีการติดตั้งใช้งานมานานเกิดการหยุดให้บริการบ่อยครั้ง ทำให้กระทบกับการทำงานของบุคลากรของ สคร. ทั้งนี้อุปกรณ์บางรายการทางบริษัทเจ้าของผลิตภัณฑ์ได้กำหนดการหยุดรับประกันการบำรุงรักษาและการสนับสนุนด้านอะไหล่ ซึ่งมีความเสี่ยงต่อภัยคุกคามจากการถูกโจมตีทางระบบเครือข่าย เพื่อแก้ไขปัญหาที่อาจจะเกิดขึ้นจากการหยุดทำงานของอุปกรณ์ระบบเครือข่ายสื่อสาร และเป็นการเพิ่มประสิทธิภาพระบบรักษาความมั่นคงปลอดภัยสารสนเทศ สร้างความน่าเชื่อถือในการใช้งาน จึงจำเป็นต้องดำเนินโครงการจัดหาอุปกรณ์ระบบรักษาความมั่นคงปลอดภัยสารสนเทศและอุปกรณ์เครื่องข่ายเพื่อทดแทนของเดิม

๒. วัตถุประสงค์

เพื่อจัดหาอุปกรณ์ระบบรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ และอุปกรณ์เครือข่ายเพื่อทดแทนของเดิมที่มีสภาพเก่าเนื่องจากมีการใช้งานมานาน และสิ้นสุดการรับประกันการบำรุงรักษาอุปกรณ์จากบริษัทเจ้าของผลิตภัณฑ์แล้ว

๓. คุณสมบัติของผู้เสนอราคา

๓.๑ มีความสามารถตามกฎหมาย

๓.๒ ไม่เป็นบุคคลล้มละลาย

๓.๓ ไม่อยู่ระหว่างเลิกกิจการ

๓.๔ ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราวเนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

๓.๕ ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วน ผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

๓.๖ มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

๓.๗ เป็นบุคคลธรรมดาหรือนิติบุคคล ผู้มีอาชีพขายพัสดุที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

๓.๘ ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

๓.๙ ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่ รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

๓.๑๐ ผู้ยื่นข้อเสนอต้องลงทะเบียนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement : e - GP) ของกรมบัญชีกลาง

๓.๑๑ ผู้ยื่นข้อเสนอต้องมีหนังสือรับรองผลิตภัณฑ์จากบริษัทผู้ผลิตหรือบริษัทผู้ผลิต (สาขาประเทศไทย) มาแสดงว่าเป็นผู้ที่ได้รับการแต่งตั้งให้เป็นผู้แทนจำหน่ายซอฟต์แวร์อย่างถูกต้องโดยตรงจากบริษัทผู้ผลิต

/๔. ขอบเขตงาน...

๔. ขอบเขตงาน

จัดหาอุปกรณ์ระบบรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ และอุปกรณ์เครือข่าย ดังนี้

๔.๑ อุปกรณ์ตรวจสอบและป้องกันภัยคุกคามระบบเว็บแอพพลิเคชั่น (Web Application Firewall) จำนวน ๑ ชุด

๔.๒ ระบบบริหารจัดการเก็บข้อมูลจราจรทางคอมพิวเตอร์และวิเคราะห์เหตุการณ์ผิดปกติ (Security Information and Event Management (SIEM)) จำนวน ๑ ระบบ

๔.๓ อุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall) สำหรับเครือข่าย Internet จำนวน ๒ ชุด

๔.๔ อุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall) สำหรับเครือข่าย Extranet จำนวน ๒ ชุด

๔.๕ อุปกรณ์บริหารจัดการ IP Address จำนวน ๑ ชุด

๕. รูปแบบรายการหรือคุณลักษณะเฉพาะ

๕.๑ อุปกรณ์ตรวจสอบและป้องกันภัยคุกคามระบบเว็บแอพพลิเคชั่น (Web Application Firewall) จำนวน ๑ ชุด มีคุณลักษณะเฉพาะอย่างน้อย ดังนี้

๑) เป็นอุปกรณ์ประเภท Hardware Appliance ซึ่งได้รับการออกแบบมาเพื่อทำหน้าที่รักษาความปลอดภัยระบบเครือข่าย Web Application โดยเฉพาะ

๒) ระบบทุกระบบภายในตัวอุปกรณ์ต้องทำงานโดยไม่จำกัดสิขสิทธิ์จำนวนผู้ใช้ (Unlimited User Licenses)

๓) มี Network Interface แบบ ๑๐/๑๐๐/๑๐๐๐ Ethernet (RJ-๔๕) อย่างน้อย ๔ ports โดยสามารถ Bypass Port อย่างน้อย ๒ ports และแบบ Gigabit Fiber (SFP) ที่รองรับการติดตั้ง SFP Transceivers ไม่น้อยกว่า ๔ ports

๔) มีความเร็วในการส่งผ่านข้อมูล (WAF Throughput) ไม่น้อยกว่า ๑.๓ Gbps

๕) สามารถทำงานได้ในรูปแบบ In-Line (Bridge), Transparent, True Transparent Proxy, Reverse Proxy, Offline Sniffing และ WCCP ได้

๖) สามารถทำ Server Health Check หรือ Health Monitors เพื่อตรวจสอบการตอบสนองของเครื่องคอมพิวเตอร์แม่ข่าย

๗) สามารถทำ SSL negotiations และ Encryption แทน Server ตัวจริง (SSL Offload)

๘) สามารถตรวจสอบ Traffic ที่มีการเข้ารหัสได้ (HTTPS inspection)

๙) สามารถทำ Policy ในรูปแบบ Single Server, Server Load Balance หรือ Content Routing หรือ Local Traffic Policies ได้

๑๐) สามารถทำการตรวจสอบและป้องกัน IP Black List และ Botnet กับฐานข้อมูลข้างนอกได้ (IP Reputation service)

๑๑) สามารถกำหนดเงื่อนไขการตรวจสอบ Brute Force Login attack พร้อมกับระบบต้องทำการ Block ได้เมื่อถึง Threshold ที่กำหนด

๑๒) สามารถทำการตรวจสอบ และป้องการเชื่อมต่อจาก BOT โดยใช้ Signature และ CAPTCHA ได้เป็นอย่างน้อย และมีคุณสมบัติสามารถกำหนด policy ตาม Geolocation ของต้นทางได้

/๑๓) มีความสามารถ...

๑๓) มีความสามารถในการป้องกันภัยคุกคามในรูปแบบต่างๆ ดังต่อไปนี้ได้

๑๓.๑) Cross site scripting

๑๓.๒) SQL injection

๑๓.๓) Session Hijacking

๑๓.๔) Cookie Tampering

๑๓.๕) Cookie Poisoning

๑๓.๖) Cross site Request Forgery

๑๓.๗) Command Injection

๑๓.๘) Remote File Inclusion

๑๓.๙) Forms Tampering หรือ Parameter Tampering

๑๓.๑๐) Search engine Hacking หรือ Web Scraping

๑๓.๑๑) Directory Traversal หรือ Path Traversal

๑๓.๑๒) Hidden Field Manipulation

๑๓.๑๓) Behavioral Dos หรือ Layer ๗ Dos

๑๔) สามารถป้องกันการโจมตีที่ถูกระบุไว้ใน OWASP Top ๑๐ ของปีล่าสุดได้

๑๕) สามารถตรวจจับ (scan) และป้องกัน Malware หรือ Malicious จากการ Upload file ได้

๑๖) มีคุณสมบัติ Cloud-based Sandbox เพื่อตรวจจับ Unknown Malware ได้

๑๗) มีความสามารถในการทำ Authentication Offload เพื่อช่วยลดภาระการทำงานของเครื่องคอมพิวเตอร์แม่ข่าย โดยสามารถทำงานร่วมกับฐานข้อมูล ภายในอุปกรณ์ LDAP และ Radius ได้

๑๘) สามารถป้องกันและตรวจสอบการถูกเปลี่ยนข้อมูลบน Website ได้ (Anti Web Defacement)

๑๙) สามารถตรวจสอบหาช่องโหว่ที่มีความเสี่ยงต่อการถูกโจมตีได้ (Web Application Vulnerability Assessments)

๒๐) รองรับการทำงานในรูปแบบของ High-Availability แบบ Active/Passive และ Active/Active Clustering ได้

๒๑) สามารถเก็บ Log ไว้ในตัวอุปกรณ์เอง และส่งออกไปยัง Syslog ได้

๒๒) สามารถทำ Report ในรูปแบบ PDF หรือ HTML หรือ MS Word ได้

๒๓) สามารถส่ง Alert ผ่าน E-mail ได้

๒๔) สามารถสร้าง Admin Profile เพื่อกำหนดสิทธิสำหรับผู้ดูแลระบบในการเข้าถึงที่มีสิทธิไม่เท่ากันได้

๒๕) สามารถบริหารจัดการผ่านทาง Console Port, HTTP, HTTPS และ SSH ได้

๒๖) สามารถทำ Data Guard หรือ Data Masking หรือ DLP เพื่อป้องกันข้อมูลรั่วไหลได้

๒๗) อุปกรณ์ที่เสนอต้องมีเครื่องหมายการค้า ที่ได้รับการยอมรับในระดับ Leader หรือ Challenger จาก Gartner Magic Quadrant ด้าน Web Application Firewall ในปี ค.ศ. ๒๐๑๙ หรือ ๒๐๒๐

/๕.๒ ระบบ...

๕.๒ ระบบบริหารจัดการเก็บข้อมูลจราจรทางคอมพิวเตอร์และวิเคราะห์เหตุการณ์ผิดปกติ (Security Information and Event Management (SIEM)) จำนวน ๑ ระบบ มีคุณลักษณะเฉพาะอย่างน้อย ดังนี้

๑) เป็นอุปกรณ์ประเภท Hardware Appliance ออกแบบมาสำหรับวิเคราะห์เหตุการณ์ภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศ (Security Information and Event Management) โดยเฉพาะ

๒) ระบบที่เสนอมีการทำงานแบบ Scalable Architecture

๓) ระบบที่เสนอสามารถเสนอซอฟต์แวร์ตรวจสอบและแจ้งเตือนประกอบร่วมได้ เพื่อให้ระบบมีคุณสมบัติครบถ้วน

๔) สามารถทำงานแบบ Cluster โดยรับและวิเคราะห์ข้อมูลได้ไม่น้อยกว่า ๑,๕๐๐ เหตุการณ์ต่อวินาที (Events per Second)

๕) สามารถรองรับเหตุการณ์จากอุปกรณ์ได้อย่างน้อย ๑๐๐ อุปกรณ์

๖) สามารถเชื่อมโยงเหตุการณ์จาก Source ต่าง ๆ เข้าด้วยกัน (Correlation) ทั้งแบบ Real-time เพื่อหาต้นตอของภัยคุกคาม โดยมี Predefined Rule มาพร้อมกับระบบไม่น้อยกว่า ๕๐ Rules และสามารถ Customize เพิ่มเติมได้

๗) มี Predefined Dashboard มาพร้อมกับระบบ เพื่อใช้สำหรับวิเคราะห์ข้อมูลเหตุการณ์แบบ Real-time ในรูปแบบของแผนภูมิ (Chart) และตาราง (Table) และสามารถ Customize เพิ่มเติมได้

๘) สามารถแบ่งแยกกลุ่มของปูมเหตุการณ์ (Event Log) ตามแผนก สาขา ในการใช้งานระบบใหญ่ๆ ที่มีความซับซ้อน หรือสามารถแบ่งแยกปูมเหตุการณ์ (Event Log) ตามรายชื่อลูกค้าในกรณีที่ใช้งานในลักษณะของ MSSP (Management Security Service Provider) หรือ MSP (Managed Service Provider) เพื่อความสะดวกในการตรวจสอบข้อมูล

๙) รองรับการบริหารจัดการรายละเอียดของอุปกรณ์หรือระบบต้นทางของ Log (Asset Management) เช่น ประเภทของอุปกรณ์ และสถานที่ตั้ง เป็นต้น

๑๐) สามารถแสดงผลการวิเคราะห์ข้อมูลได้ทั้งแบบ NOC (Network Operation Center) และ SOC (Security Operation Center)

๑๑) สามารถบันทึกข้อมูล หรือเหตุการณ์ได้ในตัวอุปกรณ์เองโดยมีความจุไม่น้อยกว่า ๒๐ TB

๑๒) สามารถวิเคราะห์เปรียบเทียบข้อมูลระหว่างไอพีแอดเดรส กับรายชื่อผู้ใช้งานที่ใช้งานไอพีแอดเดรสนั้นๆ อยู่ (Identity Mapping)

๑๓) มีระบบบริหารจัดการเหตุการณ์ (Incident Management) ในตัว (Built-in Ticketing System) โดยต้องไม่อาศัย Third Party อื่น ๆ

๑๔) มี Predefined Report มาพร้อมกับระบบไม่น้อยกว่า ๕๐ รูปแบบ และสามารถ Customize เพิ่มเติมได้ไม่น้อยกว่า ๑๐ รายงาน และรองรับการทำรายงานที่เกี่ยวข้องกับมาตรฐาน PCI, SOX, ISO/IEC ๒๗๐๐๑, FISMA HIPAA ได้เป็นอย่างน้อย

๑๕) สามารถแจ้งเตือนแบบ Real-time เมื่อมีเหตุการณ์ตรงตามเงื่อนไขที่สร้างไว้ และเหตุการณ์ผิดปกติของตัวอุปกรณ์ผ่าน Email ได้เป็นอย่างน้อย

๑๖) สามารถบริหารจัดการผ่าน Web Interface ที่มีการเข้ารหัสได้ (HTTPS)

/๑๗) สามารถ...

๑๗) สามารถเข้ารหัสข้อมูลเพื่อใช้ยืนยันความถูกต้องของข้อมูลที่จัดเก็บตามมาตรฐาน SHA-๒๕๖ หรือดีกว่า

๑๘) สามารถกำหนดระยะเวลาการเก็บข้อมูล (Retention Policy) ของแต่ละอุปกรณ์ต้นทาง โดยมีระยะเวลาที่แตกต่างกันได้

๑๙) รองรับคุณสมบัติ UBA หรือ UEBA เพื่อช่วยในการตรวจสอบพฤติกรรมของผู้ใช้ในระบบ

๕.๓ อุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall) สำหรับเครือข่าย Internet จำนวน ๒ ชุด โดยแต่ละชุดต้องมีคุณลักษณะเฉพาะอย่างน้อย ดังนี้

๑) เป็นอุปกรณ์ Firewall ชนิด Next Generation Firewall แบบ Appliance

๒) อุปกรณ์จะต้องมี Interface สำหรับเชื่อมต่อระบบเครือข่ายแบบ Gigabit Ethernet (RJ-๔๕) ไม่น้อยกว่า ๘ ports, และแบบ Gigabit Fiber (SFP) ที่รองรับการติดตั้ง SFP Transceivers ไม่น้อยกว่า ๘ ports และ แบบ ๑๐-Gigabit Fiber (SFP+) ที่รองรับการติดตั้ง SFP+ Transceivers ไม่น้อยกว่า ๒ ports

๓) สามารถกำหนดนโยบายการใช้งาน (Interface Rule หรือ Topology Setting) สำหรับ Network Interface เป็น LAN, WAN หรือ DMZ ได้

๔) สามารถกำหนด Interface Zone ที่ผู้ดูแลระบบกำหนดขึ้นมาเองได้โดยอิสระ หรือสามารถกำหนด Interface ให้ทำงานเป็น Port สำหรับ HA ได้ โดยอุปกรณ์ที่เสนอต้องทำงานร่วมกันแบบ High Availability (HA) โดยไม่ต้องเสียค่าใช้จ่ายเพิ่ม

๕) มี Firewall Throughput ไม่น้อยกว่า ๓๕ Gbps

๖) สามารถรับการเชื่อมต่อพร้อมกัน (Concurrent Sessions) TCP ได้ไม่น้อยกว่า ๗,๘๐๐,๐๐๐ Sessions และรองรับ New Session per Second ได้ไม่น้อยกว่า ๔๐๐,๐๐๐ session per second

๗) สามารถตรวจสอบและป้องกันการโจมตีเครือข่ายประเภท IPS Throughput ได้ไม่น้อยกว่า ๙ Gbps และรองรับ Threat Prevention Throughput ไม่น้อยกว่า ๗ Gbps เมื่อเปิดใช้งาน Firewall, Application control, IPS และ AntiMalware พร้อมกัน

๘) สามารถทำการเชื่อมโยง IPsec VPN ซึ่งมีความเร็วในการทำงานไม่น้อยกว่า ๑๘ Gbps

๙) สามารถทำการเชื่อมโยง SSL VPN จากเครื่อง Client ไม่น้อยกว่า ๕๐๐ Users

๑๐) สามารถบริหารการจัดการอุปกรณ์ผ่าน Console และ Web Browser เช่น Firefox หรือ Google Chrome ได้

๑๑) สามารถตรวจจับและป้องกัน Virus ที่ผ่านมากับโปรโตคอล HTTP, IMAP, SMTP, POP๓, MAPI และ FTP ได้

๑๒) สามารถป้องกัน Spam Email ด้วยวิธี IP address check, URL check และ Email checksum ได้

๑๓) มีระบบป้องกัน Web Application (Web Application Firewall)

๑๔) สามารถตรวจสอบและป้องกันการบุกรุกรูปแบบต่างๆ อย่างน้อย ดังนี้ Syn Flood, UDP Flood, ICMP Flood, IP Address Spoofing, Port Scan, DoS or DDoS, Teardrop Attack, Land Attack, IP Fragment, ICMP Fragment เป็นต้นได้

/๑๕) สามารถ...

๑๕) สามารถใช้งานตามมาตรฐาน IPv๖ ได้

๑๖) รองรับการตรวจสอบผู้ใช้งาน (User Authenticator) กับ ฐานข้อมูลผู้ใช้งานภายในอุปกรณ์ (Local User), Active Directory (AD) และ Radius รวมถึงสามารถทำงานแบบ Single Sign-On กับฐานข้อมูลผู้ใช้งานบน Active Directory (AD) และ Radius ได้

๑๗) สามารถทำงานแบบ Two Factor Authentication ได้โดยไม่ต้องติดตั้ง Token Server

๑๘) สามารถแบ่งระดับของผู้ดูแลระบบได้หลายระดับเพื่อความปลอดภัยของการจัดการอุปกรณ์ได้ Administrator Profile

๑๙) สามารถ Routing แบบ Static, Dynamic Routing ได้

๒๐) สามารถส่ง Log แบบ Syslog ตามมาตรฐาน RFC-๓๑๙๕ หรือ RFC-๕๔๒๔ และ CEF ไปยัง Server ภายนอกได้มากกว่า ๑ Server

๒๑) สามารถกำหนดช่วงเวลา Update Signature ใหม่ ได้อย่างน้อยทุกๆ ๑ ชั่วโมง

๒๒) สามารถทำงานลักษณะ Virtual Domains หรือ Virtual Systems ได้อย่างน้อย ๑๐ Virtual Domains หรือ Virtual Systems

๒๓) มี Power Supply แบบ Redundant หรือ Hot Swap จำนวน ๒ หน่วย

๒๔) อุปกรณ์ที่เสนอต้องมีเครื่องหมายการค้า ที่ได้รับการยอมรับในระดับ Leader จาก Gartner Magic Quadrant ด้าน Networks Firewall ในปี ค.ศ. ๒๐๑๙ หรือ ๒๐๒๐

๕.๔ อุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall) สำหรับเครือข่าย Extranet จำนวน ๒ ชุด โดยแต่ละชุดต้องมีคุณลักษณะเฉพาะอย่างน้อย ดังนี้

๑) เป็นอุปกรณ์ Firewall ชนิด Next Generation Firewall แบบ Appliance

๒) มี Firewall Throughput ไม่น้อยกว่า ๒ Gbps

๓) มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ ๑๐/๑๐๐/๑๐๐๐ Base-T หรือดีกว่า จำนวนไม่น้อยกว่า ๕ ports

๔) มีระบบตรวจสอบและป้องกันการบุกรุกรูปแบบต่างๆ อย่างน้อย ดังนี้ Syn Flood, UDP Flood, ICMP Flood, IP Address Spoofing, Port Scan, DoS or DDoS, Teardrop Attack, Land Attack, IP Fragment, ICMP Fragment เป็นต้นได้

๕) สามารถทำการกำหนด IP Address และ Service Port แบบ Network Address Translation (NAT) และ Port Address Translation (PAT) ได้

๖) สามารถ Routing แบบ Static, Dynamic Routing ได้

๗) สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS หรือ SSH ได้เป็นอย่างน้อย

๘) สามารถเก็บและส่งรายละเอียดและตรวจสอบการใช้งาน (Logging/Monitoring) ในรูปแบบ Syslog ได้

๙) สามารถใช้งานตามมาตรฐาน IPv๖ ได้

๑๐) อุปกรณ์ที่เสนอต้องทำงานร่วมกันแบบ High Availability (HA) โดยไม่ต้องเสียค่าใช้จ่ายเพิ่ม

/๕.๕ อุปกรณ์...

๕.๕ อุปกรณ์บริหารจัดการ IP Address จำนวน ๑ ชุด มีคุณลักษณะเฉพาะอย่างน้อย ดังนี้

๑) เป็นอุปกรณ์แบบ Appliance ทำหน้าที่เป็น DNS, DHCP และ IPAM (IP Address Management) โดยเฉพาะ

๒) มี Network Interface แบบ ๑๐/๑๐๐/๑๐๐๐ Mbps ไม่น้อยกว่า ๔ ports

๓) สามารถรับจำนวน DNS Query ไม่น้อยกว่า ๒๕,๐๐๐ DNS Query (qps) ต่อวินาที

๔) สามารถรับจำนวน DHCP Request ไม่น้อยกว่า ๕๐๐ DHCP Request (lps) ต่อวินาที

๕) สามารถใช้งานตามมาตรฐาน IPv๔ และ IPv๖ สำหรับ DNS และ DHCP Service

๖) รองรับการทำ DNSSEC เพื่อความปลอดภัยของระบบ DNS

๗) สามารถ Customized Templates ในการ Monitoring ระบบ DNS และ DHCP ได้

๘) สามารถออกรายงาน (Reporting) และแสดงสถิติ (Statistics) การทำงานของระบบและ DNS ได้ เช่น DNS Traffic, SQL queries, CPU usage, Memory usage ในรูปแบบ PDF ได้เป็นอย่างน้อย

๙) มีระบบ IP Address Management (IPAM) และสามารถตรวจสอบสถานะของ IP Address ที่มีการแจกให้ใช้งานในเครือข่ายได้

๑๐) สามารถทำ Ethernet Port Failover สำหรับ Port Management โดยเฉพาะ

๑๑) รองรับกำหนดนโยบายเพื่อควบคุมการใช้งาน (Access Control) DNS ได้

๑๒) สามารถแจ้งเตือน (Alert) ผ่านทาง E-mail เช่น แจ้งเตือนเมื่อมีการแจกหมายเลข IP Address เกินกว่า ๘๐% ใน DHCP Pool เป็นต้น

๑๓) มี Smart Architecture ที่สามารถบริหารจัดการค่า configuration ของ DNS เช่น Master/Slave, Multi- Master, Stealth และ Single server ได้เป็นอย่างน้อย

๑๔) มี Smart Architecture ที่สามารถบริหารจัดการค่า configuration ของ DHCP เช่น One-to-One, One-to-Many, Split-Scope และ Single-Sever ได้เป็นอย่างน้อย

๑๕) รองรับการทำ High Availability Management โดยสามารถ Replicate ข้อมูล Database จากอุปกรณ์หลัก (master) ไปยังอุปกรณ์ชุดสำรอง (hot standby) ให้โดยอัตโนมัติ

๑๖) สามารถกำหนดระดับสิทธิ์ในการบริหารจัดการอุปกรณ์ DNS, DHCP และ IPAM (IP Address Management) โดยแบ่งออกเป็น Group และ User พร้อมทั้งสามารถกำหนดสิทธิ์ตาม modules, pages และ objects ได้

๑๗) สามารถบริหารจัดการอุปกรณ์ผ่านทาง Secured Web Management

๑๘) รองรับการส่งข้อมูล log ผ่านทาง Syslog protocol ได้

๑๙) สามารถติดตั้งในตู้ Rack มาตรฐาน ๑๙ นิ้ว

๖. เงื่อนไขทั่วไป

๖.๑ คุณลักษณะเฉพาะของอุปกรณ์และระบบทุกรายการ ผู้ขายต้องเสนอคุณลักษณะเฉพาะไม่ต่ำกว่าคุณลักษณะเฉพาะที่ สคร. กำหนด

๖.๒ ราคาของระบบคอมพิวเตอร์ที่เสนอให้รวมค่าซอฟต์แวร์ ค่าติดตั้ง และค่าใช้จ่ายอื่นๆ ทั้งหมดแล้ว สคร. ไม่ต้องเสียค่าใช้จ่ายใดๆ เพิ่มเติม

/๗. เงื่อนไข...

๗. เงื่อนไขการฝึกอบรม

๗.๑ ผู้ขายต้องเสนอแผนการจัดฝึกอบรมอุปกรณ์และระบบของโครงการ โดยต้องส่งแผนการฝึกอบรมให้กับคณะกรรมการตรวจรับพัสดุของ สคร. พิจารณาภายใน ๓๐ วัน นับถัดจากวันลงนามในสัญญา

๗.๒ ผู้ขายต้องดำเนินการจัดการฝึกอบรมการใช้งานอุปกรณ์และระบบในข้อ ๕ โดยผู้ขายเป็นผู้รับผิดชอบค่าใช้จ่ายทั้งหมดที่เกิดขึ้นในการจัดฝึกอบรมในข้อ ๗.๑

๘. เงื่อนไขในการติดตั้ง ส่งมอบงาน และตรวจรับพัสดุ

ผู้ขายต้องส่งมอบอุปกรณ์และระบบทั้งหมด รวมถึงอุปกรณ์อื่นๆ ที่เกี่ยวข้อง หรือเอกสารอื่นใดที่เกี่ยวข้องให้ สคร. ภายใน ๑๒๐ วัน นับถัดจากวันลงนามในสัญญา โดยแบ่งเป็น ๓ งวดงาน ดังนี้

งวดที่ ๑: ภายใน ๓๐ วัน นับถัดจากวันลงนามในสัญญาให้ส่งมอบงาน ดังนี้

๑) แผนการดำเนินงานโครงการ

๒) แผนการจัดฝึกอบรมของโครงการ

งวดที่ ๒: ภายใน ๙๐ วัน นับถัดจากวันลงนามในสัญญาให้ส่งมอบงาน ดังนี้

๑) ส่งมอบอุปกรณ์และระบบทุกรายการ

งวดที่ ๓: ภายใน ๑๒๐ วัน นับถัดจากวันลงนามในสัญญาหลังจากดำเนินการดังนี้

๑) ติดตั้ง และกำหนดค่าการทำงานของอุปกรณ์และระบบในข้อ ๕ ทั้งหมด ให้เชื่อมต่อกับเครือข่ายสื่อสารคอมพิวเตอร์ของ สคร. ได้ และจัดหาช่างหรือผู้เชี่ยวชาญ อย่างน้อย ๑ คน เพื่อ Standby ในการรับแจ้งและแก้ไขปัญหาที่อาจจะเกิดขึ้นหลังจากการติดตั้งอุปกรณ์แล้วอย่างน้อย ๓ วันทำการ

๒) จัดฝึกอบรมการใช้งานอุปกรณ์และระบบในข้อ ๕ ในระดับผู้ดูแลระบบ พร้อมจัดทำเอกสารฝึกอบรมให้กับเจ้าหน้าที่ สคร. จำนวนไม่น้อยกว่า ๕ คน

๓) จัดทำคู่มือการใช้งานอุปกรณ์และระบบในข้อ ๕ จำนวน ๕ ชุด พร้อมทั้งบันทึกไฟล์คู่มือการใช้งานดังกล่าวลงใน Flash Drive หรือดีกว่า จำนวน ๓ ชุด ส่งมอบให้ สคร.

อนึ่ง ในระหว่างที่การติดตั้งส่งมอบและตรวจรับยังไม่สมบูรณ์ สคร. มีสิทธิที่จะใช้อุปกรณ์และระบบในส่วนที่ส่งมอบแล้วได้ก่อน และหากมีเหตุให้ต้องเลิกสัญญาอันเนื่องจากความผิดของผู้ขายเอง ผู้ขายไม่มีสิทธิที่จะเรียกร้องค่าเสียหายใดๆ อันเกิดจากการใช้ระบบงานในระหว่างที่การติดตั้งส่งมอบ และตรวจรับยังไม่สมบูรณ์

๙. ระยะเวลาดำเนินงาน

ระยะเวลาดำเนินการ ๑๒๐ วัน นับถัดจากวันลงนามในสัญญา

๑๐. งบประมาณ

งบประมาณจำนวน ๑๐,๐๐๐,๐๐๐ บาท (สิบล้านบาทถ้วน) รวมภาษีมูลค่าเพิ่ม

๑๑. เงื่อนไขการชำระเงิน

สคร. จะชำระเงินเมื่อผู้ขายได้ส่งมอบงานตามงวดงานที่กำหนด ถูกต้อง ครบถ้วน และได้รับความเห็นชอบจากคณะกรรมการตรวจรับพัสดุ และ สคร. ได้พิจารณาให้ความเห็นชอบการตรวจรับงานของคณะกรรมการตรวจรับพัสดุแล้ว โดยการชำระเงินแบ่งออกเป็นงวดๆ ดังนี้

งวดเงินที่ ๑: ชำระเงินจำนวนร้อยละ ๑๐ ของจำนวนเงินตามสัญญา เมื่อคณะกรรมการตรวจพัสดุได้พิจารณาตรวจรับงาน งวดที่ ๑ เสร็จสิ้น และ สคร. ได้พิจารณาให้ความเห็นชอบการตรวจรับงานของคณะกรรมการตรวจรับพัสดุแล้ว

/งวดเงินที่ ๒...

งวดเงินที่ ๒: ชำระเงินจำนวนร้อยละ ๔๐ ของจำนวนเงินตามสัญญา เมื่อคณะกรรมการตรวจรับพัสดุได้พิจารณาตรวจรับงาน งวดที่ ๒ เสร็จสิ้น และ สคร. ได้พิจารณาให้ความเห็นชอบการตรวจรับงานของคณะกรรมการตรวจรับพัสดุแล้ว

งวดเงินที่ ๓: ชำระเงินจำนวนร้อยละ ๕๐ ของจำนวนเงินตามสัญญา เมื่อคณะกรรมการตรวจรับพัสดุได้พิจารณาตรวจรับงาน งวดที่ ๓ เสร็จสิ้น และ สคร. ได้พิจารณาให้ความเห็นชอบการตรวจรับงานของคณะกรรมการตรวจรับพัสดุแล้ว

๑๒. การชำระค่าปรับ

๑๒.๑ ผู้ขายต้องดำเนินการส่งมอบงานทั้งสิ้นให้แล้วเสร็จภายใน ๑๒๐ วัน นับถัดจากวันลงนามในสัญญา มิฉะนั้น ผู้ขายต้องชำระค่าปรับเป็นรายวันให้ สคร. ในอัตราร้อยละ ๐.๒๐ ของราคาในสัญญาซื้อจนกว่างานจะแล้วเสร็จ

๑๒.๒ กรณีที่ สคร. เห็นว่าผู้ขายไม่อาจปฏิบัติตามสัญญาต่อไปได้หรือทำงานล่วงเลยกำหนดเวลาแล้วเสร็จเกินกว่ากึ่งหนึ่งของระยะเวลาในสัญญา สคร. สงวนสิทธิในการเลิกสัญญาเสียเมื่อใดก็ได้ โดยผู้ขายต้องชดใช้ค่าเสียหายอันเกิดขึ้นจากการดำเนินงานไม่แล้วเสร็จตามสัญญาและจะเรียกร้องใดๆ ต่อ สคร. ไม่ได้ทั้งสิ้น

๑๓. เงื่อนไขการรับประกัน

ผู้ขายต้องรับประกันความชำรุดบกพร่องของสิ่งของที่ส่งมอบทั้งหมด เป็นเวลาไม่น้อยกว่า ๑ ปี นับตั้งแต่คณะกรรมการตรวจรับพัสดุ และ สคร. พิจารณาให้ความเห็นชอบและอนุมัติให้รับงาน โดยผู้ขายต้องซ่อมแซมแก้ไขให้ใช้การได้ดีดังเดิมภายใน ๘ ชั่วโมง นับตั้งแต่ที่ได้รับแจ้งความชำรุดบกพร่อง หากเกิน ๘ ชั่วโมง ผู้ขายต้องจัดหาอุปกรณ์มาทดแทนชั่วคราวจนกว่าจะซ่อมแซมแก้ไขเสร็จ และหากไม่สามารถซ่อมแซมแก้ไขอุปกรณ์ดังกล่าวได้ภายใน ๓๐ วัน นับตั้งแต่วันที่ได้รับแจ้งความชำรุดบกพร่อง ผู้ขายต้องนำอุปกรณ์ที่มีความสามารถและคุณลักษณะเฉพาะไม่ต่ำกว่าอุปกรณ์เดิมมาเปลี่ยนทดแทนและกำหนดค่าการทำงาน (Configuration) อุปกรณ์ดังกล่าว ให้สามารถใช้งานร่วมกับระบบเครือข่ายคอมพิวเตอร์ของ สคร. ได้ดีดังเดิม

๑๔. ลิขสิทธิ์ Software

ในกรณีที่บุคคลภายนอกกล่าวอ้างหรือใช้สิทธิเรียกร้องใดๆ ว่ามีการละเมิดลิขสิทธิ์ หรือสิทธิบัตรเกี่ยวกับอุปกรณ์คอมพิวเตอร์ และหรือซอฟต์แวร์ที่เสนอ ผู้ขายต้องดำเนินการทั้งปวง เพื่อให้การกล่าวอ้างหรือการเรียกร้องดังกล่าวระงับสิ้นไปโดยเร็ว ผู้ขายต้องเป็นผู้ชำระค่าเสียหายและค่าใช้จ่ายต่างๆ ที่เกิดขึ้นทั้งหมด

๑๕. หลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอ

พิจารณาโดยใช้เกณฑ์ราคาประกอบกับเกณฑ์อื่น โดยกำหนดเกณฑ์และน้ำหนักการให้คะแนน ดังนี้

/หลักเกณฑ์...

หลักเกณฑ์	น้ำหนัก	การให้คะแนน
๑. ราคา	ร้อยละ ๘๕	- เสนอราคาต่ำสุด (รวมภาษีมูลค่าเพิ่มแล้ว) ได้ ๑๐๐ คะแนน สำหรับผู้เสนอราคาในลำดับรองลงมา ให้ได้คะแนนลดหลั่นตามสัดส่วนข้อเสนอด้านราคาที่แตกต่างกัน
๒. เกณฑ์อื่น	ร้อยละ ๑๕	

เกณฑ์อื่น ประกอบด้วย ๑) ข้อเสนอด้านเทคนิค ร้อยละ ๑๐
๒) บริการหลังการขาย ร้อยละ ๕

๑) ข้อเสนอด้านเทคนิค (ระบบบริหารจัดการเก็บข้อมูลจราจรทางคอมพิวเตอร์และวิเคราะห์เหตุการณ์ผิดปกติ (Security Information and Event Management (SIEM))) ร้อยละ ๑๐ ประกอบด้วย

๑.๑) สามารถทำงานแบบ Cluster ร้อยละ ๕

หลักเกณฑ์	น้ำหนัก	การให้คะแนน
สามารถทำงานแบบ Cluster โดยรับและวิเคราะห์ข้อมูลได้ ๑,๕๐๐ เหตุการณ์ต่อวินาที (Events per Second)	ร้อยละ ๕	๒๐ คะแนน
สามารถทำงานแบบ Cluster โดยรับและวิเคราะห์ข้อมูลได้ ๒,๐๐๐ เหตุการณ์ต่อวินาที (Events per Second) และรองรับการขยายได้มากกว่า ๕,๐๐๐ เหตุการณ์ต่อวินาที (Events per Second) ได้ในอนาคต โดยไม่ต้องเปลี่ยนอุปกรณ์		๖๐ คะแนน
สามารถทำงานแบบ Cluster โดยรับและวิเคราะห์ข้อมูลได้ ๒,๕๐๐ เหตุการณ์ต่อวินาที (Events per Second) และรองรับการขยายได้มากกว่า ๑๒,๐๐๐ เหตุการณ์ต่อวินาที (Events per Second) ได้ในอนาคต โดยไม่ต้องเปลี่ยนอุปกรณ์		๑๐๐ คะแนน

สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ

๑.๒) ความสามารถในการบันทึกข้อมูล หรือเหตุการณ์ ร้อยละ ๕

หลักเกณฑ์	น้ำหนัก	การให้คะแนน
สามารถบันทึกข้อมูล หรือเหตุการณ์ได้ในตัวอุปกรณ์เอง โดยมีความจุหลังทำ RAID (usable storage) ๒๐ TB บนอุปกรณ์เดียว	ร้อยละ ๕	๒๐ คะแนน
สามารถบันทึกข้อมูล หรือเหตุการณ์ได้ในตัวอุปกรณ์เอง โดยมีความจุหลังทำ RAID (usable storage) ๒๓ TB บนอุปกรณ์เดียว		๖๐ คะแนน
สามารถบันทึกข้อมูล หรือเหตุการณ์ได้ในตัวอุปกรณ์เอง โดยมีความจุหลังทำ RAID (usable storage) มากกว่า ๒๓ TB บนอุปกรณ์เดียว		๑๐๐ คะแนน

๒) บริการหลังการขาย ผู้ขายต้องดำเนินการบำรุงรักษาพัสดุที่ส่งมอบทั้งหมด ตามระยะเวลาที่ผู้ขายเสนอ พร้อมทั้งรับฟัง รวบรวม และแก้ไขปัญหาต่างๆ (ถ้ามี) ร้อยละ ๕

หลักเกณฑ์	น้ำหนัก	การให้คะแนน
เสนอการบำรุงรักษาไม่น้อยกว่า ๓ ครั้ง/ปี (ทุก ๔ เดือน)	ร้อยละ ๕	๒๐ คะแนน
เสนอการบำรุงรักษาไม่น้อยกว่า ๔ ครั้ง/ปี (ทุก ๓ เดือน)		๖๐ คะแนน
เสนอการบำรุงรักษาไม่น้อยกว่า ๖ ครั้ง/ปี (ทุก ๒ เดือน)		๑๐๐ คะแนน