แบบ บก.06

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและราคากลาง (ราคาอ้างอิง)
ในการจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง

1. ชื่อโครงการ โครงการจัดซื้ออุปกรณ์รักษาความปลอดภัยของระบบเครือข่ายไฟล์วอล (Next Generation Firewall)
2. หน่วยงานเจ้าของโครงการ ฝ่ายเทคโนโลยีสารสนเทศ การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย
3. วงเงินงบประมาณที่ได้รับจัดสรร 12,000,000.00 บาท (สิบสองล้านบาทถ้วน) รวมภาษีมูลค่าเพิ่ม
4. วันที่กำหนดราคากลาง 20 กันยายน 2562
   รวมเป็นเงินทั้งสิ้น 11,959,000.00 บาท (สิบเอ็ดล้านเก้าแสนห้าหมื่นเก้าพันบาทถ้วน) รวมภาษีมูลค่าเพิ่ม
5. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)
   5.1 สืบราคาจากบริษัท เดอะ แพรคทิเคิล โซลูชั่น จำกัด (มหาชน)
   5.2 สืบราคาจากบริษัท เน็ตวัน เน็ตเวิร์ค โซลูชั่น จำกัด
   5.3 สืบราคาจากบริษัท ซูเพิร์บ คอมพ์ จำกัด
6. รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง) ทุกคน
   6.1 นายอานันท์ หวังกุหลำ ผอ.กปค. ฝทท.
   6.2 นางสาวเนตินันทน์ ศาสนนันทน์ นิติกร 7 รก.หน.สญ.2 กสญ.1 ฝกม.
   6.3 นายเสกสรรค์ วงศ์ปรีดากร พนักงานบริหารพัสดุ 7 จพ. กพท. ฝจบ.
   6.4 นายสรกฤช ฉัตรมาลัย พนักงานบริหารระบบคอมพิวเตอร์ 5 คค. กปค. ฝทท.
   6.5 นายกฤษฎ์ธิวัฒน์ ขจรพันธ์ พนักงานบริหารระบบคอมพิวเตอร์ 7 คค. กปค. ฝทท.

ขอบเขตของงานจัดซื้ออุปกรณ์รักษาความปลอดภัย
ของระบบเครือข่ายไฟล์วอล (Next Generation Firewall)

1. เหตุผลและความจำเป็น

การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย (รฟม.) ได้มีการติดตั้งและใช้งานอุปกรณ์รักษาความปลอดภัยของระบบเครือข่ายไฟล์วอล ตั้งแต่ปี 2553 โดยใช้งานในการกรองข้อมูล (Data) ที่เข้า-ออก ในระบบเครือข่าย เพื่อป้องกันภัยคุกคามในระบบสารสนเทศและระบบเครือข่าย อย่างไรก็ตาม อุปกรณ์ดังกล่าว ผู้ผลิตได้กำหนดการสิ้นสุดของระยะเวลาในการบำรุงรักษาแล้ว จึงจำเป็นต้องมีการจัดซื้ออุปกรณ์รักษาความปลอดภัยของระบบเครือข่ายไฟล์วอลขึ้นมาทดแทน

2. วัตถุประสงค์

เพื่อทดแทนอุปกรณ์รักษาความปลอดภัยของระบบเครือข่ายสื่อสารข้อมูลเดิม ในการป้องกันภัยคุกคามทางระบบสารสนเทศ การปิดช่องโหว่ และป้องกันการโจมตีระบบเครือข่ายสื่อสารข้อมูลในรูปแบบใหม่ที่เกิดขึ้นในปัจจุบันและอนาคตได้อย่างมีประสิทธิภาพ

3. คุณสมบัติของผู้ยื่นข้อเสนอ

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราวเนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วน ผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 เป็นนิติบุคคลผู้มีอาชีพขายพัสดุที่ประกวดราคาซื้อด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกันซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่ รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

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

3.11 ผู้ยื่นข้อเสนอต้องมีผลงานในการขายพร้อมติดตั้งอุปกรณ์รักษาความปลอดภัยของระบบเครือข่ายไฟล์วอล (Next Generation Firewall) ให้กับส่วนราชการ หน่วยงานตามกฎหมายว่าด้วยระเบียบราชการส่วนท้องถิ่น หน่วยงานของรัฐ รัฐวิสาหกิจ หรือหน่วยงานเอกชนที่ รฟม. เชื่อถือได้ ที่ได้ดำเนินการแล้วเสร็จภายในระยะเวลาไม่เกิน 5 ปี นับถึงวันที่ยื่นข้อเสนอประกวดราคา โดยมีมูลค่าสัญญาไม่น้อยกว่า 4,800,000 บาท (สี่ล้านแปดแสนบาทถ้วน) จำนวนอย่างน้อย 1 สัญญา

7

/โดย...

โดยผู้ยื่นข้อเสนอจะต้องแนบสำเนาหนังสือรับรองผลงาน และสำเนาสัญญา รวมทั้งต้องแนบขอบเขตของงานดังกล่าวมาพร้อมกับการยื่นข้อเสนอ

4. หลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอ

ในการพิจารณาคัดเลือกข้อเสนอครั้งนี้ รฟม. จะพิจารณาตัดสินโดยใช้หลักเกณฑ์ราคาประกอบเกณฑ์อื่น โดยมีรายละเอียดดังนี้

4.1 ราคายื่นข้อเสนอ (Price) กำหนดน้ำหนักเท่ากับร้อยละ 40 (100 คะแนน)

4.2 คุณภาพและคุณสมบัติที่เป็นประโยชน์ต่อหน่วยงานราชการ กำหนดน้ำหนักเท่ากับร้อยละ 50 (100 คะแนน) ดังต่อไปนี้

- ผลงานของผู้ยื่นข้อเสนอ พิจารณาจากจำนวนผลงานและมูลค่าของผลงาน	ร้อยละ 5 (10 คะแนน)
- แผนการดำเนินงานระบบ พิจารณาจากแผนงานที่มีความชัดเจนต่อเนื่อง มีกิจกรรมครอบคลุม สามารถดำเนินงานตามแผนให้บรรลุเป้าหมายของโครงการภายในระยะเวลาที่กำหนดไว้	ร้อยละ 5 (10 คะแนน)
- คุณสมบัติทางเทคนิค และคุณสมบัติทางเทคนิคอื่นๆ ที่เป็นประโยชน์ต่องานโครงการดังกล่าวของ รฟม. คุณสมบัติทางเทคนิคที่สามารถวัดเป็นปริมาณได้ รวมถึงคุณสมบัติทางเทคนิคอื่นๆ	ร้อยละ 40 (80 คะแนน)

4.3 บริการหลังการขายกำหนดน้ำหนักเท่ากับร้อยละ 10 (100 คะแนน)

- พิจารณาจากระยะเวลาการรับประกันความชำรุดบกพร่อง	ร้อยละ 5 (50 คะแนน)
- พิจารณาจากข้อตกลงระดับการให้บริการ (Service Level Agreement : SLA)	ร้อยละ 5 (50 คะแนน)

5. เงื่อนไขและข้อกำหนดทั่วไป

5.1 ผู้ยื่นข้อเสนอต้องมีหนังสือแต่งตั้งการเป็นตัวแทนจำหน่ายและให้บริการเกี่ยวกับอุปกรณ์และระบบที่เสนอตามข้อ 6 จากผู้ผลิต หรือจากสาขาของผู้ผลิตในประเทศไทย โดยต้องออกให้เพื่อมายื่นข้อเสนอนี้ และหนังสือนั้นต้องมีอายุไม่เกิน 90 วัน (เก้าสิบวัน) นับถัดจากวันที่ออกจนถึงวันที่ยื่นข้อเสนอ โดยจะต้องแนบสำเนาหลักฐานมาพร้อมกับการยื่นข้อเสนอ

5.2 ผู้ยื่นข้อเสนอต้องมีเจ้าหน้าที่ผู้มีความรู้ด้านระบบเครือข่ายสื่อสารข้อมูลในระดับองค์กร เพื่อทำหน้าที่ออกแบบติดตั้งอุปกรณ์ โดยไม่ให้เกิดปัญหาหรือผลกระทบต่อระบบเครือข่ายหลักของ รฟม. โดยมีใบรับรอง (Certificate) CISSP (Certified Information Systems Security Professional) อย่างน้อย 1 คน และใบรับรองดังกล่าวต้องยังไม่หมดอายุ ณ วันที่ยื่นข้อเสนอ โดยจะต้องแนบสำเนาหลักฐานมาพร้อมกับการยื่นข้อเสนอ

5.3 อุปกรณ์ที่นำเสนอต้องเป็นของแท้ อยู่ในสภาพที่ใช้งานได้ดี เป็นรุ่นที่ยังอยู่ในสายการผลิต (Product Line) และต้องเป็นของใหม่ที่ไม่เคยถูกใช้งานมาก่อน รวมทั้งต้องไม่ถูกนำมาปรับปรุงสภาพใหม่ (Reconditioned หรือ Rebuilt) โดยจะต้องแนบสำเนาหลักฐานที่ได้รับการรับรองจากผู้ผลิตหรือสาขาของผู้ผลิตในประเทศไทยมาพร้อมกับการยื่นข้อเสนอ

5.4 อุปกรณ์ที่นำเสนอต้องได้รับรองคุณภาพตามมาตรฐานที่เกี่ยวข้องกับผลิตภัณฑ์ ดังนี้

/5.4.1 ต้อง...

5.4.1 ต้องได้รับการรับรองมาตรฐานความปลอดภัยทางไฟฟ้า ตามมาตรฐานจากสถาบัน UL หรือ EN หรือ IEC ได้เป็นอย่างน้อย

5.4.2 ต้องได้รับการรับรองมาตรฐานด้านสิ่งแวดล้อม FCC หรือ CE หรือ RoHs หรือเทียบเท่า

5.5 อุปกรณ์ที่เสนอต้องมีคุณสมบัติตรงตาม Catalog หรือ Brochure ของบริษัทผู้ผลิตที่เสนอขายตามท้องตลาด โดยมีระบบหลัก และ/หรือองค์ประกอบหลัก ที่ไม่ได้ประกอบ และ/หรือดัดแปลง เพื่อใช้เฉพาะยื่นข้อเสนอครั้งนี้ โดยผู้ยื่นข้อเสนอจะต้องระบุยี่ห้อและรุ่นของผลิตภัณฑ์ที่เสนอ พร้อมทั้งต้องมี Catalog หรือ Brochure ที่ขีดเส้นใต้ หรือทำเครื่องหมาย พร้อมหัวข้อกำกับอุปกรณ์ที่เสนอไว้ และจัดทำตารางเปรียบเทียบคุณสมบัติของแต่ละหัวข้ออย่างชัดเจน โดยจะต้องแนบสำเนาหลักฐานมาพร้อมกับการยื่นข้อเสนอ

5.6 อุปกรณ์ที่นำเสนอต้องสามารถใช้งานกับระบบไฟฟ้า 220V AC 50Hz ตามมาตรฐานของไทยได้โดยไม่ต้องใช้อุปกรณ์แปลงระบบไฟฟ้า และปลั๊กไฟฟ้าของอุปกรณ์ทุกรายการจะต้องเป็นชนิด 3 ขา (มีขาสำหรับสายดิน)

5.7 อุปกรณ์รักษาความปลอดภัยของระบบเครือข่ายไฟล์วอล (Next Generation Firewall) ต้องอยู่ใน Gartner Leader Quadrant ด้าน Enterprise Network Firewalls ปี 2018 หรือใหม่กว่า

6. ข้อกำหนดคุณลักษณะ

6.1 ผู้ชนะการยื่นข้อเสนอ (ผู้ขาย) ต้องจัดหาอุปกรณ์รักษาความปลอดภัยของระบบเครือข่ายไฟล์วอล (Next Generation Firewall) พร้อมติดตั้ง จำนวนไม่น้อยกว่า 2 ชุด โดยมีคุณลักษณะอย่างน้อยหรือดีกว่าดังนี้

6.1.1 เป็นอุปกรณ์ Appliance ที่ออกแบบมาสำหรับรักษาความปลอดภัยของเครือข่ายโดยเฉพาะ

6.1.2 เป็นอุปกรณ์รักษาความปลอดภัยประเภท Next Generation Firewall (NGFW)

6.1.3 ใช้สถาปัตยกรรมแบบ Single Pass และมีการทำงานของ Control Plane และ Data Plane ที่แยกออกจากกัน หรือเป็นอุปกรณ์ที่มี Security Processor Unit (SPU) หรือที่เทียบเท่าที่ได้รับการออกแบบมาเพื่อป้องกันระบบเครือข่ายโดยเฉพาะ

6.1.4 มี Application Firewall Throughput ไม่น้อยกว่า 6 Gbps

6.1.5 มี Threat Protection Throughput ไม่น้อยกว่า 3 Gbps

6.1.6 สามารถรองรับการเชื่อมต่อได้สูงสุด ไม่น้อยกว่า 2,000,000 การเชื่อมต่อ

6.1.7 สามารถรองรับการเชื่อมต่อใหม่ (New Session per Second) ได้ไม่น้อยกว่า 84,000 การเชื่อมต่อ/วินาที

6.1.8 มีพอร์ต 10/100/1000 แบบ RJ-45 หรือดีกว่า ไม่น้อยกว่า 12 พอร์ต

6.1.9 มีพอร์ต 10 Gigabit Ethernet แบบ SFP+ ไม่น้อยกว่า 8 พอร์ต

6.1.10 มีพอร์ต 10/100/1000 ไว้สำหรับ Management แบบ Out-of-Band ไม่น้อยกว่า 1 พอร์ต

6.1.11 สามารถทำ High Availability (HA) แบบ Active/Passive และ Active/Active ได้

6.1.12 มี Storage แบบ SSD ไม่น้อยกว่า 240 GB

6.1.13 มี IPSec VPN Throughput ไม่น้อยกว่า 3.2 Gbps และรองรับ VPN Tunnel ไม่น้อยกว่า 4,000 tunnels

6.1.14 สามารถทำงานแบบ SSL VPN โดยสามารถใช้งาน ได้ไม่น้อยกว่า 2,000 Active Concurrent Users

6.1.15 สามารถใช้งาน Client VPN (Remote Access) โดยต้องมีคุณสมบัติอย่างน้อยดังต่อไปนี้

6.1.15.1 มี Application ที่สามารถใช้งานผ่านระบบปฏิบัติการ Microsoft Windows, Mac OS, iOS และ Android ได้ โดย Application ดังกล่าวต้องเป็นยี่ห้อเดียวกันกับอุปกรณ์ที่นำเสนอ

/6.1.15.2 สามารถ...

6.1.15.2 สามารถ Integrate กับระบบ Authentication แบบ Multi-factor Authentication (MFA)

6.1.16 สามารถเข้ารหัส (Encryption) แบบ 3DES, AES (128 bit, 192 bit, 256 bit) และรองรับการ Authentication แบบ MD5, SHA ได้เป็นอย่างน้อย

6.1.17 สามารถตรวจสอบ Traffic ที่เข้ารหัสแบบ SSL (Inbound และ Outbound) และ SSH ได้

6.1.18 สามารถสำเนาข้อมูลที่ถูกถอดรหัส (Decryption) และส่งต่อให้อุปกรณ์อื่นตรวจสอบได้ผ่าน Mirror Port ของตัวอุปกรณ์ได้

6.1.19 สามารถรองรับมาตรฐานการทำงานต่างๆ ดังต่อไปนี้ VLAN (802.1Q), NAT, DHCP Relay, Dynamic Routing (OSPF v2 and v3, RIP, BGP), Multicast Routing (PIM, IGMP), Syslog, SNMP (V.2 and V.3)

6.1.20 สามารถทำงานในลักษณะ Layer 2, Layer 3 หรือ NAT/Route Mode, Transparent และ Tap Mode หรือ Sniffer Mode ได้

6.1.21 สามารถทำ NAT (Network Address Translation) ได้

6.1.22 สามารถทำ PAT (Port Address Translation) ได้

6.1.23 สามารถตรวจสอบผู้ใช้งาน (User Authentication/Identification) กับระบบ Microsoft Active Directory, LDAP, RADIUS, Microsoft Exchange เป็นอย่างน้อย เพื่อใช้ในการตรวจสอบการเข้าใช้งานอุปกรณ์ได้

6.1.24 สามารถควบคุมการใช้งาน Application ได้ไม่น้อยกว่า 1,900 application โดยครอบคลุมถึงกลุ่ม Application ต่างๆ เช่น Files-sharing หรือ Storage/Backup, Encrypted-tunnel หรือ Remote Access หรือ Proxy, Gaming, Instant Messaging หรือ Social Media, Internet Conferencing หรือ Collaboration และ P2P เป็นอย่างน้อย

6.1.25 สามารถทำ Application Level Gateway (ALG) หรือ Session Helpers สำหรับโปรโตคอล เช่น FTP, SIP, H.323, RTSP, Oracle/SQLNet/TNS และ MGCP ได้เป็นอย่างน้อย

6.1.26 สามารถทำ QoS แบบ Guaranteed, Maximum และ Priority Bandwidth โดยกำหนดนโยบายการทำ QoS (Traffic shaping policy) ตาม Application, User, Source, Destination, Interface และ IPSec VPN Tunnel ได้เป็นอย่างน้อย

6.1.27 สามารถกำหนด Virtual Router หรือ VRF ได้ไม่น้อยกว่า 10 ชุด และรองรับ Security Zone ไม่น้อยกว่า 60 Zones

6.1.28 มีระบบป้องกันภัยคุกคาม (Threat Prevention) โดยมี IPS, Antivirus และ Antispyware (หรือ Anti-Bot) โดยสามารถรองรับ Throughput ไม่น้อยกว่า 3 Gbps เมื่อเปิดทำงานพร้อมกัน และมีคุณสมบัติอย่างน้อยดังต่อไปนี้

6.1.28.1 สามารถตรวจจับและป้องกัน Vulnerability Exploits, Buffer Overflow หรือ Evasion Techniques แบบต่างๆ, DoS/DDoS, Non-RFC Compliant Protocol, Port Scans, Host Sweeps หรือ ICMP Sweep, Malformed Packets หรือ IP Protocol with Malformed Option, IP Defragmentation หรือ IP Packet Fragmentation และ TCP Reassembly หรือ URL&HTML Obfuscation ได้เป็นอย่างน้อย รวมทั้งสามารถปรับแต่งรูปแบบของภัยคุกคาม (Custom signatures) ได้ตามความต้องการ

/6.1.28.2 สามารถ...

6.1.28.2 สามารถป้องกัน Malware ประเภทต่างๆ ได้แก่ Virus, Spyware, Trojan และ Botnet ได้เป็นอย่างน้อย

6.1.28.3 สามารถตรวจจับและป้องกัน Virus บนโปรโตคอล HTTP, FTP, IMAP, POP3, SMTP, SMB ได้

6.1.28.4 สามารถทำ DNS Sinkhole หรือ DNS Filter เพื่อป้องกันการเข้าถึง Malicious Domain และเฝ้าระวังผู้ใช้ที่มีการเรียกใช้งานไปยัง Malicious Domain

6.1.29 สามารถทำงานแบบ URL filtering บนตัวอุปกรณ์ได้ โดยมีการแบ่งเว็บไซต์ออกเป็นกลุ่ม (Categories) และสามารถกำหนด Whitelist และ Blacklist ได้

6.1.30 สามารถป้องกันการเข้าถึงเว็บไซต์ที่ไม่อนุญาตโดยทางอ้อม ผ่านทาง Search Engine Cache (เช่น Google cache) และ Translation Site (เช่น Google translate) ได้

6.1.31 สามารถป้องกันการแสดงผลเนื้อหาที่ไม่เหมาะสม (Adult content) จากการค้นหาบน Search provider หลักๆ เช่น Google, Bing และ Yahoo เป็นต้น

6.1.32 สามารถควบคุมประเภทของไฟล์ที่อนุญาตให้ส่งผ่านระบบเครือข่ายได้รวมทั้งสามารถป้องกันการรั่วไหลของข้อมูลออกจากระบบเครือข่าย เช่น หมายเลขบัตรเครดิต และสามารถสร้างรูปแบบการตรวจจับได้ตามความต้องการ

6.1.33 สามารถบริหารจัดการอุปกรณ์แบบ Web-based Management (HTTPS) และ Command Line Interface ได้

6.1.34 สามารถเก็บข้อมูลการใช้งาน (Logging) หรือสามารถส่ง Syslog ไปจัดเก็บยังอุปกรณ์ภายนอกได้

6.1.35 สามารถสร้างรายงาน (Report) ต่างๆ เช่น User Activity Report, Application Report, Threat/Attack Report, Bot-net Report, Anti-Virus Report, URL Filtering Report ได้เป็นอย่างน้อย โดยสามารถทำการปรับแต่งรายงาน (Custom Report) และส่งออก (Export) ให้อยู่ในรูปแบบ PDF, XML และ CSV ได้เป็นอย่างน้อย หรือรองรับการทำงานร่วมกันกับระบบจัดเก็บข้อมูลการใช้งานเพื่อสร้างรายงานประเภทต่างๆ ได้

6.1.36 มี Redundant Power Supply แบบ Hot-swap หรือ Hot-plug อย่างน้อย 2 ชุด

6.2 ผู้ขายต้องจัดหาระบบบริหารจัดการอุปกรณ์รักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์แบบศูนย์รวม (Centralized Management Firewall) จำนวนไม่น้อยกว่า 1 ระบบ โดยจะต้องมีคุณสมบัติอย่างน้อยหรือดีกว่าดังนี้

6.2.1 เป็นระบบในรูปแบบของ Virtual Appliance หรือ Software ที่ออกแบบมาเพื่อบริหารจัดการอุปกรณ์ Next Generation Firewall ที่เสนอมาในโครงการนี้ โดยเฉพาะ

6.2.2 สามารถรองรับอุปกรณ์ Next Generation Firewall ได้ไม่น้อยกว่า 8 อุปกรณ์

6.2.3 สามารถสร้าง Configuration Template ได้ และกำหนดให้ทำการปรับปรุง (Deploy) ไปยังอุปกรณ์ที่เสนอได้

6.2.4 สามารถบริหารจัดการการทำงานของอุปกรณ์ Next Generation Firewall ที่นำเสนอได้

6.2.5 สามารถเชื่อมต่อกับอุปกรณ์ Next Generation Firewall ที่นำเสนอผ่านโปรโตคอล SSL หรือเทียบเท่า

6.2.6 สามารถตรวจสอบการแก้ไขหรือเปลี่ยนแปลงการตั้งค่า (Configuration) ของอุปกรณ์ Next Generation Firewall ได้

6.2.7 สามารถ Upgrade Firmware ของอุปกรณ์ Next Generation Firewall ได้ และสามารถกำหนดเวลาในการ Upgrade ได้

/6.2.8 สามารถ...

6.2.8 สามารถพิสูจน์ตัวตนของผู้ดูแลระบบ (Administrator) โดยใช้ฐานข้อมูลจาก Local Database และ RADIUS ได้เป็นอย่างน้อย

6.2.9 สามารถกำหนดสิทธิและระดับความสำคัญให้กับผู้ดูแลระบบได้

6.2.10 สามารถบริหารจัดการอุปกรณ์ผ่าน Web Interface และ SSH ได้เป็นอย่างน้อย

6.2.11 สามารถเรียกดูสรุปข้อมูลของ Data ในรูปแบบของกราฟฟิคได้ โดยสามารถปรับแต่งรายงานตามการใช้งาน (Custom Report) และ Export ให้อยู่ในรูปแบบ PDF ได้เป็นอย่างน้อย พร้อมทั้งสามารถตั้งเวลาในการส่งรายงานผ่าน Email ได้ โดยสามารถทำรายงานต่างๆ ได้อย่างน้อยดังนี้

6.2.11.1 Top Application, Application Categories

6.2.11.2 Top Source, User, Destination

6.2.11.3 Top Threats, Attackers and Victims

6.2.11.4 User Activity Report

6.2.12 สามารถรับข้อมูลจราจรคอมพิวเตอร์จากอุปกรณ์ Next Generation Firewall อย่างน้อยดังนี้

6.2.12.1 สามารถจัดเก็บข้อมูล Log ไม่น้อยกว่า 5,000 เหตุการณ์ต่อวินาที (Log Rate) และสามารถจัดเก็บข้อมูล Log ไม่น้อยกว่า 25 GB ต่อวัน

6.2.12.2 สามารถทำ Forensic Analysis โดยการรวบรวมและคัดกรองเหตุการณ์จากข้อมูลได้

6.2.12.3 สามารถเก็บข้อมูลจราจรคอมพิวเตอร์ดังต่อไปนี้ได้

- IP Address ต้นทาง (Source IP Address)
- IP Address ปลายทาง (Destination IP Address)
- Service Port ปลายทาง (Destination Port)
- วันและเวลาของการเชื่อมต่อ
- ชื่อผู้ใช้งานเมื่อมีการระบุตัวตน (Authentication)
- Application ที่ใช้งาน

6.2.12.4 สามารถแสดงข้อมูลการใช้งานแบบ Real-Time และ Historical ได้

6.2.12.5 สามารถค้นหาข้อมูลของ Log ที่ต้องการได้

6.2.12.6 สามารถสร้างรายงาน (Report) ข้อมูลจากอุปกรณ์ Next Generation Firewall ได้

6.2.12.7 สามารถกำหนดสิทธิและระดับการเข้าถึงข้อมูลให้กับผู้ดูแลระบบได้

6.2.13 กรณีที่ไม่สามารถทำตามข้อกำหนดที่ 6.2.12 ได้ภายในระบบชุดเดียวกัน ผู้ขายจะต้องเสนออุปกรณ์หรือระบบที่สามารถทำได้ตามข้อกำหนดดังกล่าว

6.2.14 ระบบที่นำเสนอต้องเป็นยี่ห้อเดียวกับ ข้อ 6.1

6.3 ผู้ขายต้องจัดหา Software Module ที่มีความสามารถในการทำ Security Inspection หรือ Decryption สำหรับ SSL/TLS Traffic ทั้ง Inbound และ Outbound ของอุปกรณ์ F5 รุ่น Big-IP10800 จำนวนอย่างน้อย 2 ชุด โดยมีคุณสมบัติอย่างน้อยหรือดีกว่าดังนี้

6.3.1 สามารถทำงานบน Hardware SSL และมี Throughput ไม่น้อยกว่า 40 Gbps bulk encryption

6.3.2 สามารถทำ Deployment Modes ในรูปแบบ Inline Layer 3, Inline Layer 2, Web Proxies, Explicit/Transparent Proxy, Receive-Only และ ICAP-based ได้เป็นอย่างน้อย

6.3.3 สามารถใช้ Algorithm หรือ Cipher Agility แบบ GCM, ECC, Camellia, DSA และ RSA ได้เป็นอย่างน้อย

/6.3.4 สามารถ...

6.3.4 สามารถรองรับ RSA ได้ไม่น้อยกว่า 80,000 TPS (2K Keys) และ ECC ได้ไม่น้อยกว่า 48,000 TPS (ECDSA P-256)

6.3.5 สามารถรองรับ SSL/TLS Protocol แบบ TLS1.0, TLS1.1, TLS1.2 และ TLS1.3 ได้เป็นอย่างน้อย

6.3.6 รองรับการใช้งาน URL Filtering โดยมีฐานข้อมูลเพื่อทำการกรอง IP Reputation และ Geolocation ได้

6.3.7 สามารถทำ Dynamic Service Chaining โดยสามารถทำ Service Insertion, Service Monitoring, และ Load Balancing ได้เป็นอย่างน้อย

6.3.8 สามารถทำการเข้ารหัสและถอดรหัส (Encrypted Traffic and Decrypted Traffic) ให้อุปกรณ์อื่นๆ เช่น Next Generation Firewall, DLP Scanners, Web Application Firewalls (WAF), Intrusion Prevention Systems (IPS) และ Malware Analysis Tools ได้

6.3.9 สามารถแสดงผล SSL Analytic ที่สามารถปรับเปลี่ยนรูปแบบการแสดงผล (Customizable View SSL Data/Statistic) ในรูปแบบกราฟ Chart, ตาราง (Table Capabilities) และ Timeline ได้

6.3.10 สามารถแสดงผลเพื่อสร้างรายงาน (Reporting) และตั้งเวลาการออกรายงาน (Automatic Reporting Schedule) ได้

6.3.11 สามารถทำงานร่วมกันแบบ Active/Standby และ Active/Active ได้

6.3.12 สามารถดูข้อมูลสถิติเปรียบเทียบ (Comparing Statistics) ทั้งแบบ Top Virtual Servers, Top Site Decrypted, Client Ciphers และ Protocols ได้เป็นอย่างน้อย

6.4 ผู้ขายต้องจัดหาระบบบริหารจัดการบัญชีผู้ใช้งานสิทธิ์ขั้นสูง (Privileged Account Management) จำนวนอย่างน้อย 1 ชุด โดยมีคุณสมบัติอย่างน้อยหรือดีกว่าดังนี้

6.4.1 เป็นระบบที่ออกแบบมาโดยเฉพาะ เพื่อทำหน้าที่ควบคุมความปลอดภัย Privileged Account โดยสามารถบริหารจัดการรหัสผ่าน และควบคุมการเบิกใช้งาน เพื่อลดความเสี่ยงจากการถูกโจมตี

6.4.2 ต้องมีสิทธิ์สำหรับผู้ใช้งานระบบ จำนวนไม่น้อยกว่า 20 Users

6.4.3 สามารถบริหารจัดการรหัสผ่านอุปกรณ์ปลายทาง จำนวนไม่น้อยกว่า 400 ระบบ

6.4.4 สามารถเข้ารหัสข้อมูลของ Privileged Account ด้วย Algorithm แบบ AES-256, RSA-2048 หรือดีกว่า โดยผ่านการรับรองมาตรฐาน FIPS140-2

6.4.5 สามารถเปลี่ยนรหัสผ่านของบัญชีผู้ใช้งานบนระบบปลายทางได้ โดยไม่ต้องติดตั้ง Agent (Agentless)

6.4.6 สามารถบริหารจัดการบัญชีผู้ใช้งานและรหัสผ่านของระบบต่อไปนี้ได้

6.4.6.1 Operating System: Windows Servers, Redhat Linux, VMware ESX/ESXi

6.4.6.2 Network and Security: Checkpoint Firewall, Bluecoat, Cisco, Fortinet, Palo Alto

6.4.7 สามารถบริหารจัดการรหัสผ่านตามคุณสมบัติได้อย่างน้อย ดังนี้

6.4.7.1 สามารถเปลี่ยนรหัสผ่านของ Privileged Account ตามช่วงเวลาที่กำหนด

6.4.7.2 สามารถเปลี่ยนรหัสผ่านของ Privileged Account หลังจากการใช้งานโดยอัตโนมัติ

6.4.7.3 สามารถกำหนดความยาวและองค์ประกอบของรหัสผ่าน เช่น ตัวอักษรใหญ่ (Upper Case), ตัวอักษรเล็ก (Lower Case), ตัวเลข (Digit) และอักขระพิเศษ (Special Character) ได้

/6.4.8 สามารถ...

6.4.8 สามารถกำหนด Workflow ในการใช้งานตามคุณสมบัติได้อย่างน้อย ดังนี้

6.4.8.1 สามารถทำงานแบบ Dual Control โดยผู้ใช้ต้องได้รับการอนุมัติก่อนที่จะเรียกดูรหัสผ่านได้

6.4.8.2 สามารถกำหนดจำนวนผู้อนุมัติได้

6.4.8.3 สามารถแจ้งเตือนทางอีเมล ในกระบวนการร้องขอและอนุมัติ

6.4.9 ต้องมี Web Portal ที่ออกแบบเฉพาะกับอุปกรณ์ Mobile เพื่อใช้ในการร้องขอรหัสผ่าน และอนุมัติการใช้งาน

6.4.10 สามารถตรวจสอบและค้นหา Privileged Account รวมทั้งประเมินความเสี่ยง สำหรับระบบปฏิบัติการ Windows, Unix, Hard-coded Credentials และ Pass-the-Hash Vulnerabilities ได้

6.4.11 สามารถเชื่อมต่อไปยังระบบปลายทาง (Transparent Connection) ตามคุณสมบัติอย่างน้อย ดังนี้

6.4.11.1 สามารถเข้าสู่ระบบปลายทางได้ โดยไม่ต้องแสดงรหัสผ่านให้ผู้ใช้ทราบ

6.4.11.2 สามารถเชื่อมต่อไปยังระบบ Application โดยตรง โดยใช้ Universal Connector โดยสามารถรองรับ Microsoft SQL Management Studio, VMware VSphere Web Client ได้

6.4.12 สามารถบันทึกการใช้งาน Privileged Session ในรูปแบบของ Video Recording และ Keystrokes หรือ Commands ได้ โดยต้องรองรับการทำงานอย่างน้อย ดังนี้

6.4.12.1 Privileged SSH Sessions ในรูปแบบของ Command List

6.4.12.2 Privileged Windows Sessions ในรูปแบบของ Windows Process และ Windows Title

6.4.13 สามารถ Export เหตุการณ์ที่บันทึกได้ทั้งแบบ Video และ Text

6.4.14 สามารถทำ White List และ Black List สำหรับ SSH Commands เพื่อป้องกันการใช้งานคำสั่งที่ไม่อนุญาตบนระบบที่ควบคุมได้ โดยไม่ต้องติดตั้ง Agent

6.4.15 สามารถตรวจสอบและวิเคราะห์ภัยคุกคามจากพฤติกรรมการใช้งาน (Privileged Threat Analytics) ได้ตามคุณสมบัติอย่างน้อย ดังนี้

6.4.15.1 สามารถกำหนดเงื่อนไขเพื่อตรวจสอบพฤติกรรมการใช้งานที่มีความเสี่ยงสูง (High Risk Activities) และ แสดงผลเป็น Risk Score เพื่อระบุระดับความเสี่ยงของแต่ละ Privileged Session ได้

6.4.15.2 สามารถตรวจสอบและวิเคราะห์พฤติกรรมการใช้งานของ Privileged User เพื่อสร้างเป็น Baseline และแจ้งเตือนหากพบพฤติกรรมที่ผิดปกติ

6.4.15.3 สามารถตรวจจับพฤติกรรมการใช้งานที่ผิดปกติได้ โดยสามารถ Suspend หรือ Terminate Session การใช้งานนั้นได้โดยอัตโนมัติ

6.4.16 ระบบที่จัดเก็บข้อมูลสำคัญ ต้องสามารถทำงานในลักษณะ High Availability และ Disaster Recovery ได้ โดยมีลิขสิทธิ์สำหรับติดตั้งระบบดังกล่าวอย่างน้อย ดังนี้

6.4.16.1 Cluster ที่ศูนย์ข้อมูลหลัก เพื่อสามารถทำ HA จำนวน 1 ชุด

6.4.16.2 DR ที่ศูนย์ข้อมูลสำรอง เพื่อสามารถทำ Disaster Recovery จำนวน 1 ชุด

6.4.16.3 มีลิขสิทธิ์สำหรับติดตั้งระบบทดสอบ (Test License) ใน Developer หรือ UAT อย่างน้อย 2 ชุด

/6.4.17 มี...

6.4.17 มีการทำงานแบบ Agent ที่ติดตั้งบน Application หรือ Batch Server เพื่อกำจัด Hard-coded Credential ที่อยู่ใน Source Code หรือ Configuration Files และมีลิขสิทธิ์สำหรับติดตั้งใช้งานได้ไม่น้อยกว่า 1 Agent

6.4.18 ระบบที่จัดเก็บข้อมูลสำคัญ ต้องได้รับมาตรฐาน Command Criteria Certified EAL 2+ หรือดีกว่า

7. ขอบเขตของการดำเนินงานและการส่งมอบงาน

7.1 จัดให้มีการประชุมเริ่มงาน (Kick off Meeting) เพื่อนำเสนอแผนการดำเนินงานในการออกแบบ ติดตั้งและทดสอบ ให้พิจารณาก่อนการดำเนินงานติดตั้งจริงภายใน 15 วัน (สิบห้าวัน) นับถัดจากวันที่ลงนามในสัญญา

7.2 ดำเนินการจัดหา ออกแบบ ติดตั้ง และทดสอบระบบ พร้อมทั้งจัดการฝึกอบรมให้แก่เจ้าหน้าที่ของ รฟม. ให้แล้วเสร็จ พร้อมส่งมอบภายใน 120 วัน (หนึ่งร้อยยี่สิบวัน) นับถัดจากวันลงนามในสัญญา

7.3 ผู้ขายต้องจัดหา Transceiver Module แบบ 10GBase-SR ชนิด SFP+ เพื่อใช้ร่วมกับอุปกรณ์ในข้อ 6.1 จำนวนไม่น้อยกว่า 16 ชุด พร้อมส่งมอบภายใน 120 วัน (หนึ่งร้อยยี่สิบวัน) นับถัดจากวันลงนามในสัญญา

7.4 ผู้ขายต้องจัดหา Hard Disk ที่สามารถติดตั้งกับ Cisco UCS C240 M5 ที่ รฟม. มีและใช้งานอยู่ได้ จำนวนไม่น้อยกว่า 7 ลูก โดยต้องมีคุณสมบัติอย่างน้อยดังนี้

7.4.1 เป็น Hard Disk ขนาด 2.5 นิ้ว ชนิด Enterprise Value SSD

7.4.2 มีขนาดความจุต่อตัวไม่น้อยกว่า 1.9 TB

7.5 ผู้ขายต้องจัดหาเครื่องคอมพิวเตอร์สำหรับมอนิเตอร์ระบบ จำนวน 1 ชุด โดยต้องมีคุณสมบัติอย่างน้อยดังนี้

7.5.1 เป็นคอมพิวเตอร์แบบ All in one โดยมีจอภาพ, หน่วยประมวลผล, หน่วยความจำ อยู่ในตัวอุปกรณ์ตัวเดียวกัน

7.5.2 มีหน่วยประมวลผลกลาง (CPU) 8th Gen Core i5 หรือรุ่นล่าสุดที่มีในท้องตลาด ที่มีความเร็วไม่น้อยกว่า 3 GHz 6 Cores

7.5.3 มีหน่วยความจำหลัก ที่มีความจุรวมไม่น้อยกว่า 16 GB แบบ DDR4 หรือดีกว่า

7.5.4 มี Hard Disk ที่มีความจุรวมไม่น้อยกว่า 512 GB แบบ SSD หรือดีกว่า

7.5.5 มีหน่วยควบคุมการแสดงผล ที่มีหน่วยความจำหลักความจุรวมไม่น้อยกว่า 4 GB (แยกจากหน่วยความจำหลัก) แบบ GDDR5 โดยรองรับการเชื่อมต่อแบบ HDMI ได้เป็นอย่างน้อย

7.5.6 มีช่องเชื่อมต่อระบบเครือข่าย Gigabit Ethernet จำนวนไม่น้อยกว่า 1 ช่อง

7.5.7 สามารถเชื่อมต่อเครือข่ายไร้สาย (Wireless) ตามมาตรฐาน 802.11a/b/g/n/ac ได้เป็นอย่างน้อย

7.5.8 มีช่องเชื่อมต่อแบบ USB-C จำนวนไม่น้อยกว่า 2 พอร์ต และรองรับการส่งสัญญาณภาพผ่านพอร์ตดังกล่าวได้

7.5.9 มีช่องเชื่อมต่อตามมาตรฐาน USB3.0 หรือดีกว่า จำนวนรวมไม่น้อยกว่า 4 ช่อง

7.5.10 มีช่องต่อหูฟังขนาด 3.5 มม. จำนวนไม่น้อยกว่า 1 ช่อง

7.5.11 มีช่องเสียบการ์ด SDXC จำนวนไม่น้อยกว่า 1 ช่อง

7.5.12 มีจอภาพขนาดไม่น้อยกว่า 27 นิ้ว และมีความละเอียด 5120 x 2880 เป็นอย่างน้อย

7.5.13 มีซอฟต์แวร์ระบบปฏิบัติการ ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย

7.5.14 มี Mouse แบบไร้สาย ที่มีความสามารถใช้งานแบบ Multi-Touch โดยเป็นยี่ห้อเดียวกันกับเครื่องคอมพิวเตอร์ที่นำเสนอ

7.5.15 มี Keyboard แบบไร้สาย ที่มีตัวอักษรภาษาไทยและภาษาอังกฤษติดบนแป้นกดอย่างถาวร และเป็นยี่ห้อเดียวกันกับเครื่องคอมพิวเตอร์ที่นำเสนอ

/7.6 ผู้ขาย...

7.6 ผู้ขายต้องจัดส่งบุคลากรที่ได้เสนอไว้ เข้ามาดำเนินการออกแบบ ติดตั้งระบบที่เสนอให้สามารถใช้งานร่วมกับระบบคอมพิวเตอร์ของ รฟม. ได้อย่างมีประสิทธิภาพ

7.7 ผู้ขายต้องรับผิดชอบค่าใช้จ่ายทั้งหมดในการเดินสายสัญญาณภายในโครงการนี้ทั้งหมด

7.8 หลังจากที่ผู้ขายได้ดำเนินงานต่างๆ เรียบร้อยแล้ว ผู้ขายต้องจัดส่งรายงานผลการดำเนินงาน และเอกสารอื่นๆ ที่เกี่ยวข้องในรูปแบบเอกสารสี และรูปแบบ Digital Files ที่สามารถแก้ไขปรับปรุงได้ เช่น .doc, .xls, .vsd เป็นต้น โดยรายงานต้องมีรายละเอียดครอบคลุมดังนี้

7.8.1 สรุปผลการดำเนินงานออกแบบ ติดตั้งและทดสอบอุปกรณ์ ที่เป็นไปตามเงื่อนไขต่างๆ ตามข้อ 7.1 – 7.9

7.8.2 แผนผังระบบเครือข่ายสื่อสารข้อมูล (Network Diagram) และแผนผังอุปกรณ์ที่ได้ติดตั้ง

7.9 ผู้ขายต้องดำเนินงานต่างๆ และส่งมอบงานให้แก่ รฟม. โดยการส่งมอบงานที่เป็นเอกสาร ผู้ขายต้องจัดทำเป็นรูปเล่มต้นฉบับอย่างละ 2 ชุด และสำเนาจำนวนไม่น้อยกว่าคณะกรรมการตรวจรับพัสดุ พร้อม Digital Files โดยบรรจุลงใน USB Flash Drive จำนวน 2 ชุด

7.10 คณะกรรมการตรวจรับพัสดุจะทดสอบ ตรวจรับผลิตภัณฑ์ที่เสนอตามสัญญานี้ ต่อเมื่อคณะกรรมการตรวจรับพัสดุ รฟม. ได้รับหนังสือแจ้งจากผู้ขายว่าได้ติดตั้งผลิตภัณฑ์ทั้งหมดเสร็จเรียบร้อยพร้อมที่จะส่งมอบแล้ว โดยผู้ขายต้องทำหนังสือแจ้งให้คณะกรรมการตรวจรับพัสดุรับทราบก่อนวันส่งมอบและตรวจรับไม่น้อยกว่า 3 วัน (สามวัน) ทำการของ รฟม.

7.11 กรณีมีรายการใด ประมาณการผิดพลาด หรือตกหล่น ในส่วนของอุปกรณ์ควบใดๆ ส่งผลให้อุปกรณ์นั้น หรือระบบโดยภาพรวม ไม่สามารถทำงานได้ตามความต้องการของ รฟม. ให้ถือเป็นความรับผิดชอบของผู้ขายจัดหาเพิ่มเติมเพื่อให้ระบบสามารถทำงานได้ตามที่ทาง รฟม. ได้กำหนดไว้ โดยไม่คิดค่าใช้จ่ายอื่นใดเพิ่มเติม

8. การฝึกอบรมและคู่มือ

8.1 เมื่อทำการออกแบบ ติดตั้ง และทดสอบผลิตภัณฑ์ทั้งหมดแล้วเสร็จ ผู้ขายต้องจัดทำร่างคู่มือผู้ดูแลระบบ (Technical Manual) แสดงรายละเอียดเป็นภาษาไทยพร้อมรูปภาพที่ประกอบไปด้วย ขั้นตอนการติดตั้ง (Install & Configuration) ขั้นตอนการบริหารจัดการระบบและอุปกรณ์ต่างๆ แผนผังการเชื่อมระบบเครือข่าย และแผนผังการติดตั้ง (Rack Diagram) อย่างละเอียดสำหรับใช้ประกอบการทำงานได้จริง ส่งเป็นเอกสารให้คณะกรรมการตรวจรับพัสดุเห็นชอบก่อนการจัดทำเป็นคู่มือฉบับสมบูรณ์ เมื่อคณะกรรมการตรวจรับพัสดุเห็นชอบแล้ว ให้ผู้ขายจัดทำคู่มือดังกล่าวเป็นเอกสารสีฉบับสมบูรณ์ พร้อมไฟล์ต้นฉบับของเอกสารทั้งหมดบรรจุลง USB Flash Drive จำนวน 4 ชุด โดยผู้ขายต้องดำเนินการให้แล้วเสร็จก่อนทำการฝึกอบรมการใช้งาน

8.2 การฝึกอบรมเจ้าหน้าที่ผู้ดูแลระบบ ผู้ขายต้องเสนอหัวข้อการอบรมเชิงปฏิบัติการ พร้อมเอกสารที่จะใช้ฝึกอบรมที่เป็นภาษาไทย โดยเนื้อหาการฝึกอบรมต้องเป็นไปตามมาตรฐานของผลิตภัณฑ์ที่เสนอซึ่งต้องครอบคลุมเนื้อหาที่เกี่ยวข้องกับ การติดตั้ง กำหนดค่า บริหารจัดการ และการแก้ปัญหา ให้ คณะกรรมการตรวจรับพัสดุพิจารณาเห็นชอบก่อนทำการฝึกอบรม โดยต้องฝึกอบรมให้แล้วเสร็จก่อนการส่งมอบระบบทั้งหมด

8.3 ผู้ขายต้องทำการฝึกอบรมเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ (ฝทท.) ที่เป็นผู้ดูแลระบบอย่างน้อย 4 คน

8.4 ในการฝึกอบรม ผู้ขายต้องจัดเตรียมวิทยากร เอกสารการฝึกอบรม อาหารว่างจำนวน 2 มื้อ และอาหารกลางวันจำนวน 1 มื้อต่อวัน ตามจำนวนที่ ฝทท. กำหนด

8.5 หากผู้ขายไม่ดำเนินการฝึกอบรมได้ทันก่อนการส่งมอบตามสัญญานี้ รฟม. จะดำเนินการจัดส่งเจ้าหน้าที่ผู้ดูแลระบบ ตามจำนวนที่ ฝทท. กำหนด ไปฝึกอบรมกับบริษัทที่รับฝึกอบรมภายนอก โดยค่าใช้จ่ายทั้งหมดที่เกิดจากการฝึกอบรม ผู้ขายยินยอมให้ รฟม. หักค่าใช้จ่ายดังกล่าวออกจากค่าพัสดุหรือหลักประกันการปฏิบัติตามสัญญา

/9. ระยะ...

9. ระยะเวลาดำเนินงาน

ระยะเวลาการดำเนินงาน 120 วัน (หนึ่งร้อยยี่สิบวัน) นับถัดจากวันลงนามในสัญญา

10. วงเงินในการจัดหา

12,000,000 บาท (สิบสองล้านบาทถ้วน)

11. การรับประกัน

11.1 ผู้ขายจะต้องรับประกันความชำรุดบกพร่องของงาน ที่เกิดขึ้นภายในระยะเวลาไม่น้อยกว่า 3 ปี นับถัดจากวันที่ รฟม. ได้รับมอบงาน โดยต้องรีบจัดการซ่อมแซมแก้ไขให้ใช้การได้ดีดังเดิมภายใน 1 วันทำการของ รฟม. นับถัดจากวันที่ได้รับแจ้งความชำรุดบกพร่อง

11.2 ผู้ขายจะต้องจัดให้มีเจ้าหน้าที่ที่มีความเชี่ยวชาญและมีประสบการณ์เพื่อเริ่มดำเนินการภายใน 4 ชั่วโมง นับตั้งแต่เวลาที่ รฟม. ได้แจ้งความชำรุดบกพร่องให้ผู้ขายทราบทางโทรศัพท์ โทรศัพท์เคลื่อนที่ โทรสาร หรือจดหมายอิเล็กทรอนิกส์ (E-mail)

11.3 อะไหล่หรือวัสดุอุปกรณ์ที่ใช้ในการซ่อมแซมแก้ไข กรณีการให้ใช้เป็นการชั่วคราว จะต้องมีคุณสมบัติไม่ต่ำกว่าของเดิม กรณีการเปลี่ยนวัสดุอุปกรณ์ให้ใหม่ วัสดุอุปกรณ์นั้นจะต้องมีคุณสมบัติไม่ต่ำกว่าของเดิม เป็นของใหม่ที่ไม่เคยถูกใช้งานมาก่อนและไม่เป็นของเก่าเก็บ

11.4 ผู้ขายต้องรับประกันลิขสิทธิ์การใช้งานต่างๆ ที่ใช้งานภายในโครงการนี้ทั้งหมด เป็นระยะเวลาไม่น้อยกว่า 3 ปี นับถัดจากวันที่ รฟม. ได้รับมอบงาน

11.5 กรณีที่มีการเคลื่อนย้าย หรือเปลี่ยนแปลงค่า (Re-config) ของระบบและ/หรืออุปกรณ์ ที่ได้ติดตั้งตามสัญญานี้ รฟม. มีสิทธิที่จะแจ้งให้ผู้ขายมาดำเนินการให้ รฟม. ได้ตลอดอายุสัญญา โดย รฟม. ไม่เสียค่าใช้จ่ายใดๆ เพิ่มเติมทั้งสิ้น

12. การชำระเงิน

การชำระเงินตามสัญญานี้ เป็นการชำระแบบรายงวด ซึ่งเป็นราคารวมภาษีมูลค่าเพิ่ม ตลอดจนภาษีอากรอื่นๆ และค่าใช้จ่ายทั้งปวงแล้ว โดยมีรายละเอียดการชำระเงินแบ่งเป็นงวด 3 งวด ดังนี้

งวดที่ 1 ชำระเงินร้อยละ 25 ของมูลค่าตามสัญญา เมื่อผู้ขายได้ดำเนินการตามข้อ 7.1 เรียบร้อยแล้ว และ รฟม. หรือคณะกรรมการตรวจรับพัสดุ ได้ตรวจรับงานถูกต้องครบถ้วนแล้ว

งวดที่ 2 ชำระเงินร้อยละ 45 ของมูลค่าตามสัญญา เมื่อผู้ขายได้ส่งมอบอุปกรณ์และระบบตามข้อ 6 ครบถ้วนสมบูรณ์ และ รฟม. หรือคณะกรรมการตรวจรับพัสดุ ได้ตรวจรับงานถูกต้องครบถ้วนแล้ว

งวดที่ 3 ชำระเงินร้อยละ 30 ของมูลค่าตามสัญญา เมื่อผู้ขายได้ส่งมอบงานตามข้อ 7 ครบถ้วนสมบูรณ์ และ รฟม. หรือคณะกรรมการตรวจรับพัสดุ ได้ตรวจรับงานถูกต้องครบถ้วนแล้ว

13. อัตราค่าปรับ

13.1 กรณีส่งมอบระบบ และ/หรือ อุปกรณ์ ล่าช้าเกินกว่าระยะเวลาที่ได้กำหนดไว้ในข้อ 9 บางรายการหรือทั้งหมด หรือมีคุณสมบัติไม่ถูกต้องตามรายละเอียดและคุณลักษณะที่กำหนด หรือส่งมอบแล้วแต่ยังไม่สามารถใช้งานได้ หรือจัดฝึกอบรมให้แก่เจ้าหน้าที่ รฟม. ล่าช้าเกินกว่ากำหนดในสัญญา รฟม. มีสิทธิบอกเลิกสัญญาได้ ในกรณีที่ รฟม. ไม่ใช้สิทธิบอกเลิกสัญญา ผู้ขายจะต้องชำระค่าปรับให้ รฟม. เป็นรายวัน (เศษของวันให้นับเป็นหนึ่งวัน) ในอัตราร้อยละ 0.1 (ศูนย์จุดหนึ่ง) ของมูลค่าตามสัญญา โดยนับถัดจากวันครบกำหนดส่งมอบตามสัญญาจนถึงวันที่ผู้ขายได้ติดตั้ง จัดฝึกอบรมและส่งมอบระบบ และ/หรือ อุปกรณ์ ที่ได้มาตามสัญญาให้แก่ รฟม. จนถูกต้องครบถ้วน

/13.2 กรณี...

13.2 กรณีที่ผู้ขายไม่เริ่มดำเนินการซ่อมแซมแก้ไขภายในเวลา 4 ชั่วโมง นับแต่เวลาที่ รฟม. ได้แจ้งความชำรุดบกพร่องดังกล่าวตามข้อ 11.2 ผู้ขายยินยอมให้ รฟม. ปรับเป็นรายชั่วโมง ในอัตราชั่วโมงละ 1,200 บาท (หนึ่งพันสองร้อยบาทถ้วน)

13.3 กรณีที่ผู้ขายไม่สามารถซ่อมแซมแก้ไขความชำรุดบกพร่อง หรือขัดข้องของผลิตภัณฑ์ตามรายการในสัญญานี้ตามข้อ 11.1 ผู้ขายจะต้องชำระค่าปรับให้ รฟม. เป็นรายวัน (เศษของวันให้ปรับเป็นหนึ่งวัน) ในอัตราวันละ 6,000 บาท (หกพันบาทถ้วน)

13.4 กรณีที่ รฟม. ใช้สิทธิบอกเลิกสัญญา นอกจากยินยอมให้ รฟม. คิดค่าปรับตามข้อ 13.1 นับแต่วันผิดสัญญาจนถึงวันบอกเลิกสัญญาแล้ว ผู้ขายยินยอมให้ รฟม. ริบหลักประกันสัญญาเป็นจำนวนทั้งหมด หรือแต่บางส่วนก็ได้แล้วแต่ รฟม. จะเห็นสมควร

14. การขอขยายระยะเวลาส่งมอบงาน

ในกรณีที่มีเหตุสุดวิสัยหรือเหตุใดๆ อันเนื่องมาจากความผิดหรือบกพร่องของ รฟม. หรือพฤติการณ์อันหนึ่งอันใดที่ผู้ขายไม่ต้องรับผิดตามกฎหมาย ทำให้ผู้ขายไม่สามารถทำงานให้แล้วเสร็จตามเงื่อนไขและกำหนดเวลาแห่งสัญญานี้ได้ ผู้ขายจะต้องแจ้งเหตุหรือพฤติกรรมดังกล่าวพร้อมหลักฐานเป็นลายลักษณ์อักษรให้ รฟม. ทราบ เพื่อขอขยายเวลาทำงานออกไปภายใน 15 วัน (สิบห้าวัน) นับแต่วันที่เหตุนั้นเกิดขึ้น โดยผู้ขายไม่มีสิทธิเรียกร้องค่าใช้จ่ายเพิ่มเติม

ถ้าผู้ขายไม่ปฏิบัติให้เป็นไปตามความในวรรคหนึ่ง ให้ถือว่าผู้ขายได้สละสิทธิเรียกร้องในการขอขยายเวลาทำงานออกไปโดยไม่มีเงื่อนไขใดๆ ทั้งสิ้น เว้นแต่กรณีเหตุเกิดจากความผิดหรือความบกพร่องของ รฟม. ซึ่งมีหลักฐานชัดแจ้งหรือ รฟม. ทราบดีอยู่แล้วตั้งแต่ต้น

การขยายกำหนดเวลาทำงานตามวรรคหนึ่ง ให้อยู่ในดุลยพินิจของ รฟม. ที่จะพิจารณาตามที่เห็นสมควร

15. ข้อสงวนสิทธิ์ในการยื่นข้อเสนอและอื่นๆ

15.1 เงินสำหรับงานจัดซื้อครั้งนี้ ได้มาจากแหล่งเงินรายได้ของ รฟม.

การลงนามในสัญญาจะกระทำได้ต่อเมื่อ รฟม. ได้รับอนุมัติเงินสำหรับจัดซื้อครั้งนี้จากแหล่งเงินรายได้ของ รฟม.แล้วเท่านั้น

15.2 ถ้าผู้ขายจะต้องสั่งหรือนำสิ่งของดังกล่าวเข้ามาจากต่างประเทศและของนั้นต้องนำเข้ามาโดยทางเรือในเส้นทางที่มีเรือไทยเดินอยู่ และสามารถให้บริการรับขนได้ตามที่รัฐมนตรีว่าการกระทรวงคมนาคมประกาศกำหนด ผู้ยื่นข้อเสนอซึ่งเป็นผู้ขายจะต้องปฏิบัติตามกฎหมายว่าด้วยการส่งเสริมการพาณิชยนาวี ดังนี้

15.2.1 แจ้งการสั่งหรือนำสิ่งของที่ซื้อขายดังกล่าวเข้ามาจากต่างประเทศต่อกรมเจ้าท่าภายใน 7 วัน นับตั้งแต่วันที่ผู้ขายสั่ง หรือซื้อของจากต่างประเทศ เว้นแต่เป็นของรัฐมนตรีว่าการกระทรวงคมนาคมประกาศยกเว้นให้บรรทุกโดยเรืออื่นได้

15.2.2 จัดการให้สิ่งของที่ซื้อขายดังกล่าวบรรทุกโดยเรือไทย หรือเรือที่มีสิทธิเช่นเดียวกับเรือไทย จากต่างประเทศมายังประเทศไทย เว้นแต่จะได้รับอนุญาตจากกรมเจ้าท่า ให้บรรทุกสิ่งของนั้นโดยเรืออื่นที่มิใช่เรือไทย ซึ่งจะต้องได้รับอนุญาตเช่นนั้นก่อนบรรทุกของลงเรืออื่น หรือเป็นของรัฐมนตรีว่าการกระทรวงคมนาคมประกาศยกเว้นให้บรรทุกโดยเรืออื่น

15.2.3 ในกรณีที่ไม่ปฏิบัติตาม 15.2.1 หรือ 15.2.2 ผู้ขายจะต้องรับผิดตามกฎหมายว่าด้วยการส่งเสริมการพาณิชยนาวี

15.3 ผู้ยื่นข้อเสนอซึ่ง รฟม. ได้คัดเลือกแล้ว ไม่ไปทำสัญญาหรือข้อตกลงซื้อเป็นหนังสือภายในเวลาที่กำหนด ดังระบุไว้ในสัญญา รฟม. จะริบหลักประกันการยื่นข้อเสนอ หรือเรียกร้องจากผู้ออกหนังสือค้ำประกันการยื่นข้อเสนอทันที

/และอาจ...

และอาจพิจารณาเรียกร้องให้ชดใช้ความเสียหายอื่น (ถ้ามี) รวมทั้งจะพิจารณาให้เป็นผู้ทิ้งงาน ตามระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ

15.4 รฟม. สงวนสิทธิ์ที่จะแก้ไขเพิ่มเติมเงื่อนไข หรือข้อกำหนดในแบบสัญญาหรือข้อตกลงซื้อเป็นหนังสือ ให้เป็นไปตามความเห็นของสำนักงานอัยการสูงสุด (ถ้ามี)

15.5 ในกรณีที่เอกสารใดๆ ที่เกี่ยวข้องกับการยื่นข้อเสนอครั้งนี้ มีความขัดแย้งกัน ผู้ยื่นข้อเสนอจะต้องปฏิบัติตามคำวินิจฉัยของ รฟม. คำวินิจฉัยดังกล่าวให้ถือเป็นที่สุด และผู้ยื่นข้อเสนอไม่มีสิทธิเรียกร้องค่าใช้จ่ายใดๆ เพิ่มเติม

15.6 รฟม. อาจประกาศยกเลิกการจัดซื้อในกรณีต่อไปนี้ได้ โดยที่ผู้ยื่นข้อเสนอจะเรียกร้องค่าเสียหายใดๆ จาก รฟม. ไม่ได้

15.6.1 รฟม. ไม่ได้รับการจัดสรรเงินที่ใช้ในการจัดซื้อหรือที่ได้รับจัดสรร แต่ไม่เพียงพอที่จะทำการจัดซื้อครั้งนี้ต่อไป

15.6.2 มีการกระทำที่เข้าลักษณะผู้ยื่นข้อเสนอที่ชนะการจัดซื้อหรือที่ได้รับการคัดเลือกมีผลประโยชน์ร่วมกัน หรือมีส่วนได้สียกับผู้ยื่นข้อเสนอรายอื่น หรือขัดขวางการแข่งขันอย่างเป็นธรรม หรือสมยอมกันกับผู้ยื่นข้อเสนอรายอื่น หรือเจ้าหน้าที่ในการเสนอราคา หรือส่อว่ากระทำการทุจริตอื่นใดในการเสนอราคา

15.6.3 การทำการจัดซื้อครั้งนี้ต่อไปอาจก่อให้เกิดความเสียหายแก่ รฟม. หรือกระทบต่อประโยชน์สาธารณะ

15.6.4 กรณีอื่นในทำนองเดียวกับ 15.6.1, 15.6.2 และ 15.6.3 ตามที่กำหนดในกฎกระทรวง ซึ่งออกตามความในกฎหมายว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ

15.7 ผู้ขายที่เข้าถึงระบบเทคโนโลยีสารสนเทศของ รฟม. ต้องปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของ รฟม. และจะต้องรักษาความลับต่างๆ ที่ได้จากการปฏิบัติงานโดยห้ามมิให้ผู้ขายนำข้อมูลส่วนหนึ่งส่วนใดหรือทั้งหมดที่ได้จากการปฏิบัติงานใน รฟม. ไปทำซ้ำ เผยแพร่ หรือวิเคราะห์ประมวลผลเพื่อการอื่นใด ไม่ว่าการกระทำดังกล่าวจะเป็นการหาผลประโยชน์หรือไม่ก็ตาม หาก รฟม. ตรวจพบผู้ขายจะต้องชดใช้ค่าเสียหายเป็นจำนวนเงินไม่น้อยกว่ามูลค่าทั้งหมดที่กำหนดไว้ในสัญญา ทั้งนี้ การรักษาความลับให้มีผลนับตั้งแต่วันที่ลงนามในสัญญานี้ และมีผลอยู่ตลอดไปแม้ว่าสัญญานี้ครบกำหนดระยะเวลา หรือสิ้นสุดลงไม่ว่าด้วยเหตุผลใดๆ

15.8 รฟม. มีสิทธิในการตรวจสอบการเข้าถึงข้อมูล และมีสิทธิในการยกเลิกการให้สิทธิต่างๆ แก่เจ้าหน้าที่ที่ผู้ขายส่งเข้ามาปฏิบัติงาน

15.9 ระบบปฏิบัติการและซอฟต์แวร์ที่ผู้ขายจัดหาเพื่อใช้ในโครงการนี้ทั้งหมด รฟม. ต้องได้รับเอกสารสิทธิ (Software License) และ/หรือ สิทธิการใช้งานได้อย่างถูกต้องตามกฎหมาย โดยเอกสารสิทธิดังกล่าว รฟม. จะเป็นเจ้าของเอกสารสิทธิทั้งหมด

****

หมายเลขโทรศัพท์ติดต่อเพื่อขอทราบข้อมูลเพิ่มเติม 02-716-4000 ต่อ 2540, 1454