ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและราคากลาง (ราคาอ้างอิง)

ในการจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง

1. ชื่อโครงการ **การจัดหาผู้ให้บริการระบบป้องกันการบุกรุกเครือข่าย** (Intrusion Prevention System Service)

   /หน่วยงานเจ้าของโครงการ **ฝ่ายเทคโนโลยีสารสนเทศ**

2. วงเงินงบประมาณที่ได้รับจัดสรร **800,000.- บาท (แปดแสนบาทถ้วน)**

3. วันที่กำหนดราคากลาง (ราคาอ้างอิง) 14 ต.ค. 2557

   เป็นเงิน 800,000.- บาท (แปดแสนบาทถ้วน) ราคา/หน่วย (ถ้ามี) - บาท

4. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)

   4.1 **บริษัท ดาต้าโปร คอมพิวเตอร์ ซิสเต็มส์ จำกัด**

   4.2 บริษัท พอยท์ ไอที คอนซัลทิ่ง จำกัด

5. รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง) ทุกคน

5.1	นายบุญลักษณ์	ฉวีวงศ์วิวัฒน์	ผู้ช่วยผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ
5.2	นายวันชัย	เทพพิชัยยานนท์	ผู้บริหารส่วนบริการและปฏิบัติการ เทคโนโลยีสารสนเทศ ฝ่ายเทคโนโลยีสารสนเทศ
5.3	นางอุรสา	พงษ์เสรี	ผู้บริหารส่วนจัดซื้อ ฝ่ายธุรการ

ผนวก 1
ขอบเขตงาน และเงื่อนไขการให้บริการ
การจัดหาผู้ให้บริการระบบป้องกันการบุกรุกเครือข่าย

---

1. ข้อกำหนดทั่วไป

1.1 ต้องเสนอราคาค่าบริการระบบป้องกันการบุกรุกเครือข่าย ซึ่งรวมถึงการจัดหา Hardware และ Software เพื่อบริหารจัดการระบบ การปรับปรุงรูปแบบของการป้องกันการบุกรุกเครือข่ายที่มีอยู่เดิมให้เป็นรูปแบบใหม่ การติดตั้ง การทดสอบ การรับประกันการใช้งาน สิทธิการใช้งาน การฝึกอบรม คู่มือและเอกสารสนับสนุนการใช้งาน ตลอดจนการดำเนินการอื่น ๆ ที่จำเป็น รวมถึงการดูแลและบริหารจัดการระบบให้สามารถทำงานได้อย่างมีประสิทธิภาพ ตลอดระยะเวลา 1 ปี

1.2 ต้องทำการปรับปรุงรูปแบบของการป้องกันการบุกรุกเครือข่ายที่มีอยู่เดิม (Tipping Point IPS) ให้เป็นรูปแบบใหม่ เพื่อให้การทำงานเป็นไปอย่างมีประสิทธิภาพสูงสุด

1.3 ต้องเสนอระบบป้องกันการบุกรุกเครือข่าย ที่สามารถทำงานร่วมกับระบบเครือข่าย (Network) ระบบเครื่องคอมพิวเตอร์แม่ข่าย (Server) ระบบจัดเก็บข้อมูล (SAN) ระบบการสำรองข้อมูล (Backup) และระบบการรักษาความปลอดภัยของระบบสารสนเทศ (Security) ของธนาคารได้อย่างมีประสิทธิภาพ

2. ระบบป้องกันการบุกรุกเครือข่ายมีรายการ จำนวน และคุณลักษณะด้านเทคนิคขั้นต่ำ ดังนี้

2.1 เครื่องคอมพิวเตอร์แม่ข่าย เพื่อบริหารจัดการระบบฯ จำนวน 1 ชุด โดยมีคุณสมบัติขั้นต่ำ ดังนี้

2.1.1 มีหน่วยประมวลผล (CPU) แบบ Quad Core Intel Xeon ทำงานที่สัญญาณนาฬิกาไม่น้อยกว่า 2.0 GHz

2.1.2 มีหน่วยความจำหลัก (RAM) ขนาดไม่น้อยกว่า 24 GB

2.1.3 มีหน่วยความจำสำรองแบบจานแม่เหล็ก (Hard Disk) ที่มีความจุรวมหลังการทำ Raid1 หรือ Raid5 ไม่น้อยกว่า 1 TB

2.1.4 มี Power Supply แบบ Redundant Power Supply

2.1.5 มีระบบปฏิบัติการที่มีลิขสิทธิ์การใช้งานถูกต้องตามกฎหมาย

2.1.6 มีพอร์ตเชื่อมต่อเครือข่าย (Network Interface) แบบ Gigabit Ethernet จำนวนไม่น้อย 4 พอร์ต

2.2 อุปกรณ์ป้องกันการบุกรุกเครือข่าย (IPS) จำนวน 1 ระบบ มีคุณสมบัติอย่างน้อย ดังนี้

2.2.1 ต้องเป็น Hardware Appliance ที่ถูกออกแบบมาเพื่อทำหน้าที่ เป็นอุปกรณ์ป้องกันการบุกรุกเครือข่าย IPS (Intrusion Prevention System) โดยเฉพาะ

2.2.2 ต้องไม่เป็นอุปกรณ์ลักษณะ UTM (Unified Threat Management)

2.2.3 มีหน่วยประมวลผลแบบ ASIC (Application-specific integrated circuit หรือ x86 Architecture4

2.2.4 สามารถทำงานแบบทดแทนกันได้ (High Availability)

2.2.5 สามารถทำ Hardware Bypass ในกรณี Hardware หรือ Software เกิดปัญหา โดยสามารถเลือก Fail-open หรือ Fail-Close ในแต่ละ segment ได้

2.2.6 มี IPS Throughput ไม่น้อยกว่า 1 Gbps

2.2.7 รองรับ Concurrent connection ได้พร้อมกันไม่ต่ำกว่า 750,000 Connection

2.2.8 สามารถติดตั้งในตู้ Rack ขนาดมาตรฐาน 19 นิ้วได้

2.2.9 สามารถรองรับการทำงานดังต่อไปนี้ได้

2.2.9.1 In-Line

2.2.9.2 SPAN Port

2.2.9.3 TAP

2.2.10 มี Interface Gigabit Ethernet ชนิด 1000BaseTX (10/100/1000) ไม่น้อยกว่า 8 พอร์ท

2.2.11 รองรับการใช้งานได้ไม่น้อยกว่า 4 Segment

2.2.12 มีพอร์ตสำหรับการบริหารจัดการตัวอุปกรณ์ (Management Port) แยกออกมาต่างหาก โดยไม่รวมกับพอร์ตที่ใช้ในการเฝ้าดูแลการบุกรุกและใช้งาน

2.2.13 สามารถป้องกันการบุกรุกในรูปแบบดังต่อไปนี้ได้

2.2.13.1 Worms

2.2.13.2 Viruses

2.2.13.3 Trojans

2.2.13.4 Phishing

2.2.13.5 Spyware

2.2.13.6 VoIP

2.2.13.7 Botnets

2.2.13.8 DoS

2.2.13.9 DDoS

2.2.13.10 Backdoors

2.2.14 สามารถป้องกันการโจมตีแบบ Zero-day ได้

2.2.15 สามารถตรวจสอบและป้องกันการโจมตีที่มีการเข้ารหัสด้วย SSL encryption ได้ครบทุก Segments

2.2.16 สามารถกำหนดรูปแบบการทำงานของ Action กับ Event ที่เกิดขึ้นดังต่อไปนี้ได้

2.2.16.1 Alert

2.2.16.2 Block

2.2.16.3 Log

2.2.17 สามารถกำหนดรูปแบบของการ Update signature ดังต่อไปนี้ได้

2.2.17.1 Manual

2.2.17.2 Automatic

2.2.18 สามารถแจ้งเตือนการบุกรุกดังต่อไปนี้ได้

2.2.18.1 E-Mail

2.2.18.2 SNMP

2.2.18.3 SYSLOG

2.2.19 สามารถทำงานร่วมกับ Packet encapsulation decoding ได้ดังนี้

2.2.19.1 IPv6

2.2.19.2 V4-in-V4, V4-in-V6, V6-in-V4 และ V6-in-V6 tunnels

2.2.19.3 MPLS

2.2.19.4 GRE

2.2.19.5 Q-in-Q Double VLAN

2.2.20 สามารถสร้างรายงาน และจัดส่งรายงานผ่านทางอีเมล์โดยอัตโนมัติในรูปแบบต่อไปนี้ได้

2.2.20.1 Daily

2.2.20.2 Weekly

2.2.20.3 Monthly

2.2.21 สามารถนำออกรายงาน (Export) ในรูปแบบมาตรฐานดังต่อไปนี้ได้

2.2.21.1 PDF

2.2.21.2 CSV

2.2.21.3 HTML

2.3 บริการระบบป้องกันการบุกรุกเครือข่ายที่เสนอ ผู้เสนอราคาต้องเป็นผู้มีสิทธิในการใช้งานได้อย่างถูกต้องตามกฎหมาย และต้องจัดให้ธนาคารมีสิทธิใช้งานได้โดยไม่ละเมิดลิขสิทธิ์ของผู้อื่น รวมทั้งรับผิดชอบในกรณีที่มีการกล่าวหาฟ้องร้องหรือเรียกค่าเสียหายใด ๆ จากเจ้าของลิขสิทธิ์หรือผู้เรียกร้องอื่นใด

3. **การให้การสนับสนุนระหว่างการใช้บริการ** (Support)

3.1 ตลอดระยะเวลาการให้บริการผู้เสนอราคาที่ได้รับการคัดเลือกต้องจัดให้มีพนักงานที่มีความรู้ความชำนาญเกี่ยวกับระบบป้องกันการบุกรุกเครือข่าย พร้อมหมายเลขโทรศัพท์ที่สามารถติดต่อได้สะดวก เพื่อให้คำปรึกษา ตอบข้อซักถาม ให้ความช่วยเหลือหรือแก้ไขปัญหาเบื้องต้น (On Phone Support) ทุกวันตลอด 24 ชั่วโมง

3.2 หากระบบป้องกันการบุกรุกเครือข่าย เกิดเหตุขัดข้อง ชำรุด หรือมีข้อบกพร่องและธนาคารเห็นว่าการให้ความช่วยเหลือตามข้อ 3.1 ไม่อาจแก้ไขปัญหาได้ ผู้เสนอราคาที่ได้รับการคัดเลือกต้องเข้าดำเนินการตรวจสอบ แก้ไข ปรับปรุง ระบบป้องกันการบุกรุกเครือข่าย แบบ Onsite Service (24 x 7) ณ สถานที่ติดตั้งตามวิธีการ และ/หรือช่องทางแก้ไขที่มีประสิทธิภาพมากกว่า โดยจะต้องดำเนินการดังนี้

3.2.1 ติดต่อกลับธนาคารภายใน 4 ชั่วโมง นับจากที่ได้รับแจ้งเหตุจากธนาคาร

3.2.2 แก้ไขเหตุขัดข้อง ความชำรุดบกพร่องหรือนำอุปกรณ์ชุดสำรองที่มีประสิทธิภาพไม่ด้อยกว่าเดิม ส่งมอบและติดตั้งให้ธนาคารใช้งานทดแทนระบบป้องกันการบุกรุกเครือข่ายที่ชำรุด เพื่อให้ใช้งานได้ตามความต้องการภายใน 24 ชั่วโมง นับจากที่ได้รับแจ้งเหตุจากธนาคาร

4. **ด้านการฝึกอบรม**

4.1 ต้องจัดฝึกอบรมการใช้งานและจัดทำเอกสารให้กับเจ้าหน้าที่ผู้ดูแลระบบของธนาคาร โดยรองรับผู้เข้ารับการฝึกอบรมได้ไม่น้อยกว่า 3 คน

4.2 จัดทำคู่มืออย่างน้อยรายการละ 1 ชุด ดังต่อไปนี้

4.2.1 คู่มือการ Configure

4.2.2 คู่มือการ Backup/Restore

4.2.3 คู่มือการใช้งานระบบ