ร่างขอบเขตงาน (Term of Reference)

ประกวดราคาซื้อโครงการปรับปรุงอุปกรณ์เพื่อรองรับการดำเนินงานด้านความมั่นคงปลอดภัย ให้สอดคล้องตามระเบียบ และ พ.ร.บ. ต่างๆ

.....

1. ความเป็นมา

ตามแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร พ.ศ. 2557 – 2558 ของโรงงานไพ่ กรมสรรพสามิต นั้น มีโครงการปรับปรุงอุปกรณ์เพื่อรองรับการดำเนินงานด้านความมั่นคงปลอดภัยให้สอดคล้องตามระเบียบ และ พ.ร.บ. ต่างๆ เพื่อปรับปรุง และควบคุมกระบวนการดำเนินงานด้านสารสนเทศภายในองค์กร ให้รองรับมาตรฐาน IPV6 และสอดคล้องตาม ระเบียบ และ พ.ร.บ. ต่างๆ ด้านเทคโนโลยีสารสนเทศ ให้มีประสิทธิภาพมากยิ่งขึ้นและสามารถตอบสนองต่อการบริหารการเปลี่ยนแปลงภายในองค์กรและเทคโนโลยีได้ทันท่วงที จึงได้มีการโครงการปรับปรุงอุปกรณ์เพื่อรองรับการดำเนินงานด้านความมั่นคงปลอดภัยให้สอดคล้องตามระเบียบ และ พ.ร.บ. ต่างๆ ดังนี้

2. วัตถุประสงค์

ปรับปรุงอุปกรณ์เพื่อรองรับการดำเนินงานด้านความมั่นคงปลอดภัยให้สอดคล้องตามระเบียบ และ พ.ร.บ. ต่างๆ

3. คุณสมบัติผู้เสนอราคา

3.1 ผู้ประสงค์จะเสนอราคาต้องเป็นนิติบุคคลผู้มีอาชีพขายพัสดุที่ประกวดราคาซื้อด้วยวิธีการทางอิเล็กทรอนิกส์

3.2 ผู้ประสงค์จะเสนอราคาต้องไม่เป็นผู้ที่ถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานของทางราชการและได้แจ้งเวียนชื่อแล้วหรือไม่เป็นผู้ได้รับผลของการสั่งให้นิติบุคคลหรือบุคคลอื่นเป็นผู้ทิ้งงานตามระเบียบของทางราชการ

3.3 ผู้ประสงค์จะเสนอราคาต้องไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ประสงค์จะเสนอราคาได้มีคำสั่งให้สละสิทธิ์และความคุ้มกันเช่นว่านั้น

3.4 ผู้ประสงค์จะเสนอราคาต้องไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ประสงค์จะเสนอราคารายอื่น และต้องไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ให้บริการตลาดกลางอิเล็กทรอนิกส์ ณ วันประกาศประกวดราคาซื้อด้วยวิธีการทางอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรม ตามข้อ 1.6

3.5 ผู้ประสงค์จะเสนอราคาต้องผ่านการคัดเลือกผู้มีคุณสมบัติเบื้องต้นในการซื้อของโรงงานไพ่ กรมสรรพสามิต

3.6 ผู้ประสงค์จะเสนอราคาจะต้องแสดงแคตตาล็อกและจัดทำเอกสารประกอบรายละเอียดพัสดุดังกล่าวพร้อมคุณสมบัติ ประกอบต่างๆและ/หรือคุณสมบัติอื่นๆที่ดีกว่าหรืออุปกรณ์พิเศษอื่นๆประกอบเพิ่มเติม

3.7 ผู้ประสงค์จะเสนอราคาต้องเป็นเจ้าของผลิตภัณฑ์ที่นำเสนอหรือต้องได้รับอนุญาตจากบริษัทเจ้าของผลิตภัณฑ์ที่เสนอให้เป็นตัวแทนจำหน่าย (Agent) ในประเทศไทย หรือได้รับการรับรองจากตัวแทนจำหน่ายในประเทศไทยที่ได้รับการแต่งตั้ง ให้เป็นผู้แทนจำหน่าย (Dealer) ในประเทศไทยโดยต้องยื่นเอกสารหลักฐานที่สามารถตรวจสอบและเชื่อถือได้มาพร้อมในวันยื่นข้อเสนอทางเทคนิค เพื่อประกอบการพิจารณา

3.8 ผู้ประสงค์จะเสนอราคาจะต้องยืนยันว่าพัสดุที่เสนอเป็นรุ่นที่ยังอยู่ในสายการผลิตในวันที่ยื่นซองประกวดราคา และเป็นของแท้ของใหม่ไม่เคยใช้งานมาก่อนไม่เป็นของเก่าเก็บอยู่ในสภาพที่จะใช้งานได้ทันทีไม่เป็นเครื่องที่ถูกนำมาปรับปรุงสภาพใหม่ (Reconditioned หรือ Rebuilt) และมีคุณลักษณะเฉพาะตรงตามที่กำหนดไว้ในเอกสารประกวดราคาและไม่ด้อยกว่าข้อกำหนด เงื่อนไขต่างๆ ที่ระบุไว้

3.9 อุปกรณ์รายการต่างๆ ที่เสนอต้องสามารถทำงานร่วมกับเครื่องคอมพิวเตอร์และระบบเครือข่ายเดิมของโรงงานไพ่ กรมสรรพสามิต ได้อย่างมีประสิทธิภาพ

3.10 ผู้ประสงค์จะเสนอราคาต้องจัดทำเอกสารแสดงการเปรียบเทียบรายละเอียด ข้อเสนอด้านคุณลักษณะเฉพาะของการปรับปรุง และควบคุมกระบวนการดำเนินงานด้านสารสนเทศภายในองค์กร ให้รองรับมาตรฐาน IPV6 และสอดคล้องตาม ระเบียบ และ พ.ร.บ. ต่างๆ ตามเอกสารการประกวดราคาซื้อด้วย วิธีการทางอิเล็กทรอนิกส์ จำนวน 2 ชุด โดยให้จัดทำในรูปแบบ ดังนี้

หัวข้อ	รายละเอียดของคุณลักษณะเฉพาะของการปรับปรุง และควบคุมกระบวนการดำเนินงานด้านสารสนเทศภายในองค์กร ให้รองรับมาตรฐาน IPV6 และสอดคล้องตาม ระเบียบ และ พ.ร.บ. ต่างๆ	ข้อเสนอของบริษัท	เอกสารอ้างอิง
ระบุหัวข้อให้ตรงกับที่โรงงานไพ่ กรมสรรพสามิต กำหนด	ให้คัดลอกคุณลักษณะเฉพาะของการปรับปรุง และควบคุมกระบวนการดำเนินงานด้านสารสนเทศภายในองค์กร ให้รองรับมาตรฐาน IPV6 และสอดคล้องตาม ระเบียบ และ พ.ร.บ. ต่างๆ	ให้ระบุคุณลักษณะเฉพาะของการปรับปรุง และควบคุมกระบวนการดำเนินงานด้านสารสนเทศภายในองค์กร ให้รองรับมาตรฐาน IPV6 และสอดคล้องตาม ระเบียบ และ พ.ร.บ. ต่างๆ ที่เสนอและตรงตามวัตถุประสงค์การใช้งานของโรงงานไพ่ กรมสรรพสามิต โดยไม่ด้อยกว่าข้อกำหนด เงื่อนไขต่างๆ ที่ระบุไว้	ให้ระบุหรืออ้างอิง ถึงเอกสารในข้อเสนอที่เกี่ยวข้องและขีดเส้นใต้ คุณลักษณะที่เสนอในแคตตาล็อกหรือเอกสารที่เกี่ยวข้อง

3.11 บุคคลหรือนิติบุคคลที่จะเข้าเป็นคู่สัญญาต้องไม่อยู่ในฐานะเป็นผู้ไม่แสดงบัญชีรายรับรายจ่าย หรือแสดงบัญชีรายรับรายจ่ายไม่ถูกต้องครบถ้วนในสาระสำคัญ

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

3.13 คู่สัญญาต้องรับจ่ายเงินผ่านบัญชีเงินฝากกระแสรายวัน เว้นแต่การรับจ่ายเงินแต่ละครั้งซึ่งมีมูลค่าไม่เกินสามหมื่นบาทคู่สัญญาอาจรับจ่ายเป็นเงินสดก็ได้

4. รายการปรับปรุง และควบคุมกระบวนการดำเนินงานด้านสารสนเทศภายในองค์กร ให้รองรับมาตรฐาน IPV6 และสอดคล้องตาม ระเบียบ และ พ.ร.บ. ต่างๆ

4.1 ระบบปรับเทียบเวลา	จำนวน 1 ชุด
4.2 อุปกรณ์จัดเก็บ Log	จำนวน 1 ชุด
4.3 อุปกรณ์ป้องกันการบุกรุก (Intrusion Prevention System : IPS) ภายนอกองค์กร(External IPS)	จำนวน 1 ชุด
4.4 อุปกรณ์ป้องกันการบุกรุก (Intrusion Prevention System : IPS) ภายในองค์กร(Internal IPS)	จำนวน 1 ชุด
4.5 อุปกรณ์ไฟร์วอลล์สำหรับป้องกันเว็บแอพพลิเคชั่น (Web Application Firewall : WAF)	จำนวน 1 ชุด
4.6 อุปกรณ์ Core/Distributed Switch เพื่อรองรับ IPV6	จำนวน 1 ชุด
4.7 อุปกรณ์กระจายสัญญาณ (L3 Switch)	จำนวน 4 ชุด

5. รายละเอียดคุณลักษณะเฉพาะรายการปรับปรุง และควบคุมกระบวนการดำเนินงานด้านสารสนเทศภายในองค์กร ให้รองรับมาตรฐาน IPV6 และสอดคล้องตาม ระเบียบ และ พ.ร.บ. ต่างๆ

5.1 ระบบปรับเทียบเวลา จำนวน 1 ชุด

5.1.1 เป็นอุปกรณ์ที่รับสัญญาณเวลาจากดาวเทียม GPS และให้บริการเวลามาตรฐานแก่ระบบคอมพิวเตอร์และอุปกรณ์เครือข่ายที่รองรับ NTP ,SNTP Protocol โดยตัวเครื่องมีอุปกรณ์เสาอากาศและสายนำสัญญาณมาพร้อมกันกับเครื่อง

5.1.2 มี Port แบบ 10Base-T/100Base-TX อย่างน้อย 1 Port

5.1.3 มี Serial Port RS-232 สำหรับตั้งค่าและมี Dual USB ports สำหรับเชื่อมต่อเพื่อ back up และ restore ค่า configuration ได้

5.1.4 มีลักษณะการทำงานได้ทั้งแบบ Stratum 1 และ Stratum 2

5.1.5 สามารถรับสัญญาณดาวเทียมได้12 Channel หรือดีกว่าและรองรับ Single Satellite Timing

5.1.6 รองรับระบบ Internet Protocol ได้ทั้ง IPv4 และ IPv6

5.1.7 รองรับ NTP request ไม่ต่ำกว่า 3,200 requests ต่อ 1 วินาที

5.1.8 มีค่าความแม่นยำของ GPS เท่ากับหรือดีกว่า 50 nanosecond

5.1.9 มีค่า client synchronization accuracy on LAN อยู่ระหว่าง 0.5-2 millisecond

5.1.10 มีค่าความเสถียร Holdover accuracy ของสัญญาณนาฬิกาไม่เกิน 21 millisecond ต่อวันเมื่อไม่สามารถรับสัญญาณ GPS ได้

5.1.11 สามารถทำงานในระบบ Stratum 2 กับ NTP server เครื่องอื่นได้อัตโนมัติเมื่อสัญญาณ GPS เกิดขัดข้อง

5.1.12 หน้าเครื่อง (Front Panel) มีไฟ LED แบบสามสีแสดงสถานการณ์ทำงาน Sync. สถานะ Network ,NTP activity และ Alarm ได้

5.1.13 มี Secure Web-base Management และ NTP Client Software

5.1.14 รองรับโปรโตคอล SNMP v3 ,Custom MIB ,Telnet และมีโปรโตคอลรักษาความปลอดภัย SSH,SSL,HTTPS , หรือดีกว่า

5.1.15 รองรับ Network Protocol ดังต่อไปนี้ NTP(v2,v3 ,v4),NTP Unicast/Multicast/Broadcast,SNTP,TIME,DAYTIME,MD5Authentication ,HTTP,DHCP,SNMPv3,IPv4 ,IPv6,

5.1.16 ใช้กับระบบไฟฟ้าของประเทศไทย 220 VAC 50-60 Hz ได้โดยไม่ใช้อุปกรณ์เพิ่ม

5.1.17 เป็นอุปกรณ์ที่สามารถติดตั้งในตู้ Rack 19 นิ้วได้โดยไม่ต้องดัดแปลงเพิ่ม

5.1.18 รองรับมาตรฐานความปลอดภัย UL ,CE(RoHS),PSE,China RoHS และ FCC

5.2 อุปกรณ์จัดเก็บ Log จำนวน 1 ชุด

5.2.1 เป็นอุปกรณ์ Appliance หรือsoftware Appliance ที่สามารถเก็บรวบรวมเหตุการณ์ (logs or Events)ที่เกิดขึ้นในอุปกรณ์ที่เป็น appliances และ non-appliances เช่น Firewall, Network Devicesต่าง ๆ, ระบบปฏิบัติการ, ระบบ appliances, ระบบเครือข่าย และระบบฐานข้อมูล เป็นต้น ได้อย่างน้อย 15 อุปกรณ์ต่อระบบ โดยสามารถแสดงผลอยู่ภายใต้รูปแบบ (format) เดียวกันได้

5.2.2 สามารถจัดเก็บ log file ได้ถูกต้อง ตรงตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

5.2.3 มีระบบ Search Engine ที่คล้ายกับการค้นหาข้อมูลผ่านทาง Google (Google like) ที่ช่วยให้การค้นหาข้อมูลจราจรทางคอมพิวเตอร์ที่ต้องการเป็นไปอย่างรวดเร็ว และรองรับการค้นหาโดยใช้ Common Search Syntax เช่น Boolean operators, wild cards, regular expressions เป็นต้น

5.2.4 สามารถตรวจสอบข้อมูลจราจรทางคอมพิวเตอร์ตามความต้องการ (Monitor Logs and Events) โดยแจ้งเตือนเมื่อมีข้อมูลจราจรทางคอมพิวเตอร์ที่ต้องการตรวจสอบเกิดขึ้นของเครือข่าย ผ่านทาง Email, SNMP, JMS (JAVA Messaging Service) และ Batch Script ได้

5.2.5 สามารถเก็บ Log File ในรูปแบบ Syslog ของอุปกรณ์ เช่น Router, Switch, Firewall, VPN, Server เป็นต้น ได้

5.2.6 สามารถรองรับการแจ้งเตือน (Alert) ในรูปแบบอีเมลล์ ได้เป็นอย่างน้อย

5.2.7 สามารถจัดเก็บข้อมูลเหตุการณ์ต่อวินาที (Events per Seconds) ได้ไม่น้อยกว่า 20,000 eps หรือไม่น้อยกว่า 2 GB ต่อวัน

5.2.8 สามารถทำการ Authentication ผู้ใช้งานผ่าน Active Directory หรือ Local Database ได้

5.2.9 มีระบบการเข้ารหัสข้อมูลเพื่อใช้ยืนยันความถูกต้องของข้อมูลที่จัดเก็บตามมาตรฐาน MD5 หรือ SHA-1 หรือดีกว่า

5.2.10 สามารถจัดทำรายงานในรูปแบบตาราง และ Graphic ได้หลายแบบ ได้แก่ Line Chart, Bar Chart, Pie Chart ได้อย่างน้อย

5.2.11 สามารถสร้างรายงาน (Report) ตามประเภทต่างๆ ดังต่อไปนี้:

5.2.11.1 Columns distinct value aggregation (group by) Report

5.2.11.2 Complex computation and statics Report

5.2.11.3 automatic content analysis Report

5.2.11.4 events similarity Report

5.2.11.5 Compliance Report

5.2.12 สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS, Command Line Interface และ Secure Shell (SSH) ได้

5.2.13 สามารถทำการสำรองข้อมูล (Data Back up) ไปยังอุปกรณ์จัดเก็บข้อมูลภายนอก เช่น Tape หรือ DVD หรือ External Storage เป็นต้น ได้

5.2.14 สามารถติดตั้งในตู้ Rack มาตรฐาน 19 นิ้ว

5.3 อุปกรณ์ป้องกันการบุกรุก (Intrusion Prevention System : IPS) ภายนอกองค์กร (External IPS) จำนวน 1 ชุด

5.3.1 เป็นอุปกรณ์ (Hardware Appliance) ที่ออกแบบมาเพื่อป้องกันการบุกรุกทางเครือข่าย (Intrusion Prevention System) และทำงานบน Tilera multicore processor Architecture โดยไม่มี Hard drive ภายในอุปกรณ์ และไม่ใช่อุปกรณ์ UTM (Unified Threat Management)

5.3.2 มี Network Interface แบบ Copper Ethernet ports (10BASE-T/100BASE-TX/1000BASE-T) ไม่น้อยกว่า 8 พอร์ต

5.3.3 มี Management Port แบบ 10/100/1000 Mbps ไม่น้อยกว่า 4 พอร์ต

5.3.4 สามารถทำงานได้ในโหมด Passive และ In-line หรือ ดีกว่า

5.3.5 รองรับการตรวจจับและป้องกันการโจมตีเครือข่ายได้ไม่น้อยกว่า 4 Network Segments

5.3.6 รองรับ Throughput ได้ไม่น้อยกว่า 2.4 Gbps และมีค่าความช้า (Typical Latency) ไม่เกิน 50 uSec

5.3.7 รองรับจำนวนการเชื่อมต่อพร้อมกัน (Concurrent Connection) ไม่น้อยกว่า 1,000,000 Connections ต่อวินาที

5.3.8 สามารถป้องกันการโจมตีชนิดฉับพลัน (Denial of Service Attacks) เช่น SYN Flood ได้ไม่น้อยกว่า 1,000,000 SYN ต่อวินาที

5.3.9 มีความสามารถทำงานแบบอุปกรณ์ firewall เช่น รองรับการทำ firewall policy และstatefull firewall บนตัวอุปกรณ์เพื่อเป็นการป้องกันการโจมตีได้อย่างมีประสิทธิภาพและลดการทำงานของอุปกรณ์ firewall เดิมของเครือข่าย

5.3.10 สามารถป้องกันการเจาะระบบ (Exploits) เข้ามาที่จุดอ่อนและช่องโหว่ (Vulnerabilities)

5.3.11 สามารถทำ Deep File Inspection เพื่อป้องกันการโจมตีในระดับ File เช่น MS-Word Exploits หรือมีความสามารถในการตรวจจับไวรัสคอมพิวเตอร์ที่แฝงมากับไฟล์

5.3.12 สามารถ Block การใช้งาน Applications ที่ไม่พึงประสงค์เช่น Bit Torrent, eDonkey, Skype และ FastTrack ได้เป็นอย่างน้อย

5.3.13 รองรับการทำ Application Rate Limits และ Connection Limits

5.3.14 สามารถตรวจสอบการโจมตีจาก Vulnerability Signatures และ Attack Signatures

5.3.15 รองรับการทำ Protocol และ File Validation เพื่อตรวจสอบความผิดปกติของ Protocol และ File

5.3.16 สามารถป้องกันภัยคุกคามสำหรับระบบ VoIP

5.3.17 สามารถตรวจจับวิธีการบุกรุกและป้องกันเครือข่ายได้อย่างน้อยดังนี้ Signature matching, Protocol / Packet Anomalies, Statistical anomaliesหรือ Application anomalies, Overflow, Worm, Virus, Backdoor Program, Trojan Horse, Port Scanning, Spy ware, Packet Analysis, DoS, DDoS

5.3.18 สามารถทำการตรวจสอบ Traffic อย่างละเอียด (Deep Packet Inspection) โดยตรวจสอบ โปรโตคอล HTTP, FTP, DNS, SMTP, Telnet, SSH, MS-RPC และ MS-CIFS ได้เป็นอย่างน้อย

5.3.19 สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS หรือ SSH ได้เป็นอย่างน้อย

5.3.20 มี Application เฉพาะสำหรับเก็บ Log ของอุปกรณ์ IPS พร้อมระบบในการทำ Report และ Analyze ข้อมูล (Forensic) ของอุปกรณ์ IPS รวมถึงสามารถแจ้งเตือนในกรณีที่เกิดภัยคุกคามให้เจ้าหน้าที่ดูแลระบบทราบได้

5.3.21 สามารถส่ง Log ออกมาเก็บที่อุปกรณ์เก็บบันทึก Log ภายนอกได้ เช่น SIM หรือ SIEM

5.3.22 มีระบบในการทำรายงาน (Report) โดยเฉพาะแยกออกจากตัวอุปกรณ์ IPS ประกอบด้วยความสามารถ ดังต่อไปนี้

5.3.22.1 ระบบสามารถส่ง Report ทาง Email ได้โดยอัตโนมัติ

5.3.22.2 มี Dashboard ในการเฝ้าระวัง (Monitor) Security Event ที่ตรวจจับโดยอุปกรณ์IPS แบบ Real-time

5.3.22.3 มีระบบในการทำ Forensic เพื่อวิเคราะห์ Security Eventที่ตรวจจับโดยอุปกรณ์ IPS

5.3.23 รองรับการ Update IPS Signature

5.3.24 สามารถทำงานได้อย่างต่อเนื่อง (Bypass Traffic) โดยช่องสัญญาณ In-Line Mode สามารถรับส่งข้อมูลได้ตามปกติ เมื่ออุปกรณ์เกิดปัญหา

5.3.25 รองรับการทำการสำรองระบบ(High Availability)แบบ Active-Active หรือ Active/Standby

5.3.26 รองรับการทำงานแบบ Protection Cluster เพื่อรองรับการขยายการใช้งานได้ในอนาคต

5.3.27 มีระบบสำรองไฟแบบ Redundant Hot-swappable Power Supply

5.3.28 สามารถใช้งานตามมาตรฐาน IPv6 ได้

5.3.29 อุปกรณ์ที่นำเสนอต้องผ่านการทดสอบจาก Double NSS Lab Test และ Tolly Up to Spec Certified เพื่อยืนยันประสิทธิภาพการใช้งาน

5.3.30 สามารถติดตั้งในตู้ Rack มาตรฐาน 19 นิ้ว

5.3.31 อุปกรณ์สามารถ update signature ได้ตลอดระยะเวลาไม่น้อยกว่า 1 ปี

5.4 อุปกรณ์ป้องกันการบุกรุก (Intrusion Prevention System : IPS) ภายในองค์กร (Internal IPS) จำนวน 1 ชุด

5.4.1 เป็นอุปกรณ์ (Hardware Appliance) ที่ออกแบบมาเพื่อป้องกันการบุกรุกทางเครือข่าย (Intrusion Prevention System) และทำงานบน Tilera multicore processor Architecture โดยไม่มี Hard drive ภายในอุปกรณ์ และไม่ใช่อุปกรณ์ UTM (Unified Threat Management)

5.4.2 มี Network Interface แบบ Copper Ethernet ports (10BASE-T/100BASE-TX/1000BASE-T) ไม่น้อยกว่า 8 พอร์ต

5.4.3 มี Management Port แบบ 10/100/1000 Mbps ไม่น้อยกว่า 4 พอร์ต

5.4.4 รองรับการตรวจจับและป้องกันการโจมตีเครือข่ายได้ไม่น้อยกว่า 4 Network Segments

5.4.5 รองรับ Throughput ได้ไม่น้อยกว่า 600 Mbps และมีค่าความช้า (Typical Latency) ไม่เกิน 50 uSec

5.4.6 รองรับจำนวนการเชื่อมต่อพร้อมกัน (Concurrent Connection) ไม่น้อยกว่า 256,000 Connections ต่อวินาที

5.4.7 สามารถป้องกันการโจมตีชนิดฉับพลัน (Denial of Service Attacks) เช่น SYN Flood ได้ไม่น้อยกว่า 500,000 SYN ต่อวินาที

5.4.8 มีความสามารถทำงานแบบอุปกรณ์ firewall เช่น รองรับการทำ firewall policy และstatefull firewall บนตัวอุปกรณ์เพื่อเป็นการป้องกันการโจมตีได้อย่างมีประสิทธิภาพและลดการทำงานของอุปกรณ์ firewall เดิมของเครือข่าย

5.4.9 สามารถป้องกันการเจาะระบบ (Exploits) เข้ามาที่จุดอ่อนและช่องโหว่ (Vulnerabilities)

5.4.10 สามารถทำ Deep File Inspection เพื่อป้องกันการโจมตีในระดับ File เช่น MS-Word Exploits หรือมีความสามารถในการตรวจจับไวรัสคอมพิวเตอร์ที่แฝงมากับไฟล์

5.4.11 สามารถ Block การใช้งาน Applications ที่ไม่พึงประสงค์เช่น Bit Torrent, eDonkey, Skype และ FastTrack ได้เป็นอย่างน้อย

5.4.12 รองรับการทำ Application Rate Limits และ Connection Limits

5.4.13 สามารถตรวจสอบการโจมตีจาก Vulnerability Signatures และ Attack Signatures

5.4.14 รองรับการทำ Protocol และ File Validation เพื่อตรวจสอบความผิดปกติของ Protocol และ File

5.4.15 สามารถป้องกันภัยคุกคามสำหรับระบบ VoIP

5.4.16 สามารถตรวจจับวิธีการบุกรุกและป้องกันเครือข่ายได้อย่างน้อยดังนี้ Signature matching, Protocol / Packet Anomalies, Statistical anomaliesหรือ Application anomalies, Overflow, Worm, Virus, Backdoor Program, Trojan Horse, Port Scanning, Spy ware, Packet Analysis, DoS, DDoS

5.4.17 สามารถทำการตรวจสอบ Traffic อย่างละเอียด (Deep Packet Inspection) โดยตรวจสอบโปรโตคอล HTTP, FTP, DNS, SMTP, Telnet, SSH, MS-RPC และ MS-CIFS ได้เป็นอย่างน้อย

5.4.18 สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS ได้เป็นอย่างน้อย

5.4.19 มี Application เฉพาะสำหรับเก็บ Log ของอุปกรณ์ IPS พร้อมระบบในการทำ Report และ Analyze ข้อมูล (Forensic) ของอุปกรณ์ IPS รวมถึงสามารถแจ้งเตือนในกรณีที่เกิดภัยคุกคามให้เจ้าหน้าที่ดูแลระบบทราบได้

5.4.20 สามารถส่ง Log ออกมาเก็บที่อุปกรณ์เก็บบันทึก Log ภายนอกได้ เช่น SIM หรือ SIEM

5.4.21 มีระบบในการทำรายงาน (Report) โดยเฉพาะแยกออกจากตัวอุปกรณ์ IPS ประกอบด้วยความสามารถ ดังต่อไปนี้

5.4.21.1 ระบบสามารถส่ง Report ทาง Email ได้โดยอัตโนมัติ

5.4.21.2 มี Dashboard ในการเฝ้าระวัง (Monitor) Security Event ที่ตรวจจับโดยอุปกรณ์ IPS แบบ Real-time

5.4.21.3 มีระบบในการทำ Forensic เพื่อวิเคราะห์ Security Eventที่ตรวจจับโดยอุปกรณ์ IPS

5.4.22 รองรับการ Update IPS Signature

5.4.23 สามารถทำงานได้อย่างต่อเนื่อง (Bypass Traffic) โดยช่องสัญญาณ In-Line Mode สามารถรับส่งข้อมูลได้ตามปกติ เมื่ออุปกรณ์เกิดปัญหา

5.4.24 รองรับการทำการสำรองระบบ (High Availability) แบบ Active-Active หรือ Active/Standby

5.4.25 รองรับการทำงานแบบ Protection Cluster เพื่อรองรับการขยายการใช้งานได้ในอนาคต

5.4.26 สามารถใช้งานตามมาตรฐาน IPv6 ได้

5.4.27 อุปกรณ์ที่นำเสนอต้องผ่านการทดสอบจาก Double NSS Lab Test และ Tolly Up to Spec Certified เพื่อยืนยันประสิทธิภาพการใช้งาน

5.4.28 สามารถติดตั้งในตู้ Rack มาตรฐาน 19 นิ้ว

5.4.29 อุปกรณ์สามารถ update signature ได้ตลอดระยะเวลาไม่น้อยกว่า 1 ปี

5.5 อุปกรณ์ไฟร์วอลล์สำหรับป้องกันเว็บ(Web Application Firewall : WAF) จำนวน 1 ชุด

5.5.1 อุปกรณ์ที่นำเสนอจะต้องเป็น Hardware Appliance ทำหน้าที่ในการป้องกันระบบงานด้านWeb Application หรือ Web Serviceโดยเฉพาะ

5.5.2 มี Network Interface สำหรับการ Management แยก โดยไม่รวมกับจุดเชื่อมต่อการใช้งาน

5.5.3 สามารถรองรับ Throughput ได้ 300 Mbps เป็นอย่างน้อย

5.5.4 สามารถรองรับการเชื่อมต่อ Http อย่างน้อย 9,000 Transactions ต่อวินาที

5.5.5 สามารถรองรับการเชื่อมต่อ Https อย่างน้อย 5,000 Transactions ต่อวินาที

5.5.6 สามารถรองรับ Concurrent Connection ได้อย่างน้อย 2,000,000 Connection

5.5.7 สามารถบริหารจัดการอุปกรณ์โดยผ่านทาง Web Base, CLI ได้เป็นอย่างน้อย

5.5.8 รองรับการทำงานแบบ High Variability แบบ Active-Active, Active-Standby ได้

5.5.9 สามารถตรวจจับพฤติกรรมการใช้งาน Web Application ของผู้ที่เข้ามาใช้บริการ Web Application บนเครื่องคอมพิวเตอร์แม่ข่ายต่างๆ ได้

5.5.10 อุปกรณ์ที่นำเสนอจะต้องสามารถทำงานแบบ In-Line (Bridge) หรือ Transparent และ Span-mode (Monitor) สำหรับตรวจสอบพฤติกรรมได้เป็นอย่างน้อย

5.5.11 มีระบบจัดการ Log โดยสามารถแสดง Alert หรือแจ้งเตือนในกรณีที่เกิดเหตุการณ์ต่างๆ ได้

5.5.12 โดยสามารถ Alert ผ่านทาง SMTP และ/หรือ SNMP ได้เป็นอย่างน้อย

5.5.13 สามารถส่ง Syslog Server หรือสามารถส่งข้อมูลไปยังระบบ SIM / SIEM ได้

5.5.14 รองรับระบบ Centralized Management ซึ่งเป็นอุปกรณ์เสริม เพื่อใช้ช่วยในส่วนของการบริหารจัดการอุปกรณ์ให้ง่ายขึ้นในกรณีที่มีจำนวน Application เป็นจำนวนมาก

5.5.15 สามารถทำงานร่วมกับ NTP หรือ SNTP ได้ เพื่อให้สามารถ Sync เวลาจาก Time Server ได้

5.5.16 รองรับการแก้ไข Input Content Filtering กรณีที่เป็นคำหยาบหรือคำต้องห้ามได้เป็นอย่างน้อย

5.5.17 รองรับการป้องกันการ Attack ด้วยวิธีต่างๆ ด้วยรูปแบบอย่างน้อย ดังต่อไปนี้

5.5.17.1 Cross-site Scripting

5.5.17.2 Cookie Poisoning

5.5.17.3 Buffer Overflow

5.5.17.4 Error Handling

5.5.17.5 SQL injection

5.5.17.6 URI Access Control

5.5.17.7 Website Defacement

5.5.18 บริษัทที่เป็นเจ้าของผลิตภัณฑ์ Web Application Firewall มีใบรับรอง ของ Common Criteria EAL-4 และ PCI DSSและมีใบรับรองที่ผ่านการทดสอบ IPv6 อย่างสมบูรณ์เป็นอย่างน้อย

5.5.19 สามารถทำการ Bypass Network Traffic ในกรณีที่เกิดเหตุขัดข้องกับตัวอุปกรณ์

5.5.20 มี Network Interface แบบ 10/100/1000 Base-TX ไม่น้อยกว่า 8 พอร์ต

5.5.21 มีระบบ Dashboard แสดงสถานะการทำงานของอุปกรณ์และการโจมตีที่เกิดขึ้นแบบ Real-time โดยสามารถแสดงให้เห็นว่าการโจมตีหรือเจาะระบบมาจากประเทศใด และมีรายละเอียดประกอบ เช่น สามารถแสดง SQL Statement ที่ระบบวิเคราะห์ว่าผิดปกติ เป็นต้น

5.5.22 สามารถทำรายงานการถูกโจมตีได้ในรูปแบบ HTML หรือ PDF หรือ XLS หรือดีกว่าโดยมีรายงานสรุปผลการโจมตี และแยกประเภทการถูกโจมตี โดยสามารถระบุ เป็นช่วงวัน เดือน ปี ได้ และส่งข้อมูล Report เข้าทาง E-mail ของผู้ดูแลระบบได้

5.5.23 สามารถติดตั้งในตู้เก็บอุปกรณ์มาตรฐานขนาด 19 นิ้วได้

5.5.24 อุปกรณ์สามารถ update signature ได้ตลอดระยะเวลาไม่น้อยกว่า 1 ปี

5.6 อุปกรณ์ Core/Distributed Switch เพื่อรองรับ IPV6 จำนวน 1 ชุด

5.6.1 เป็นอุปกรณ์ที่สามารถทำหน้าที่ routing และ switching ได้ในอุปกรณ์ชุดเดียวกัน

5.6.2 รองรับการทำงาน IPV6 ได้เป็นอย่างน้อย หรือดีกว่า

5.6.3 เป็นอุปกรณ์ที่มี Back-plane หรือ Switching Fabric หรือ Switching Capacity ไม่น้อยกว่า 88 Gbps หรือดีกว่า

5.6.4 อุปกรณ์ต้องมีพอร์ตแบบ 10/100/1000 Base-T จำนวนไม่น้อยกว่า 24 พอร์ต

5.6.5 ต้องสามารถทำงานแบบ Virtual LAN (VLAN) ตามมาตรฐาน IEEE 802.1Q ได้อย่างน้อย 256 VLAN หรือดีกว่า

5.6.6 เป็นอุปกรณ์ที่สามารถทำงานตามมาตรฐานข้อกำหนดของ IEEE ดังนี้

5.6.6.1 IEEE 802.3ad

5.6.6.2 IEEE802.1s

5.6.6.3 IEEE 802.3x

5.6.6.4 IEEE 802.1p

5.6.6.5 IEEE 802.1d

5.6.6.6 IEEE 802.1w

5.6.7 ต้องสามารถรองรับจำนวน MAC address ได้ไม่น้อยกว่า 8,000 MAC address

5.6.8 ต้องสามารถรองรับโปรโตคอล DHCP และ TFTP ได้เป็นอย่างน้อย

5.6.9 ต้องสามารถทำงานกับ Internet Group Management Protocol (IGMP) ได้เป็นอย่างน้อย

5.6.10 ต้องสามารถทำงานตามมาตรฐานโพรโตคอลการบริหารเครือข่าย (Network Management Protocol) ต่อไปนี้ได้เป็นอย่างน้อย

5.6.10.1 SNMP (Simple Network Management Protocol)

5.6.10.2 RMON (Remote Monitoring)

5.6.11 ต้องสามารถทำ Port Mirror ได้เป็นอย่างน้อย

5.6.12 ต้องสามารถรองรับการ Authentication ของผู้ใช้ได้ทั้ง IEEE802.1x และ Mac address ได้เป็นอย่างน้อย หรือดีกว่า

5.6.13 อุปกรณ์ที่เสนอต้องได้รับการตรวจสอบความปลอดภัย (Safety Certifications) จากหน่ายงาน CSA หรือ UL หรือ EN เป็นอย่างน้อย

5.6.14 อุปกรณ์ที่เสนอต้องได้รับการตรวจสอบการแพร่กระจายของสนามแม่เหล็กไฟฟ้า (Electromagnetic Emissions Certifications) จากหน่วยงาน FCC หรือ EN หรือ CSA เป็นอย่าง น้อย

5.7 อุปกรณ์กระจายสัญญาณ (L3 Switch) จำนวน 4 ชุด

5.7.1 มีลักษณะการทำงานไม่น้อยกว่า Layer 3 ของ OSI Model

5.7.2 มี Switch Capacity ไม่น้อยกว่า 128 Gbps

5.7.3 มีประสิทธิภาพในการส่งผ่านข้อมูล Forwarding Rate อย่างน้อย 95 Mpps

5.7.4 รองรับ Mac Address ได้ไม่น้อยกว่า 8,000 Mac Address

5.7.5 มีพอร์ต Gigabit Ethernet แบบ 10/100/1000BaseT และ Combo RJ-45/SFP รวมกันจำนวนไม่น้อยกว่า 24 พอร์ต

5.7.6 สามารถทำ Port Loopback Detection เพื่อป้องกันไม่ให้ระบบการทำงานของอุปกรณ์ Switch ล่มในกรณีที่เกิด Loop ในเครือข่าย

5.7.7 สามารถทำ Auto-Negotiation สำหรับ Port Speed และ Duplex Mode ได้

5.7.8 สามารถทำ Link Aggregation และ Trunk Links ได้

5.7.9 สามารถทำงานร่วมกับอุปกรณ์อื่นๆ ตามมาตรฐาน IEEE802.1D, IEEE802.1w, IEEE802.1s IEEE802.1p และ IEEE802.1q

5.7.10 สนับสนุนการทำ IGMPv3 Snooping ได้เป็นอย่างน้อย

5.7.11 สนับสนุนการทำ VLAN ได้ไม่น้อยกว่า 1,000 VLAN

5.7.12 รองรับการทำ IPv6 Hardware-based IP Routing ได้

5.7.13 รองรับการทำ Policy Based Routing (PBR) ได้เป็นอย่างน้อย

5.7.14 สนับสนุนการทำ Port Security ได้

5.7.15 สามารถบริหารจัดการอุปกรณ์ผ่านทางโปรแกรม Web Browser ได้

5.7.16 มี Console Port เพื่อต่อ Terminal กำหนดค่าการทำงานของอุปกรณ์ และสำหรับตรวจสอบระบบได้

5.7.17 สามารถ Upload/Download Configuration file ผ่านทาง FTP/TFTP Server ได้

5.7.18 สนับสนุนระบบ Network Management ตามมาตรฐาน CLI, Telnet, SNMPv3, RMON

5.7.19 สามารถทำงานกับระบบไฟฟ้าในประเทศไทยแบบ 220 VAC, 50Hz ได้

5.7.20 ผ่านการรับรองตามมาตรฐานความปลอดภัย FCC, VCCI-A และ CE

5.7.21 อุปกรณ์ฯต้องสามารถติดตั้งบน Rack 19" ได้

6. การติดตั้ง

6.1 ผู้ชนะการประกวดราคาจะต้องจัดส่งไฟล์ภาพถ่ายแบบดิจิทัลก่อนการติดตั้งและติดตั้งสมบูรณ์แล้วให้กับโรงงานไพ่ กรมสรรพสามิต สำหรับใช้ประกอบการตรวจรับ

6.2 ผู้ชนะการประกวดราคาต้องทำการติดตั้ง พร้อมปรับแต่ง (Config) ค่าต่างๆ ของอุปกรณ์ทั้งหมด ให้สามารถทำงานร่วมกับเครื่องคอมพิวเตอร์แม่ข่าย และระบบเครือข่ายของโรงงานไพ่ ให้สามารถทำงานร่วมกันได้อย่างมีประสิทธิภาพ ตามที่ได้มีการออกแบบในเอกสารที่ส่งมอบงานงวดที่ 1 ที่ผ่านความเห็นชอบจากคณะกรรมการตรวจรับ

6.3 ผู้ชนะการประกวดราคาจะต้องทำงานด้วยความระมัดระวังและดูแลอาคาร สถานที่ ซึ่งไม่อยู่ในข้อกำหนดของสัญญา ให้อยู่ในสภาพเดิม หากปรากฏว่าเกิดการชำรุด เสียหาย จากการกระทำของผู้ชนะการประกวดราคา ผู้ชนะการประกวดราคาจะต้องซ่อมแซมให้อยู่ในสภาพเดิม โดยผู้ชนะการประกวดราคาต้องรับผิดชอบค่าใช้จ่ายทั้งหมดที่เกิดขึ้น และไม่มีสิทธิ์เรียกร้องค่าเสียหายที่เกิดขึ้นจากโรงงานไพ่ กรมสรรพสามิต

6.4 ผู้ชนะการประกวดราคาต้องจัดหาสายไฟฟ้า วัสดุอุปกรณ์ทั้งหมด และติดตั้งระบบไฟฟ้าตามมาตรฐานผู้ผลิตจากจุดจ่ายไฟของโรงงานไพ่ กรมสรรพสามิต ไปยังปลั๊กรางสายไฟภายในตู้สำหรับจัดเก็บเครื่องคอมพิวเตอร์และอุปกรณ์ เพื่อให้ต้องการปรับปรุง และควบคุมกระบวนการดำเนินงานด้านสารสนเทศภายในองค์กร ให้รองรับมาตรฐาน IPV6 และสอดคล้องตาม ระเบียบ และ พ.ร.บ. ต่างๆ สามารถใช้งานได้อย่างสมบูรณ์และมีประสิทธิภาพ ตรงตามวัตถุประสงค์ของโรงงานไพ่ กรมสรรพสามิต

6.5 ผู้ชนะการประกวดราคาจะต้องดำเนินการเชื่อมโยงอุปกรณ์ที่เสนอกับระบบเครือข่าย เครื่องแม่ข่ายคอมพิวเตอร์แม่ข่าย และอุปกรณ์อื่นๆ ของโรงงานไพ่ กรมสรรพสามิต ให้สามารถใช้งานได้อย่างมีประสิทธิภาพ

6.6 ผู้ชนะการประกวดราคาต้องส่งมอบ CD หรือ DVD บรรจุ คู่มือการใช้งานของทุกรายการอุปกรณ์ที่เสนอในโครงการ โปรแกรมหรือระบบงาน เอกสารต่าง ๆ ของ อุปกรณ์ที่นำเสนอทั้งหมด คู่มือของระบบงานแบบเบ็ดเสร็จ (User Manual) และคู่มือปฏิบัติงานและการบำรุงรักษา พร้อมแผ่น CD หรือ DVD ที่มีรายละเอียดตามเอกสาร จำนวน 3 ชุด

7. การส่งมอบงาน

ระยะเวลาดำเนินการ 60 วัน นับถัดจากวันลงนามในสัญญาซื้อขาย โดยผู้ชนะการประกวดราคาต้องดำเนินการส่งมอบงาน ดังนี้

7.1 ผู้ชนะการประกวดราคาต้องส่งมอบแผนการดำเนินงาน และแผนการออกแบบการเชื่อมโยงอุปกรณ์ตามสัญญาซื้อทั้งหมด กับระบบเครือข่ายของโรงงานไพ่ กรมสรรพสามิต ภายใน 15 วัน นับถัดจากวันลงนามในสัญญาซื้อขาย

7.2 ผู้ชนะการประกวดราคาต้องส่งมอบอุปกรณ์ตามสัญญาซื้อทั้งหมด ภายใน 50 วัน นับถัดจากวันลงนามในสัญญาซื้อขาย

7.3 ผู้ชนะการประกวดราคาดำเนินการติดตั้ง และ config ค่าอุปกรณ์ตามงานงวดที่ 2 ทั้งหมดตามผลการส่งมอบงานงวดที่ 1 ที่ผ่านความเห็นชอบจากคณะกรรมการตรวจรับ และดำเนินการทดสอบการเชื่อมต่อระหว่างเครื่องลูกข่าย และเครื่องแม่ข่ายทั้งหมด กับระบบเครือข่ายโรงงานไพ่ กรมสรรพสามิต ให้สามารถทำงานได้อย่างมีประสิทธิภาพและเป็นไปตามการกำหนดตามแนวทางการดำเนินงานด้านการรักษา

ของระบบเทคโนโลยีสารสนเทศที่โรงงานไพ่ กรมสรรพสามิต ภายใน 60 วัน นับถัดจากวันลงนามในสัญญาซื้อขาย

8. การชำระเงิน

แบ่งจ่ายเงินเป็น 3 งวด ดังนี้

งวดที่ 1 จำนวนร้อยละ 10 ของมูลค่าสัญญาซื้อขาย เมื่อผู้ชนะการประกวดราคาส่งมอบงานตามข้อ 7.1 แล้วเสร็จ และคณะกรรมการตรวจรับได้ตรวจรับงานดังกล่าวเรียบร้อยแล้ว

งวดที่ 2 จำนวนร้อยละ 50 ของมูลค่าสัญญาซื้อขาย เมื่อผู้ชนะการประกวดราคาส่งมอบงานตามข้อ 7.2 แล้วเสร็จ และคณะกรรมการตรวจรับได้ตรวจรับงานดังกล่าวเรียบร้อยแล้ว

งวดที่ 3 จำนวนร้อยละ 40 ของมูลค่าสัญญาซื้อขาย เมื่อผู้ชนะการประกวดราคาส่งมอบงานตามข้อ 7.3 แล้วเสร็จ และคณะกรรมการตรวจรับได้ตรวจรับงานดังกล่าวเรียบร้อยแล้ว

9. การรับประกัน

9.1 ผู้ชนะการประกวดราคาต้องรับประกันพัสดุทุกรายการที่ได้มีการจัดส่งให้กับโรงงานไพ่ กรมสรรพสามิตเป็นระยะเวลา 1 ปี รวมค่าแรงและอะไหล่และบริการ ณ สถานที่ติดตั้ง (Onsite Service Warranty) และควบคุมกระบวนการดำเนินงานด้านสารสนเทศภายในองค์กร ให้รองรับมาตรฐาน IPV6 และสอดคล้องตาม ระเบียบ และ พ.ร.บ. ต่างๆ ข้างต้นและให้บริการ ณ สถานที่ติดตั้งและใช้งานโดยไม่คิดค่าใช้จ่ายใดๆ ทั้งสิ้น

9.2 ผู้ชนะการประกวดราคาจะต้องรับประกันความชำรุดบกพร่องและการใช้งานของอุปกรณ์ที่เสนอเป็นเวลา 360 วัน นับถัดจากวันที่คณะกรรมการได้ตรวจรับงานเรียบร้อยแล้วในงวดสุดท้าย ในกรณีที่อุปกรณ์เกิดชำรุดเสียหาย ขัดข้องในช่วงเวลาการรับประกัน ผู้ชนะการประกวดราคาจะต้องดำเนินการซ่อมบำรุงหรือเปลี่ยนอุปกรณ์ดังกล่าว ให้แล้วเสร็จภายใน 1 วันทำการ หลังจากการได้รับแจ้งจากโรงงานไพ่โดยไม่คิดมูลค่าใดๆ ทั้งสิ้น หากผู้ชนะการประกวดราคาไม่ดำเนินการแก้ไขข้อขัดข้องให้แล้วเสร็จได้ภายใน 1 วันทำการ ผู้ชนะการประกวดราคาต้องถูกปรับรายวันในอัตราวันละ 1,000 บาท (หนึ่งพันบาทถ้วน) จนกว่าจะดำเนินการแก้ไขแล้วเสร็จ เว้นเสียแต่ว่าผู้ชนะการประกวดราคาจะสามารถจัดหาอุปกรณ์ที่มีคุณภาพทัดเทียมกันหรือดีกว่ามาทดแทน เพื่อให้ระบบเครือข่ายด้านความปลอดภัยของโรงงานไพ่ สามารถทำงานได้อย่างต่อเนื่อง จนกว่าจะดำเนินการซ่อมแซมหรือแก้ไขปัญหาให้แล้วเสร็จ

9.3 ผู้ชนะการประกวดราคาต้องมีการตรวจสอบการทำงานของพัสดุที่นำเสนอทุกๆ 3 เดือน และจัดทำรายงานสรุปส่งให้ โรงงานไพ่ กรมสรรพสามิต ตลอดระยะเวลาการประกัน

10. การฝึกอบรม

ผู้ชนะการประกวดราคาต้องเสนอหลักสูตรการฝึกอบรม ให้โรงงานไพ่ กรมสรรพสามิต พิจารณาให้ความเห็นชอบ ภายใน 30 วัน นับถัดจากวันลงนามในสัญญาซื้อขาย

ลำดับ	หลักสูตรการฝึกอบรม	จำนวนผู้เข้าอบรมไม่เกิน (คน)	จำนวนรุ่น	ระยะเวลาต่อรุ่น
(1)	หลักสูตรสำหรับผู้ดูแลระบบ และ Help Desk	5	2	ไม่น้อยกว่า 2 วันทำการ

<u>หมายเหตุ:</u> กำหนดให้ 1 วันทำการ เท่ากับ 6 ชั่วโมง

10.1 ผู้ชนะการประกวดราคาต้องเสนอรายละเอียดการฝึกอบรมโดยระบุ ชื่อหลักสูตรวิชาและเนื้อหา จำนวนวัน เวลา ที่จะฝึกอบรม

10.2 ผู้ชนะการประกวดราคาต้องเป็นผู้ดำเนินงานและรับผิดชอบค่าใช้จ่ายทั้งหมดในการจัดเตรียมสถานที่ที่จัดให้มีการฝึกอบรม การจัดเตรียมเอกสาร อุปกรณ์ที่ใช้ในการฝึกอบรม ค่าวิทยากร ค่าใช้จ่ายในการเดินทาง ค่าอาหารและค่าใช้จ่ายอื่นๆ ที่เกี่ยวข้องกับการฝึกอบรม

10.3 ผู้ชนะการประกวดราคาต้องจัดทำคู่มือที่ใช้ในการฝึกอบรม ฝึกการใช้งาน และเอกสารอื่นๆที่จำเป็นในการฝึกอบรมที่ครบถ้วนสมบูรณ์ เป็นภาษาไทยและง่ายต่อการเข้าใจ ทั้งนี้ผู้เข้ารับการฝึกอบรมจะได้คู่มือในการฝึกอบรม 1 ชุด/คน

10.4 ก่อนการฝึกอบรม ผู้ชนะการประกวดราคาจะต้องส่งรายละเอียดหลักสูตรการฝึกอบรม พร้อมประวัติวิทยากรให้ โรงงานไพ่ กรมสรรพสามิต พิจารณาให้ความเห็นชอบก่อนดำเนินการ

10.5 การฝึกอบรม ต้องประกอบไปด้วยทั้งภาคทฤษฎี และปฏิบัติเพื่อให้ผู้เข้ารับการฝึกอบรมสามารถทดสอบความรู้ และทำงานได้จริง

10.6 ผู้ชนะการประกวดราคา ต้องจัดเตรียมการฝึกอบรม และต้องจัดเตรียมเครื่องคอมพิวเตอร์ประกอบการฝึกอบรมสำหรับผู้เข้าอบรม 1 คนต่อ 1 เครื่อง

10.7 วิทยากรในการอบรม จะต้องมีประสบการณ์ ความรู้ความสามารถที่เกี่ยวข้องกับการใช้และมีทักษะในการถ่ายทอดการใช้อุปกรณ์ตามที่ผู้ชนะการประกวดราคาได้เสนอมาในสัญญาซื้อฉบับนี้

11. การรักษาความลับ

11.1 ผู้ชนะการประกวดราคาจะต้องจัดเก็บรักษาข้อมูลต่างๆ ที่เกี่ยวกับการดำเนินงานที่ผู้ชนะการประกวดราคาได้รับจาก โรงงานไพ่ กรมสรรพสามิต และข้อมูลต่างๆ ที่ผู้ชนะการประกวดราคาได้จัดทำขึ้นเนื่องจากการดำเนินงานตามสัญญานี้อย่างเป็นความลับของโรงงานไพ่ กรมสรรพสามิต ซึ่งต่อไปในสัญญานี้เรียกว่า **"ข้อมูลที่เป็นความลับ"** โดยผู้ชนะการประกวดราคาต้องหามาตรการในการจัดเก็บข้อมูลที่เป็นความลับให้มิดชิด รวมทั้งไม่เปิดเผย หรือเผยแพร่ หรือกระทำด้วยวิธีการใดให้บุคคลอื่นใดที่มิใช่คู่สัญญาภายใต้สัญญาจ้างนี้ หรือมิใช่บุคคลที่ โรงงานไพ่ กรมสรรพสามิต ได้อนุญาตเป็นลายลักษณ์อักษรให้มีส่วนเกี่ยวข้องที่จะรับทราบข้อมูลที่เป็นความลับภายใต้สัญญานี้ ได้ทราบถึงข้อมูลที่เป็นความลับดังกล่าว เว้นแต่จะเป็นการ

เปิดเผยข้อมูลดังกล่าวให้แก่เจ้าหน้าที่ผู้ปฏิบัติงานของผู้ชนะการประกวดราคาที่ต้องเกี่ยวข้องโดยตรงกับข้อมูลดังกล่าวเท่านั้น และผู้ชนะการประกวดราคาจะต้องจัดให้เจ้าหน้าที่ผู้ปฏิบัติงานดังกล่าวได้ผูกพันและปฏิบัติตามเงื่อนไขในการรักษาข้อมูลที่เป็นความลับเช่นว่านั้นด้วย

11.2 ผู้ชนะการประกวดราคาจะยังคงต้องผูกพันข้อมูลที่เป็นความลับดังกล่าว ตราบที่ข้อมูลที่เป็นความลับดังกล่าวยังคงเป็นความลับของโรงงานไพ่ กรมสรรพสามิต อยู่แม้ว่าการจ้างตามสัญญานี้ได้สิ้นสุดลงแล้วไม่ว่าด้วยประการใด ๆ

11.3 หากข้อมูลที่เป็นความลับของโรงงานไพ่ ได้ถูกเปิดเผยไม่ว่าทั้งหมดหรือแต่บางส่วน หรือกระทำด้วยวิธีการใดให้บุคคลอื่นใดที่มิใช่คู่สัญญาภายใต้สัญญาจ้างนี้ หรือมิใช่บุคคลที่ โรงงานไพ่ กรมสรรพสามิต ได้อนุญาตเป็นลายลักษณ์อักษรให้มีส่วนเกี่ยวข้องที่จะรับทราบข้อมูลที่เป็นความลับภายใต้สัญญานี้ ผู้ชนะการประกวดราคาจะต้องรับผิดชอบต่อผลที่เกิดขึ้นโดยไม่สามารถเรียกร้องค่าเสียหายใดๆ จากโรงงานไพ่ กรมสรรพสามิตได้ และโรงงานไพ่ กรมสรรพสามิต มีสิทธิบอกเลิกสัญญาได้ทันที

โครงการปรับปรุงอุปกรณ์เพื่อรองรับการดำเนินงานด้านความมั่นคงปลอดภัยให้สอดคล้อง ตามระเบียบ และ พ.ร.บ. ต่างๆ

รายการ	จำนวน	ราคาหน่วย/ (บาท)	ราคารวม (บาท)
1. ระบบปรับเทียบเวลา	1 ชุด		
2. อุปกรณ์จัดเก็บ Log	1 ชุด		
3. อุปกรณ์ป้องกันการบุกรุก (Intrusion Prevention System : IPS) ภายนอกองค์กร(External IPS)	1 ชุด		
4. อุปกรณ์ป้องกันการบุกรุก (Intrusion Prevention System : IPS) ภายในองค์กร(Internal IPS)	1 ชุด		
5. อุปกรณ์ไฟร์วอลล์สำหรับป้องกันเว็บแอพพลิเคชั่น (Web Application Firewall : WAF)	1 ชุด		
6. อุปกรณ์ Core/Distributed Switch เพื่อรองรับ IPV6	1 ชุด		
7. อุปกรณ์กระจายสัญญาณ (L3 Switch)	4 ชุด		
รวมเป็นเงิน			
ภาษีมูลค่าเพิ่ม (Vat 7%)			
รวมเป็นเงินทั้งสิ้น			
รวมเป็นเงินทั้งสิ้น (ตัวอักษร)			