ประกาศสถาบันมะเร็งแห่งชาติ

เรื่อง ประกวดราคาซื้อระบบPACS ระยะที่ ๒ด้วยวิธีการทางอิเล็กทรอนิกส์

สถาบันมะเร็งแห่งชาติ มีความประสงค์จะประกวดราคาซื้อ ระบบ PACS ระยะที่ ๒ จำนวน ๑ ระบบ ด้วยวิธีการทางอิเล็กทรอนิกส์

ผู้ประสงค์จะเสนอราคาจะต้องมีคุณสมบัติ ดังต่อไปนี้

๑.เป็นนิติบุคคลผู้มีอาชีพขายพัสดุที่ประกวดราคาซื้อด้วยวิธีการทางอิเล็กทรอนิกส์ ดังกล่าว ซึ่งมีผลงานประเภทเดียวกัน ในวงเงินไม่น้อยกว่า ๕,๐๐๐,๐๐๐.๐๐ บาท (ห้าล้านบาทถ้วน)

๒. ไม่เป็นผู้ที่ถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานของทางราชการและได้แจ้งเวียนชื่อแล้วหรือไม่เป็นผู้ที่ได้รับผลของการสั่งให้นิติบุคคลหรือบุคคลอื่นเป็นผู้ทิ้งงานตามระเบียบของราชการ

๓. ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ประสงค์จะเสนอราคารายอื่น และ/หรือต้องไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ให้บริการตลาดกลางอิเล็กทรอนิกส์ ณ วันประกาศประกวดราคาซื้อด้วยวิธีการทางอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรม

๔. ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ประสงค์จะเสนอราคาได้มีคำสั่งให้สละสิทธิ์และความคุ้มกันเช่นว่านั้น

๕. ผู้ประสงค์จะเสนอราคาที่จะเข้าเป็นคู่สัญญาต้องไม่อยู่ในฐานะเป็นผู้ไม่แสดงบัญชีรายรับรายจ่าย หรือแสดงบัญชีรายรับรายจ่ายไม่ถูกต้องครบถ้วนในสาระสำคัญ

๖. ผู้ประสงค์จะเสนอราคาที่จะเข้าเป็นคู่สัญญากับหน่วยงานของรัฐซึ่งได้ดำเนินการจัดซื้อจัดจ้างด้วยระบบอิเล็กทรอนิกส์ (e-Government Procurement : e-GP) จะต้องลงทะเบียนในระบบอิเล็กทรอนิกส์ของกรมบัญชีกลางที่เว็บไซต์ศูนย์ข้อมูลจัดซื้อจัดจ้างภาครัฐด้วย

๗. คู่สัญญาต้องรับจ่ายเงินผ่านบัญชีเงินฝากกระแสรายวัน เว้นแต่การรับจ่ายเงินแต่ละครั้งซึ่งมีมูลค่าไม่เกินสามหมื่นบาทคู่สัญญาอาจรับจ่ายเป็นเงินสดก็ได้

กำหนดยื่นเอกสารประกวดราคาซื้อด้วยวิธีการทางอิเล็กทรอนิกส์ ในวันที่ .....

ระหว่างเวลา.....น. ถึง.....น. ณ.....

.....

และประกาศรายชื่อผู้มีสิทธิ์ได้รับการคัดเลือกให้เข้าเสนอราคาในวันที่ .....

ผู้สนใจ...

ผู้สนใจติดต่อขอรับ /ซื้อเอกสารประกวดราคาซื้อด้วยวิธีการทางอิเล็กทรอนิกส์ ในราคาชุดละ - บาท ได้ที่ ฝ่ายพัสดุและบำรุงรักษา สถาบันมะเร็งแห่งชาติ ถนนพระราม ๖ เขตราชเทวี กรุงเทพฯ ระหว่างวันที่ ถึงวันที่ ตั้งแต่เวลา ดูรายละเอียดได้ที่เว็บไซต์ www.nci.go.th หรือสอบถามทางโทรศัพท์หมายเลข ในวันและเวลาราชการ

ประกาศ ณ

ร่างขอบเขตของงาน (Terms of Reference : TOR)
ระบบ (PACS) ระยะที่ 2
สถาบันมะเร็งแห่งชาติ

.....

1. ความเป็นมา

ด้วยสถาบันมะเร็งแห่งชาติได้ดำเนินการติดตั้งระบบจัดการและส่งข้อมูลภาพทางการแพทย์ (PACS) ระยะที่ 0 และระยะที่ 1 แล้วนั้นจึงมีความประสงค์จะดำเนินการประกวดราคา จัดซื้อพร้อมติดตั้งอุปกรณ์สำหรับระบบจัดเก็บและส่งข้อมูลภาพทางการแพทย์ (PACS) ระยะที่ 2 เพื่อวางระบบเครือข่ายคอมพิวเตอร์ในการรับส่งข้อมูล ให้พร้อมในการให้บริการทางระบบจัดเก็บและส่งข้อมูลภาพทางการแพทย์ (PACS) พร้อมทั้งรองรับ ระบบ สารสนเทศ และระบบงานต่างๆ ของสถาบันมะเร็ง อันจะทำให้ การให้บริการประชาชนที่เข้ามาติดต่อกับทางสถาบันฯได้อย่างรวดเร็ว ปลอดภัย และมีประสิทธิภาพสูงสุด โดยจำเป็นต้องจัดหาอุปกรณ์ที่ใช้งานร่วมกันได้ เพื่อให้เกิดระบบที่มีประสิทธิภาพ สามารถใช้งานร่วมกันได้อย่างเชื่อมโยงและเป็นระบบที่มีเสถียรภาพและให้บริการได้อย่างมั่นคง ต่อเนื่อง และปลอดภัยต่อระบบเทคโนโลยีสารสนเทศ อีกทั้งการออกแบบการทำงานระบบเครือข่ายคอมพิวเตอร์แบบ High Availability (HA) และยังเป็นการออกแบบที่พัฒนาต่อยอดให้สามารถรองรับเทคโนโลยีใหม่ที่จะเกิดในอนาคตได้ด้วย

2. วัตถุประสงค์

2.1 เพื่อให้ระบบจัดเก็บและส่งข้อมูลภาพทางการแพทย์ (PACS) ของสถาบันมะเร็งแห่งชาติ มีระบบเครือข่ายคอมพิวเตอร์ที่สามารถรองรับการให้บริการ และมีประสิทธิภาพในการรับ-ส่งข้อมูลได้อย่างต่อเนื่อง รวดเร็ว ปลอดภัย มั่นคง และทันต่อสถานการณ์ พร้อมทั้งรองรับ ระบบสารสนเทศ และระบบงานต่างๆ ของสถาบันมะเร็ง

2.2 เพื่อลดโอกาสความเสี่ยงของการไม่สามารถให้บริการสารสนเทศ

2.3 เพื่อให้สามารถรองรับการพัฒนาเทคโนโลยีใหม่ที่มีการออกแบบพัฒนาต่อยอดในอนาคตได้

3. คุณสมบัติของผู้ประสงค์จะเสนอราคา

3.1 ผู้ประสงค์จะเสนอราคาต้องเป็นผู้มีอาชีพขายพัสดุที่ประกวดราคาซื้อด้วยวิธีการทางอิเล็กทรอนิกส์

3.2 ผู้ประสงค์จะเสนอราคาต้องไม่เป็นผู้ที่ถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานของทางราชการและได้แจ้งเวียนชื่อแล้ว หรือไม่เป็นผู้ที่ได้รับผลของการสั่งให้นิติบุคคลหรือบุคคลอื่นเป็นผู้ทิ้งงานตามระเบียบของทางราชการ

3.3 ผู้ประสงค์จะเสนอราคาต้องไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ประสงค์จะเสนอราคารายอื่น และไม่เป็นผู้มีผลประโยชน์ร่วมกันระหว่างผู้ประสงค์จะเสนอราคากับผู้ให้บริการตลาดกลางอิเล็กทรอนิกส์ ณ วันประกาศประกวดราคาจ้างด้วยวิธีการทางอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรม

3.4 ผู้ประสงค์จะเสนอราคาต้องไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ประสงค์จะเสนอราคาได้มีคำสั่งให้สละสิทธิ์ความคุ้มกันเช่นว่านั้น

3.5 บุคคลหรือนิติบุคคลที่จะเข้าเป็นคู่สัญญาต้องไม่อยู่ในฐานะเป็นผู้ไม่แสดงบัญชีรายรับรายจ่าย หรือแสดงบัญชีรายรับรายจ่ายไม่ถูกต้องครบถ้วนในสาระสำคัญ

3.6 ผู้ประสงค์...

3.6 ผู้ประสงค์จะเสนอราคา ที่จะเข้าเป็นคู่สัญญากับหน่วยงานของรัฐซึ่งได้ดำเนินการจัดซื้อจัดจ้างด้วยระบบอิเล็กทรอนิกส์ (e-Government Procurement : e-GP) ต้องลงทะเบียนในระบบอิเล็กทรอนิกส์ของกรมบัญชีกลางที่เว็บไซต์ศูนย์ข้อมูลจัดซื้อจัดจ้างภาครัฐด้วย

3.7 คู่สัญญาต้องรับจ่ายเงินผ่านบัญชีเงินฝากกระแสรายวัน เว้นแต่การรับจ่ายเงินแต่ละครั้งซึ่งมีมูลค่าไม่เกินสามหมื่นบาทคู่สัญญาอาจรับจ่ายเป็นเงินสดก็ได้

3.8 ผู้ประสงค์จะเสนอราคาต้องเป็นนิติบุคคล และมีผลงานเดียวกันกับงานที่ประกวดราคา ด้วยวิธีการทางอิเล็กทรอนิกส์ มาแล้วไม่น้อยกว่า ๑ โครงการ ในวงเงินไม่น้อยกว่า ๕,๐๐๐,๐๐๐.๐๐ บาท (ห้าล้านบาทถ้วน) ต่อหนึ่งสัญญา เป็นเวลาไม่เกิน ๕ ปี นับถึงวันยื่นเอกสารประกวดราคา และเป็นผลงานที่เป็นคู่สัญญาโดยตรงกับส่วนราชการ หน่วยงานตามกฎหมายว่าด้วยระเบียบบริหารราชการส่วนท้องถิ่น รัฐวิสาหกิจ หรือหน่วยงานเอกชนที่ สถาบันมะเร็งแห่งชาติ เชื่อถือ

4. คุณลักษณะเฉพาะของครุภัณฑ์

(รายละเอียดคุณสมบัติตามเอกสารแนบท้าย)

5. กำหนดระยะเวลาส่งมอบงาน

ระยะเวลาดำเนินงานไม่เกิน 150 วัน นับถัดจากวันลงนามในสัญญาซื้อขาย

10. วงเงินในการจัดหา

ในวงเงิน 9,800,000.00 บาท (เก้าล้านแปดแสนบาทถ้วน)

สถานที่ติดต่อเพื่อขอทราบข้อมูลเพิ่มเติม หรือเสนอแนะ วิจารณ์ หรือแสดงความคิดเห็นโดยเปิดเผยได้ที่

ฝ่ายพัสดุและบำรุงรักษา สถาบันมะเร็งแห่งชาติ
268/1 ถนนพระราม 6 เขตราชเทวี
กรุงเทพมหานคร 10400
โทร 0-2354-7028-33 ต่อ 1504,1505
โทรสาร 0-2644-6753

ร่างขอบเขตของงาน (Terms of Reference : TOR)
โครงการซื้อ ระบบ PACS ระยะที่ 2
สถาบันมะเร็งแห่งชาติ

****

1. อุปกรณ์กระจายสัญญาณ Distributed Switch จำนวน 2 ชุด แต่ละชุดมีคุณลักษณะอย่างน้อยดังต่อไปนี้

1.1 มีลักษณะการทำงานไม่น้อยกว่า Layer 3

1.2 เป็นระบบแบบ Modular Operating System เพื่อรองรับการทำงานแบบไม่มีการหยุดพักได้

1.3 มีพอร์ต 10Gigabit Ethernet แบบ SFP+ จำนวนไม่น้อยกว่า 24 พอร์ต ต่อ Switch

1.4 ติดตั้ง transceiver แบบ 10Gbase-LR จำนวนไม่น้อยกว่า 17 พอร์ต

1.5 มี Power Supply ที่ติดตั้งภายในอุปกรณ์จำนวนไม่น้อยกว่า 2 ชุด โดยสามารถทำงานแบบ Redundant และ Hot Swap (Hot plug) ได้

1.6 มี Switching Bandwidth หรือ Switching Fabric สูงสุดไม่น้อยกว่า 720 Gbps และ มีค่า Forwarding Rate หรือ throughput สูงสุดไม่น้อยกว่า 500 Mpps ต่อ Switch

1.7 มีพอร์ตชนิด Stack โดยเฉพาะ ไม่น้อยกว่า 2 port โดยมีความเร็วในการ Stack รวมไม่น้อยกว่า 230Gbps ต่อ Switch สามารถต่อเชื่อมแบบ Stack ได้ไม่น้อยกว่า 8 ชุด หรือ มีโครงสร้าง แบบ Modular Chassis จำนวนไม่น้อยกว่า 8 Slot โดยมีความเร็วรวมไม่น้อยกว่า 230Gbps ต่อ Slot โดยรองรับ port 10G Ethernet ได้ไม่น้อยกว่า 192 port ต่อ Chassis

1.8 อุปกรณ์ต้องสามารถรองรับการขยายความเร็วในการ Stack รวมสูงสุดได้ไม่น้อยกว่า 512Gbps ต่อ Switch หรือ มีโครงสร้าง แบบ Modular Chassis โดยรองรับการขยายความเร็ว สูงสุดรวมไม่น้อยกว่า 512Gbps ต่อ Slot

1.9 สามารถทำ Routing ตามโปรโตคอลมาตรฐาน IP แบบ RIPv1/2 OSPF (OSPFv2), Policy Base Routing และ VRRP ได้โดยตัว Switch เองเป็นอย่างน้อย และรองรับการเพิ่มความสามารถแบบ IS-IS และ BGP4 ได้

1.10 สามารถทำ IPv6 Routing แบบ RIPng และ OSPFv3 ได้โดยตัว Switch เองเป็นอย่างน้อย และรองรับการเพิ่มความสามารถแบบ BGP4 for IPv6 (BGP4+ หรือ RFC2283), IS-ISv6 ได้

1.11 รองรับการเพิ่มความสามารถเชื่อมต่อแบบ Virtual Ethernet Port Aggregator (VEPA, 802.1Qbg) หรือ VN-Tag (802.1Qbh)

1.12 สามารถทำงานแบบ Multi-chassis Ether Channel (MEC) หรือ Multi-Switch Link aggregation ได้

1.13 มีคุณสมบัติด้านความปลอดภัยดังนี้

1.13.1 สามารถทำ User Authentication ก่อนเข้าใช้งาน Switch อย่างน้อย ดังนี้

- สามารถทำการ user Authentication ให้กับผู้ใช้งาน (User) ก่อนจะอนุญาตให้เข้าใช้งาน Switch ได้ในแบบ 802.1x, MAC base และ Web Base Authentication ได้โดยตัว Switch เอง

สามารถทำการ...

- สามารถทำการ MAC base Authentication และ Web Base Authentication ให้กับผู้ใช้งาน (User) ก่อนจะอนุญาตให้เข้าใช้งาน Switch โดยสามารถสร้างและใช้รายการผู้ใช้งานบน Local Database ของ Switch เอง โดยสามารถกำหนด user name, password และ VLAN ของแต่ละ user ได้ ในกรณีที่ อุปกรณ์ที่เสนอไม่สามารถทำ Authentication Local Database ได้ให้เสนออุปกรณ์ Access Control Server ภายนอก ที่มีเครื่องหมายการค้าเดียวกันกับ Switch ที่เสนอ หรือเสนออุปกรณ์ภายนอก ทำหน้าที่ดังกล่าวร่วมกับ Switch ที่เสนอได้ (ในกรณีที่เสนออุปกรณ์ภายนอก ต้องเสนออุปกรณ์ภายนอกจำนวนเท่ากับจำนวน Switch ที่เสนอ)

1.13.2 สามารถตรวจจับป้องกันการโจมตี ได้อย่างน้อยดังนี้

- Denial of Service (DoS) Protection โดย เก็บ Packet Header เพื่อวิเคราะห์ และ ทำการสร้าง Hardware ACL เพื่อควบคุมการ Flow ของข้อมูล โดยตัว Switch เอง หรือ มีอุปกรณ์ทำหน้าที่ NAC (Post-NAC) ภายนอก จำนวนเท่ากับจำนวน Switch ที่เสนอ โดยสามารถทำหน้าที่ดังกล่าวร่วมกับ Switch ที่เสนอได้
- สามารถป้องกันการโจมตีแบบ Protocol Anomaly Protection โดยใช้ built-in hardware chipsets หรือ ASIC ของตัว Switch เอง และ Switch สามารถป้องกันการโจมตี Network Attack ได้อย่างน้อยดังนี้ SYN attack, SQL Slammer, SShredder, SNMP vulnerabilities, tcp denial of service, smurf, LAND attack, tcp syn flooding ,UDP service denial, IP Spoofing Attacks และ Hijacked Terminal Connections และ สามารถป้องกันการโจมตี Host Attack ได้อย่างน้อยดังนี้ Teardrop, boink, opentear, jolt2, newtear, nestea, syndrop, fraggle, papasmurf, synk4, raped, winfreeze, ping –f, ping of death, pepsi5, Latierra, Winnuke, Simping, Sping, Ascend, Stream และ Octopus โดยตัว Switch เอง (ในกรณีที่อุปกรณ์ที่เสนอไม่สามารถตรวจจับป้องกันการจู่โจม ดังกล่าวข้องต้นได้ ให้ผู้ประสงค์จะเสนอราคาจัดหาอุปกรณ์ IPS ภายนอก จำนวนเท่ากับจำนวน Switch ที่เสนอ โดยมี IPS Throughput ต่อ อุปกรณ์ ไม่น้อยกว่า 20 Gbps และ มี port 10G Ethernet ไม่น้อยกว่า 4 port โดยอุปกรณ์ต้องได้มาตรฐาน ICSA หรือ NSS ด้าน IPS)

1.13.3 สามารถทำ Identity Management โดยสามารถทำงานร่วมกับ LDAP Server และ Kerberos Snooping ได้ หรือ มีอุปกรณ์ NAC (Pre-NAC) ภายนอก ที่มี เครื่องหมายการค้าเดียวกันกับ Switch ที่เสนอ หรือ มีอุปกรณ์ทำหน้าที่ Identity Management ภายนอก (ในกรณีที่เสนออุปกรณ์ภายนอก ต้องเสนออุปกณ์ภายนอกจำนวนเท่ากับจำนวน Switch ที่เสนอ)

1.13.4 สนับสนุนการทำ Authentication สำหรับการบริหารจัดการ (network Management) แบบ Terminal Access Controller Access Control System Plus (TACACS+) และ Radius

1.13.5 อุปกรณ์...

1.13.5 อุปกรณ์ที่เสนอต้องได้การรับรอง (certification) ตามมาตรฐานการรักษาความปลอดภัย Common Criteria ระดับ EAL3+ หรือดีกว่า หรือ ติดตั้งอุปกรณ์ hardware Firewall Module ที่ได้มาตรฐาน Common Criteria ระดับ EAL3+ หรือดีกว่า ในตัว Switch หรือ มีอุปกรณ์ Firewall ภายนอก ที่มี Firewall throughput ไม่น้อยกว่า 40 Gbps ที่ได้มาตรฐาน Common Criteria ระดับ EAL3+ ดีกว่า จำนวนเท่ากับจำนวน Switch ที่เสนอ

1.14 สามารถทำงานได้ตามมาตรฐานการจัดแบ่ง VLAN ได้ไม่น้อยกว่า 4,000 VLAN พร้อมกัน (Active VLAN) ต่อ Switch

1.15 สามารถทำ Multicast แบบ IGMPv1/2/3 Snooping, IPv6 MLDv1, IPv6 MLDv2 และ PIM Snooping ได้เป็นอย่างน้อย โดยตัว Switch เอง

1.16 สามารถทำ Net-Flow หรือ SFlow ได้ โดยตัว Switch เอง

1.17 สามารถทำงานตามมาตรฐาน Ethernet Automatic Protection Switching (EAPS, RFC3619) หรือ resilient packet ring (RPR, IEEE 802.17) หรือ MPLS-TE (RFC2702) โดยตัว Switch เอง

1.18 สนับสนุนการบริหารจัดการแบบ RMON2 (RFC 2021) หรือ SMON (RFC 2613) หรือ เสนออุปกรณ์ภายนอก จำนวนเท่ากับจำนวน Switch ที่เสนอ

1.19 อุปกรณ์ต้องได้รับการรับรองมาตรฐาน FCC, UL และ EN เป็นอย่างน้อย

1.20 ผู้ประสงค์จะเสนอราคา ต้องได้รับการแต่งตั้งโดยตรงจากบริษัทผู้ผลิตหรือบริษัทผู้ผลิตสาขาประจำประเทศไทยให้เป็นตัวแทนจำหน่าย ในโครงการนี้

1.21 ผู้ประสงค์จะเสนอราคาต้องได้รับการรับรอง จากผู้ผลิตหรือผู้ผลิต หรือ บริษัทผู้ผลิตสาขาประเทศไทยโดยตรง ว่ามี ความสามารถด้านการติดตั้ง การสนับสนุนด้านเทคนิค และ การบริการหลังการขายสำหรับโครงการนี้ และ รับรองว่าอุปกรณ์ที่เสนอในโครงการเป็นของใหม่ ยังอยู่ในสายการผลิต โดยมีหนังสือรับรองจากผู้ผลิตหรือผู้ผลิตสาขาประเทศไทยโดยตรง

2. อุปกรณ์กระจายสัญญาณ Access Switch แบบที่ 1 จำนวน 5 ชุด
แต่ละชุดมีคุณลักษณะอย่างน้อยดังต่อไปนี้

2.1 มีลักษณะการทำงานไม่น้อยกว่า Layer 3

2.2 เป็นระบบแบบ Modular Operating System เพื่อรองรับการทำงานแบบไม่มีการหยุดพักได้

2.3 มีพอร์ต Gigabit Ethernet แบบ 10/100/1000 Base-T PoE แบบ RJ-45 จำนวนไม่น้อยกว่า 20 พอร์ต

2.4 มีพอร์ต Gigabit Ethernet แบบ SFP จำนวนไม่น้อยกว่า 4 พอร์ต

2.5 มีพอร์ต 10Gigabit Ethernet แบบ SFP+ หรือ XFP หรือ XENPAK หรือ X2 จำนวนไม่น้อยกว่า 2 พอร์ต

2.6 ติดตั้ง transceiver แบบ 10 Gbase-LR จำนวนไม่น้อยกว่า 2 พอร์ต สำหรับอุปกรณ์ชุดที่ 1-4 และจำนวนไม่น้อยกว่า 1 พอร์ตสำหรับอุปกรณ์ชุดที่ 5

2.7 มี Switching Bandwidth หรือ Switching Fabric สูงสุดรวมไม่น้อยกว่า 128 Gbps และมีค่า Forwarding Rate หรือ throughput สูงสุดรวมไม่น้อยกว่า 95 Mpps ต่อ Switch

2.8 มีพอร์ต Stack โดยเฉพาะที่มีความเร็วสูงสุดรวมไม่น้อยกว่า 40Gbps ต่อ Switch หรือมีโครงสร้างแบบ Modular Chassis โดยต้องมีความเร็วไม่น้อยกว่า 40Gbps ต่อ Slot

2.9 สามารถ...

2.9 สามารถต่อเชื่อมแบบ Stack ได้ไม่น้อยกว่า 8 ชุด หรือ มีโครงสร้าง แบบ Modular Chassis จำนวนไม่น้อยกว่า 8 Slot ที่สามารถรองรับ Module แบบ Distributed Forwarding ที่มี port 10/100/1000 Base-T ไม่น้อยกว่า 20 port ต่อ module ได้

2.10 สามารถทำ Routing ตามโปรโตคอลมาตรฐาน IP แบบ Static, Policy Base Routing และ RIPv1/2 ได้โดยตัว Switch เองเป็นอย่างน้อย และรองรับการเพิ่มความสามารถแบบ OSPF (OSPFv2) ได้

2.11 สามารถทำ IPv6 Routing แบบ Static และ RIPng ได้โดยตัว Switch เองเป็นอย่างน้อย และรองรับการเพิ่มความสามารถแบบ OSPFv3 ได้ในอนาคต

2.12 สามารถทำงานแบบ Multi-chassis Ether Channel (MEC) หรือ Multi-Switch Link aggregation ได้

2.13 รองรับการ stack กับอุปกรณ์ distributed Switch ที่เสนอได้ หรือ ในกรณีที่เสนออุปกรณ์ แบบ Modular Chassis อุปกรณ์ต้องรองรับการใช้ Interface Module ร่วมกับอุปกรณ์ distributed Switch ที่เสนอได้

2.14 มีคุณสมบัติด้านความปลอดภัยดังนี้

2.14.1 สามารถทำ User Authentication ก่อนเข้าใช้งาน Switch อย่างน้อยดังนี้

- สามารถทำการ user Authentication ให้กับผู้ใช้งาน (User) ก่อนจะอนุญาตให้เข้าใช้งาน Switch ได้ในแบบ 802.1x, MAC base และ Web Base Authentication ได้ โดยตัว Switch เอง
- สามารถทำการ MAC base Authentication และ Web Base Authentication ให้กับผู้ใช้งาน (User) ก่อนจะอนุญาตให้เข้าใช้งาน Switch โดยสามารถสร้างและใช้รายการผู้ใช้งานบน Local Database ของ Switch เอง โดยสามารถกำหนด user name, password และ VLAN ของแต่ละ user ได้ ในกรณีที่ อุปกรณ์ที่เสนอไม่สามารถทำ Authentication Local Database ได้ให้เสนออุปกรณ์ Access Control Server ภายนอก ที่มี เครื่องหมายการค้าเดียวกันกับ Switch ที่เสนอ หรือเสนออุปกรณ์ภายนอก ทำหน้าที่ดังกล่าวร่วมกับ Switch ที่เสนอได้ (ในกรณีที่เสนออุปกรณ์ภายนอก ต้องเสนออุปกณ์ภายนอกจำนวนเท่ากับจำนวน Switch ที่เสนอ)

2.14.2 สามารถตรวจจับป้องกันการโจมตี ได้อย่างน้อยดังนี้

- Denial of Service (DoS) Protection โดย เก็บ Packet Header เพื่อวิเคราะห์ และ ทำการ สร้าง Hardware ACL เพื่อควบคุมการ Flow ของข้อมูล โดยตัว Switch เอง หรือ มีอุปกรณ์ทำหน้าที่ NAC (Post-NAC) ภายนอก จำนวนเท่ากับจำนวน Switch ที่เสนอ โดยสามารถทำหน้าที่ดังกล่าวร่วมกับ Switch ที่เสนอได้

สามารถป้องกัน...

- สามารถป้องกันการโจมตีแบบ Protocol Anomaly Protection โดยใช้ built-in hardware chipsets หรือ ASIC ของตัว Switch เอง และ Switch สามารถป้องกันการโจมตี Network Attack ได้อย่างน้อยดังนี้ SYN attack, SQL Slammer, SShredder, SNMP vulnerabilities, tcp denial of service, smurf, LAND attack, tcp syn flooding ,UDP service denial, IP Spoofing Attacks และ Hijacked Terminal Connections และ สามารถป้องกันการโจมตี Host Attack ได้อย่างน้อยดังนี้ Teardrop, boink, opentear, jolt2, newtear, nestea, syndrop, fraggle, papasmurf, synk4, raped, winfreeze, ping –f, ping of death, pepsi5, Latierra, Winnuke, Simping, Sping, Ascend, Stream และ Octopus โดยตัว Switch เอง (ในกรณีที่อุปกรณ์ที่เสนอไม่สามารถตรวจจับป้องกันการจู่โจม ดังกล่าวข้องต้นได้ ให้ผู้ประสงค์จะเสนอราคาจัดหาอุปกรณ์ IPS ภายนอก จำนวนเท่ากับจำนวน Switch ที่เสนอ โดยมี IPS Throughput ต่อ อุปกรณ์ ไม่น้อยกว่า 20 Gbps และ มี port 10G Ethernet ไม่น้อยกว่า 4 port โดยอุปกรณ์ต้องได้มาตรฐาน ICSA หรือ NSS ด้าน IPS)

2.14.3 สามารถทำ Identity Management โดยสามารถทำงานร่วมกับ LDAP Server และ Kerberos Snooping ได้ หรือ มีอุปกรณ์ NAC (Pre-NAC) ภายนอก ที่มี เครื่องหมายการค้าเดียวกันกับ Switch ที่เสนอ หรือ มีอุปกรณ์ทำหน้าที่ Identity Management ภายนอก (ในกรณีที่เสนออุปกรณ์ภายนอก ต้องเสนออุปกณ์ภายนอกจำนวนเท่ากับจำนวน Switch ที่เสนอ)

2.14.4 อุปกรณ์ที่เสนอต้อง ทำงานแบบ CLEAR-Flow (หรือ custom-tailor flow-specific policies) ได้ และ ได้การรับรอง (certification) ตามมาตรฐานการรักษาความปลอดภัย Common Criteria ระดับ EAL3+ หรือดีกว่า หรือ ติดตั้งอุปกรณ์ hardware Firewall Module ที่ได้มาตรฐาน Common Criteria ระดับ EAL3+ หรือดีกว่า ในตัว Switch หรือ มีอุปกรณ์ Firewall ภายนอก ที่มี Firewall throughput ไม่น้อยกว่า 40 Gbps ที่ได้มาตรฐาน Common Criteria ระดับ EAL3+ หรือดีกว่า จำนวนเท่ากับจำนวน Switch ที่เสนอ

2.15 สามารถทำงานได้ตามมาตรฐานการจัดแบ่ง VLAN ได้ไม่น้อยกว่า 4,000 VLAN พร้อมกัน (Active VLAN) ต่อ Switch

2.16 สามารถทำ Multicast แบบ IGMPv1/2/3 Snooping , PIM Snooping และ IPv6 MLDv1 ได้เป็นอย่างน้อย โดยตัว Switch เอง

2.17 สามารถทำ Net-Flow หรือ SFlow ได้ โดยตัว Switch เอง

2.18 สามารถทำงานตามมาตรฐาน Ethernet Automatic Protection Switching (EAPS, RFC3619) หรือ resilient packet ring (RPR, IEEE 802.17) หรือ MPLS-TE (RFC2702) โดยตัว Switch เอง

2.19 สนับสนุนการบริหารจัดการแบบ RMON2 (RFC 2021) หรือ SMON (RFC 2613) หรือ เสนออุปกรณ์ภายนอก จำนวนเท่ากับจำนวน Switch ที่เสนอ

2.20 สนับสนุนการทำงานแบบ IS-IS TRAFFIC ENGINEERING (RFC 3784) หรือ IS-IS Routing ได้

2.21 อุปกรณ์ต้องได้รับการรับรองมาตรฐาน FCC, UL และ EN เป็นอย่างน้อย

2.22 เป็นอุปกรณ์...

2.22 เป็นอุปกรณ์ที่มีเครื่องหมายการค้าหรือมีผู้ผลิต หรืออยู่ภายใต้เจ้าของผลิตภัณฑ์ เดียวกันกับ Distributed Switch ที่เสนอ

2.23 ผู้ประสงค์จะเสนอราคา ต้องได้รับการแต่งตั้งโดยตรงจากบริษัทผู้ผลิตหรือบริษัทผู้ผลิตสาขาประจำประเทศไทยให้เป็นตัวแทนจำหน่าย ในโครงการนี้

2.24 ผู้ประสงค์จะเสนอราคาต้องได้รับการรับรอง จากผู้ผลิตหรือผู้ผลิตหรือบริษัทผู้ผลิตสาขาประเทศไทยโดยตรง ว่ามีความสามารถด้านการติดตั้ง การสนับสนุนด้านเทคนิค และ การบริการหลังการขายสำหรับโครงการนี้ และ รับรองว่าอุปกรณ์ที่เสนอในโครงการเป็นของใหม่ ยังอยู่ในสายการผลิต โดยมีหนังสือรับรองจากผู้ผลิตหรือผู้ผลิตสาขาประเทศไทยโดยตรง

3. อุปกรณ์กระจายสัญญาณ Access Switch แบบที่ 2 จำนวน 16 ชุด
แต่ละชุดมีคุณลักษณะอย่างน้อยดังต่อไปนี้

3.1 มีลักษณะการทำงานไม่น้อยกว่า Layer 3

3.2 เป็นระบบแบบ Modular Operating System เพื่อรองรับการทำงานแบบไม่มีการหยุดพักได้

3.3 มีพอร์ต Gigabit Ethernet แบบ 10/100/1000 Base-T PoE แบบ RJ-45 จำนวนไม่น้อยกว่า 44 พอร์ต

3.4 มีพอร์ต Gigabit Ethernet แบบ SFP จำนวนไม่น้อยกว่า 4 พอร์ต

3.5 มีพอร์ต 10Gigabit Ethernet แบบ SFP+ หรือ XFP หรือ XENPAK หรือ X2 จำนวนไม่น้อยกว่า 2 พอร์ต

3.6 ติดตั้ง transceiver แบบ 10Gbase-LR จำนวนไม่น้อยกว่า 2 พอร์ต สำหรับอุปกรณ์ชุดที่ 1-5 และจำนวนไม่น้อกว่า 1 พอร์ตสำหรับอุปกรณ์ชุดที่ 6-16

3.7 มี Switching Bandwidth หรือ Switching Fabric สูงสุดรวมไม่น้อยกว่า 256 Gbps และมีค่า Forwarding Rate หรือ throughput สูงสุดรวมไม่น้อยกว่า 130 Mpps ต่อ Switch

3.8 มีพอร์ต Stack โดยเฉพาะที่มีความเร็วสูงสุดรวมไม่น้อยกว่า 40Gbps ต่อ Switch หรือมีโครงสร้างแบบ Modular Chassis โดยต้องมีความเร็วไม่น้อยกว่า 40Gbps ต่อ Slot

3.9 สามารถต่อเชื่อมแบบ Stack ได้ไม่น้อยกว่า 8 ชุด หรือ มีโครงสร้าง แบบ Modular Chassis จำนวนไม่น้อยกว่า 8 Slot ที่สามารถรองรับ Module แบบ Distributed Forwarding ที่มี port 10/100/1000 Base-T ไม่น้อยกว่า 44 port ต่อ module ได้

3.10 สามารถทำ Routing ตามโปรโตคอลมาตรฐาน IP แบบ Static, Policy Base routing และ RIPv1/2 ได้โดยตัว Switch เองเป็นอย่างน้อย และรองรับการเพิ่มความสามารถแบบ OSPF (OSPFv2) ได้

3.11 สามารถทำ IPv6 Routing แบบ Static และ RIPng ได้โดยตัว Switch เองเป็นอย่างน้อย และรองรับการเพิ่มความสามารถแบบ OSPFv3 ได้

3.12 สามารถทำงานแบบ Multi-chassis Ether Channel (MEC) หรือ Multi-Switch Link aggregation ได้

3.13 รองรับการ stack กับอุปกรณ์ distributed Switch ที่เสนอได้ หรือ ในกรณีที่เสนออุปกรณ์ แบบ Modular Chassis อุปกรณ์ต้องรองรับการใช้ Interface Module ร่วมกับอุปกรณ์ distributed Switch ที่เสนอได้

3.14 มีคุณสมบัติ...

3.14 มีคุณสมบัติด้านความปลอดภัยดังนี้

3.14.1 สามารถทำ User Authentication ก่อนเข้าใช้งาน Switch อย่างน้อยดังนี้

- สามารถทำการ user Authentication ให้กับผู้ใช้งาน (User) ก่อนจะอนุญาตให้เข้าใช้งาน Switch ได้ในแบบ 802.1x, MAC base และ Web Base Authentication ได้ โดยตัว Switch เอง
- สามารถทำการ MAC base Authentication และ Web Base Authentication ให้กับผู้ใช้งาน (User) ก่อนจะอนุญาตให้เข้าใช้งาน Switch โดยสามารถสร้างและใช้รายการผู้ใช้งานบน Local Database ของ Switch เอง โดยสามารถกำหนด user name, password และ VLAN ของแต่ละ user ได้ ในกรณีที่ อุปกรณ์ที่เสนอไม่สามารถทำ Authentication Local Database ได้ให้เสนออุปกรณ์ Access Control Server ภายนอก ที่มี เครื่องหมายการค้าเดียวกันกับ Switch ที่เสนอ หรือเสนออุปกรณ์ภายนอก ทำหน้าที่ดังกล่าวร่วมกับ Switch ที่เสนอได้ (ในกรณีที่เสนออุปกรณ์ภายนอก ต้องเสนออุปกณ์ภายนอกจำนวนเท่ากับจำนวน Switch ที่เสนอ)

3.14.2 สามารถตรวจจับป้องกันการโจมตี ได้อย่างน้อยดังนี้

- Denial of Service (DoS) Protection โดย เก็บ Packet Header เพื่อวิเคราะห์ และ ทำการ สร้าง Hardware ACL เพื่อควบคุมการ Flow ของข้อมูล โดยตัว Switch เอง หรือ มีอุปกรณ์ทำหน้าที่ NAC (Post-NAC) ภายนอก จำนวนเท่ากับจำนวน Switch ที่เสนอ โดยสามารถทำหน้าที่ดังกล่าวร่วมกับ Switch ที่เสนอได้
- สามารถป้องกันการโจมตีแบบ Protocol Anomaly Protection โดยใช้ built-in hardware chipsets หรือ ASIC ของตัว Switch เอง และ Switch สามารถป้องกันการโจมตี Network Attack ได้อย่างน้อยดังนี้ SYN attack, SQL Slammer, SShredder, SNMP vulnerabilities, tcp denial of service, smurf, LAND attack, tcp syn flooding ,UDP service denial, IP Spoofing Attacks และ Hijacked Terminal Connections และสามารถป้องกันการโจมตี Host Attack ได้อย่างน้อยดังนี้ Teardrop, boink, opentear, jolt2, newtear, nestea, syndrop, fraggle, papasmurf, synk4, raped, winfreeze, ping –f, ping of death, pepsi5, Latierra, Winnuke, Simping, Sping, Ascend, Stream และ Octopus โดยตัว Switch เอง (ในกรณีที่อุปกรณ์ที่เสนอไม่สามารถตรวจจับป้องกันการจู่โจม ดังกล่าวข้องต้นได้ ให้ผู้ประสงค์จะเสนอราคาจัดหาอุปกรณ์ IPS ภายนอก จำนวนเท่ากับจำนวน Switch ที่เสนอ โดยมี IPS Throughput ต่อ อุปกรณ์ ไม่น้อยกว่า 20 Gbps และ มี port 10G Ethernet ไม่น้อยกว่า 4 port โดยอุปกรณ์ต้องได้มาตรฐาน ICSA หรือ NSS ด้าน IPS)

3.14.3 สามารถทำ Identity Management โดยสามารถทำงานร่วมกับ LDAP Server และ Kerberos Snooping ได้ หรือ มีอุปกรณ์ NAC (Pre-NAC) ภายนอก ที่มี เครื่องหมายการค้าเดียวกันกับ Switch ที่เสนอ หรือ มีอุปกรณ์ทำหน้าที่ Identity Management ภายนอก (ในกรณีที่เสนออุปกรณ์ภายนอก ต้องเสนออุปกรณ์ภายนอกจำนวนเท่ากับจำนวน Switch ที่เสนอ)

3.14.4 อุปกรณ์ที่เสนอ...

3.14.4 อุปกรณ์ที่เสนอต้องทำงานแบบ CLEAR-Flow (หรือ custom-tailor flow-specific policies) ได้ และ ได้การรับรอง (certification) ตามมาตรฐานการรักษาความปลอดภัย Common Criteria ระดับ EAL3+ หรือดีกว่า หรือ ติดตั้งอุปกรณ์ hardware Firewall Module ที่ได้มาตรฐาน Common Criteria ระดับ EAL3+ หรือดีกว่า ในตัว Switch หรือ มีอุปกรณ์ Firewall ภายนอก ที่มี Firewall throughput ไม่น้อยกว่า 40 Gbps ที่ได้มาตรฐาน Common Criteria ระดับ EAL3+ หรือดีกว่า จำนวนเท่ากับจำนวน Switch ที่เสนอ

3.15 สามารถทำงานได้ตามมาตรฐานการจัดแบ่ง VLAN ได้ไม่น้อยกว่า 4,000 VLAN พร้อมกัน (Active VLAN) ต่อ Switch

3.16 สามารถทำ Multicast แบบ IGMPv1/2/3 Snooping, PIM Snooping และ IPv6 MLDv1 ได้เป็นอย่างน้อย โดยตัว Switch เอง

3.17 สามารถทำ Net-Flow หรือ SFlow ได้ โดยตัว Switch เอง

3.18 สามารถทำงานตามมาตรฐาน Ethernet Automatic Protection Switching (EAPS, RFC3619) หรือ resilient packet ring (RPR, IEEE 802.17) หรือ MPLS-TE (RFC2702) โดยตัว Switch เอง

3.19 สนับสนุนการบริหารจัดการแบบ RMON2 (RFC 2021) หรือ SMON (RFC 2613) หรือ เสนออุปกรณ์ภายนอก จำนวนเท่ากับจำนวน Switch ที่เสนอ

3.20 สนับสนุนการทำงานแบบ IS-IS TRAFFIC ENGINEERING (RFC 3784) หรือ IS-IS Routing ได้

3.21 อุปกรณ์ต้องได้รับการรับรองมาตรฐาน FCC, UL และ EN เป็นอย่างน้อย

3.22 เป็นอุปกรณ์ที่มีเครื่องหมายการค้าหรือมีผู้ผลิต หรืออยู่ภายใต้เจ้าของลิตภัณฑ์ เดียวกันกับ Distributed Switch ที่เสนอ

3.23 ผู้ประสงค์จะเสนอราคา ต้องได้รับการแต่งตั้งโดยตรงจากบริษัทผู้ผลิตหรือบริษัทผู้ผลิตสาขาประจำประเทศไทยให้เป็นตัวแทนจำหน่าย ในโครงการนี้

3.24 ผู้ประสงค์จะเสนอราคาต้องได้รับการรับรอง จากผู้ผลิตหรือผู้ผลิตหรือบริษัทผู้ผลิตสาขาประเทศไทยโดยตรง ว่ามี ความสามารถด้านการติดตั้ง การสนับสนุนด้านเทคนิค และ การบริการหลังการขายสำหรับโครงการนี้ และ รับรองว่าอุปกรณ์ที่เสนอในโครงการเป็นของใหม่ ยังอยู่ในสายการผลิต โดยมีหนังสือรับรองจากผู้ผลิตหรือผู้ผลิตสาขาประเทศไทยโดยตรง

4 อุปกรณ์กระจายสัญญาณ Server Farm Switch จำนวน 2 ชุด แต่ละชุดมีคุณลักษณะอย่างน้อยดังต่อไปนี้

4.1 มีลักษณะการทำงานไม่น้อยกว่า Layer 3

4.2 เป็นระบบแบบ Modular Operating System เพื่อรองรับการทำงานแบบไม่มีการหยุดพักได้

4.3 มีพอร์ต Gigabit Ethernet แบบ 10/100/1000 Base-T แบบ RJ-45 จำนวนไม่น้อยกว่า 20 พอร์ต

4.4 มีพอร์ต Gigabit Ethernet แบบ SFP จำนวนไม่น้อยกว่า 4 พอร์ต

4.5 มีพอร์ต 10Gigabit Ethernet แบบ SFP+ หรือ XFP หรือ XENPAK หรือ X2 จำนวนไม่น้อยกว่า 2 พอร์ต

4.6 ติดตั้ง transceiver แบบ 10G base-LR จำนวนไม่น้อยกว่า 1 พอร์ต

4.7 มี Switching Bandwidth หรือ Switching Fabric สูงสุดรวมไม่น้อยกว่า 128 Gbps และมีค่า Forwarding Rate หรือ throughput สูงสุดรวมไม่น้อยกว่า 95 Mpps ต่อ Switch

4.8 มีพอร์ต Stack โดยเฉพาะที่มีความเร็วสูงสุดรวมไม่น้อยกว่า 40 Gbps ต่อ Switch หรือมีโครงสร้างแบบ Modular Chassis โดยต้องมีความเร็วไม่น้อยกว่า 40Gbps ต่อ Slot

4.9 สามารถต่อเชื่อม...

4.9 สามารถต่อเชื่อมแบบ Stack ได้ไม่น้อยกว่า 8 ชุด หรือ มีโครงสร้าง แบบ Modular Chassis จำนวนไม่น้อยกว่า 8 Slot ที่สามารถรองรับ Module แบบ Distributed Forwarding ที่มี port 10/100/1000 Base-T ไม่น้อยกว่า 20 port ต่อ module ได้

4.10 สามารถทำRouting ตามโปรโตคอลมาตรฐานIP แบบ Static, Policy Base Routing และ RIPv1/2 ได้ โดยตัว Switch เองเป็นอย่างน้อย และรองรับการเพิ่มความสามารถแบบOSPF (OSPFv2) ได้

4.11 สามารถทำ IPv6 Routing แบบ Static และ RIPng ได้โดยตัว Switch เองเป็นอย่างน้อย และรองรับการเพิ่มความสามารถแบบ OSPFv3 ได้

4.12 สามารถทำงานแบบMulti-chassis Ether Channel (MEC) หรือ Multi-Switch Link aggregation ได้

4.13 รองรับการ stack กับอุปกรณ์ distributed Switch ที่เสนอได้ หรือ ในกรณีที่เสนออุปกรณ์ แบบ Modular Chassis อุปกรณ์ต้องรองรับการใช้ Interface Module ร่วมกับอุปกรณ์ distributed Switch ที่เสนอได้

4.14 มีคุณสมบัติด้านความปลอดภัยดังนี้

4.14.1 สามารถทำ User Authentication ก่อนเข้าใช้งาน Switch อย่างน้อยดังนี้

- สามารถทำการ user Authentication ให้กับผู้ใช้งาน (User) ก่อนจะอนุญาตให้เข้าใช้งาน Switch ได้ในแบบ 802.1x, MAC base และ Web Base Authentication ได้ โดยตัว Switch เอง
- สามารถทำการ MAC base Authentication และ Web Base Authentication ให้กับผู้ใช้งาน (User) ก่อนจะอนุญาตให้เข้าใช้งาน Switch โดยสามารถสร้างและใช้รายการผู้ใช้งานบน Local Database ของ Switch เอง โดยสามารถกำหนด user name, password และ VLAN ของแต่ละ user ได้ ในกรณีที่ อุปกรณ์ที่เสนอไม่สามารถทำ Authentication Local Database ได้ให้เสนออุปกรณ์ Access Control Server ภายนอก ที่มี เครื่องหมายการค้าเดียวกันกับ Switch ที่เสนอ หรือเสนออุปกรณ์ภายนอก ทำหน้าที่ดังกล่าวร่วมกับ Switch ที่เสนอได้ (ในกรณีที่เสนออุปกรณ์ภายนอก ต้องเสนออุปกณ์ภายนอกจำนวนเท่ากับจำนวน Switch ที่เสนอ)

4.14.2 สามารถตรวจจับป้องกันการโจมตี ได้อย่างน้อยดังนี้

- Denial of Service (DoS) Protection โดย เก็บ Packet Header เพื่อวิเคราะห์ และ ทำการ สร้าง Hardware ACL เพื่อควบคุมการ Flow ของข้อมูล โดยตัว Switch เอง หรือ มีอุปกรณ์ทำหน้าที่ NAC (Post-NAC) ภายนอก จำนวนเท่ากับจำนวน Switch ที่เสนอ โดยสามารถทำหน้าที่ดังกล่าวร่วมกับ Switch ที่เสนอได้
- สามารถป้องกันการโจมตีแบบ Protocol Anomaly Protection โดยใช้ built-in hardware chipsets หรือ ASIC ของตัว Switch เอง และ Switch สามารถป้องกันการโจมตี Network Attack ได้อย่างน้อยดังนี้ SYN attack, SQL Slammer, SShredder, SNMP vulnerabilities, tcp denial of service, smurf, LAND attack, tcp syn flooding, UDP service denial, IP Spoofing Attacks และ Hijacked Terminal Connections และ สามารถป้องกันการโจมตี Host Attack ได้อย่างน้อยดังนี้ Teardrop, boink, opentear, jolt2, newtear, nestea, syndrop, fraggle, papasmurf, synk4, raped, winfreeze, ping –f, ping of death, pepsi5, Latierra, Winnuke, Simping, Sping, Ascend, Stream และ

Octopus...

Octopus โดยตัว Switch เอง (ในกรณีที่อุปกรณ์ที่เสนอไม่สามารถตรวจจับป้องกันการจู่โจม ดังกล่าวข้องต้นได้ ให้ผู้ประสงค์จะเสนอราคาจัดหาอุปกรณ์ IPS ภายนอก จำนวนเท่ากับจำนวน Switch ที่เสนอ โดยมี IPS Throughput ต่อ อุปกรณ์ ไม่น้อยกว่า 20 Gbps และ มี port 10G Ethernet ไม่น้อยกว่า 4 port โดยอุปกรณ์ต้องได้มาตรฐาน ICSA หรือ NSS ด้าน IPS)

4.14.3 สามารถทำ Identity Management โดยสามารถทำงานร่วมกับ LDAP Server และ Kerberos Snooping ได้ หรือ มีอุปกรณ์ NAC (Pre-NAC) ภายนอก ที่มี เครื่องหมายการค้าเดียวกันกับ Switch ที่เสนอ หรือ มีอุปกรณ์ทำหน้าที่ Identity Management ภายนอก (ในกรณีที่เสนออุปกรณ์ภายนอก ต้องเสนออุปกรณ์ภายนอกจำนวนเท่ากับจำนวน Switch ที่เสนอ)

4.14.4 อุปกรณ์ที่เสนอต้อง ทำงานแบบ CLEAR-Flow (หรือ custom-tailor flow-specific policies) ได้ และ ได้การรับรอง (certification) ตามมาตรฐานการรักษาความปลอดภัย Common Criteria ระดับ EAL3+ หรือดีกว่า หรือ ติดตั้งอุปกรณ์ hardware Firewall Module ที่ได้มาตรฐาน Common Criteria ระดับ EAL3+ หรือดีกว่า ในตัว Switch หรือ มีอุปกรณ์ Firewall ภายนอก ที่มี Firewall throughput ไม่น้อยกว่า 40 Gbps ที่ได้มาตรฐานCommon Criteria ระดับ EAL3+ หรือดีกว่า จำนวนเท่ากับจำนวนSwitch ที่เสนอ

4.15 สามารถทำงานได้ตามมาตรฐานการจัดแบ่ง VLAN ได้ไม่น้อยกว่า 4,000 VLAN พร้อมกัน (Active VLAN) ต่อ Switch

4.16 สามารถทำ Multicast แบบ IGMPv1/2/3 Snooping, PIM Snooping และ IPv6 MLDv1 ได้เป็นอย่างน้อย โดยตัว Switch เอง

4.17 สามารถทำ Net-Flow หรือ SFlow ได้

4.18 สามารถทำงานตามมาตรฐาน Ethernet Automatic Protection Switching (EAPS, RFC3619) หรือ resilient packet ring (RPR, IEEE 802.17) หรือ MPLS-TE (RFC2702) โดยตัว Switch เอง

4.19 สนับสนุนการบริหารจัดการแบบ RMON2 (RFC 2021) หรือ SMON (RFC 2613) หรือ เสนออุปกรณ์ภายนอก จำนวนเท่ากับจำนวน Switch ที่เสนอ

4.20 สนับสนุนการทำงานแบบ IS-IS TRAFFIC ENGINEERING (RFC 3784) หรือ IS-IS Routing ได้

4.21 อุปกรณ์ต้องได้รับการรับรองมาตรฐาน FCC, UL และ EN เป็นอย่างน้อย

4.22 เป็นอุปกรณ์ที่มีเครื่องหมายการค้าหรือมีผู้ผลิต หรืออยู่ภายใต้เจ้าของลิตภัณฑ์ เดียวกันกับ Distributed Switch ที่เสนอ

4.23 ผู้ประสงค์จะเสนอราคา ต้องได้รับการแต่งตั้งโดยตรงจากบริษัทผู้ผลิตหรือบริษัทผู้ผลิตสาขาประจำประเทศไทยให้เป็นตัวแทนจำหน่าย ในโครงการนี้

4.24 ผู้ประสงค์จะเสนอราคาต้องได้รับการรับรอง จากผู้ผลิตหรือผู้ผลิตหรือบริษัทผู้ผลิตสาขาประเทศไทยโดยตรง ว่ามี ความสามารถด้านการติดตั้ง การสนับสนุนด้านเทคนิค และ การบริการหลังการขายสำหรับโครงการนี้ และ รับรองว่าอุปกรณ์ที่เสนอในโครงการเป็นของใหม่ ยังอยู่ในสายการผลิตโดยมีหนังสือรับรองจากผู้ผลิตหรือผู้ผลิตสาขาประเทศไทยโดยตรง

5 อุปกรณ์...

5 อุปกรณ์บริหารจัดการเครือข่ายไร้สาย Wireless LAN Controller จำนวน 1 ชุด
โดยมีคุณลักษณะอย่างน้อยดังต่อไปนี้

5.1 เป็นระบบบริหารจัดการ Authentication, Authorization และ Accounting (AAA) หรือสามารถเก็บ user database เช่น user name และ password บนตัวอุปกรณ์ได้

5.2 สามารถตรวจสอบผู้ใช้ในการเข้าใช้สิทธิ์ (Authentication) ระบบเครือข่าย

5.3 สนับสนุนการเข้ารหัสแบบWEP Encryption 64 และ 128 bit, TKIP RC4 128 bits และ CCMP AES

5.4 สามารถทำ QoS (Quality of Service) โดยกำหนดความสำคัญของทราฟฟิกได้แบบ Multiple priority queues SSID

5.5 มีพอร์ต Gigabit Ethernet แบบ 10/100/1000Base-T อย่างน้อย 4 Port สำหรับการเชื่อมต่อเข้ากับเครือข่าย

5.6 ต้องทำงานร่วมกับ Access Point ไม่น้อยกว่า 43 Access Point และรองรับ Access Point สูงสุดไม่น้อยกว่า 64 Access Point

5.7 ต้องรองรับคุณสมบัติ Stateful Firewall เพื่อใช้ในการกำหนดสิทธิ์การใช้งาน (Policy) และมี Firewall Throughput ไม่ต่ำกว่า 4Gbps หรือใช้อุปกรณ์ภายนอกโดยต้องมี Firewall Throughput ไม่ต่ำกว่า 4Gbps และมีพอร์ต 10/100/1000BaseT อย่างน้อย 2 พอร์ต

5.8 สามารถทำ Advanced Wireless LAN Intrusion Detection System ได้ โดยสามารถตรวจจับ Unauthorized ad-hoc client, ASLEAP attack, AirJack attack และ DoS ได้เป็นอย่างน้อย หรือใช้อุปกรณ์ภายนอกโดยต้องมีคุณสมบัติอย่างน้อยดังนี้ มีพอร์ต 10/100/1000 Mbps ไม่น้อยกว่า 2 พอร์ต และมี IPS Throughput ไม่น้อยกว่า 4Gbps พร้อมทั้งสามารถตรวจจับ Unauthorized ad-hoc client, ASLEAP attack และ Airjack attack ได้เป็นอย่างน้อย และสามารถป้องกันการโจมตีประเภท DoS ได้เป็นอย่างน้อย

5.9 ทำงานเป็น DHCP Server เพื่อ แจก IP Address ให้กับ เครื่องลูกข่าย ได้ และสามารถใช้งานร่วมกับ DHCP Server อื่นๆในระบบได้

5.10 สามารถทำการตรวจสอบ Interfere ที่มาจาก Wi-Fi Network และ Non Wi-Fi source เช่น 2.4 GHz cordless phone, Microwave Oven, Analog Video Camera, Gaming Console

5.11 มีความสามารถในการทำ spectrum analysis chart เช่น FFT Duty Cycle, Real-Time FFT, Swept Spectrogram

5.12 สามารถตรวจสอบสิทธิและบริหารจัดการ Access Point ที่ต่อเข้าในระบบได้

5.13 มี Encryption throughput 3DES ไม่น้อยกว่า 4 Gbps หรือใช้อุปกรณ์ภายนอกที่มี Encryption throughput 3DES ไม่น้อยกว่า 4 Gbps

5.14 มีความสามารถในการทำ High Availability ระหว่าง Controller ได้ โดยใช้หลักการทำงานแบบ VRRP หรือเทียบเท่า

5.15 สามารถรองรับการทำ User Load Balance หรือ Spectrum Load Balance บนอุปกรณ์ Wireless Security Switch หรือบน Access Point ได้

5.16 สามารถรองรับการทำ Authentication แบบ EAP, EAP-TLS, EAP-SIM, EAP-TTLS, EAP-MD5, EAP-TLV, และ EAP-FAST ถ้าอุปกรณ์ไม่สามารถรองรับได้ ให้เสนออุปกรณ์ภายนอกได้ เช่น รองรับการทำงานควบคู่กับอุปกรณ์ Wireless Management Software เพื่อบริหาร wireless network ได้

5.17 รองรับมาตรฐาน...

5.17 รองรับมาตรฐาน Security standards ต่อไปนี้ WPA, WPA2, 802.11i, 802.1x, MAC authentication, X.509 certificates, RADIUS AAA, Local AAA หรือ Internal database, Web-based captive portal authentication เป็นอย่างน้อย

5.18 สามารถรองรับและสนับสนุนการทำ location tracking ได้

5.19 สามารถรองรับและสนับสนุนการทำGuest access ได้ โดยผ่าน web browser หรือ captive portal

5.20 สามารถ generate guest ticket เช่น create user name และ password สำหรับ guest ได้ รวมทั้งสามารถกำหนดเวลาการเข้าใช้งานระบบ wireless สำหรับ guest ได้ เช่นกำหนดวันหมดอายุ หรือ จำกัดการใช้งานเป็นชั่วโมง

5.21 มีความสามารถในการควบคุมการปรับเปลี่ยน channel และ power โดยอัตโนมัติ

5.22 สามารถรองรับการทำ RF Plan ได้ โดยการใส่ Floor Plan เข้าไปในระบบเพื่อ plan จำนวน Access Point หรือเสนออุปกรณ์ภายนอกช่วยในการทำงานได้

5.23 สามารถทำการบริหารจัดการปริมาณการใช้งานได้ (Bandwidth Contract)

5.24 รองรับการตรวจจับ และ แสดงตำแหน่ง Access Point แปลกปลอม (Rogue Access Point) ได้

5.25 ต้องมีคุณสมบัติการทำ fast roaming ได้

5.26 มีความสามารถในการทำ Device Fingerprint เพื่อตรวจสอบ client ที่เข้ามาในระบบว่าเป็น client ประเภทใด หรือใช้อุปกรณ์ภายนอกช่วยในการทำงานได้

5.27 อุปกรณ์จะต้องมีความสามารถในการทำ Band Steering เพื่อผลักให้ Client ที่รองรับ 5 GHz สามารถใช้งานที่ 5 GHz ได้โดยอัตโนมัติ

5.28 สามารถ บริหารจัดการและกำหนดค่าให้กับอุปกรณ์ผ่านทาง Web Browser, Console port, SSH, SNMP หรือ ระบบ Wireless Network

5.29 ผู้ประสงค์จะเสนอราคา ต้องได้รับการแต่งตั้งโดยตรงจากบริษัทผู้ผลิตหรือบริษัทผู้ผลิตสาขาประจำประเทศไทยให้เป็นตัวแทนจำหน่าย ในโครงการนี้

5.30 ผู้ประสงค์จะเสนอราคาต้องได้รับการรับรอง จากผู้ผลิตหรือผู้ผลิตหรือบริษัทผู้ผลิตสาขาประเทศไทยโดยตรง ว่ามี ความสามารถด้านการติดตั้ง การสนับสนุนด้านเทคนิค และ การบริการหลังการขายสำหรับโครงการนี้ และ รับรองว่าอุปกรณ์ที่เสนอในโครงการเป็นของใหม่ ยังอยู่ในสายการผลิต โดยมีหนังสือรับรองจากผู้ผลิตหรือผู้ผลิตสาขาประเทศไทยโดยตรง

6 อุปกรณ์ Wireless Access Point จำนวน 43 ชุด โดยแต่ละชุดมีคุณลักษณะอย่างน้อยดังต่อไปนี้

6.1 เป็นอุปกรณ์ที่ใช้คลื่นความถี่วิทยุในการรับส่งข้อมูลโดยใช้งานย่านความถี่ 2.4 GHz และ 5 GHz (Dual Radio) ทำงานแบบ Access Point

6.2 เป็นอุปกรณ์ที่รองรับการทำงาน MIMO ไม่น้อยกว่า 3x3

6.3 มีคุณสมบัติสนับสนุนมาตรฐาน IEEE802.1a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n

6.4 มีพอร์ต Ethernet แบบ10/100/1000BaseT สำหรับการเชื่อมต่อเข้ากับเครือข่ายและรองรับ Power in Line หรือ PoE ตามมาตรฐาน IEEE802.3af/ IEEE802.3at ได้ ไม่น้อยกว่า 2 Port

6.5 อุปกรณ์จะต้องรองรับ data rate ที่ 450 Mbps ต่อ radio

6.6 สามารถรองรับการบริหารจัดการความถี่ RF Management, ความแรงของสัญญาณ และ Traffic หรือ Client Load ให้กับ อุปกรณ์ Access Point เมื่อใช้งานร่วมกับ Wireless Security Switch หรือ Wireless Controller ได้

6.7 สามารถ...

6.7 สามารถทำการตรวจสอบผู้ใช้งานเพื่อไม่ให้เข้าใช้งานกับระบบได้ (MAC Address Authentication) เมื่อใช้งานร่วมกับ Wireless Controller ที่เสนอ

6.8 สามารถรองรับการใช้งานร่วมกับ DHCP Server ได้

6.9 รองรับมาตรฐาน IEEE 802.1x, WEP, WPA และ WPA2 เมื่อใช้งานร่วมกับ Wireless Security Switch หรือ Wireless Controller

6.10 สามารถ บริหารจัดการ และกำหนดค่าให้กับอุปกรณ์ผ่านทาง Web Browser จาก Controller ได้

6.11 อุปกรณ์จะต้องมีพอร์ต Console อย่างน้อย 1 พอร์ตเพื่อใช้ในการ set up ตัว Access Point

6.12 เป็นอุปกรณ์ที่มีเครื่องหมายการค้าหรือมีผู้ผลิต หรืออยู่ภายใต้เจ้าของผลิตภัณฑ์ เดียวกันกับอุปกรณ์บริหารจัดการเครือข่ายไร้สาย Wireless LAN Controller ที่เสนอ

6.13 ผู้ประสงค์จะเสนอราคา ต้องได้รับการแต่งตั้งโดยตรงจากบริษัทผู้ผลิตหรือบริษัทผู้ผลิตสาขาประจำประเทศไทยให้เป็นตัวแทนจำหน่าย ในโครงการนี้

6.14 ผู้ประสงค์จะเสนอราคาต้องได้รับการรับรอง จากผู้ผลิตหรือผู้ผลิตหรือบริษัทผู้ผลิตสาขาประเทศไทยโดยตรง ว่ามี ความสามารถด้านการติดตั้ง การสนับสนุนด้านเทคนิค และ การบริการหลังการขายสำหรับโครงการนี้ และ รับรองว่าอุปกรณ์ที่เสนอในโครงการเป็นของใหม่ ยังอยู่ในสายการผลิตโดยมีหนังสือรับรองจากผู้ผลิตหรือผู้ผลิตสาขาประเทศไทยโดยตรง

7 ติดตั้งสายสัญญาณแบบ UTP Cat6 สำหรับ Access Point จำนวน 43 จุด โดยมีคุณลักษณะเฉพาะอย่างน้อยดังต่อไปนี้

7.1 เป็นสายสัญญาณชนิด Category 6 หรือดีกว่า

7.2 สายสัญญาณ UTP เป็นสายทองแดงตีเกลียว 4 คู่ ชนิด Unshielded Twisted Pair

7.3 สามารถรองรับการใช้งานแบบ IEEE 802.3, Ethernet10BASE-T และ 100BASE-TX and 1000BASE-T (Gigabit Ethernet)

7.4 มีฉนวนเปลือกนอกเป็น PVC Jacket

7.5 มีคุณสมบัติอย่างน้อยตามมาตรฐานของ ANSI/TIA/EIA-568-B.2-1 Category 6

7.6 ต้องเป็นผลิตภัณฑ์ที่มีเครื่องหมายการค้าเดียวกันกับสายใยแล้วนำแสง (Fiber Optic) ที่เสนอ

8 อุปกรณ์ตรวจจับและป้องกันการบุกรุกบนระบบเครือข่าย (Intrusion Prevention System) จำนวน 1 ระบบ มีคุณลักษณะอย่างน้อยดังต่อไปนี้

8.1 เป็นอุปกรณ์แบบ Hardware Appliance ที่ออกแบบมาเพื่อทำหน้าที่ป้องกันการบุกรุกบนระบบเครือข่าย (IPS) โดยเฉพาะ โดยไม่ใช่อุปกรณ์แบบ UTM หรืออุปกรณ์ Firewall ที่ทำงานแบบ IPS

8.2 มีผลการทดสอบ หรือ ได้รับการรับรอง จาก จาก ICSA และ NSS Labs เป็นอย่างน้อย

8.3 ได้รับการประเมินจากหน่วยงานที่น่าเชื่อถือให้อยู่ในกลุ่มผู้นำ (Leader) ของกลุ่มตลาดอุปกรณ์ IPS จาก Gartner IPS Magic Quadrant เป็นอย่างน้อย

8.4 มีความสามารถในการตรวจจับ (IPS Throughput) สูงสุดไม่น้อยกว่า 2 Gbps ต่อ อุปกรณ์

8.5 อุปกรณ์สามารถ...

8.5 อุปกรณ์สามารถรับ Concurrent Connections (หรือ Session) สูงสุดไม่น้อยกว่า 15,000,000 Concurrent Connections (หรือ Session) หรือ เสนออุปกรณ์ IPS รุ่นเดียวกับที่เสนอเพิ่มโดยทำงานแบบ Active/Active หรือ load balance เพื่อให้ได้ Concurrent Connections (หรือ Session) รวมสูงสุดไม่น้อยกว่า 15,000,000 Concurrent Connections (หรือ Session)

8.6 ระบบจะต้องถูกออกแบบมาเพื่อทำงานร่วมกับเครือข่ายโดยไม่เกิดผลกระทบ โดยจะต้องมีค่า Latency ไม่เกิน 150 microseconds

8.7 อุปกรณ์ที่เสนอต้องมีโครงสร้างแบบ Modular interface ที่สามารถรองรับการติดตั้ง module แบบ 10Gb Ethernet ได้ รวมสูงสุดไม่น้อยกว่า 6 พอร์ต ภายในตัวอุปกรณ์ที่เสนอ หรือ มีช่องเสียบ 10Gb ethernet แบบ SFP+ หรือ XFP มาพร้อมไม่น้อยกว่า 6 ช่อง

8.8 ติดตั้ง Network Interface แบบ 1Gbps Copper ไม่น้อยกว่า 8 พอร์ต

8.9 มีพอร์ตสำหรับบริหารจัดการอุปกรณ์แบบ 10/100/1000 Ethernet หรือดีกว่า อย่างน้อย 1 พอร์ต และ Serial Port อย่างน้อย 1 port (Out of band management)

8.10 อุปกรณ์ต้องสามารถทำ Hardware Bypass ในกรณี Hardware/Software เกิดปัญหารวมถึงกรณีไฟฟ้าดับ โดยสามารถเลือก Fail-open หรือ Fail-Close ในแต่ละ segment ได้ หรือเสนออุปกรณ์ต่อพ่วงได้

8.11 สามารถป้องกันการโจมตีและการบุกรุกเครือข่ายได้อย่างน้อยดังนี้

- 8.11.1 ป้องกันการระบาดของ Virus และ Worm
- 8.11.2 ป้องกันการโจมตีแบบ Denial of Server (DoS) Attack และ DDoS ได้
- 8.11.3 ป้องกันการบุกรุกแบบ Vulnerability Exploit, Reconnaissance (port scan/sweep)
- 8.11.4 ป้องกันเทคนิคการหลบซ่อนการโจมตีแบบ IP Defragmentation, TCP Stream Segmentation, RPC Fragmentation, URL Obfuscation, HTML Obfuscation, HTML Evasion และ FTP Evasion ได้
- 8.11.5 ป้องกันได้ตั้งแต่ระดับ Layer 2 (ARP) Attacks
- 8.11.6 ป้องกันเครือข่ายและสามารถตรวจจับวิธีการบุกรุกดังนี้ Overflow, Backdoor Program, Trojan Horse และ Spy ware

8.12 สามารถแจ้งเตือนและโต้ตอบการโจมตีด้วยวิธีต่อไปนี้

- 8.12.1 Drop เมื่อเกิดเหตุการณ์ถึงจำนวนที่ตั้งไว้ (Threshold)
- 8.12.2 ติดต่อกับอุปกรณ์ภายนอกเพื่อป้องกันข้อมูลไม่ให้วิ่งผ่าน (external remediation) โดยสามารถทำงานร่วมกับอุปกรณ์เครือข่ายเช่น Router ได้

8.13 มี Power Supply จำนวนไม่น้อยกว่า 2 ชุด

8.14 สามารถใช้งานมาตรฐาน IPv6 ทั้งการจัดการ IPS และการตรวจสอบข้อมูลการโจมตี โดยผ่านการทดสอบจากหน่วยงานที่น่าเชื่อถือเช่น ICSA หรือ USGv6

8.15 ได้รับมาตรฐาน ความปลอดภัย FCC, UL หรือ CE เป็นอย่างน้อย

8.16 สามารถบริหารจัดการอุปกรณ์ได้ผ่าน Command-line หรือ GUI โดยผ่านเว็บแบบ HTTPS ได้เป็นอย่างน้อย

8.17 มีระบบบริหารจัดการ...

8.17 มีระบบบริหารจัดการจากศูนย์กลางแบบ Software หรือ Hardware เพื่อจัดการอุปกรณ์ โดยมีความสามารถอย่างน้อยดังต่อไปนี้

8.17.1 สามารถจัดการจัดเก็บ Log และสามารถส่ง Log ไปที่ระบบจัดเก็บ Log ศูนย์กลาง (Centralized Log Management)

8.17.2 สามารถบริหารจัดการนโยบายเรื่องความปลอดภัย และส่งไปยังอุปกรณ์ได้ โดยจะต้องไม่มีผลกระทบต่อการตรวจสอบการโจมตีระหว่างที่มีการติดตั้งนโยบายความปลอดภัยชุดใหม่

8.17.3 สามารถแสดงสถานการณ์ทำงานของอุปกรณ์ (Dashboard) โดยสามารถแสดงถึงสถานการณ์ถูกโจมตีของระบบเครือข่าย และสามารถเลือกแสดงในระดับความรุนแรงที่สนใจได้ โดยสามารถเลือกแสดงเฉพาะการโจมตีที่มีผลกระทบอย่างรุนแรงกับเครือข่ายที่กำหนดได้

8.17.4 สามารถปรับแต่งการแสดงผลของ Dashboard โดยกำหนดเงื่อนไขที่ต้องการแสดง (search criteria) ได้เอง รวมถึงสามารถปรับช่วงเวลาการแสดงข้อมูลได้อย่างน้อยเป็นชั่วโมง หรือ วัน

8.17.5 สามารถกำหนดให้มีการดึงข้อมูล (signature/rule) จากผู้ผลิตได้อัตโนมัติ

8.17.6 อนุญาตให้ผู้ใช้สามารถสร้างรูปแบบการตรวจสอบเองได้ (custom signature/rule) โดยมีเครื่องมือ หรือ GUI เพื่อช่วยในการสร้าง

8.17.7 สามารถจัดเก็บข้อมูลที่มีการโจมตี (Packet Capture) และสามารถเรียกดูได้โดยตรงจากอุปกรณ์บริหารจัดการ

8.18 ระบบจะต้องสามารถให้คำแนะนำและปรับแต่งนโยบายเรื่องความปลอดภัยได้อย่างอัตโนมัติ โดยอาศัยข้อมูลได้ทั้งจากการทำ Passive Scan หรือ Active Scan

8.19 รองรับการรับข้อมูลจากอุปกรณ์ภายนอก เช่นระบบ Vulnerability Management หรือข้อมูลจากระบบเครือข่ายเช่น Net flow เพื่อนำมาใช้ในการประเมินความเสี่ยงของระบบได้

8.20 ผู้ประสงค์จะเสนอราคา ต้องได้รับการแต่งตั้งโดยตรงจากบริษัทผู้ผลิตหรือบริษัทผู้ผลิตสาขาประจำประเทศไทยให้เป็นตัวแทนจำหน่าย ในโครงการนี้

8.21 ผู้ประสงค์จะเสนอราคาต้องได้รับการรับรอง จากผู้ผลิตหรือผู้ผลิตหรือบริษัทผู้ผลิตสาขาประเทศไทยโดยตรง ว่ามี ความสามารถด้านการติดตั้ง การสนับสนุนด้านเทคนิค และ การบริการหลังการขายสำหรับโครงการนี้ และ รับรองว่าอุปกรณ์ที่เสนอในโครงการเป็นของใหม่ ยังอยู่ในสายการผลิต โดยมีหนังสือรับรองจากผู้ผลิตหรือผู้ผลิตสาขาประเทศไทยโดยตรง

9 ติดตั้งสายสัญญาณแบบใยแก้วนำแสง (Fiber Optic) ชนิด Single Mode จำนวน 1 ระบบ โดยมีคุณลักษณะเฉพาะอย่างน้อยดังต่อไปนี้

9.1 ติดตั้งสายสัญญาณใยแก้วนำแสง (Fiber Optic) ขนาด 6 Core จากห้อง Data Center ชั้น4 อาคารวิเคราะห์ฯ ไปยังตู้ Rack ตามชั้น 1-9 ภายในอาคารวิเคราะห์ฯ จำนวนไม่น้อยกว่า 9 links

9.2 ติดตั้งสายสัญญาณใยแก้วนำแสง (Fiber Optic) ขนาด 6 Core จากห้อง Data Center ชั้น4 อาคารวิเคราะห์ฯ ไปยังตู้ Rack ตามชั้น 1-5 อาคารดำรงฯ จำนวนไม่น้อยกว่า 5 links

9.3 ติดตั้งสายสัญญาณ...

9.3 ติดตั้งสายสัญญาณใยแก้วนำแสง (Fiber Optic) ขนาด 6 Core จากห้อง Data Center ชั้น3 อาคารดำรงฯ ไปยังตู้ Rack ตามชั้น 1-5 อาคารดำรงฯ จำนวนไม่น้อยกว่า 5 links

9.4 ติดตั้งสายสัญญาณใยแก้วนำแสง (Fiber Optic) ขนาด 6 Core จากห้อง Data Center ชั้น3 อาคารดำรงฯ ไปยังตู้ Rack ตามชั้น 1-9 อาคารวิเคราะห์ฯ จำนวนไม่น้อยกว่า 9 links

9.5 ติดตั้งสายสัญญาณใยแก้วนำแสง (Fiber Optic) ขนาด 6 Core จากห้อง Data Center ชั้น4 อาคารวิเคราะห์ฯ ไปยังตู้ Rack อาคารสันทนาการ จำนวนไม่น้อยกว่า 1 links

9.6 ติดตั้งสายสัญญาณใยแก้วนำแสง (Fiber Optic) ขนาด 12 Core จากห้อง Data Center ชั้น4 อาคารวิเคราะห์ฯ ไปยัง Datacenter อาคารดำรงฯ ชั้น 3 จำนวนไม่น้อยกว่า 1 link

9.7 ติดตั้งสายสัญญาณใยแก้วนำแสง (Fiber Optic) ขนาด 6 Core จากห้อง Data Center ชั้น3 อาคารดำรงฯ ไปยัง อาคารสันทนาการ จำนวนไม่น้อยกว่า 1 link

9.8 ข้อกำหนดทางด้านเทคนิคและคุณลักษณะเฉพาะของอุปกรณ์ ระบบสายใยแก้วนำแสง (Fiber Optic) อย่างน้อยดังต่อไปนี้

9.8.1 คุณลักษณะเฉพาะของสายสัญญาณใยแก้วนำแสง (Fiber Optic) ต้องมีคุณสมบัติอย่างน้อยดังต่อไปนี้

9.8.1.1 เป็นสายใยแก้วนำแสงชนิด Single Mode แบบติดตั้งภายนอกอาคาร (Outdoor Fiber Optic Cable) มีโครงสร้างเป็นแบบ Central Loose Tube เป็นแบบชนิด PSP Armored

9.8.1.2 สายใยแก้วนำแสง ต้องมีฉนวนเปลือกนอกเป็น Polyethylene (PE) Outer Sheath

9.8.1.3 สายใยแก้วนำแสง ต้องมีโครงสร้างเป็น Parallel Double Steel Wire และ PSP อยู่ล้อมรอบสายเพื่อเพิ่มความแข็งแรงให้กับสายใยแก้วนำแสง

9.8.1.4 สายใยแก้วนำแสง ต้องมี Water proof tape อยู่ระหว่าง PSP Armored กับ Loose Tube อยู่ล้อมรอบสาย เพื่อป้องกันน้ำและความชื้น

9.8.1.5 เป็นสายใยแก้วนำแสงที่มีโครงสร้างเป็น Loose Tube ภายใน Loose Tube มีส่วนประกอบที่เป็น Jelly Compound เพื่อป้องกันในส่วนของ Fiber Optic Cores และ Loose Tube

9.8.1.6 สายเคเบิ้ลใยแก้วนำแสง ต้องผ่านการรับรองมาตรฐาน TIA/EIA 568-B.3, IEC 794 เป็นอย่างน้อย

9.8.1.7 สายสัญญาณใยแก้วนำแสงที่เสนอต้องมีบริษัทฯแม่ของบริษัทเจ้าของผลิตภัณฑ์ตั้งอยู่ในแถบยุโรป หรืออเมริกา หรือญี่ปุ่น โดยมีเอกสารอ้างอิงระบุสถานที่ชัดเจน

9.8.1.8 รับประกันการใช้งานทั้งระบบอย่างน้อย 25 ปี (25 Years systems warranty) จากเจ้าของผลิตภัณฑ์

10. ข้อกำหนดทั่วไป...

10 ข้อกำหนดทั่วไป

10.1 ผู้ประสงค์จะเสนอราคาจะต้องดำเนินการจัดหา ติดตั้ง และปรับแต่ง (Customize) อุปกรณ์ที่เสนอในโครงการฯ ให้สามารถใช้งานร่วมกับระบบและอุปกรณ์ต่างๆ ของทางสถาบันมะเร็งแห่งชาติได้อย่างถูกต้องและมีประสิทธิภาพ

10.2 ผู้ประสงค์จะเสนอราคาจะต้องทำตารางเปรียบเทียบรายละเอียดของข้อกำหนดการจัดซื้อโครงการระบบจัดเก็บและส่งข้อมูลภาพทางการแพทย์(PACS)ระยะที่2 เพื่อวางระบบเครือข่ายคอมพิวเตอร์ในการรับส่งข้อมูล สถาบันมะเร็งแห่งชาติ ที่เสนอเป็นรายข้อทุกข้อ โดยใช้ตัวอย่างแบบฟอร์มการเปรียบเทียบตามตารางที่ 1 ในกรณีที่ต้องมีการอ้างอิงถึงข้อความอื่นในเอกสารที่เสนอมา ผู้ประสงค์จะเสนอราคาจะต้องระบุให้ชัดเจน พร้อมทั้งให้หมายเหตุหรือขีดเส้นใต้ หรือระบายสี หรือทำเครื่องหมาย พร้อมเขียนหัวข้อกำกับไว้ให้ตรงกัน เพื่อให้ง่ายต่อการตรวจสอบกับเอกสารเปรียบเทียบ ทั้งนี้สถาบันมะเร็งแห่งชาติขอสงวนสิทธิที่อาจจะไม่พิจารณาผู้ประสงค์จะเสนอราคาที่ไม่ดำเนินการตามเงื่อนไขดังกล่าว

ตารางที่ 1 ตารางเปรียบเทียบคุณสมบัติข้อกำหนดทางเทคนิค

อ้างถึงข้อ	ข้อกำหนด/อุปกรณ์ที่ต้องการ	ข้อกำหนด/อุปกรณ์ที่นำเสนอ	เอกสารอ้างอิง

และให้เสนอค่าบำรุงรักษาหลังจากหมดระยะเวลาประกันมาให้พิจารณาด้วย

10.3 ผู้ประสงค์จะเสนอราคาจะต้องจัดทำแผนดำเนินการ หรือแผนการติดตั้งอุปกรณ์ในโครงการฯ โดยกำหนดระยะเวลาในการดำเนินการแต่ละกิจกรรมอย่างชัดเจนภายใน 15 วันทำการหลังจากการลงนามในสัญญา

10.4 ผู้ประสงค์จะเสนอราคาจะต้องทำการศึกษาและวางแผนร่วมกับเจ้าหน้าที่ผู้รับผิดชอบของทางสถาบันมะเร็งแห่งชาติ ในการวิเคราะห์และออกแบบระบบ กำหนดจุดการติดตั้งอุปกรณ์แต่ละอุปกรณ์ในโครงการ ให้ครบถ้วนถูกต้องตามข้อกำหนด

11 เงื่อนไขการดำเนินการติดตั้ง

11.1 ผู้ประสงค์จะเสนอราคาต้องติดตั้งอุปกรณ์ทั้งหมดที่จัดหาตามโครงการนี้ ณ สถาบันมะเร็งแห่งชาติ

11.2 ผู้ประสงค์จะเสนอราคาต้องทำการติดตั้งและเคลื่อนย้ายอุปกรณ์ตามที่สถาบันฯ กำหนด หากมีค่าใช้จ่ายในการติดตั้งเพิ่มเติมเพื่อให้สามารถติดตั้งอุปกรณ์ตามโครงการได้ ผู้ประสงค์จะเสนอราคาจะต้องเป็นผู้รับผิดชอบค่าใช้จ่าย

11.3 ในระหว่างการติดตั้งอุปกรณ์ตามโครงการ จะต้องไม่มีผลกระทบต่อการทำงานของระบบงานต่างๆ หรือก่อให้เกิดความเสียหายแก่ระบบเครือข่าย อุปกรณ์เครือข่าย หรืออุปกรณ์อื่นๆ ของสถาบันฯ หากเกิดผลกระทบหรือความเสียหาย ผู้ประสงค์จะเสนอราคาต้องดำเนินการแก้ไขให้สามารถใช้งานได้ตามปกติและต้องรับผิดชอบค่าใช้จ่ายในการแก้ไขปัญหาที่เกิดขึ้นหรือเปลี่ยนอุปกรณ์ที่เกิดความเสียหาย โดยไม่คิดค่าใช้จ่ายใดๆ เพิ่มเติมกับสถาบันฯ

11.4 ภายหลังการ...

11.4 ภายหลังการตรวจรับอุปกรณ์แล้ว ผู้ประสงค์จะเสนอราคาจะต้องให้คำปรึกษา แนะนำ ชี้แจง รวมทั้งอบรมในกรณีมีการเปลี่ยนแปลง ปรับปรุงโปรแกรมของอุปกรณ์ที่สถาบันฯ จัดหาตามโครงการนี้ รวมทั้งกรณีที่สถาบันฯร้องขอ ผู้ประสงค์จะเสนอราคาจะต้องสนับสนุนและปฏิบัติตามการร้องขอดังกล่าว

11.5 ผู้ประสงค์จะเสนอราคาต้องทำแบบ Shop drawing สำหรับการติดตั้งและแผนงานให้ทางผู้ว่าจ้างก่อนดำเนินการติดตั้งจริง

11.6 การติดตั้งสายสัญญาณ ต้องออกแบบ ให้มี รางเหล็ก สำหรับเส้นทางหลักของสายสัญญาณ เพื่อสะดวกในการเพิ่มเติมในอนาคต พร้อมพื้นที่สำรองในอนาคต

11.7 การแยกสายสัญญาณออกจาก เส้นทางหลัก ต้องใช้อุปกรณ์ต่อเชื่อม ตามมาตรฐาน พร้อมมีอุปกรณ์ป้องกัน เช่น ท่อเหล็ก หรือบล็อก หรือคอนเน็คเตอร์ หรือราง หรือท่อพีวีซี สำหรับแนวดิ่ง

11.8 ต้องมีการจัดสายสัญญาณให้เรียบร้อยทั้งด้านปลายสายที่Patch Panel และ Patch Cord

11.9 การเดินสายสัญญาณใยแก้วนำแสง

11.9.1 การเดินสายใยแก้วนำแสงต้องเดินไปตามเส้นทางหลักในกรณีที่แยกสายออกให้ใช้ท่อเหล็ก EMT หรือ ท่ออ่อนกันน้ำ

11.9.2 การโค้งงอของสายสัญญาณใยแก้วนำแสงต้องไม่เกินตามมาตรฐานที่กำหนดของคุณลักษณะของสายที่เสนอมา

11.9.3 ต้องมีการเผื่อปลายสายสัญญาณที่ตู้ Rack cabinet ไม่น้อย 5 เมตร สำหรับตู้ติดพนัง และไม่น้อยกว่า 8 เมตรสำหรับตู้ตั้งพื้น

11.9.4 การเข้าสายสัญญาณใยแก้วนำแสงเป็นแบบ Fusion Splice ระหว่างสาย Pig tail และต้องมีกล่องใส่เพื่อป้องกัน (Splice Tray) พร้อมอุปกรณ์ปลอกป้องกันการเชื่อมต่อ (Slip)

11.9.5 ผู้ประสงค์จะเสนอราคาต้องทำการส่งมอบเอกสารดังต่อไปนี้หลังการติดตั้งเสร็จ As-built Layout plan, Riser diagram และ Test Report OTDR

11.9.6 ต้องมีสัญลักษณ์ เพื่อบอกเส้นทางของสายสัญญาณนั้น โดยสามารถมองเห็นชัดเจนที่สายก่อนเข้า Patch Panel Fiber

11.10 ข้อมูลของสถาบันฯ ถือเป็นความลับทางราชการ ห้ามมิให้นำไปเผยแพร่ ทั้งนี้หากเกิดความเสียหายในส่วนหนึ่งส่วนใดอันเนื่องจากการดำเนินการของผู้ประสงค์จะเสนอราคา ผู้ประสงค์จะเสนอราคาจะต้องแสดงความรับผิดชอบ หากข้อมูลสารสนเทศหรือข้อกำหนดต่างๆ บนเครือข่ายของสถาบันฯสูญหาย ถูกเผยแพร่หรือเป็นเหตุให้เกิดความเสียหายต่อความมั่นคงและความปลอดภัยของสถาบันฯ ซึ่งเป็นผลจากการดำเนินงานของผู้ประสงค์จะเสนอราคา ผู้ประสงค์จะเสนอราคาจะต้องรับผิดชอบต่อความเสียหายและความบกพร่องของระบบรักษาความปลอดภัยนั้น

11.11 ผู้ประสงค์จะเสนอราคาจะต้องรับผิดชอบเรื่องการขนย้ายขยะมูลฝอย และเศษวัสดุออกจากพื้นที่ปฏิบัติงานทุกครั้งและหากมีค่าใช้จ่ายที่เกิดขึ้นจากการขนย้ายขยะมูลฝอย และเศษวัสดุ ผู้ประสงค์จะเสนอราคาจะต้องเป็นผู้รับผิดชอบ

12 เงื่อนไขการรับประกัน...

12 เงื่อนไขการรับประกันบำรุงรักษา

12.1 ผู้ขายต้องรับประกันการตรวจซ่อมบำรุงรักษา และการแก้อุปกรณ์ที่เสียหาย เนื่องจากการใช้งานของอุปกรณ์และระบบเครือข่ายคอมพิวเตอร์ตามปกติ เป็นระยะเวลาไม่น้อยกว่า 1 ปี และทำการบำรุงรักษา (Preventive Maintenance) อย่างน้อย 3เดือนต่อ 1ครั้ง โดยไม่คิดค่าใช้จ่ายใดๆ ทั้งสิ้น หากอุปกรณ์ตัวใดที่มีอายุการรับประกันมากกว่า 1 ปีจากบริษัทเจ้าของผู้ผลิต ผู้ขายจะต้องรับผิดชอบในการประสานการตรวจซ่อมบำรุงจากบริษัทผู้ผลิตหรือผู้ค้าโดยตรง แทน สถาบันมะเร็งแห่งชาติ

12.2 การแก้ไข/ซ่อมบำรุงอุปกรณ์และระบบเครือข่ายคอมพิวเตอร์ต้องดำเนินการซ่อมแซมแก้ไขภายใน1ชั่วโมงนับแต่ได้รับแจ้งจากสถาบันมะเร็งแห่งชาติและ ให้แล้วเสร็จสามารถใช้งานได้ภายใน 1วันทำการ นับจากวันที่ได้รับการแจ้งตรวจซ่อม หรือตามที่ได้กำหนดในเอกสารคุณลักษณะเฉพาะของอุปกรณ์ที่ได้กำหนดไว้ หากผู้ขายละเลยหรือไม่สามารถแก้ไขได้ในระยะเวลาที่กำหนด สถาบันมะเร็งแห่งชาติ มีสิทธิจัดหาบริษัทอื่นมาทำการซ่อมแซม แก้ไขระบบแทนได้ แต่ผู้ขายจะต้องรับผิดชอบค่าใช้จ่ายทั้งหมดที่เกิดขึ้นจากการซ่อมแซมดังกล่าว และผู้ขายจะต้องถูกปรับในอัตราชั่วโมงละ 2 ,000 บาท (สองพันบาท) เศษของชั่วโมงให้นับเป็น1ชั่วโมง สำหรับจำนวนชั่วโมงที่ใช้ในการคำนวณค่าปรับ ให้นับตั้งแต่เวลาที่สถาบันมะเร็งแห่งชาติได้แจ้งผู้ขายทราบถึงความชำรุดบกพร่องจนกว่าจะซ่อมแซมแล้วเสร็จสมบูรณ์

13 เงื่อนไขการฝึกอบรม

ผู้ประสงค์จะเสนอราคาต้องจัดหลักสูตรอบรมเจ้าหน้าที่ของสถาบันมะเร็งแห่งชาติ จำนวนไม่น้อยกว่า 5 คน พร้อมเอกสารประกอบการฝึกอบรม และคู่มือการใช้งานและบำรุงรักษาอุปกรณ์ระบบต่างๆ โดยมีระยะเวลาการฝึกอบรมอย่างน้อย ดังนี้

13.1 อุปกรณ์ Distributed Switch ระยะเวลาการฝึกอบรม ไม่น้อยกว่า 6 ชั่วโมง

13.2 อุปกรณ์ Access Switch แบบที่ 1 และ 2 ระยะเวลาการฝึกอบรม ไม่น้อยกว่า 6 ชั่วโมง

13.3 อุปกรณ์ Wireless LAN Controller ระยะเวลาการฝึกอบรม ไม่น้อยกว่า 6 ชั่วโมง

13.4 อุปกรณ์ตรวจจับและป้องกันการบุกรุกบนระบบเครือข่าย (Intrusion Prevention System) ระยะเวลาการฝึกอบรม ไม่น้อยกว่า 6 ชั่วโมง