(ร่าง)

ขอบเขตของงาน (Terms of Reference : TOR)

และเอกสารประกวดราคาโครงการจัดหาซอฟต์แวร์ที่มีลิขสิทธิ์

1. ความเป็นมา

เนื่องจาก สำนักงานเลขาธิการสภาผู้แทนราษฎร มีระบบการประชาสัมพันธ์ ระบบการนำเสนอข้อมูล และการบริการต่าง ๆ ผ่านเครือข่ายอินเตอร์เน็ตแก่บุคลากรของรัฐสภา และประชาชนทั่วไป การจัดทำรูปแบบการนำเสนอข้อมูล ความรู้ ข่าวสารต่าง ๆ โดยใช้สื่อผสม นำเสนอผ่านจอภาพ LCD หรือผ่านเครือข่ายอินเตอร์เน็ตด้วยฟรีแวร์ ซึ่งมีระยะเวลาการใช้งานจำกัด ดังนั้น เพื่อให้สำนักงานฯ มีซอฟต์แวร์ระบบการออกแบบและบริหารจัดการการถ่ายทอดสื่อผสม(Multimedia)แบบเครือข่าย และซอฟต์แวร์ผลิตสื่อผสม(Multimedia) ที่ทันสมัย รวมทั้งซอฟต์แวร์ระบบช่วยป้องกันสแปมเมล์ มัลแวร์ สปายแวร์ และไวรัสบนเกตเวย์ ที่ครบวงจร ในการเพิ่มศักยภาพระบบการนำเสนอข้อมูลและการให้บริการข้อมูลผ่านระบบเครือข่ายอินเตอร์เน็ตของรัฐสภา จึงจำเป็นต้องจัดหาซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย

2. วัตถุประสงค์

2.1 เพื่อให้มีและใช้ชุดซอฟต์แวร์ระบบการถ่ายทอดสื่อผสม(Multimedia)แบบเครือข่าย ชุดซอฟต์แวร์ตัดต่อวิดีโอ และชุดระบบช่วยป้องกันสแปมเมล์ มัลแวร์ สปายแวร์ และไวรัสบนเกตเวย์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย

2.2 เพื่อให้ซอฟต์แวร์ในข้อ 2.1 เป็นซอฟต์แวร์ที่มีรูปแบบการทำงานครบวงจรไม่จำกัดระยะเวลาการใช้งาน

3. คุณสมบัติผู้เสนอราคา

3.1 ต้องเป็นนิติบุคคลที่จดทะเบียนในประเทศไทย ซึ่งมีวัตถุประสงค์ในการประกอบธุรกิจเกี่ยวกับการขายและ/หรือการให้เช่า/ให้เช่าซื้อระบบคอมพิวเตอร์หรือซอฟต์แวร์ที่มีลิขสิทธิ์ โดยตรงมาแล้วเป็นเวลาไม่น้อยกว่า 3 ปี นับจนถึงวันยื่นเอกสารประกวดราคา

3.2 ต้องมีทุนจดทะเบียนไม่น้อยกว่า 3 ล้านบาท (สามล้านบาท) โดยมีหลักฐานการจดทะเบียนซึ่งสำนักทะเบียนธุรกิจ กรมพัฒนาธุรกิจการค้า ออกให้หรือรับรองให้ไม่เกิน 6 เดือน นับจนถึงวันยื่นเอกสารประกวดราคา

3.3 ผู้เสนอราคาต้องเป็นตัวแทนจำหน่ายระบบคอมพิวเตอร์ทั้ง Hardware และ Software ในประเทศไทยที่ถูกต้องตามกฎหมาย และได้รับการสนับสนุนจากเจ้าของผลิตภัณฑ์เป็นอย่างดีในด้านที่ปรึกษาและผู้เชี่ยวชาญ โดยต้องมีหนังสือรับรองการแต่งตั้งให้เป็นตัวแทนฯ และหนังสือนั้นต้องมีอายุไม่เกิน 90 วัน นับจากวันที่ออกจนถึงวันที่ยื่นเอกสารประกวดราคา ยกเว้น Software ที่นำมาสนับสนุนการใช้งานกับระบบ

3.4 ผู้เสนอราคาต้องไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกันซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้เสนอราคาได้มีคำสั่งให้สละสิทธิ์และความคุ้มกันเช่นว่านั้น

3.5 ผู้เสนอราคาต้องไม่เป็นผู้ที่ถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานของทางราชการ หรือห้ามติดต่อหรือห้ามเข้าเสนอราคากับทางราชการ และได้แจ้งเวียนชื่อแล้ว หรือไม่เป็นผู้ที่ได้รับผลของการสั่งให้นิติบุคคลหรือบุคคลอื่นเป็นผู้ทิ้งงานตามระเบียบของทางราชการ

3.6 ผู้เสนอราคาต้องเสนอรายชื่อบุคลากรที่จะรองรับการติดตั้ง ดูแล บำรุงรักษาการใช้งานตามรายการซอฟต์แวร์ที่จัดหาอย่างน้อยระบบละ 2 คน

3.7 ผู้เสนอราคาต้องเป็นผู้ผ่านการติดตั้งซอฟต์แวร์ที่จัดหาบนระบบคอมพิวเตอร์สำเร็จและใช้งานได้มาแล้ว ให้แก่หน่วยงานราชการ รัฐวิสาหกิจ หรือเอกชน อย่างน้อย 3 ราย ภายในระยะเวลา 3 ปี นับจากวันที่งานแล้วเสร็จ จนถึงวันยื่นเอกสารประกวดราคาซื้อจ้างด้วยวิธีการทางอิเล็กทรอนิกส์ ในวงเงินรายละไม่ต่ำกว่า 1 ล้านบาทต่อหนึ่งสัญญา โดยแนบสำเนาหนังสือคู่สัญญาหรือหนังสือรับรองผลงานที่ออกโดยหัวหน้าหน่วยงานหรือผู้มีอำนาจปฏิบัติงานแทนโดยถูกต้องตามกฎหมาย

3.8 ผู้เสนอราคาและผู้ซื้อซองเอกสารประกวดราคาต้องเป็นรายเดียวกันเท่านั้น

3.9 ผู้เสนอราคาต้องไม่เป็นผู้ที่มีผลประโยชน์ร่วมกันกับผู้เสนอราคารายอื่น และ/หรือต้องไม่เป็นผู้ที่มีผลประโยชน์ร่วมกันระหว่างผู้เสนอราคากับผู้ให้บริการตลาดกลางอิเล็กทรอนิกส์ ณ วันประกาศประกวดราคาจ้างด้วยวิธีการทางอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรมในการประกวดราคาซื้อจ้างด้วยวิธีการทางอิเล็กทรอนิกส์ ครั้งนี้

3.10 สำนักงานฯ ขอสงวนสิทธิ์ในการยกเลิกสัญญาและเรียกค่าเสียหาย หากตรวจสอบภายหลัง พบว่าผู้เสนอราคาใช้หนังสือรับรองคุณสมบัติเฉพาะของซอฟต์แวร์บางรายการที่ไม่ได้ระบุรายละเอียดไว้ในแคตตาล็อก ซึ่งไม่สามารถดำเนินการได้ตรงตามที่ระบุไว้ในหนังสือรับรอง

3.11 กำหนดยืนราคาไม่น้อยกว่า 60 วัน นับจากวันที่ยื่นซองเอกสารประกวดราคา

4. แบบรูปรายการ หรือคุณสมบัติเฉพาะ

4.1 ซอฟต์แวร์ระบบการถ่ายทอดสื่อผสม (Multimedia) แบบเครือข่าย จำนวน 1 ระบบ

ซอฟต์แวร์ระบบการถ่ายทอดสื่อผสม(Multimedia)แบบเครือข่าย เป็นซอฟต์แวร์ที่ใช้ในการสื่อสารด้วยภาพและเสียง ในรูปแบบของกระจายข่าวสารข้อมูลจากศูนย์กลาง ไปยังกลุ่มเป้าหมายที่ต้องการได้ในทันที โดยมีวัตถุประสงค์ เพื่อผสมผสานการเคลื่อนไหวทั้งภาพและเสียงไปยังจอภาพทุกชนิดที่ติดตั้งอยู่ในจุดสนใจต่างๆ ซึ่งอาจโดยการสื่อสารผ่านทางอินเตอร์เน็ตหรือเครือข่ายอื่นๆ ซึ่งจอภาพทุกชนิดแต่ละแห่งจะถ่ายทอดทั้งภาพและเสียงตามข้อมูลที่ได้กำหนดไว้ไปยังจอแสดงผลซึ่ง ได้แก่ TVs, Plasmas, Projectors, Videowalls, LEDs หรือจอชนิดอื่นๆ โดยมีคุณลักษณะเฉพาะดังนี้

4.1.1 เป็นระบบที่ประกอบด้วยโปรแกรมย่อยในชุดเดียวกัน ได้แก่ โปรแกรมการออกแบบ โปรแกรมการควบคุมระบบเครือข่าย โปรแกรมการควบคุมการถ่ายทอดสื่อผสม(Multimedia) และโปรแกรมแสดงผล ทั้งนี้ไม่รวมโปรแกรมสนับสนุนอื่นๆ เช่น โปรแกรมสนับสนุนการออกแบบสื่อ เป็นต้น

4.1.2 สามารถใช้งานกับเครื่องฯ ที่เชื่อมต่อกับระบบเครือข่าย และเครื่องฯ ที่ไม่เชื่อมต่อกับระบบเครือข่ายได้

4.1.3 สามารถควบคุมการทำงานได้จากส่วนกลาง ได้แก่ ควบคุมการถ่ายทอดสื่อ ควบคุมการทำงานของเครื่องในระบบเครือข่ายทั้งหมด และตรวจสอบการทำงานของระบบทั้งหมดได้ โดยไม่ต้องอาศัยระบบอื่น ๆ

4.1.4 สามารถใช้งานได้กับเครื่องคอมพิวเตอร์ที่มีระบบปฏิบัติการ Windows XP Professional ขึ้นไป

4.1.5 สามารถใช้งานได้กับภาพนิ่ง ภาพเคลื่อนไหวและแอนิเมชั่น (Animation) ได้แก่รูปแบบไฟล์ประเภท Animate GIF, Flash, Mpeg1, Mpeg2, AVI เป็นอย่างน้อย โดยสามารถใช้งานได้ทันที โดยไม่ต้องทำการแปลงไฟล์

4.1.6 สามารถนำเสนอสื่อผสมด้วยเทคนิค Streaming ได้ทั้งแบบเต็มหน้าจอและเฉพาะบางส่วนของหน้าจอ

4.1.7 สามารถนำเสนอสัญญาณสดจากสถานีโทรทัศน์ได้ทั้งแบบเต็มหน้าจอ และเฉพาะบางส่วนของหน้าจอ

4.1.8 สามารถใช้งานเสียงได้ ทั้งไฟล์รูปแบบ WAV, MP3 และ CD AUDIO โดยสามารถใช้งานได้ทันที โดยไม่ต้องทำการเปลี่ยนแปลงไฟล์

4.1.9 สามารถแสดงผลข้อความวิ่งและสามารถควบคุมทิศทาง และความเร็วในการแสดงผลได้

4.1.10 ต้องใช้งานแบบโต้ตอบกับผู้ใช้งานได้ (Interactive Kiosks)

4.1.11สามารถใช้งานร่วมกับระบบภายนอกอื่น ๆ ได้ เช่น ระบบฐานข้อมูล ระบบอินเทอร์เน็ต โดยสามารถนำข้อมูล และรูปภาพมาแสดงผลในระบบได้ทันที

4.1.12 สามารถกำหนดรหัสการใช้งาน (User name/Password) ในการควบคุมการรับ/ส่งข้อมูลได้

4.1.13 มีระบบบันทึกข้อมูลการทำงาน และการแสดงผล ทำให้สามารถตรวจสอบ วิเคราะห์การทำงาน หรือปัญหาที่เกิดขึ้นได้ง่าย

4.1.14 สามารถแสดงผลกับตู้ Kiosk ระบบจอสัมผัส (Touch Screen) ได้

ระบบการออกแบบ

4.1.15 สามารถดูตัวอย่างของสื่อที่นำมาออกแบบได้ และดูตัวอย่างสื่อที่ออกแบบแล้วพร้อมทั้งแก้ไขได้ทันที ไม่ต้องมีการแปลงรูปแบบก่อนดูตัวอย่าง

4.1.16 มีการทำงานแบบ Layer หรือแบบ WYSIWYG

4.1.17 สามารถกำหนดความละเอียดในการแสดงผลได้

4.1.18 สามารถกำหนดให้มีการใช้งานแบบโต้ตอบ (Interactive) ได้ โดยสามารถเลือกให้เป็นทั้งแบบปุ่มกด กดเลือกโดยใช้เมาส์ และกำหนดเป็นปุ่มกดอื่น ๆ บนคีย์บอร์ด

4.1.19 สามารถออกแบบการวางสื่อได้อย่างอิสระ

4.1.20 สามารถควบคุมการแสดงผลของสื่อประเภท Animation ให้เล่น หยุด หรือกำหนดรอบของการเล่นซ้ำได้ตามต้องการ

4.1.21 สามารถควบคุมเวลาในการแสดงผลขององค์ประกอบต่าง ๆ ทั้งหมดที่นำมาออกแบบได้ ทั้งแบบกำหนดช่วงเวลาแสดงผล แบบกำหนดช่วงเวลาที่ไม่ให้แสดงผลได้ โดยการกำหนดล่วงหน้า และแบบที่มีการแทรกการแสดงผลได้ ด้วยการกำหนดเป็นเวลา วัน วันที่ สัปดาห์ เดือน ปี

4.1.22 สามารถแสดงผลการตั้งเวลาการทำงานของแต่ละหน้าได้

4.1.23 สามารถพัฒนาสื่อผสม(Multimedia) แบบใช้งานในระบบที่สามารถมีการโต้ตอบกับผู้ใช้งานได้

4.1.24 สามารถทำสื่อออกมาในรูปแบบภาพเคลื่อนไหว ได้อย่างน้อย 2 ชนิด จากมาตรฐานต่อไปนี้ Mpeg , AVI , Animate GIF , WMV , SWF โดยสามารถสร้างสื่อด้วยตัวระบบเองหรืออาศัยโปรแกรมสนับสนุนอื่นได้

4.1.25 สามารถแก้ไขสื่อที่เป็นแฟ้มข้อมูล ประเภทข้อความ (Text) ได้

4.1.26 สามารถทำงานแบบ Transparency ได้เป็นอย่างน้อย

4.1.27 มีชุดซอฟต์แวร์ Sony Vegas Pro รุ่นล่าสุดที่มีลิขสิทธิ์ สำหรับสนับสนุนการออกแบบสื่อ จำนวน 1 ชุด และการ์ด IEEE 1394 อย่างน้อย 2 พอร์ต จำนวน 5 ชุด

ระบบควบคุมเครือข่าย

4.1.28 สามารถควบคุมการรับ/ส่งข้อมูล โดยกำหนดแบบเฉพาะเครื่อง แบบกลุ่ม และทุกเครื่องฯ ได้พร้อมๆ กัน ที่สามารถกำหนดเวลาการทำงานได้แบบอัตโนมัติ

4.1.29 สามารถแบ่งกลุ่มของเครื่องลูกข่ายได้ตามที่ต้องการ

4.1.30 สามารถควบคุมการรับ/ส่งข้อมูลได้

4.1.31 สามารถตรวจสอบสถานะการทำงานของเครื่องลูกข่ายได้

4.1.32 สามารถกำหนดให้มีผู้ดูแลระบบได้หลายคน โดยมีระบบควบคุมการทำงานแบบลำดับชั้น พร้อมทั้งมีระบบผู้ใช้ และระบบรหัสผ่านที่ปลอดภัย

4.1.33 สามารถควบคุมการทำงานของระบบแบบระยะไกลได้ โดยการทำงานผ่านระบบเครือข่ายคอมพิวเตอร์

4.1.34 ต้องมีระบบเก็บสถานะการทำงานและข้อมูลความผิดพลาดของระบบ อย่างน้อย ดังนี้

- วัน เวลา การปรับปรุงข้อมูล
- การ เปิด ปิด เครื่อง
- การใช้งานของผู้ดูแลระบบ

ระบบแสดงผล (เครื่องลูกข่าย)

4.1.35 ต้องมีระบบเก็บสถานะการทำงานและข้อมูลความผิดพลาดของระบบ อย่างน้อย ดังนี้

- วัน เวลา การปรับปรุงข้อมูล
- การ เปิด ปิด เครื่อง
- การใช้งานของผู้ดูแลระบบ

4.1.36 สามารถกำหนดให้มีการแสดงผลตามความละเอียดที่ต้องการ และปรับความละเอียดในการแสดงผลแบบอัตโนมัติ

4.1.37 สามารถแสดงผลทั้งแบบเต็มจอ และแบบเป็นหน้าต่าง โดยสามารถกำหนดตำแหน่งในการแสดงผลได้ เพื่อให้เหมาะสมกับจอแสดงผลแต่ละประเภท

4.1.38 สามารถควบคุมลำดับการแสดงผลบนหน้าจอได้ทั้งแบบอัตโนมัติ และโดยการสั่งงานของผู้ดูแลระบบ สามารถสั่งแทรกหน้าที่ต้องการได้ทันที

4.2. ระบบช่วยป้องกันสแปมเมล์ มัลแวร์ สปายแวร์ และไวรัสบนเกตเวย์ 1 ระบบ ประกอบด้วย ระบบ Security Mail Gateway จำนวน 1 ชุด ต้องมีคุณสมบัติอย่างน้อยดังนี้

4.2.1 เป็นระบบที่ออกแบบมาเฉพาะด้านที่ผ่านการ Hardening และ การออกแบบเฉพาะสำหรับการรับส่ง อีเมล์ Messaging รองรับการโปรโตคอลการสื่อสารแบบ SMTP, ESMTP, Secure SMTP over TLS (สามารถทำการเข้ารหัสได้ที่ 2048 bit RSA, 265-bit-AES)

4.2.2 มีประสิทธิภาพในการรับส่ง เมล์ ได้ไม่น้อยกว่า 150,000 Message/Hour ที่ขนาดเมล์เฉลี่ยไม่น้อยกว่า 15 KB และรองรับจำนวน Connection ได้ไม่น้อยกว่า 10,000 Connection พร้อมๆกันสามารถรองรับการทำงานไม่ต่ำกว่า 2,000 users และสามารถขยายได้ในอนาคต

4.2.3 สามารถเชื่อมต่อระบบเครือข่ายแบบ Gigabit Ethernet ได้ไม่น้อยกว่า 2 พอร์ต (1000 BaseT)และมีระบบเฉพาะสำหรับการจัดการจำนวน 1 พอร์ต

4.2.4 มีความสามารถในการป้องกันการโจมตีจากระบบภายนอกดังต่อไปนี้ได้เป็นอย่างน้อย

- Denial of Service (DoS)
- Direct Harvest Attack (DHA)
- Stack/Buffer Overflow Attack

4.2.5 มีระบบ Mail Monitoring สำหรับตรวจสอบการสื่อสารระบบ เมล์จากภายนอกที่ติดต่อเข้ามาสู่ระบบว่าอยู่ในระดับปกติหรือไม่ และตรวจสอบปัญหาที่เกิดขึ้นกับระบบสื่อสารเมล์แบบ Real Time โดยสามารถจำแนกได้ อย่างน้อยดังนี้

- แบ่งตาม domain และ IP address
- ปริมาณเมล์ที่ส่งเข้ามาในระบบต่อชั่วโมง/วัน/สัปดาห์
- แสดงข้อมูลทางสถิติแบบของปริมาณเมล์สแปมที่ได้รับ

- แสดงข้อมูลทางสถิติแบบของปริมาณเมล์ไวรัสที่ได้รับ
- แสดงปริมาณเมล์ที่ถูก Reject หรือ Traffic Rate Limit

4.2.6 มีระบบควบคุมแหล่งที่ส่งสแปมเข้าสู่ระบบในปริมาณที่มากผิดปกติหรือต้องสงสัย โดยต้องทำงานได้ อย่างน้อยดังนี้

- Reject Connection กับแหล่งที่มีประวัติชัดเจนว่ามีการส่ง สแปม ตลอดเวลา
- ควบคุมและกำหนดปริมาณเมล์ที่เข้ามาสู่ระบบในระดับของจำนวน Connection

4.2.7 มีระบบจัดการปัญหา สแปม จากแหล่งที่มาต่างๆที่มีประวัติ (Reputation)ไม่ดี โดยต้องทำงานได้ อย่างน้อยดังนี้

- ตรวจแหล่งที่มาของผู้ส่งเมล์เข้ามาในระบบจากระบบฐานข้อมูลภายในของระบบและข้อมูลพื้นฐาน เช่น Domain/IP Address, ปริมาณเมล์และปริมาณสแปมที่เข้ามาสู่ระบบ
- Reject Connection กับแหล่งที่มีประวัติชัดเจนว่ามีการส่ง สแปม

4.2.8 มีระบบที่แบ่งกลุ่มผู้ส่ง อีเมล์ เข้าระบบได้ ดังนี้

- กลุ่มผู้ที่มีประวัติดี (White List/Trust List)
- กลุ่มต้องสงสัยหรือไม่เคยติดต่อ (Suspect List / Unknown List)
- กลุ่มมีประวัติไม่ดี (Black List) โดยต้องมีระบบการตรวจสอบประวัติของแหล่งที่มา (Reputation)เพื่อจำแนกความน่าเชื่อถือของผู้ส่งได้

4.2.9 มีระบบบริหารจัดการ อีเมล์ ที่มีการรับและส่งได้ ดังนี้

- มีระบบสำหรับการ Track Mail เพื่อตรวจสอบ Status ของ เมล์ ว่าได้รับส่งถึงปลายทางเรียบร้อยดีหรือไม่(Mail Delivery)
- มีระบบการส่ง Report แบบอัตโนมัติไปยังผู้ดูแลระบบหรือสร้าง Report ทั้งรายวัน/
- รายสัปดาห์/รายเดือน เพื่อให้ผู้ดูแลระบบได้รับรายงานการทำงานที่สำคัญเช่น ปริมาณการรับส่ง เมล์ ต่อวัน,ผู้ใช้งานสูงสุด ,ปริมาณ Virus Mail , Spam Mail รวมทั้งผู้ใช้งานสูงสุด และปริมาณผู้ที่ได้รับไวรัสเมล์สูงสุด 10 อันดับแรก

4.2.10 มีระบบป้องกัน Virus ใหม่ๆที่เกิดขึ้นไม่ให้เกิดการแพร่ระบาดเข้ามาในระบบ โดยที่ Engine จะต้องทำงานอัตโนมัติและสามารถกรอง อีเมล์ ที่ต้องสงสัยว่าเป็น Virus รูปแบบใหม่เข้าไปเก็บไว้ใน Quarantine ได้

4.2.11 ระบบการป้องกัน สแปม (Anti-Spam) สามารถรองรับการทำงานของ engine ในการตรวจสอบ อีเมล์ แบบ Content-based ได้

4.2.12 มีระบบการป้องกันปัญหา สแปม ที่สามารถป้องกัน Phishing เมล์และ อีเมล์ที่ใช้ในการแพร่กระจาย Spyware โดยสามารทำงานได้เป็นอย่างน้อยดังนี้

- มีการตรวจสอบรูปแบบโครงสร้าง (Context) ของอีเมล์ในแต่ละฉบับว่าเป็น สแปม, Phishing, Spywares หรือไม่
- สามารถตรวจสอบ และสามารถกรองอีเมล์แต่ละฉบับที่เป็น สแปม, Phishing, หรือมี Spyware ได้
- สามารถ Update Pattern ได้ ทุก 15 นาที เช่น Anti virus, Spam pattern, Phishing, Spywares เป็นอย่างน้อย

4.2.13 มีระบบการกักเก็บอีเมล์ (Quarantine) ที่ถูกตรวจสอบแล้วว่าเป็น สแปม ได้ โดยมีความสามารถในการทำงานดังต่อไปนี้

- สามารถเก็บ (Quarantine)ในตัวอุปกรณ์อีเมล์เกตเวย์ (On-Box) ได้
- สามารถที่จะแยกอีเมล์ที่ถูกกักเก็บไว้ใน Quarantine ของแต่ละผู้ใช้งานได้เองโดยอัตโนมัติ (End-User Quarantine) โดยระบบสามารถที่จะอนุญาตให้ผู้ใช้งานเข้ามาดูอีเมล์ที่ถูกกักเก็บของตัวเองไว้ได้
- สามารถส่งอีเมล์สรุปรายละเอียดของผู้ใช้แต่ละคนได้ว่า ณ ปัจจุบันผู้ใช้มีอีเมล์อะไรบ้างที่ถูกกักเก็บอยู่ใน Quarantine โดยสามารถที่จะกำหนดได้
- มีระบบการทำ Security Content Policy Management ซึ่งสามารถ Block และควบคุมประเภทของ File เช่น File Type หรือข้อความที่ไม่เหมาะสมต่างๆ ที่ใช้ในการรับและส่งผ่านระบบเมล์

4.2.14 สามารถกำหนด Policy ของการสื่อสารตามประเภทของกลุ่มผู้ใช้งานเพื่อควบคุมการรับส่งเมล์ออกจากระบบได้ รวมทั้งสามารถทำงานร่วมกับ LDAP Server ในการกำหนด Policyได้

4.2.15 มีระบบการบริหารจัดการ อย่างน้อยดังนี้

- Web Interface (HTTP and HTTPS)
- Command Line Interface (Console and Secure Shell)

4.2.16 รองรับการทำงานแบบควบคุมที่ศูนย์กลาง (Centralized Management) สำหรับระบบที่ใช้งานอุปกรณ์มากกว่า 1 ชุด

4.2.17 มีระบบการส่ง SNMP และ Syslog ไปยัง 3rd Party Solution เพื่อรองรับการทำงานของ Logging and Monitoring System ขององค์กรได้

ระบบ Web Security Gateway จำนวน 2 ชุด มีคุณสมบัติอย่างน้อยดังนี้

4.2.18 เป็นระบบที่ออกแบบมาเฉพาะด้าน ที่ผ่านการ Hardening และ การออกแบบเฉพาะสำหรับการทำงานเป็น Web Gateway รองรับโปรโตคอลการสื่อสารแบบ HTTP และ FTP โดยต้องรองรับการทำ HTTPS ได้ในอนาคตโดยมีเอกสารรับรองจากผู้ผลิต และต้องเพิ่มระบบการทำ HTTPS โดยไม่คิดค่าใช้จ่าย มีระบบเชื่อมต่อระบบเครือข่ายแบบ Gigabit Ethernet ได้ไม่น้อยกว่า 4 พอร์ต (1000 BaseT)

4.2.19 รองรับจำนวน Connection ได้ไม่น้อยกว่า 100,000 Connection พร้อมๆ กัน สามารถใช้งานได้ไม่น้อยกว่า 2,000 users

4.2.20 สามารถป้องกันการโจมตีจากระบบภายนอกได้ อย่างน้อยดังนี้

- Denial of Service(DoS)
- Stack/Buffer Overflow Attack

4.2.21 สามารถทำงานได้ทั้งแบบ Forward Mode และ Transparent Mode โดยใช้งานร่วมกับ L4 Switch

4.2.22 มีระบบ Monitoring เพื่อตรวจสอบการใช้งานของระบบว่ามีการเรียกใช้งานไปยัง เว็บไซต์ที่มีประวัติที่ไม่ดีหรือมี Malware อยู่ โดยสามารถแสดงข้อมูลทางสถิติแบบ Real-Time จำแนกได้ ดังนี้

- ปริมาณการเรียกใช้งาน เว็บไซต์ ที่ผิด Policy
- ปริมาณการเรียกใช้งาน เว็บไซต์ ที่มีอันตราย
- ปริมาณการตรวจจับ Malware
- ปริมาณการเรียกใช้งาน เว็บไซต์ ทั้งหมด

4.2.23 มีระบบ Real Time Monitoring เพื่อตรวจสอบข้อมูลการใช้งาน ได้ โดยสามารถแสดงข้อมูลทางสถิติแบบ Real-Time จำแนกได้ ดังนี้

- ปริมาณการใช้งาน Bandwidth เฉลี่ยในช่วงเวลาที่ผ่านมา
- จำนวน Concurrent Connection
- ปริมาณการใช้งาน Resource ของอุปกรณ์

4.2.24 มีระบบ Real Time Monitoring เพื่อตรวจสอบข้อมูลการใช้งานของผู้ใช้งานได้โดยสามารถแสดงข้อมูลทางสถิติแบบ Real-Time จำแนกได้ ดังนี้

- ตรวจจับการเรียกใช้งาน เว็บไซต์ ที่มี Malware
- ตรวจจับลักษณะของการติด Spyware และ Virus

4.2.25 มีระบบจัดการปัญหา Malwares และ Phishing Website จาก เว็บไซต์ ต่างๆที่มีประวัติไม่ดี โดยสามารถทำงานได้อย่างน้อย ดังนี้

- ตรวจสอบประวัติของ เว็บไซต์ ต่างๆที่มีการเรียกใช้ว่ามีประวัติดีหรือไม่ จากทั้งระบบ Reputation Scoring และ ข้อมูลพื้นฐานเกี่ยวกับ เว็บไซต์ นั้นๆ
- Reject Connection ในกรณีที่มีการเรียกใช้งาน เว็บไซต์ ที่มีประวัติชัดเจนว่าเป็นเว็บไซต์ ที่ถูกใช้ในการแพร่กระจาย Web-based Malwares และที่ถูกระบุว่าเป็น Phishing Websites

4.2.26 มีระบบการป้องกัน Malwares, Phishing, Spyware, Trojans, Worms โดยสามารถทำงานได้อย่างน้อย ดังนี้

- มีการป้องกันข้อมูลต่างๆที่เข้ามาสู่ผู้ใช้งานผ่านทาง เว็บไซต์ ที่เป็น Malwares ได้

- มีการ Update Pattern ทุกๆ 15 นาที เช่น Malwares, Phishing, Spyware, Trojans, Worms เป็นต้น

4.2.27 มีระบบการส่ง หรือ สร้าง Report ทั้งรายวัน/รายสัปดาห์/รายเดือน แบบอัตโนมัติเพื่อให้ผู้ดูแลระบบได้รับรายงาน ดังนี้

- รายงานการใช้งาน Transactions ที่ไม่ดี
- รายงานการตรวจจับ Malwares
- รายงานเครื่องผู้ใช้งานที่ติด Spyware หรือ Virus

4.2.28 มีระบบการทำ Security Content Policy Management ซึ่งสามารถ Block หรือควบคุมประเภทของ File เช่น File Type หรือข้อความที่ไม่เหมาะสมต่างๆ ที่ใช้

4.2.29 สามารถทำงานร่วมกับระบบ Authenticate กับ LDAP, Active Directory ได้

4.2.30 มีระบบการบริหารจัดการ อย่างน้อยดังนี้

- Web Interface (HTTP and HTTPS)
- Command Line Interface (Console and Secure Shell)

4.2.31 มีระบบการส่ง SNMP และ Syslog ไปยัง 3rd Party Solution เพื่อรองรับการทำงานของ Logging and Monitoring System ขององค์กรได้

5. ระยะเวลาดำเนินการ

ระยะเวลาดำเนินการ 30 วัน นับถัดจากวันที่ลงนามในสัญญา

6. ระยะเวลาการส่งมอบงาน

ดำเนินการส่งมอบและติดตั้งซอฟต์แวร์ที่มีลิขสิทธิ์ ให้แล้วเสร็จภายในเวลา 30 วัน นับถัดจากวันที่ลงนามในสัญญา

6.1 เงื่อนไขการส่งมอบ

6.1.1 ผู้ชนะการประกวดราคาต้องทำการติดตั้งและส่งมอบซอฟต์แวร์ที่มีลิขสิทธิ์ ภายใน 30 วัน นับถัดจากวันที่ลงนามในสัญญา โดยต้องส่งแผนการส่งมอบและกำหนดการฝึกอบรมให้สำนักงานฯ ทราบเป็นลายลักษณ์อักษรล่วงหน้าอย่างน้อย 3 วันทำการ

6.1.2 การติดตั้งส่งมอบ และการตรวจรับที่สมบูรณ์

การติดตั้งและส่งมอบซอฟต์แวร์ที่มีลิขสิทธิ์ จะถือว่าเสร็จสมบูรณ์เมื่อมีการตรวจรับซอฟต์แวร์ที่บันทึกบนซีดีหรือบันทึกบนดีวีดี รวมทั้งต้องผ่านการทดสอบการใช้งานบนเครื่องคอมพิวเตอร์ทั่วไปและบนตู้แสดงผลข้อมูล(Kiosk) แล้วว่าสามารถใช้งานร่วมกันได้อย่างมีประสิทธิภาพ

อนึ่ง ในระหว่างที่การติดตั้งส่งมอบและตรวจรับยังไม่สมบูรณ์ สำนักงานฯมีสิทธิที่จะใช้ซอฟต์แวร์ลิขสิทธิ์ในส่วนที่ส่งมอบแล้วได้ และหากมีเหตุให้ต้องเลิกสัญญาอันเนื่องจากความผิดนัดของผู้ชนะการ

ประกวดราคาฯเอง ผู้ชนะการประกวดราคาไม่มีสิทธิที่จะเรียกร้องค่าเสียหายใดๆอันเกิดจากการใช้ซอฟต์แวร์ลิขสิทธิ์นั้น ในระหว่างที่การติดตั้งส่งมอบและตรวจรับ ยังไม่สมบูรณ์

6.1.3 คณะกรรมการตรวจรับพัสดุจะตรวจรับซอฟต์แวร์ลิขสิทธิ์ทั้งหมดตามรายละเอียดในสัญญาซื้อขายซอฟต์แวร์ลิขสิทธิ์ เมื่อสำนักงานฯได้รับหนังสือแจ้งจากผู้ขายว่าได้ติดตั้งเสร็จเรียบร้อยแล้วพร้อมที่จะส่งมอบซอฟต์แวร์ลิขสิทธิ์

6.2 การส่งมอบคู่มือ

ผู้ขายต้องส่งมอบคู่มือการใช้งานซอฟต์แวร์แต่ละรายการทั้งภาษาไทยและภาษาอังกฤษอย่างน้อยรายการละ 2 ชุด

6.3 เงื่อนไขการอบรม

6.3.1 ผู้ขายต้องจัดการฝึกอบรมบุคลากรของสำนักงาน เพื่อรองรับการใช้งานซอฟต์แวร์ที่จัดซื้อแต่ละรายการได้อย่างมีประสิทธิภาพโดยไม่คิดค่าใช้จ่ายเพิ่มเติม ดังต่อไปนี้

6.3.2 การติดตั้งและการใช้งานซอฟต์แวร์ระบบการถ่ายทอดสื่อผสม(Multimedia)แบบเครือข่าย จำนวนไม่น้อยกว่า 10 คน ระยะเวลาอบรมไม่น้อยกว่า 18 ชั่วโมง

6.3.3 การติดตั้งและการใช้งานซอฟต์แวร์ชุดตัดต่อวีดีโอ จำนวนไม่น้อยกว่า 20 คน ระยะเวลาอบรมไม่น้อยกว่า 18 ชั่วโมง

6.3.4 การบริหารจัดการ และดูแลซอฟต์แวร์ระบบช่วยป้องกันสแปมเมล์ มัลแวร์ สปายแวร์ และไวรัสบนเกตเวย์ จำนวนไม่น้อยกว่า 10 คน ระยะเวลาอบรมไม่น้อยกว่า 12 ชั่วโมง

6.3.5 การฝึกอบรมจะต้องเป็นการฝึกอบรมเชิงปฏิบัติการและมีคู่มือประกอบการอบรม

6.3.6 ผู้ขายต้องทำแผนการฝึกอบรมส่งมอบให้แก่สำนักงานฯ พิจารณาเห็นชอบก่อน จึงจะดำเนินการฝึกอบรมได้

7.การรับประกัน

รับประกันการใช้งานสินค้าเป็นเวลาอย่างน้อย 3 ปี นับจากวันตรวจรับงานเสร็จสมบูรณ์ โดยผู้ขายต้องมีบุคลากรที่มีประสบการณ์ในการติดตั้งและใช้งานซอฟต์แวร์ที่มีลิขสิทธิ์ เพื่อสนับสนุนบริการหลังการขายทุกครั้งตามที่สำนักงานฯ ร้องขอตลอดระยะเวลาการรับประกันโดยไม่คิดค่าใช้จ่ายใด ๆ ทั้งสิ้น

ทั้งนี้ ระบบช่วยป้องกันสแปมเมล์ มัลแวร์ สปายแวร์ และไวรัสบนเกตเวย์ ต้องสามารถ Update License Software จากเจ้าของผลิตภัณฑ์ได้ตลอดระยะเวลารับประกันและต้องเข้ามาตรวจสอบระบบทุกๆ 3 เดือน โดยไม่คิดค่าใช้จ่ายใด ๆ ทั้งสิ้น

8.วงเงินในการจัดหา

กำหนดราคากลางเป็นเงิน 4,778,500 บาท (สี่ล้านเจ็ดแสนเจ็ดหมื่นแปดพันห้าร้อยบาทถ้วน) ซึ่งเป็นราคาที่รวมค่าติดตั้ง ค่าฝึกอบรม ค่าดำเนินการอื่น ๆ ค่ากำไรและค่าภาษีมูลค่าเพิ่ม 7% ไว้ด้วยแล้ว

..... ประธานกรรมการ
(นางพรรษมน ไทยวัฒนานุกูล)

..... กรรมการ
(นางพจนา อุตสาหะ)

..... กรรมการ
(นายเทอดศักดิ์ สินสมบูรณ์ทอง)

..... กรรมการ
(นางสาวนทิยา วิวัฒน์วานิชกุล)

..... กรรมการ
(นางสาวสุพิญญ์ชานันท์ ทาระกรรม)

..... กรรมการและเลขานุการ
(นายปัญจสารน์ ไสยแก้ว)