รายละเอียดคุณลักษณะเฉพาะของพัสดุที่จะจัดหา
งานจ้างเหมาวงจรเช่าสำหรับสื่อสารข้อมูลพร้อมสัญญาณอินเตอร์เน็ตสำหรับองค์กรโดยเฉพาะ และบริหารจัดการการใช้งาน (Service) ตามความต้องการของหน่วยงาน

---

๑. บทนำ

กองทางหลวงพิเศษระหว่างเมือง กรมทางหลวง มีความประสงค์จะจ้างเหมาบริการเชื่อมโยงเครือข่ายระบบสื่อสารข้อมูลและวงจรสัญญาณอินเตอร์เน็ต เพื่อใช้ในการเชื่อมต่อระหว่างหน่วยงานที่อาคารกองทางหลวงพิเศษระหว่างเมือง ถ.ศรีอยุธยา กับหน่วยงานที่อาคาร CCB (ลาดกระบัง)เพื่อใช้งานติดต่อสื่อสารระหว่างหน่วยงานภายในของกองทางหลวงฯ (Intranet Network) ซึ่งปัจจุบันมีการติดต่อสื่อสารของระบบงานต่าง ๆ ภายในของกองทางหลวงระหว่างเมืองเพื่อสนับสนุนให้ภารกิจหลักบรรลุตามเป้าประสงค์

ดังนั้นเพื่อให้การสื่อสารข้อมูลระหว่างหน่วยงานต่าง ๆ ของกองทางหลวงฯเป็นไปอย่างมีประสิทธิภาพ จึงจำเป็นต้องมีการเชื่อมโยงโครงข่ายสื่อสารข้อมูลแบบเฉพาะส่วน (Private Network) โดยจะใช้วิธีจ้างเหมาคู่สาย (Leased Line) พร้อมอุปกรณ์ต่อพ่วงและเช่าวงจรอินเตอร์เน็ตสำหรับองค์กรโดยเฉพาะจากผู้ให้บริการซึ่งคุ้มค่าและประหยัดค่าใช้จ่ายกว่าการดำเนินการติดตั้งเองระหว่าง อาคารกองทางหลวงพิเศษระหว่างเมือง ถ.ศรีอยุธยา เขตราชเทวี กทม. กับอาคาร CCB (ลาดกระบัง) ตั้งอยู่ที่บริเวณทางแยกต่างระดับลาดกระบังทางหลวงพิเศษหมายเลข ๗ เขตลาดกระบัง กทม.และอาคาร CCB พัทยา โดยมีรายละเอียดการเช่าเพื่อใช้งานตามข้อกำหนดต่าง ๆ ดังนี้

ผู้สนใจที่มีคุณสมบัติตามข้อกำหนดและมีความประสงค์จะรับจ้างทำงานดังกล่าวจะต้องจัดทำข้อเสนอด้านเทคนิคยื่นเสนอกรมทางหลวง โดยกองทางหลวงพิเศษระหว่างเมือง พิจารณาคัดเลือกให้เป็นผู้มีสิทธิเสนอราคาตามพระราชบัญญัติว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐพ.ศ.๒๕๖๐

๒. คำจำกัดความ

๒.๑ กท.	หมายถึง	กองทางหลวงพิเศษระหว่างเมือง กรมทางหลวง
๒.๒ ผู้ว่าจ้าง	หมายถึง	กรมทางหลวง โดยกองทางหลวงพิเศษระหว่างเมือง
๒.๓ ผู้รับจ้าง	หมายถึง	ผู้ยื่นข้อเสนอที่มีคุณสมบัติตามข้อ ๙ ซึ่งได้รับการพิจารณาคัดเลือกและลงนามในสัญญาจ้างฯ
๒.๔ ผู้เสนอราคา	หมายถึง	นิติบุคคล หรือกลุ่มนิติบุคคล ที่มีคุณสมบัติตามข้อ ๙ และมีสิทธิ์เข้ายื่นข้อเสนอเพื่อให้บริการตามโครงการนี้
๒.๕ อาคารกองทางหลวงพิเศษระหว่างเมือง	หมายถึง	อาคารหมายเลข ๑๙ บริเวณกรมทางหลวง ถนนศรีอยุธยา แขวงราชเทวี เขตราชเทวี กทม.

๒.๖ อาคารCCB (ลาดกระบัง)	หมายถึง	อาคารศูนย์ CCB (ลาดกระบัง) ตั้งอยู่บริเวณทางแยกต่างระดับลาดกระบัง ทางหลวงพิเศษหมายเลข ๗ แขวงทับยาว เขตลาดกระบัง กทม.
๒.๗ อาคารCCB (พัทยา)	หมายถึง	อาคารศูนย์ CCB (ด่านฯ มอเตอร์เวย์พัทยา) ตั้งอยู่บริเวณทางหลวงพิเศษหมายเลข ๗ ต.หนองปรือ อ.บางละมุง จ.ชลบุรี
๒.๘ ระบบสื่อสารข้อมูลฯ	หมายถึง	ระบบโครงข่ายสื่อสารข้อมูลเฉพาะส่วน (Private Network) ระหว่างอาคารกองทางหลวงพิเศษระหว่างเมืองกับอาคารศูนย์ CCB (ลาดกระบัง) และวงจรสื่อสารอินเตอร์เน็ตระหว่างอาคารที่เชื่อมต่อพร้อมอุปกรณ์ต่อพ่วงต่าง ๆ ทั้งที่เป็น Hardware และ Software
๒.๙ ระบบสารสนเทศ	หมายถึง	ระบบสารสนเทศของกท. อาทิเช่น ระบบงานพัสดุ ระบบเว็บไซต์ของ กท. ระบบเบิกจ่ายน้ำมัน ระบบบริหารงานบุคคล ระบบบัญชีและการเงิน ฯลฯ

๓. วัตถุประสงค์และขอบเขตงาน

๓.๑. เพื่อจัดหาและให้บริการเครือข่ายเฉพาะส่วน (Private Network) เพื่อการสื่อสารข้อมูลระหว่างอาคารกองทางหลวงพิเศษระหว่างเมือง กรมทางหลวง กับ อาคาร CCB (ลาดกระบัง) ตามเอกสารแนบหมายเลข ๑

๓.๒. เพื่อจัดหาและให้บริการวงจรสื่อสารอินเตอร์เน็ต สำหรับหน่วยงานต่าง ๆ ของกองทางหลวงพิเศษระหว่างเมือง ตามเอกสารแนบหมายเลข ๒ , ๓

๓.๓. เพื่อจัดหาและติดตั้งอุปกรณ์โครงข่ายสื่อสารข้อมูลฯ และอุปกรณ์ต่อพ่วงต่าง ๆ ทั้งที่เป็น Hardware และ Software เพื่อการเชื่อมโยงโครงข่ายสื่อสารข้อมูลของหน่วยงานต่าง ๆ ของกองทางหลวงพิเศษระหว่างเมืองให้มีประสิทธิภาพมีความปลอดภัยต่อการใช้งานตามคุณลักษณะตามเอกสารแนบหมายเลข ๔

๓.๔. จัดทำรายงานการวิเคราะห์การใช้งานเครือข่ายเฉพาะส่วน (Private Network) และการใช้วงจรสื่อสารอินเตอร์เน็ตของหน่วยงานต่าง ๆ ภายใต้การกำกับดูแลของกองทางหลวงพิเศษระหว่างเมือง เพื่อพัฒนา ปรับปรุง และกำหนดนโยบายการใช้งานให้เกิดประสิทธิภาพสูงสุด

๔. เงื่อนไขและข้อกำหนด

๔.๑. ข้อกำหนดทั่วไป

๔.๑.๑. ผู้รับจ้างจะต้องจัดทำรายงานแผนการดำเนินงาน เพื่อเสนอความเห็นชอบต่อคณะกรรมการฯ และหากมีการเปลี่ยนแปลงรูปแบบรายงานหรือแผนการดำเนินงานจะต้องขอความเห็นชอบทุกครั้ง

๔.๑.๒. ผู้รับจ้างจะต้องจัดทำรายงานการวิเคราะห์การใช้งานระบบสื่อสารข้อมูลฯ แสดงรายงานการใช้งานของคู่สายเครือข่ายเฉพาะส่วน (Private Network) และอินเตอร์เน็ตทุกเดือน

ทั้งนี้ ในการจัดทำจะต้องสรุปผลการดำเนินงานในแต่ละเดือน โดยแยกรายละเอียดงานเป็นอย่างน้อย ๓ แห่ง คือ การเชื่อมต่อโครงข่ายสื่อสารข้อมูลบริเวณ อาคารกองทางหลวงพิเศษระหว่างเมือง อาคาร CCB (ลาดกระบัง) และอาคาร CCB พัทยาหรือจุดอื่น ๆ ตามที่ผู้ว่าจ้างกำหนด

๔.๑.๓. ผู้รับจ้างต้องจัดให้มีผู้เชี่ยวชาญทางด้านเทคโนโลยีเครือข่ายเพื่อวิเคราะห์และจัดทำรายงานผลพร้อมให้คำปรึกษาและแนะนำในการกำหนดนโยบายด้านการใช้งานระบบฯเครือข่าย พร้อมเสนอแนะแนวทางการบริหารจัดการสัญญาณอินเตอร์เน็ตและต้องมีเจ้าหน้าที่เทคนิคเพื่อติดต่อประสานงานเพื่อดำเนินการแก้ไขปัญหาในการใช้งานระบบเครือข่าย

๔.๑.๔. ผู้รับจ้างจะต้องจัดส่งแผนผังเครือข่ายและอุปกรณ์ต่อพ่วงในโครงการและอุปกรณ์ที่เกี่ยวข้องภายใน ๓๐ วัน หลังจากลงนามในสัญญา และหากมีการปรับปรุงแผนผังเครือข่ายผู้รับจ้างจะต้องจัดส่งฉบับปรับปรุงล่าสุดให้ผู้รับจ้างก่อนเสร็จสิ้นโครงการ

๔.๑.๕. ผู้รับจ้างจะต้องจัดหา Public IP จำนวนไม่น้อยกว่า ๑๒๔ เลขหมาย พร้อมจัดทำทะเบียนการใช้งานเลขหมายดังกล่าวและจัดส่งภายใน ๓๐ วัน หลังจากลงนามในสัญญา หากมีการเปลี่ยนแปลงแก้ไขผู้รับจ้างต้องจัดส่งทะเบียนที่ปรับปรุงล่าสุดให้ผู้รับจ้างก่อนเสร็จสิ้นโครงการ

๔.๑.๖. ต้องจัดให้มีการประชุมประจำเดือนตามที่ผู้ว่าจ้างกำหนดรวมถึงจัดทำรายงานการประชุมในทุกครั้ง โดยผู้รับจ้างเป็นผู้รับผิดชอบค่าใช้จ่ายในการดำเนินการจัดประชุมทั้งหมด

๔.๑.๗. ผู้รับจ้างต้องดำเนินการจัดหาและติดตั้งอุปกรณ์ระบบสารสนเทศฯ โดยติดตั้งจำนวนอย่างน้อย ๓ แห่ง คือ อาคารกองทางหลวงพิเศษระหว่างเมือง กรมทางหลวง อาคารศูนย์ CCB (ลาดกระบัง) และอาคารศูนย์ฯ CCB พัทยา หรือจุดอื่นๆ ตามที่ผู้ว่าจ้างกำหนด ค่าใช้จ่ายที่เกิดจากการดำเนินการดังกล่าวเป็นภาระของผู้รับจ้าง ทั้งนี้อุปกรณ์ดังกล่าวถือเป็นกรรมสิทธิ์ของผู้รับจ้าง โดยดำเนินให้แล้วเสร็จครบถ้วนและสามารถใช้งานได้

๔.๑.๘. ผู้รับจ้างจะต้องให้ความร่วมมือในการประสานงานกับโครงการอื่น เพื่อให้การทำงานของระบบฯมีประสิทธิภาพโดยสมบูรณ์และผู้รับจ้างจะต้องดำเนินงานอื่นๆ ที่เกี่ยวข้องนอกเหนือจากที่ระบุไว้ในรายการข้อกำหนดนี้ หากกองทางหลวงพิเศษระหว่างเมืองเห็นว่าจำเป็นต้องดำเนินการเพื่อให้งานมีความครบถ้วนสมบูรณ์และผู้รับจ้างจะต้องรับภาระค่าใช้จ่ายทั้งหมดที่อาจจะเกิดขึ้น

๔.๒. <u>ข้อกำหนดทางด้านเทคนิค</u>

๔.๒.๑. ดำเนินการจัดหาวงจรเช่าสำหรับสื่อสารข้อมูล (IP-VPN Network leased line) (หัว-ท้าย) เพื่อรับ-ส่งข้อมูลระหว่างหน่วยงานภายในกองทางหลวงพิเศษระหว่างเมืองโดยเฉพาะ ซึ่งเชื่อมต่อระหว่างอาคารกองทางหลวงพิเศษระหว่างเมือง กับอาคารศูนย์ CCB (ลาดกระบัง) โดยใช้เทคโนโลยีของผู้รับจ้างให้สามารถใช้งานได้ในระดับความเร็วการสื่อสารข้อมูล ไม่น้อยกว่า ๒๐ Mbps

๔.๒.๒. ดำเนินการจัดหาวงจรเช่าพร้อมสัญญาณอินเตอร์เน็ตสำหรับองค์กรโดยเฉพาะ (Private leased line Internet Service for Organization) ขนาด ๑๐๐/๓๒ (ความเร็วคู่สายภายในประเทศ อัตราการดาวน์โหลดและอัพโหลดไม่น้อยกว่า ๑๐๐ Mbps ความเร็วคู่สายต่างประเทศ อัตราการดาวน์โหลดและอัพโหลดไม่น้อยกว่า ๓๒ Mbps โดยเชื่อมต่อระหว่างอาคารกองทางหลวงพิเศษระหว่างเมืองหรืออาคารที่ผู้ว่าจ้างกำหนดไปยังผู้ให้บริการ Internet Providers เพื่อรองรับหน่วยงานภายในกำกับดูแลของกองทางหลวงพิเศษระหว่างเมือง จำนวนอย่างน้อย ๑ จุด ดังเอกสารแนบหมายเลข ๓

๔.๒.๓. ดำเนินการจัดหาวงจรเช่าพร้อมสัญญาณอินเตอร์เน็ตสำหรับองค์กรโดยเฉพาะ (Private leased line Internet Service for Organization) ขนาด ๑๐๐/๓๒ (ความเร็วคู่สายภายในประเทศ อัตราการดาวน์โหลดและอัพโหลดไม่น้อยกว่า ๑๐๐ Mbps ความเร็วคู่สายต่างประเทศ อัตราการดาวน์โหลดและอัพโหลดไม่น้อยกว่า ๓๒ Mbpsโดยเชื่อมต่อระหว่างอาคาร CCB (ลาดกระบัง)ไปยังผู้ให้บริการ Internet Providers จำนวนอย่างน้อย ๒ จุด เพื่อรองรับหน่วยงานภายในกำกับดูแลของกองทางหลวงพิเศษระหว่างเมือง ดังเอกสารแนบหมายเลข ๓

๔.๒.๔. ดำเนินการจัดหาวงจรอินเตอร์เน็ต GIGA Fiber จำนวนอย่างน้อย ๑๓ จุด ความเร็วในแต่ละจุดไม่น้อยกว่า ๑ Gbps เพื่อรองรับหน่วยงานภายในกำกับดูแลของกองทางหลวงพิเศษระหว่างเมือง ดังเอกสารแนบหมายเลข ๓

๔.๒.๕. ดำเนินการจัดหาและติดตั้งอุปกรณ์บริหารจัดการสื่อสารข้อมูลแบนด์วิชท์ (Bandwidth Management) จำนวนไม่น้อยกว่า ๑ ชุด โดยมีคุณลักษณะเฉพาะตาม เอกสารแนบหมายเลข ๔

๔.๒.๖. ดำเนินการจัดหาและติดตั้งอุปกรณ์เพิ่มประสิทธิภาพการเข้าถึงระบบเครือข่าย (Proxy) จำนวนไม่น้อยกว่า ๒ ชุด โดยมีคุณลักษณะเฉพาะตาม เอกสารแนบหมายเลข ๔

๔.๒.๗. ดำเนินการจัดหาและติดตั้งอุปกรณ์รักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์ในระดับแอพพลิเคชั่น (Application Firewall) จำนวนไม่น้อยกว่า ๓ ชุด โดยมีคุณลักษณะเฉพาะตาม เอกสารแนบหมายเลข ๔

๔.๒.๘. ดำเนินการจัดหาและติดตั้งอุปกรณ์กระจายการทำงานสำหรับเครือข่าย (Link Load Balancer) จำนวนอย่างน้อย ๓ ชุด ตามจุดที่ผู้ว่าจ้างกำหนด โดยมีคุณลักษณะเฉพาะอย่างน้อยตาม เอกสารแนบหมายเลข ๔

๔.๒.๙. ต้องดำเนินการจัดหาและติดตั้งอุปกรณ์กระจายสัญญาณไร้สาย (Access point) ที่อาคารกองทางหลวงพิเศษระหว่างเมืองจำนวนไม่น้อยกว่า ๑๔ ชุด โดยมีคุณลักษณะเฉพาะตาม เอกสารแนบหมายเลข ๔

๔.๒.๑๐. ดำเนินการจัดหา Public IP จำนวนไม่น้อยกว่า ๑๒๔ เลขหมาย ที่อาคารกองทางหลวงพิเศษระหว่างเมือง อาคารศูนย์ควบคุมฯ CCB ลาดกระบัง หรืออาคารอื่นตามที่ผู้ว่าจ้างกำหนด

๔.๒.๑๑. ดำเนินการจัดหาอุปกรณ์เครื่องคอมพิวเตอร์แม่ข่ายและระบบปฏิบัติการ จำนวนอย่างน้อย ๑ ชุด โดยมีคุณลักษณะเฉพาะตาม เอกสารแนบหมายเลข ๔

๔.๒.๑๒. ผู้รับจ้างจะต้องดำเนินการออกแบบแผนผังการเชื่อมต่อระบบเครือข่ายสื่อสารข้อมูลและเครือข่ายอินเตอร์เน็ตระหว่างอาคารกองทางหลวงพิเศษระหว่างเมือง อาคารศูนย์ควบคุมฯ CCB (ลาดกระบัง) และอาคารศูนย์ควบคุมฯ CCB (พัทยา) รวมถึงอาคารอื่นที่ผู้ว่าจ้างกำหนดพร้อมจัดหาและติดตั้งอุปกรณ์เชื่อมต่อ รวมถึงทดสอบระบบเพื่อให้การให้บริการเป็นไปโดยสมบูรณ์

๔.๓. ข้อกำหนดในการให้บริการ

๔.๓.๑. ผู้รับจ้างต้องเสนอแผนการปฏิบัติงานและแผนบำรุงรักษาตลอดระยะเวลาของสัญญา กรณีที่มีการเปลี่ยนแปลงต้องได้รับอนุมัติทุกครั้ง

๔.๓.๒. ผู้รับจ้างต้องให้บริการวงจรสำหรับสื่อสารข้อมูล (IP-VPN Network leased line) พร้อมทั้งอุปกรณ์ต่อพ่วง โดยต้องดำเนินการบำรุงรักษาตามแผนงานฯ ที่เสนอตลอดระยะเวลาของสัญญา

๔.๓.๓. ผู้รับจ้างต้องให้บริการสัญญาณอินเตอร์เน็ตอย่างต่อเนื่องตลอด ๒๔ ชั่วโมง จำนวนอย่างน้อย ๓ จุด ตามระยะเวลาของสัญญาและจะต้องจัดทำข้อเสนอเพื่อการบริหารจัดการดังภาคผนวก ข

๔.๓.๔. ผู้รับจ้างต้องดำเนินการบำรุงรักษาระบบสื่อสารข้อมูลและอุปกรณ์ต่อพ่วง โดยมีรายละเอียดดังต่อไปนี้

- บำรุงรักษาตามกำหนดเวลาของอุปกรณ์ให้เป็นไปตามระยะเวลาของข้อกำหนดของผู้ผลิตอุปกรณ์ (PM : Preventive Maintenance) อย่างน้อยเดือนละ ๑ ครั้ง
- บำรุงรักษาแบบแก้ไขเมื่ออุปกรณ์เกิดความชำรุดเสียหายหรือระบบสื่อสารข้อมูลไม่สามารถใช้งานได้ (CM : Corrective Maintenance) เมื่อได้รับแจ้งจากผู้ว่าจ้างและจะต้องเข้ามาดำเนินการแก้ไขภายใน ๓ ชั่วโมงและต้องให้แล้วเสร็จภายในกำหนดระยะเวลา ๑๒ ชั่วโมง

๔.๓.๕. ผู้รับจ้างต้องดำเนินการซ่อมแซมแก้ไขเมื่อระบบวงจรเช่าสัญญาณอินเตอร์เน็ตสำหรับองค์กรโดยเฉพาะ (Private leased line Internet Service for Organization) และอุปกรณ์ต่อพ่วงชำรุดหรือขัดข้องไม่สามารถใช้งานได้ทันทีหลังจากได้รับแจ้งเหตุจากผู้ว่าจ้างและผู้รับจ้างต้องเข้ามาดำเนินการแก้ไขภายใน ๓ ชั่วโมงและต้องให้แล้วเสร็จภายในกำหนดระยะเวลา ๑๒ ชั่วโมง

๔.๓.๖. รายการอุปกรณ์ที่จัดหาจะต้องมีคุณลักษณะตามข้อกำหนดใน เอกสารแนบหมายเลข ๔ หรือดีกว่า และหากระบบทำงานไม่สมบูรณ์และมีความจำเป็นที่จะต้องจัดหาอุปกรณ์เพิ่มเติมเพื่อให้การทำงานของระบบมีประสิทธิภาพมากขึ้น ผู้รับจ้างจะต้องจัดหาและติดตั้งตามคำร้องขอของกรมฯ และผู้รับจ้างต้องรับผิดชอบค่าใช้จ่ายที่เกิดขึ้นเต็มจำนวน

๔.๓.๗. การซ่อมแซมแก้ไขในระยะเวลารับประกันของสัญญาหากต้องเปลี่ยนอุปกรณ์บางส่วนที่ไม่สามารถใช้งานได้อุปกรณ์ที่นำมาเปลี่ยนจะต้องมีคุณสมบัติไม่ต่ำกว่าที่ใช้อยู่เดิมโดยความเห็นชอบจากผู้ว่าจ้างก่อนดำเนินการและผู้รับจ้างจะต้องเป็นผู้รับผิดชอบค่าใช้จ่ายที่เกิดขึ้นทั้งหมด

๔.๓.๘. ในการดำเนินการที่มีผลกระทบต่อการให้บริการ ให้ผู้รับจ้างต้องแจ้งเจ้าหน้าที่ของกองทางหลวงพิเศษระหว่างเมืองก่อนเข้าดำเนินการทุกครั้ง

๔.๓.๙. การประสานงาน

๔.๓.๙.๑. ผู้รับจ้างต้องต้องเสนอชื่อผู้เชี่ยวชาญด้านเทคนิคเพื่อให้คำแนะนำในการใช้งาน พร้อมเบอร์โทรศัพท์มือถือ และ E-mail ตลอดระยะเวลาในสัญญาหากมีการเปลี่ยนแปลงจะต้องขอความเห็นชอบก่อนทุกครั้ง

๔.๓.๙.๒. ผู้รับจ้างจะต้องแจ้งรายชื่อผู้ติดต่อประสานงานสำหรับการเข้าซ่อมแซมแก้ไขกรณีระบบหรืออุปกรณ์ขัดข้องหรือชำรุด พร้อมเบอร์โทรศัพท์มือถือ และอีเมลให้ผู้ว่าจ้างทราบ

๔.๔ ข้อกำหนดการเสนอเอกสารด้านเทคนิค

๔.๔.๑ ผู้เสนอราคาต้องส่งเอกสารทางด้านเทคนิคเพื่อให้ กท. พิจารณาตามภาคผนวก ก ให้ถูกต้องครบถ้วนทุกรายการ

๔.๔.๒ ผู้เสนอราคาต้องเสนอแนวทางการเชื่อมต่อระบบการสื่อสารข้อมูลและการเชื่อมต่อสัญญาณอินเตอร์เน็ตอย่างน้อย ตามเอกสารแนบหมายเลข ๑

๔.๔.๓ ผู้เสนอราคาจะต้องทำตารางเปรียบเทียบระหว่าง ข้อเสนอของผู้ยื่น กับรายการข้อกำหนดและภาคผนวกทั้งหมด เป็นรายข้อ โดยใช้ตัวอย่างแบบการเปรียบเทียบตามตารางที่ ๑ ในการเปรียบเทียบรายการดังกล่าว หากมีกรณีที่ต้องมีการอ้างอิงข้อความหรือเอกสารในส่วนอื่นที่จัดทำเสนอมา ผู้เสนอราคาต้องระบุให้เห็นอย่างชัดเจน สามารถตรวจสอบได้โดยง่าย ไว้ในเอกสารเปรียบเทียบด้วยว่า สิ่งที่ต้องการอ้างอิงถึงนั้น อยู่ในส่วนใดตำแหน่งใดของเอกสารอื่น ๆ ที่จัดทำเสนอมา สำหรับเอกสารที่อ้างอิงถึง ให้หมายเหตุหรือขีดเส้นใต้หรือระบายสีพร้อมเขียนหัวข้อกำกับไว้ เพื่อให้สามารถตรวจสอบกับเอกสารเปรียบเทียบได้ง่ายและตรงกันด้วย

อ้างถึงข้อ	ข้อกำหนดอุปกรณ์ที่/ต้องการ	ข้อกำหนดอุปกรณ์ที่/นำเสนอ	เอกสารอ้างอิง
ระบุหัวข้อให้ตรงกับหัวข้อที่ระบุในเอกสารประกวดราคา	ให้คัดลอกคุณลักษณะเฉพาะที่กำหนดในรายการข้อกำหนดและภาคผนวก มากรอกในช่องนี้	ให้ระบุคุณลักษณะเฉพาะที่ผู้เสนอราคายื่นเสนอ	ระบุหมายเลขหน้าของเอกสารอ้างอิงของผู้เสนอราคา

ตารางที่ ๑ ตารางเปรียบเทียบคุณสมบัติข้อกำหนดและรายละเอียดข้อเสนอโครงการ

๔.๔.๔ ผู้เสนอราคาต้องส่งแคตตาล็อครายการอุปกรณ์ตาม เอกสารแนบหมายเลข ๔ ของรายละเอียดคุณลักษณะเฉพาะของทุกรายการที่ผู้เสนอราคาได้เสนอเพื่อประกอบการพิจารณา สำหรับเอกสารที่ยื่นมาหากเป็นสำเนารูปถ่าย จะต้องรับรองสำเนาถูกต้อง โดยผู้มีอำนาจทำนิติกรรมแทนนิติบุคคล

๕. งบประมาณ ระยะเวลาในการดำเนินงานและค่าปรับ

๕.๑. ราคากลาง 6,950,000.00 บาท (งบประมาณ ๗,๐๐๐,๐๐๐.๐๐ บาท)

๕.๒. หลักประกันการเสนอราคา ๓๕๐,๐๐๐.๐๐ บาท

๕.๓. ระยะเวลาการจ้างเหมาบริการทั้งหมด ๑๒ เดือน

๕.๔. ค่าปรับ

ผู้ว่าจ้างจะคิดค่าปรับกรณีที่ผู้รับจ้างไม่สามารถดำเนินงานได้ตามข้อกำหนดเกี่ยวกับการให้บริการ โดยคิดค่าปรับดังต่อไปนี้

๕.๔.๑. หากการให้บริการระบบเครือข่ายอินเตอร์เน็ตหรือระบบเชื่อมโยงโครงข่ายสื่อสารข้อมูลแบบเฉพาะส่วน (Private Network) เกิดขัดข้องหรือไม่สามารถให้ บริการได้เป็นเวลาเกินกว่า ๑ ชั่วโมงติดต่อกัน หรือขัดข้องเกินกว่าครั้งละ ๑๕ นาที ตั้งแต่ ๓ ครั้งขึ้นไปภายในเวลา ๒๔ ชั่วโมง นับจากการขัดข้องในครั้งแรก ผู้ว่าจ้างขอสงวนสิทธิ์ในการปรับลดค่าเช่าบริการโดยคิดเป็นวันในอัตราวันละ ๑/๓๐ ของค่าบริการ (เศษชั่วโมงของวันคิดเป็นหนึ่งวัน) โดยหักจากค่าบริการเช่าของเดือนนั้น ๆ

๕.๔.๒. กรณีที่ผู้รับจ้างผิดสัญญานอกเหนือจากข้อกำหนดข้อ ๕.๕.๑ ผู้ว่าจ้างขอสงวนสิทธิ์ในการคิดค่าปรับต่อวันในอัตราร้อยละ ๐.๑๐ ของค่างานในสัญญา

๕.๔.๓. ระยะเวลาในการคิดคำนวณการขัดข้องหรือการชำรุดบกพร่อง เริ่มนับตั้งแต่เวลาที่ขัดข้องครั้งแรก และสิ้นสุดลงเมื่อผู้รับจ้างและผู้ว่าจ้างรับรองว่าการใช้บริการระบบสื่อสารข้อมูลสามารถใช้งานได้เป็นปกติ

๖. การบอกเลิกสัญญา

๖.๑. ในกรณีที่ผู้รับจ้างไม่เข้าดำเนินการ ติดตั้งอุปกรณ์ระบบฯหรือไม่สามารถให้บริการได้ตามข้อกำหนดนี้ ผู้ว่าจ้างขอสงวนสิทธิในการจัดหาผู้รับจ้างรายอื่นเพื่อเข้าดำเนินการจัดหาอุปกรณ์และติดตั้งระบบฯให้สามารถทำงานต่อไปได้ โดยผู้รับจ้างต้องเป็นรับผิดชอบค่าใช้จ่ายที่เกิดขึ้นทั้งหมดและไม่สามารถเรียกร้องค่าเสียหายใด ๆ ทั้งสิ้นจากผู้ว่าจ้างได้

๖.๒. ผู้ว่าจ้างมีสิทธิบอกเลิกสัญญากับผู้รับจ้างทันทีที่ผู้รับจ้างไม่ปฏิบัติตามเงื่อนไขของสัญญา โดยผู้รับจ้างต้องจ่ายค่าเสียหายให้กับผู้ว่าจ้างเต็มจำนวนตามสัญญานี้ และผู้ว่าจ้างจะพิจารณาเสนอให้ผู้รับจ้างเป็นผู้ทิ้งงานของทางราชการต่อไป

๖.๓. ผู้ว่าจ้างขอสงวนสิทธิ์ในการยกเลิกสัญญาจ้างเหมาบริการนี้ หากพิจารณาแล้วว่าผู้รับจ้างไม่สามารถดำเนินการตามข้อกำหนดได้อย่างมีประสิทธิภาพ ครบถ้วนสมบูรณ์

๗. กำหนดส่งมอบ

ผู้รับจ้างต้องจัดหาติดตั้งเชื่อมต่อระบบโครงข่ายสื่อสารและอุปกรณ์ตามข้อกำหนดให้แล้วเสร็จครบถ้วนสมบูรณ์ใช้งานได้อย่างมีประสิทธิภาพ ภายในวันที่เริ่มต้นสัญญา

๘. หลักเกณฑ์การจ่ายเงิน

จ่ายเงินเป็นรายเดือนๆ ละเท่า ๆ กัน ยกเว้นเดือนแรกและเดือนสุดท้ายจะจ่ายตามที่ปฏิบัติงานจริง โดยกำหนด ๑ เดือนมี ๓๐ วัน และจะจ่ายเมื่อคณะกรรมการตรวจรับงานได้ตรวจสอบและพิจารณาตรวจรับงานเรียบร้อยแล้ว

๙. คุณสมบัติของผู้เสนอราคา

๙.๑. ผู้มีความสามารถตามกฎหมาย

๙.๒. ไม่เป็นบุคคลล้มละลาย

๙.๓. ไม่อยู่ระหว่างเลิกกิจการ

๙.๔. ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราวเนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

๙.๕. ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วน ผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

๙.๖. มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

๙.๗. เป็นนิติบุคคลผู้มีอาชีพรับจ้างงานที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

๙.๘. ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่กรมทางหลวง ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรม ในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

๙.๙. ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทยเว้นแต่รัฐบาลของผู้ยื่นข้อเสนอ ได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

๙.๑๐. ผู้ยื่นข้อเสนอต้องลงทะเบียนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement : e – GP) ของกรมบัญชีกลาง

๙.๑๑. ผู้ยื่นข้อเสนอต้องมีผลงานและประสบการณ์ที่เกี่ยวข้องในการให้บริการสื่อสารข้อมูลหรือบริการอินเตอร์เน็ตภายในระยะเวลา ๓ ปี ก่อนการยื่นข้อเสนอไม่น้อยกว่า ๑ ผลงาน ซึ่งผลงานดังกล่าวเป็นสัญญาที่ผู้ยื่นข้อเสนอได้ทำงานแล้วเสร็จตามสัญญาและได้มีการส่งมอบงานและตรวจรับงานเรียบร้อยแล้ว โดยมูลค่างานตามสัญญาไม่น้อยกว่า ๑,๐๐๐,๐๐๐.๐๐ บาท ซึ่งเป็นผลงานในสัญญาเดียวเท่านั้น และเป็นผลงานที่เป็นคู่สัญญาโดยตรงกับส่วนราชการ หน่วยงานตาม

กฎหมายว่าด้วยระเบียบบริหารราชการส่วนท้องถิ่น รัฐวิสาหกิจในประเทศไทยหรือรัฐวิสาหกิจ โดยยื่นสำเนาหนังสือรับรองผลงานหรือสำเนาสัญญาพร้อมรับรองสำเนาถูกต้องและประทับตรา (ถ้ามี)

๙.๑๒. ผู้ยื่นข้อเสนอที่เสนอราคาในรูปแบบของ “กิจการร่วมค้า” ต้องมีคุณสมบัติ ดังนี้

๙.๑๒.๑. กรณีที่ข้อตกลงระหว่างผู้ร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงระหว่างผู้ร่วมค้าจะต้องมีการกำหนดสัดส่วนหน้าที่ และความรับผิดชอบในปริมาณงาน สิ่งของ หรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

๙.๑๒.๒. กรณีที่ข้อตกลงระหว่างผู้ร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก กิจการร่วมค้านั้นต้องใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

๙.๑๒.๓. สำหรับข้อตกลงระหว่างผู้ร่วมค้าที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารที่เชิญชวน หรือหนังสือเชิญชวน กรณีผู้ประกอบการ SMEs ที่จะเสนอราคาในรูปแบบของ“กิจการร่วมค้า” ต้องมีคุณสมบัติ ดังนี้

(๑) ผู้เข้าร่วมค้าทุกรายจะต้องเป็นผู้ประกอบการ SMEs

(๒) ผู้เข้าร่วมค้าทุกรายจะต้องเป็นผู้ประกอบการที่เป็นบุคคลธรรมดาที่ถือสัญชาติไทย หรือนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย

๑๐.หลักเกณฑ์และสิทธิในการพิจารณา

กรมทางหลวง โดย กองทางหลวงพิเศษระหว่างเมือง กำหนดหลักเกณฑ์การพิจารณาดังนี้

๑๐.๑ การพิจารณาผลการยื่นข้อเสนอประกวดราคาอิเล็กทรอนิกส์ครั้งนี้ กรมจะพิจารณาตัดสินโดยใช้หลักเกณฑ์ราคา (Price)

๑๐.๒ การพิจารณาผู้ชนะการยื่นข้อเสนอ

กรณีใช้หลักเกณฑ์ราคา (Price) ในการพิจารณาผู้ชนะการยื่นข้อเสนอ กรมจะพิจารณาจากราคารวม

๑๐.๓ หากผู้ยื่นเสนอราคาซึ่งเป็นผู้ประกอบการ SMEs เสนอราคาสูงกว่าราคาต่ำสุดของผู้ยื่นเสนอราคารายอื่นไม่เกินร้อยละ ๑๐ หน่วยงานของรัฐจะจัดซื้อจัดจ้าง จากผู้ประกอบการ SMEs ดังกล่าว

๑๐.๔ คุณสมบัติของผู้ยื่นข้อเสนอ

หากผู้ยื่นข้อเสนอรายใดมีคุณสมบัติไม่ครบถ้วนหรือไม่ถูกต้องตามข้อกำหนดหรือยื่นเอกสารหลักฐานการยื่นข้อเสนอไม่ถูกต้องหรือไม่ครบถ้วนตามเอกสารประกวดราคาจ้างด้วยวิธีการอิเล็กทรอนิกส์ (e-bidding) คณะกรรมการพิจารณาผลการประกวดราคาจะไม่รับพิจารณาราคาของผู้ยื่นข้อเสนอรายนั้น เว้นแต่เป็นข้อผิดพลาดเพียงเล็กน้อยหรือผิดแผกไปจากเงื่อนไขของเอกสารประกวดราคาอิเล็กทรอนิกส์ในส่วนที่มิใช่สาระสำคัญ ทั้งนี้ เฉพาะในกรณีที่พิจารณาแล้วเห็นว่าจะเป็นประโยชน์ต่อกรมทางหลวงเท่านั้น

๑๐.๕ กรมขอสงวนสิทธิไม่พิจารณาข้อเสนอของผู้เสนอราคาโดยไม่มีการผ่อนผัน ในกรณีดังต่อไปนี้

๑๐.๕.๑ ไม่ปรากฏชื่อผู้เสนอราคารายนั้นในบัญชีผู้รับเอกสารประกวดราคาอิเล็กทรอนิกส์ของกรมทางหลวง

๑๐.๕.๒ ไม่กรอกชื่อบุคคลหรือนิติบุคคล หรือลงลายมือชื่ออิเล็กทรอนิกส์ของผู้เสนอราคาอย่างหนึ่งอย่างใด หรือทั้งหมดในใบเสนอราคา

๑๐.๕.๓ เสนอรายละเอียดแตกต่างไปจากเงื่อนไขที่กำหนดในเอกสารประกวดราคาอิเล็กทรอนิกส์ที่เป็นสาระสำคัญหรือมีผลทำให้เกิดความได้เปรียบเสียเปรียบแก่ผู้เสนอราคารายอื่น

๑๐.๕.๔ ในการตัดสินการประกวดราคาอิเล็กทรอนิกส์ หรือในการทำสัญญา คณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์หรือกรม มีสิทธิให้ผู้เสนอราคาชี้แจงข้อเท็จจริง สภาพ ฐานะ หรือข้อเท็จจริงอื่นใดที่เกี่ยวข้องกับผู้เสนอราคาได้ กรมมีสิทธิที่จะไม่รับข้อเสนอ ไม่รับราคา หรือไม่ทำสัญญา หากหลักฐานดังกล่าวไม่มีความเหมาะสมหรือไม่ถูกต้อง

๑๐.๕.๕ กรมทรงไว้ซึ่งสิทธิที่จะไม่รับราคาต่ำสุด หรือราคาหนึ่งราคาใด หรือราคาที่เสนอทั้งหมดก็ได้ และอาจพิจารณาเลือกจ้างในจำนวน หรือขนาด หรือเฉพาะรายการหนึ่งรายการใดหรืออาจจะยกเลิกการประกวดราคาอิเล็กทรอนิกส์โดยไม่พิจารณาจัดจ้างเลยก็ได้สุดแต่จะพิจารณา ทั้งนี้เพื่อประโยชน์ของทางราชการเป็นสำคัญ และให้ถือว่าการตัดสินของกรมเป็นเด็ดขาดผู้เสนอราคาจะเรียกร้องค่าเสียหายใดๆ มิได้ รวมทั้งกรมจะพิจารณายกเลิกการประกวดราคาอิเล็กทรอนิกส์และลงโทษผู้เสนอราคาเป็นผู้ทิ้งงาน ไม่ว่าจะเป็นผู้เสนอราคาที่ได้รับการคัดเลือกหรือไม่ก็ตาม หากมีเหตุที่เชื่อถือได้ว่าการยื่นข้อเสนอกระทำการโดยไม่สุจริต เช่น การเสนอเอกสารอันเป็นเท็จ หรือใช้ชื่อบุคคลธรรมดา หรือนิติบุคคลอื่นมาเสนอราคาแทน เป็นต้น

ในกรณีที่ผู้เสนอราคารายที่เสนอราคาต่ำสุด เสนอราคาต่ำจนคาดหมายได้ว่าไม่อาจดำเนินงานตามสัญญาได้ คณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์หรือกรมจะให้ผู้เสนอราคารายนั้นชี้แจงและแสดงหลักฐานที่ทำให้เชื่อได้ว่า ผู้เสนอราคาสามารถดำเนินงานตามประกวดราคาจ้างอิเล็กทรอนิกส์ให้เสร็จสมบูรณ์ หากคำชี้แจงไม่เป็นที่รับฟังได้กรมทางหลวงมีสิทธิที่จะไม่รับข้อเสนอหรือไม่รับราคาของผู้เสนอราคารายนั้น

ในกรณีที่ปรากฏข้อเท็จจริงภายหลังจากการพิจารณาข้อเสนอว่า ผู้เสนอราคาที่มีสิทธิได้รับการคัดเลือกเป็นผู้เสนอราคาที่มีผลประโยชน์ร่วมกันกับผู้เสนอราคารายอื่น ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือเป็นผู้เสนอราคาที่กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรม กรมมีอำนาจที่จะตัดรายชื่อผู้เสนอราคาที่ได้รับคัดเลือกรายดังกล่าวออก และกรมอาจพิจารณาลงโทษผู้เสนอราคารายนั้นเป็นผู้ทิ้งงาน

ในกรณีนี้หากกรมพิจารณาเห็นว่าการยกเลิกการพิจารณาผลการเสนอราคาที่ได้ดำเนินการไปแล้วจะเป็นประโยชน์แก่ทางราชการ กรมมีอำนาจยกเลิกการพิจารณาผลการเสนอราคาดังกล่าวได้ ผู้ยื่นข้อเสนอไม่สามารถเรียกร้องค่าเสียหายใดๆ ได้

๑๑.การสงวนสิทธิในกรณีอื่น ๆ

๑๑.๑. ผู้ว่าจ้างขอสงวนสิทธิ์ในการปรับปรุงแก้ไขหรือยกเลิกข้อกำหนดดังกล่าวนี้บางส่วนหรือทั้งหมดและให้ถือว่าการพิจารณาวินิจฉัยชี้ขาดของผู้ว่าจ้างเป็นที่สุดทั้งนี้ผู้ยื่นข้อเสนอตกลงยินยอมไม่เรียกร้องค่าเสียหายไม่ว่าในกรณีใด ๆ ทั้งสิ้นจากผู้ว่าจ้าง

๑๑.๒. ผู้ว่าจ้างขอสงวนสิทธิ์ในการเปลี่ยนแปลงราคาค่างานกรณีที่กรมทางหลวงเข้าดำเนินการโครงการใด ๆ ที่ทับซ้อนกับโครงการนี้ โดยพิจารณาปรับลดค่างานตามที่กำหนดไว้ในราคาประเมิน (ราคากลาง)

๑๑.๓. เมื่อถึงวันสิ้นสุดตามสัญญาและผู้ว่าจ้างมีความประสงค์จะให้ผู้รับจ้างดำเนินการต่อตามเงื่อนไขของสัญญาที่ทำไว้ต่อกันอีกระยะหนึ่งไม่เกิน ๓๐ วัน นับถัดจากวันที่สิ้นสุดสัญญา ผู้รับจ้างต้องยินยอมดำเนินการตามความประสงค์ของผู้ว่าจ้าง

๑๑.๔. กรมทางหลวงขอสงวนสิทธิในการพิจารณาขยายอายุสัญญาตามแนวทางการพิจารณาขยายอายุสัญญาหรือการงดหรือลดค่าปรับงานจ้างเหมาของกรมทางหลวง (สิงหาคม ๒๕๖๑)

๑๑.๕. กองทางหลวงพิเศษระหว่างเมือง กรมทางหลวง จะทำสัญญาผูกพันก็ต่อเมื่อได้รับเงินประมาณการรายจ่ายเงินทุนค่าธรรมเนียมผ่านทาง ประจำปีงบประมาณ ๒๕๖๕ จากกระทรวงการคลังแล้วเท่านั้น

หมายเหตุ

ผู้สนใจสามารถวิจารณ์และเสนอข้อคิดเห็นหรือข้อเสนอแนะเกี่ยวกับร่างรายละเอียดคุณลักษณะเฉพาะของพัสดุที่จัดหางานนี้เป็นลายลักษณ์อักษร โดยไปรษณีย์ตอบรับด่วนพิเศษ (EMS) ส่งไปที่ฝ่ายบริหารงานทั่วไปกองทางหลวงพิเศษระหว่างเมือง กรมทางหลวง อาคารหมายเลข ๑๙ ถนนศรีอยุธยา เขตราชเทวี กรุงเทพฯ ๑๐๔๐๐ หรือโทรสารหมายเลข (๐๒) ๓๕๔-๔๔๖๑ หรือ Email Address : motorway@doh.go.th โดยระบุชื่อ ที่อยู่ และหมายเลขโทรศัพท์ที่สามารถติดต่อได้ ในกรณีที่เป็นนิติบุคคลให้ระบุชื่อผู้มีอำนาจลงนามผูกพันนิติบุคคล

(ลงชื่อ).....ประธานกรรมการ
(นายอดิศร์ ทองกุม)

(ลงชื่อ).....กรรมการ
(นายอภิชัย อิสริยานุกูล)

(ลงชื่อ).....กรรมการ
(นายชาคริต ดุลยรัตน์)

(ลงชื่อ).....กรรมการและเลขานุการ
(นางสาวมาริษา เพ็ชรประโคน)

เอกสารแนบหมายเลข ๑

กองทางหลวงพิเศษระหว่างเมือง

ค่าจ้างเหมาวงจรเช่าสำหรับสื่อสารข้อมูล พร้อมสัญญาณอินเตอร์เน็ตสำหรับองค์กรโดยเฉพาะ และบริหารจัดการการใช้งาน (Service) ตามความต้องการของหน่วยงาน

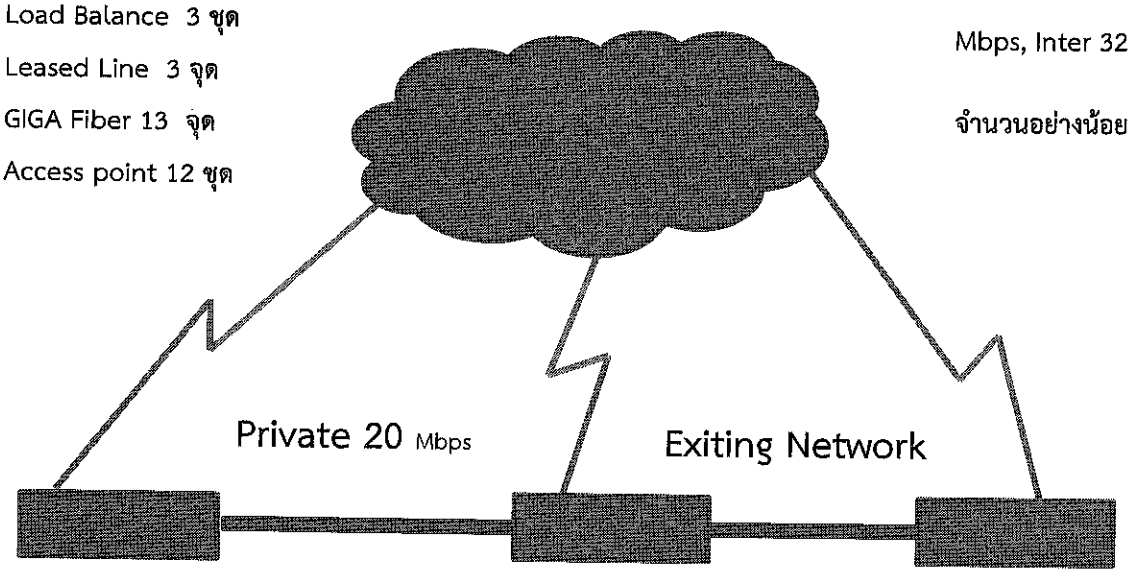
(ผังแนะนำแสดงการเชื่อมต่อระบบโครงข่ายสื่อสารข้อมูลที่ต้องการติดตั้ง)

- Proxy 2 ชุด
- Bandwidth Management 1 ชุด
- Firewall 3 ชุด
- Load Balance 3 ชุด
- Leased Line 3 จุด
- GIGA Fiber 13 จุด
- Access point 12 ชุด

Private Leased line 100/32 Mbps

With Private Internet Domestic 100 Mbps, Inter 32 Mbps

จำนวนอย่างน้อย 3 จุด



ความเร็วภายในประเทศ ๑๐๐ เมกกะบิต
ความเร็วต่างประเทศ ๓๒ เมกกะบิต
จำนวนอย่างน้อย ๓ จุด

แผนผังแสดงการเชื่อมต่อระบบโครงข่ายสื่อสารข้อมูลระหว่างหน่วยงานต่าง ๆ ของกองทางหลวงพิเศษระหว่างเมือง

เอกสารแนบหมายเลข ๒

ค่าจ้างเหมาวงจรเช่าสำหรับสื่อสารข้อมูล พร้อมสัญญาณอินเตอร์เน็ตสำหรับองค์กรโดยเฉพาะ และบริหารจัดการการใช้งาน (Service) ตามความต้องการของหน่วยงาน

---

๑. ระบบต่าง ๆ ของกองทางหลวงพิเศษระหว่างเมืองที่ใช้รับส่งข้อมูลผ่านเครือข่ายเฉพาะส่วน (Private Network) และวงจรอินเตอร์เน็ตสำหรับองค์กรโดยเฉพาะ ดังต่อไปนี้

๑.๑. ระบบงานพัสดุ จำนวน ๑ ระบบ

๑.๒. ระบบเว็บไซต์ กท. จำนวน ๑ ระบบ

๑.๓. ระบบเบิกจ่ายน้ำมัน จำนวน ๑ ระบบ

๑.๔. ระบบบริหารงานบุคคล จำนวน ๑ ระบบ

๑.๕. ระบบบริหารงานงบประมาณ จำนวน ๑ ระบบ

๑.๖. ระบบบริหารบัญชีและการเงิน จำนวน ๑ ระบบ

๑.๗. ระบบบริหารจัดการทรัพย์สิน (ซ่อมบำรุง) จำนวน ๑ ระบบ

๑.๘. ระบบบูรณาการข้อมูลเพื่อการบริหารจัดการ จำนวน ๑ ระบบ

๑.๙. ระบบ Call Center ๑๕๘๖ จำนวน ๑ ระบบ

๑.๑๐. ระบบอำนวยความปลอดภัยและจราจร (IMS) จำนวน ๑ ระบบ

๑.๑๑. ระบบติดตามรถกู้ภัย GPS Gate จำนวน ๑ ระบบ

๑.๑๒. ระบบสำรองข้อมูลและกู้คืนระบบ จำนวน ๑ ระบบ

๑.๑๓. ระบบการเข้ารหัสในการสื่อสารข้อมูลบนเครือข่ายอินเตอร์เน็ต จำนวน ๑ ระบบ

๑.๑๔. ระบบบริหารจัดการข้อมูลผู้ใช้งานอินเตอร์เน็ต จำนวน ๑ ระบบ

๑.๑๕. ระบบติดตามการเบิกจ่ายเงินทุนค่าธรรมเนียมผ่านทาง (mPlannet) จำนวน ๑ ระบบ

๒. หน่วยงานต่าง ๆ ของกองทางหลวงพิเศษระหว่างเมืองที่ใช้รับส่งข้อมูลผ่านเครือข่ายเฉพาะส่วน (Private Network) และวงจรอินเตอร์เน็ตสำหรับองค์กรโดยเฉพาะ ดังต่อไปนี้

๒.๑. ฝ่ายบริหารงานทั่วไป

๒.๒. ฝ่ายกำหนดกลยุทธ์และแผนงาน

๒.๓. ฝ่ายบริหารการร่วมลงทุน

๒.๔. ฝ่ายบริหารการดำเนินงาน

๒.๕. ฝ่ายบริหารการจัดเก็บเงินค่าธรรมเนียม

๒.๖. ฝ่ายบริหารค่าธรรมเนียมผ่านทาง

๒.๗. ฝ่ายบริหารจัดการจราจร

๒.๘. ฝ่ายตรวจสอบรายได้

๒.๙. ฝ่ายบำรุงรักษาทรัพย์สิน

๒.๑๐ ฝ่ายบริการธุรกรรมทางอิเล็กทรอนิกส์

๒.๑๑ แขวงทางหลวงพิเศษระหว่างเมือง

๓. จัดเตรียม IP จริง (Public IP) จำนวนไม่น้อยกว่า ๑๒๔ ชุด

๓.๑. อาคารกองทางหลวงพิเศษระหว่างเมือง จำนวน ๔๔ ชุด

๓.๒. อาคาร CCB (ลาดกระบัง) จำนวน ๘๐ ชุด

เอกสารแนบหมายเลข ๓

ค่าจ้างเหมาวงจรเช่าสำหรับสื่อสารข้อมูล พร้อมสัญญาณอินเตอร์เน็ตสำหรับองค์กรโดยเฉพาะ และบริหารจัดการการใช้งาน (Service) ตามความต้องการของหน่วยงาน

หน่วยงานที่ใช้อินเตอร์เน็ตภายในกองทางหลวงพิเศษระหว่างเมือง และหน่วยงานบนทางหลวงพิเศษหมายเลข ๗ และ ๙ จำนวนอย่างน้อย ๓ วงจร ดังนี้

๑.หน่วยงานภายในอาคารกองทางหลวงพิเศษระหว่างเมือง

๑.๑ ฝ่ายบริหารค่าธรรมเนียมผ่านทาง

๑.๑.๑ งานการเงิน

๑.๑.๒ งานบัญชี

๑.๑.๓ งานเงินเดือนและค่าจ้าง

๑.๑.๔ งานตรวจสอบใบสำคัญ

๑.๒ ฝ่ายบริหารงานทั่วไป

๑.๒.๑ งานสารบรรณ

๑.๒.๒ งานพัสดุและสัญญา

๑.๒.๓ งานกฎหมายและนิติกร

๑.๓ ฝ่ายกำหนดกลยุทธ์และแผนงาน

๑.๔ ฝ่ายบริหารการร่วมลงทุน

๑.๕ ฝ่ายบริหารการดำเนินงาน

๑.๖ ฝ่ายบริการธุรกรรมทางอิเล็กทรอนิกส์

๒. หน่วยงานบนทางหลวงพิเศษหมายเลข ๗ และ ๙

๒.๑ ฝ่ายตรวจสอบรายได้

๒.๑.๑ งานตรวจสอบรายได้ ๑ (สาย ๙)

๒.๑.๒ งานตรวจสอบรายได้ ๒ (สาย ๗)

๒.๒ ฝ่ายบริหารการจัดเก็บเงินค่าธรรมเนียม

๒.๒.๑ ฝ่ายจัดเก็บค่าธรรมเนียมผ่านทาง ๑ (สาย๙)

๒.๒.๒ ฝ่ายจัดเก็บค่าธรรมเนียมผ่านทาง ๒ (สาย๗)

๒.๒.๓ ฝ่ายควบคุมการจัดเก็บค่าธรรมเนียมผ่านทาง

๒.๒.๔ ฝ่ายเทคโนโลยีและระบบจัดเก็บค่าผ่านทาง

๒.๒.๕ ฝ่ายบริหารข้อมูลและสถิติ

๒.๓ ฝ่ายบำรุงรักษาทรัพย์สิน

๒.๓.๑ ฝ่ายบำรุงรักษาทรัพย์สิน สาย ๗

๒.๓.๒ ฝ่ายบำรุงรักษาทรัพย์สิน สาย ๙

๒.๓.๓ ฝ่ายบำรุงรักษาอาคารสถานที่

๒.๔ ด่านจัดเก็บค่าธรรมเนียมผ่านทาง

๒.๔.๑ ด่านฯธัญบุรี ๑,๒

๒.๔.๒ ด่านฯทับช้าง ๑

๒.๔.๓ ด่านฯทับช้าง ๒

๒.๔.๔ ด่านฯลาดกระบัง

๒.๔.๕ ด่านฯบางบ่อ

๒.๔.๖ ด่านฯบางปะกง

๒.๔.๗ ด่านฯพนัสนิคม

๒.๔.๘ ด่านฯบ้านบึง

๒.๔.๙ ด่านฯบางพระ

๒.๔.๑๐ ด่านฯหนองขาม

๒.๔.๑๑ ด่านฯโป่ง

๒.๔.๑๒ ด่านฯพัทยา

๒.๔.๑๓ ด่านฯห้วยใหญ่

๒.๔.๑๔ ด่านฯ เขาชีโอน

๒.๔.๑๕ ด่านฯ มาบตาพุด

๒.๕ ส่วนปฏิบัติการความปลอดภัยทางหลวงพิเศษระหว่างเมือง (กู้ภัย)

๒.๕.๑ งานกู้ภัยคลองหลวง

๒.๕.๒ งานกู้ภัยรามอินทรา

๒.๕.๓ งานกู้ภัยสุวรรณภูมิ

๒.๕.๔ งานกู้ภัยบางปะกง

๒.๖ หมวดการทาง จำนวน ๔ หน่วยงาน

๒.๖.๑ หมวดคลองหลวง

๒.๖.๒ หมวดลาดกระบัง

๒.๖.๓ หมวดพานทอง

๒.๖.๔ หมวดคันนายาว

๒.๗ แขวงทางหลวงพิเศษระหว่างเมือง

๒.๗.๑ ฝ่ายบริหารงานทั่วไป

๒.๗.๒ ฝ่ายวิศวกรรม

๒.๗.๓ ฝ่ายปฏิบัติการ

๒.๘ ฝ่ายบริหารจัดการจราจร (CCB ลาดกระบัง,พัทยา)

๒.๙.๑ งานบริหารการจราจร (Control Room)

๒.๙.๒ งานบริหารระบบและอุปกรณ์

๒.๙.๓ งานบริหารข้อมูลและสารสนเทศ

เอกสารแนบหมายเลข ๔

ค่าจ้างเหมาวงจรเช่าสำหรับสื่อสารข้อมูล พร้อมสัญญาณอินเตอร์เน็ตสำหรับองค์กรโดยเฉพาะ และบริหารจัดการการใช้งาน (Service) ตามความต้องการของหน่วยงาน

---

๑. คุณลักษณะเฉพาะของอุปกรณ์ที่เพิ่มประสิทธิภาพการเข้าถึงระบบเครือข่าย (Proxy)
ต้องมีคุณลักษณะเฉพาะอย่างน้อยดังนี้

๑.๑. อุปกรณ์ที่เสนอต้องเป็นอุปกรณ์แบบ Appliance ที่ถูกออกแบบมาเพื่อเร่งความเร็วการใช้งาน Application และมีระบบการรักษาความปลอดภัยในการใช้งาน โดยสามารถกำหนดนโยบายตามผู้ใช้งาน (user level policy) ได้

๑.๒. อุปกรณ์ที่เสนอต้องมีขนาดของ Hard disk ไม่น้อยกว่า ๕๐๐ GB

๑.๓. อุปกรณ์ที่เสนอต้องมีหน่วยความจำ RAM ไม่น้อยกว่า ๔ GB

๑.๔. อุปกรณ์ที่เสนอต้องมีพอร์ต ๑๐๐๐Base-T จำนวนไม่น้อยกว่า ๒ พอร์ต และสามารถเพิ่มพอร์ต ๑๐๐๐Base-T จำนวน ๔ พอร์ต หรือ ๑๐๐๐Base-F จำนวน ๔ พอร์ตได้ในอนาคต โดยต้องสามารถทำ Bypass หรือ Pass-through ได้ทั้งพอร์ตที่นำเสนอในตอนแรก และพอร์ตที่เปลี่ยนในภายหลัง

๑.๕. อุปกรณ์ที่เสนอต้องมีพอร์ตที่ใช้สำหรับบริหารจัดการโดยเฉพาะ (Port for Management) แบบ ๑๐๐Base-T จำนวนไม่น้อยกว่า ๑ พอร์ต

๑.๖. อุปกรณ์ที่เสนอสามารถรองรับจำนวนผู้ใช้งานได้โดยไม่จำกัดจำนวนผู้ใช้ (Unlimited) ในเวลาเดียวกัน (Concurrent users)

๑.๗. อุปกรณ์ที่เสนอต้องสนับสนุนการใช้งานโปรโตคอล HTTP, SSL, CIFS, FTP, MAPI, DNS, MMS, RTSP ได้

๑.๘. อุปกรณ์ที่เสนอต้องสามารถทำงานร่วมกับ IPv๖ ได้โดยสามารถใช้ IPv๖ ในการทำ authentication, authorization, logging, reporting และ policy enforcement ได้เป็นอย่างน้อย

๑.๙. อุปกรณ์ที่เสนอสามารถรองรับการเร่งความเร็ว (Acceleration), เฝ้าระวัง (monitoring), และควบคุม (control) ทราฟฟิกของ Adobe Flash streaming media ได้

๑.๑๐. อุปกรณ์ที่เสนอต้องสามารถทำ Transparent Proxy และ In-line Bridge Mode ได้ โดยไม่จำเป็นต้องกำหนดค่า Proxy address ที่ Web Browser ของเครื่องลูกข่าย

๑.๑๑. อุปกรณ์ที่เสนอต้องสนับสนุนการทำงานกับโปรโตคอล WCCP ได้ และสนับสนุนการ Return Traffic ได้ทั้งในแบบ GRE Tunnel และ Layer๒ Return ได้เป็นอย่างน้อย

๑.๑๒. อุปกรณ์ที่เสนอต้องสนับสนุนการ Cache ข้อมูลประเภท Streaming รวมถึง Windows Media Streaming, Real และ QuickTime ได้เป็นอย่างน้อย

๑.๑๓. อุปกรณ์ที่เสนอต้องสามารถรองรับ Secure Internet Content Adaptation Protocol (Secure ICAP) ในการทำงานร่วมกับระบบ Anti-Virus หรือ Third Party ได้

๑.๑๔. อุปกรณ์ที่เสนอต้องสนับสนุนการใช้งาน IP Reflect โดยเมื่อมีการเรียกใช้งาน Web อุปกรณ์ต้องสามารถ Request ออกไปได้ด้วย IP Address ของผู้ใช้งาน

๑.๑๕. อุปกรณ์ที่เสนอต้องสามารถทำ SSL Proxy เพื่อตรวจสอบ Content และกำหนด Policy เพื่อดูแลการใช้งานโปรโตคอล HTTPS หรือ SSL Traffic ได้

๑.๑๖. อุปกรณ์ที่เสนอต้องรองรับการทำ Security Authentication กับ LDAP, RADIUS, NTLM, Kerberos, CA eTrust SiteMinder และ Local password files ได้เป็นอย่างน้อย

๑.๑๗. อุปกรณ์ที่เสนอต้องมีระบบ Authentication ที่สามารถกำหนดให้ผู้ใช้งาน Logon ได้เพียงครั้งละ ๑ เครื่องได้ เพื่อป้องกันปัญหาการ Share ชื่อล็อกอิน (User account)

๑.๑๘. อุปกรณ์ที่เสนอต้องมีระบบ Authentication ที่สนับสนุนการทำ Guest Account ได้

๑.๑๙. อุปกรณ์ที่เสนอต้องสามารถบริหารจัดการผ่านทาง Web-based และ Command Line Interface ได้

๑.๒๐. อุปกรณ์ที่เสนอต้องสนับสนุนการทำ Object-Caching, Byte-Caching, Compression, Bandwidth Management และ Protocol Optimization ได้

๑.๒๑. อุปกรณ์ที่เสนอต้องมีความสามารถในการแจ้งข่าวสาร (Notification) ผ่านทาง Web Interface ได้ และต้องสนับสนุน Splash page หรือ Exception Page ได้หลายหน้า web pages และต้องอนุญาตให้ผู้ดูแลระบบสามารถ Customize เพิ่มเติมได้ ตามเหตุการณ์ (Triggers)

๑.๒๒. อุปกรณ์ที่เสนอต้องได้รับการรับรองตามมาตรฐานความปลอดภัยจาก VCCI, BSMI, FCC, UL และ CSA เป็นอย่างน้อย

๑.๒๓. อุปกรณ์ที่เสนอสามารถติดตั้งบนตู้ Standard Rack ๑๙ นิ้วได้

๑.๒๔. อุปกรณ์ที่เสนอต้องมีคุณสมบัติในการออกรายงาน ดังนี้

๑.๒๔.๑. สามารถทำงานร่วมกับ LDAP และ AD เพื่อจัดการกับสิทธิ์การเข้าถึง หรือดู Report ที่สร้างขึ้นได้

๑.๒๔.๒. ต้องสามารถรองรับการออกรายงานย้อนหลังได้ไม่น้อยกว่า ๙๐ วัน

๑.๒๔.๓. สามารถจัดเก็บรายงานในรูปแบบของ PDF และ CSV

๑.๒๔.๔. ความสามารถในการออกรายงานแบบ Top Users, Top Domain / Web sites และ Top Categories ได้

๒. อุปกรณ์บริหารจัดการสื่อสารข้อมูลแบนด์วิชท์ (Bandwidth Management)

๒.๑. อุปกรณ์ที่เสนอต้องเป็นอุปกรณ์แบบ Appliance ที่ถูกออกแบบมาเพื่อ เพิ่มความเร็วการใช้งาน Web application มีระบบรักษาความปลอดภัย (security) ผู้ใช้ โดยสามารถกำหนดนโยบายตามผู้ใช้งาน (user level policy) ได้

๒.๒. อุปกรณ์ที่เสนอต้องมีขนาดของ Hard Disk ไม่น้อยกว่า ๓ TB และมีหน่วยความจำ RAM ไม่น้อยกว่า ๑๖ GB

๒.๓. อุปกรณ์ที่เสนอต้องมีพอร์ต ๑๐๐๐BaseT จำนวนไม่น้อยกว่า ๔ พอร์ต และในจำนวนนั้นต้องสามารถทำการ bypass ทราฟฟิคแบบอัตโนมัติได้ไม่น้อยกว่า ๒ พอร์ต

๒.๔. อุปกรณ์ที่เสนอสามารถขยายเพื่อรองรับพอร์ตแบบ ๑๐G ได้อีกไม่น้อยกว่า ๔ พอร์ต ในอนาคต

๒.๕. อุปกรณ์ที่เสนอสามารถรองรับ Internet Bandwidth เมื่อทำงานเป็น Forward Proxy ได้ไม่น้อยกว่า ๑๐๐ Mbps และรองรับการขยายเพิ่มเป็น ๕๐๐ Mbps ได้ในอนาคต โดยไม่ต้องเปลี่ยนอุปกรณ์หลัก

๒.๖. อุปกรณ์ที่เสนอสามารถรองรับจำนวนผู้ใช้งาน (Employee Count) ได้ไม่น้อยกว่า ๖,๐๐๐ users และรองรับการขยายเพิ่มเป็น ๒๕,๐๐๐ users ได้ในอนาคต โดยไม่ต้องเปลี่ยนอุปกรณ์หลัก

๒.๗. อุปกรณ์ที่เสนอสามารถทำหน้าที่เป็น Forward Proxy และ Reverse Proxy ในเวลาเดียวกันได้

๒.๘. อุปกรณ์ที่เสนอต้องสามารถรองรับโปรโตคอล HTTP,HTTPS, FTP, TCP-Tunnel, Socks และ RTSP ได้เป็นอย่างน้อย และสามารถขยายเพื่อรองรับโปรโตคอล RTMP และ RTMPE ได้ในอนาคต

๒.๙. อุปกรณ์ที่เสนอสามารถถูกติดตั้งในแบบ inline ได้ทั้งแบบ bridge mode และ route mode และรองรับ Link Aggregation Control Protocol (LACP) ได้

๒.๑๐. อุปกรณ์ที่เสนอต้องสามารถรองรับโปรโตคอล WCCP ได้ และต้องสามารถทำการ forward traffic และ return bypass traffic ได้ทั้งแบบ GRE และ Layer๒

๒.๑๑. อุปกรณ์ที่เสนอต้องสามารถทำงานร่วมกับ IPv๖ ได้โดยสามารถใช้ IPv๖ ในการทำ authentication, authorization, logging, reporting และ policy enforcement ได้เป็นอย่างน้อย

๒.๑๒. อุปกรณ์ที่เสนอต้องสามารถรองรับการทำ VDO Optimization โดยใช้เทคนิค VDO Stream Splitting กับ Windows Media, Real, QuickTime และ โปรโตคอล RTSP ได้เป็นอย่างน้อย และต้องสามารถทำ VDO Caching กับ VDO ชนิด VDO On demand ได้

๒.๑๓. อุปกรณ์ที่เสนอต้องสามารถทำ Bandwidth Management เพื่อทำการจัดสรร Bandwidth ตามผู้ใช้หรือกลุ่มของผู้ใช้ได้

๒.๑๔. อุปกรณ์ที่เสนอสามารถกำหนด policy จากการใช้งานข้อมูลผ่านอุปกรณ์ได้ทั้งแบบ ตามปริมาณข้อมูล (Volume Quota) และตามจำนวนเวลาที่เข้าใช้ (Time Quota)

๒.๑๕. อุปกรณ์ที่เสนอต้องสนับสนุน Notification Page และ Exception Page ได้ และต้องอนุญาตให้ผู้ดูแลระบบสามารถทำการปรับปรุงเปลี่ยนแปลงข้อความรวมทั้งรูปภาพ ตามเหตุการณ์ (Triggers) ที่เกิดขึ้นได้

๒.๑๖. อุปกรณ์ที่เสนอต้องสามารถทำ Authentication ร่วมกับ AD, LDAP, RADIUS, NTLM, Kerberos, CA eTrust Siteminder, Oracle COREid, Novell, SAML และ Local database ได้เป็นอย่างน้อย

๒.๑๗. อุปกรณ์ที่เสนอต้องสามารถทำ Authentication กับ Active Directory ได้มากกว่า ๑ domain

๒.๑๘. ระบบ Authentication ต้องสามารถกำหนดให้ผู้ใช้งาน log on ได้เพียงครั้งละ ๑ เครื่องได้ เพื่อป้องกันปัญหาการ share ชื่อล็อกอิน (user account) และสนับสนุนการทำ Guest Account ได้

๒.๑๙. อุปกรณ์สามารถใช้ลิขสิทธิ์การทำ URL/Web ตามคุณสมบัติดังต่อไปนี้ได้เป็นอย่างน้อย

๒.๑๙.๑. มีลิขสิทธิ์ในการทำ URL/Web filtering ให้กับผู้ใช้ได้ไม่น้อยกว่า ๒๐๐ licenses

๒.๑๙.๒. มีฐานข้อมูลของเว็บไซต์จัดเป็นประเภท (Category) ไม่น้อยกว่า ๘๐ ประเภท

๒.๑๙.๓. สามารถทำการตรวจวิเคราะห์เว็บไซต์ที่ไม่มีในฐานข้อมูลได้แบบ Real Time โดยใช้เทคนิค Cloud Computing หรือ Cloud service ทำให้สามารถจัดประเภทของเว็บไซต์และตรวจสอบ Web link หรือ Content ที่ไม่ปลอดภัยได้โดยอัตโนมัติ

๒.๑๙.๔. สามารถควบคุมพฤติกรรมการใช้งานเว็บไซต์ เช่น post message, send email, upload picture , upload video , upload attachment และ download attachment ได้เป็นอย่างน้อย

๒.๑๙.๕. สามารถระบุ Category ของเว็บไซต์ ๑ เว็บ ได้ไม่น้อยกว่า ๔ Categories เพื่อความยืดหยุ่น

๒.๑๙.๖ สามารถกำหนด policy ตามระดับความเสี่ยง (Threat Risk Level) และตามประเทศที่ตั้ง (Geolocation) ของเว็บไซต์ได้

๒.๒๐. อุปกรณ์ที่เสนอรองรับการแยกประเภทของ VDO บน YouTube ได้ (YouTube Categorization)

๒.๒๑. อุปกรณ์ที่เสนอรองรับการรับความรู้ หรือ policy หรือ script จาก Cloud เพื่อทำให้สามารถ cache Web ๒.๐ หรือ Dynamic Web ได้

๒.๒๒. มีซอฟต์แวร์สำหรับไคลเอนต์ (client software) เพื่อทำ URL filtering สำหรับรองรับผู้ใช้ที่ทำงานอยู่นอกสถานที่

๒.๒๒.๑. สามารถติดตั้งบนเครื่องคอมพิวเตอร์ ที่ใช้ระบบปฏิบัติการ (Operating System) แบบWindows ได้

๒.๒๒.๒. สามารถทำ URL filtering โดยเลือกเป็นประเภทของ Web site ได้ไม่น้อยกว่า ๘๐ ประเภท (๘๐ categories) ได้

๒.๒๒.๓. สามารถกำหนด policy จากศูนย์กลางได้

๒.๒๓. อุปกรณ์ต้องผ่านการรับรองดังต่อไปนี้ IEC, UL, CSA และ EN เป็นอย่างน้อย

๒.๒๔. อุปกรณ์ที่เสนอต้องมีระบบการบริหารการจัดการแบบ Web-based management ทั้ง HTTP และ HTTPS ได้บนตัวอุปกรณ์เอง โดยไม่ต้องติดตั้ง software management แยก

๒.๒๕. อุปกรณ์ที่เสนอต้องได้รับการยอมรับให้เป็นผู้นำ (in Leader quadrant) ทางด้านอุปกรณ์รักษาความปลอดภัยเว็บ (Secure Web Gateway) จาก Gartner ในปีล่าสุด

๓. อุปกรณ์รักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์ในระดับแอพพลิเคชั่น (Application Firewall) แบบที่ ๑ โดยมีคุณสมบัติอย่างน้อยดังต่อไปนี้

๓.๑. เป็นอุปกรณ์ Appliance-Based Firewall ที่สร้างขึ้นเพื่อทำหน้าที่ตรวจจับและควบคุม Application, User, Content โดยเฉพาะ (Application Firewall) และใช้โครงสร้างสถาปัตยกรรมแบบ Single Pass Software

๓.๒. มี Network Interface แบบ ๑๐/๑๐๐/๑๐๐๐ ไม่น้อยกว่า ๘ พอร์ท และมี Interface สำหรับบริหารจัดการโดยเฉพาะ (Out of Band Management) แบบ ๑๐/๑๐๐/๑๐๐๐ ไม่น้อยกว่า ๑ พอร์ท

๓.๓. รองรับ Application Firewall Throughput ได้ไม่น้อยกว่า ๒๕๐ Mbps และจำนวนเซสชันสูงสุด (Max Sessions) ได้ไม่น้อยกว่า ๖๔,๐๐๐ sessions และ (New Sessions) ไม่น้อยกว่า ๗,๕๐๐ Sessions ต่อวินาที

๓.๔. รองรับการทำ Virtual Routers ได้ไม่น้อยกว่า ๓ Virtual Routers และ Security Zones ไม่น้อยกว่า ๒๐ Zones

๓.๕. สามารถติดตั้งในรูปแบบ Transparent Inline, Non-Inline Monitoring, L๒ และ L๓ ได้ หรือเทียบเท่า รวมทั้งสามารถติดตั้งทั้ง ๔ รูปแบบดังกล่าวได้พร้อมกัน

๓.๖. รองรับมาตรฐาน ๘๐๒.๑Q VLAN tags ได้ไม่น้อยกว่า ๔,๐๐๐ VLANs

๓.๗. สามารถทำ Routing แบบ Static, RIP, BGP, OSPF, Multicast และ Policy Based Forwarding ได้เป็นอย่างน้อย

๓.๘. สามารถทำ NAT/PAT, DHCP Servers และ DHCP Relay ได้

๓.๙. สามารถกำหนดนโยบายรักษาความปลอดภัยเพื่อควบคุมการเข้าถึงระบบเครือข่ายจาก Application, User และ Content ได้

๓.๑๐. สามารถทำการตรวจสอบทราฟฟิคที่เข้ารหัส ด้วยการทำ SSL (ทั้ง Inbound และ Outbound) และ SSH Decryption ได้

๓.๑๑. สามารถทำงานร่วมกับระบบการพิสูจน์ตัวตน (Authentication Systems) ได้แก่ Active Directory, LDAP, และ Microsoft Terminal Services เพื่อทำการติดตามผู้ใช้ได้เป็นอย่างน้อย

๓.๑๒. สามารถควบคุมประเภทของไฟล์ที่อนุญาตให้ดาวน์โหลดและอัพโหลดบนแต่ละ Application

๓.๑๓. สามารถปรับแต่ง Response Page แจ้งไปยังผู้ใช้งาน กรณีที่มีการบล็อกทราฟฟิคเกิดขึ้น รวมไปถึงหน้าลงทะเบียนเข้าใช้ระบบเครือข่ายของ Captive Portal และ SSL VPN ได้

๓.๑๔. อุปกรณ์ที่นำเสนอต้องสามารถทำ IPsec VPN (Site to Site) โดยมี IPSec VPN Throughput ได้ไม่น้อยกว่า ๕๐ Mbps

๓.๑๕. อุปกรณ์ที่นำเสนอต้องสามารถทำ Client VPN (Remote Access) บนโปรโตคอล IPSec และ SSL ได้ โดยรองรับจำนวนผู้ใช้ได้ไม่น้อยกว่า ๑๐๐ ผู้ใช้ รวมทั้งสามารถทำงานกับระบบปฏิบัติการ Windows (ทั้ง ๓๒ และ ๖๔ bits), Mac OS X, Android และ Apple iOS ได้เป็นอย่างน้อย

๓.๑๖. มีระบบป้องกันภัยคุกคาม (Threat Prevention) โดยมี IPS และ Antivirus Throughput ไม่น้อยกว่า ๑๐๐ Mbps และมีคุณสมบัติอย่างน้อยดังต่อไปนี้

๓.๑๖.๑. สามารถตรวจจับและป้องกัน Vulnerability Exploits, Buffer Overflow, DoS/ DDoS, Port scans, Host sweeps, Malformed Packets, IP defragmentation และ TCP reassembly ได้เป็นอย่างน้อย รวมทั้งสามารถปรับแต่งรูปแบบของภัยคุกคาม (Custom signatures) ได้ตามความต้องการ

๓.๑๖.๒. สามารถป้องกัน Malware ประเภทต่างๆ แบบ Stream-Based ได้แก่ Virus, Spyware download, Spyware phone home, Trojan และ Botnet ได้เป็นอย่างน้อย

๓.๑๖.๓. สามารถตรวจจับและป้องกัน Virus บนโปรโตคอล HTTP, FTP, IMAP, POP๓, SMTP, SMB รวมถึง Virus ที่ฝังตัวมากับ PDF, HTML, Javascript และ Compressed Files ได้

๓.๑๖.๔. มีระบบตรวจจับพฤติกรรมที่ไม่ประสงค์ดีแบบ Cloud-Based เพื่อใช้ระบุ Malware ประเภทใหม่ซึ่งไม่มีในฐานข้อมูลการบุกรุกโจมตีได้ รวมถึงสามารถสร้างรูปแบบการโจมตี (Signature) ดังกล่าวขึ้นมาเพื่อใช้ป้องกันระบบเครือข่ายได้โดยอัตโนมัติ

๓.๑๗. มีระบบจัดการคุณภาพการให้บริการ (Quality of Service) โดยสามารถกำหนดนโยบายเพื่อจัดการแบนวิธด์ของทราฟฟิคตาม Application, User, Source, Destination, Interface และ IPSec VPN Tunnel ได้เป็นอย่างน้อย โดยระบุการการันตี, ขอบเขตสูงสุด และลำดับความสำคัญ (Priority) ของ ทราฟฟิคได้

๓.๑๘. สามารถเรียกดูสรุปข้อมูลของ Applications และ Data ในรูปแบบของกราฟฟิคได้

๓.๑๙. สามารถทำรายงาน รวมถึงปรับแต่งรายงานตามความต้องการ ในรูปแบบ CSV และ PDF ได้เป็นอย่างน้อย พร้อมทั้งตั้งเวลาส่งรายงานผ่านทาง Email แบบอัตโนมัติได้

๓.๒๐. สามารถจัดเก็บบันทึกข้อมูลโดยส่ง Syslog และ SNMP ไปยังระบบจัดการเครือข่ายที่รองรับคุณสมบัติดังกล่าวได้

๓.๒๑. สามารถบริหารจัดการผ่านทาง Web User Interface และ Command Line Interface ได้

๓.๒๒. รองรับการติดตั้งเพื่อทำ High Availability แบบ Active-Active และ Active-Passive ได้

๓.๒๓. ผลิตภัณฑ์ที่นำเสนอนั้นต้องอยู่ใน Leader Gartner Magic Quadrant ของ Enterprise

๔. อุปกรณ์รักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์ในระดับแอพพลิเคชั่น (Application Firewall) แบบที่ ๒ โดยมีคุณสมบัติอย่างน้อยดังต่อไปนี้

๔.๑. เป็นอุปกรณ์ Appliance-Based Firewall ที่สร้างขึ้นเพื่อทำหน้าที่ตรวจจับและควบคุม Application, User, Content โดยเฉพาะ (Application Firewall) และใช้โครงสร้างสถาปัตยกรรมแบบ Single Pass Software

๔.๒. มี Network Interface แบบ ๑๐/๑๐๐/๑๐๐๐ ไม่น้อยกว่า ๑๒ พอร์ท และรองรับ Gigabit SFP ไม่น้อยกว่า ๘ พอร์ท รวมไปถึงมี Interface แบบ ๑๐/๑๐๐/๑๐๐๐ สำหรับบริหารจัดการโดยเฉพาะ (Out of Band Management) และมี Interface แบบ ๑๐/๑๐๐/๑๐๐๐ ที่รองรับการทำงานแบบ High availability โดยเฉพาะอย่างน้อย ๒ พอร์ท

๔.๓. รองรับ Application Firewall Throughput ได้ไม่น้อยกว่า ๒ Gbps และจำนวนเซสชันสูงสุด (Max Sessions) ได้ไม่น้อยกว่า ๒๕๐,๐๐๐ sessions และ (New Sessions) ไม่น้อยกว่า ๕๐,๐๐๐ Sessions ต่อวินาที

๔.๔. รองรับการทำ Virtual Routers ได้ไม่น้อยกว่า ๑๐ Virtual Routers และ Security Zones ไม่น้อยกว่า ๔๐ Zones

๔.๕. รองรับการทำ Virtual Systems และรองรับการขยายได้สูงสุดถึง ๖ Systems ในอนาคต

๔.๖. สามารถติดตั้งในรูปแบบ Transparent Inline, Non-Inline Monitoring, L๒ และ L๓ ได้ หรือเทียบเท่า รวมทั้งสามารถติดตั้งทั้ง ๔ รูปแบบดังกล่าวได้พร้อมกัน

๔.๗. รองรับมาตรฐาน ๘๐๒.๑Q VLAN tags ได้ไม่น้อยกว่า ๔,๐๐๐ VLANs

๔.๘. สามารถทำ Routing แบบ Static, RIP, BGP, OSPF, Multicast และ Policy Based Forwardingได้เป็นอย่างน้อย

๔.๙. สามารถทำ NAT/PAT, DHCP Servers และ DHCP Relay ได้

๔.๑๐. สามารถกำหนดนโยบายรักษาความปลอดภัยเพื่อควบคุมการเข้าถึงระบบเครือข่ายจาก Application, User และ Content ได้

๔.๑๑. สามารถทำการตรวจสอบทราฟฟิคที่เข้ารหัส ด้วยการทำ SSL (ทั้ง Inbound และ Outbound) และ SSH Decryption ได้

๔.๑๒. สามารถทำงานร่วมกับระบบการพิสูจน์ตัวตน (Authentication Systems) ได้แก่ Active Directory, LDAP และ RADIUS เพื่อทำการติดตามผู้ใช้ได้เป็นอย่างน้อย

๔.๑๓. สามารถควบคุมประเภทของไฟล์ที่อนุญาตให้ดาวน์โหลดและอัพโหลดบนแต่ละ Application ได้ รวมทั้งสามารถป้องกันการรั่วไหลของข้อมูล (Data Filtering) ออกจากระบบเครือข่าย เช่น หมายเลขบัตรเครดิต ได้ตามความต้องการ

๔.๑๔. สามารถปรับแต่ง Response Page แจ้งไปยังผู้ใช้งาน กรณีที่มีการบล็อกทราฟฟิคเกิดขึ้น รวมไปถึงหน้าลงทะเบียนเข้าใช้ระบบครือข่ายของ Captive Portal และ SSL VPN ได้

๔.๑๕. มีระบบป้องกันภัยคุกคาม (Threat Prevention) โดยมี Throughput ไม่น้อยกว่า ๑ Gbps และมีคุณสมบัติอย่างน้อยดังต่อไปนี้

๔.๑๕.๑. สามารถตรวจจับและป้องกัน Vulnerability Exploits, Buffer Overflow, DoS/ DDoS, Port scans, Host sweeps, Malformed Packets, IP defragmentation และ TCP reassembly ได้เป็นอย่างน้อย รวมทั้งสามารถปรับแต่งรูปแบบของภัยคุกคาม (Custom signatures) ได้ตามความต้องการ

๔.๑๕.๒. สามารถป้องกัน Malware ประเภทต่างๆ แบบ Stream-Based ได้แก่ Virus, Spyware download, Spyware phone home, Trojan และ Botnet ได้เป็นอย่างน้อย

๔.๑๕.๓. สามารถตรวจจับและป้องกัน Virus บนโปรโตคอล HTTP, FTP, IMAP, POP๓, SMTP และ SMB รวมถึง Virus ที่ฝังตัวมากับ PDF, HTML, Javas cript และ Compressed Files ได้

๔.๑๕.๔. มีระบบตรวจจับพฤติกรรมที่ไม่ประสงค์ดีแบบ Cloud-Based เพื่อใช้ระบุ Malware ประเภทใหม่ซึ่งไม่มีในฐานข้อมูลการบุกรุกโจมตีได้ รวมถึงสามารถสร้างรูปแบบการโจมตี (Signature) ดังกล่าวขึ้นมาเพื่อใช้ป้องกันระบบเครือข่ายได้โดยอัตโนมัติ

๔.๑๖. อุปกรณ์ที่นำเสนอต้องสามารถทำ IPsec VPN (Site to Site) โดยมี IPSec VPN Throughput ได้ไม่น้อยกว่า ๕๐๐ M

๔.๑๗. อุปกรณ์ที่นำเสนอต้องสามารถทำ Client VPN (Remote Access) บนโปรโตคอล IPSec และ SSL ได้ โดยรองรับจำนวนผู้ใช้ได้ไม่น้อยกว่า ๑,๐๐๐ ผู้ใช้ รวมทั้งสามารถทำงานกับระบบปฏิบัติการ Windows (ทั้ง ๓๒ และ ๖๔ bits), Mac OS X, Android และ Apple iOS ได้เป็นอย่างน้อย

๔.๑๘. มีระบบจัดการคุณภาพการให้บริการ (Quality of Service) โดยสามารถกำหนดนโยบายเพื่อจัดการแบนวิธด์ของทราฟฟิคตาม Application, User, Source, Destination, Interface และ IPSec VPN Tunnel ได้เป็นอย่างน้อย โดยระบุการการันตี, ขอบเขตสูงสุด และลำดับความสำคัญ (Priority) ของทราฟฟิคได้

๔.๑๙. สามารถเรียกดูสรุปข้อมูลของ Applications, Threats และ Data ในรูปแบบของกราฟฟิคได้

๔.๒๐. สามารถทำรายงาน รวมถึงปรับแต่งรายงานตามความต้องการ ในรูปแบบ CSV และ PDF ได้เป็นอย่างน้อย พร้อมทั้งตั้งเวลาส่งรายงานผ่านทาง Email แบบอัตโนมัติได้

๔.๒๑. สามารถจัดเก็บบันทึกข้อมูลโดยส่ง Syslog และ SNMP ไปยังระบบจัดการเครือข่ายที่รองรับคุณสมบัติดังกล่าวได้

๔.๒๒. สามารถบริหารจัดการผ่านทาง Web User Interface และ Command Line Interface ได้

๔.๒๓. รองรับการติดตั้งเพื่อทำ High Availability แบบ Active-Active และ Active-Passive ได้

๕. อุปกรณ์รักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์ในระดับแอพพลิเคชั่น (Application Firewall) แบบที่ ๓ โดยมีคุณสมบัติอย่างน้อยดังต่อไปนี้

๕.๑. เป็นอุปกรณ์ Appliance-Based Firewall ที่สร้างขึ้นเพื่อทำหน้าที่ตรวจจับและควบคุม Application, User, Content โดยเฉพาะ (Application Firewall) โดยใช้โครงสร้างสถาปัตยกรรมแบบ Single Pass Architecture

๕.๒. เป็นอุปกรณ์ที่มีการทำงานของ Control Plane และ Data Plane ที่แยกออกจากกันอย่างชัดเจน โดยสามารถติดตั้งในตู้เก็บ อุปกรณ์ขนาดมาตรฐาน ๑๙ นิ้วได้

๕.๓. มี Network Interface แบบ ๑๐/๑๐๐/๑๐๐๐ ไม่น้อยกว่า ๔ พอร์ต และช่องเชื่อมต่อแบบ Gigabit SFP ไม่น้อยกว่า ๘ พอร์ต รวมทั้งมี Interface แบบ ๑๐/๑๐๐/๑๐๐๐ เพื่อใช้สำหรับบริหารจัดการโดยเฉพาะ (Out of Band Management) ไม่น้อยกว่า ๑ พอร์ต โดยแยกออกจาก Network Interface ปกติ

๕.๔. มี Interface สำหรับการทำ high availability โดยเฉพาะแบบ ๑๐/๑๐๐/๑๐๐๐ ไม่น้อยกว่า ๒ พอร์ต และ พอร์ต RJ๔๕ ๑ พอร์ตสำหรับการ console

๕.๕. มี Application Firewall หรือ Next Generation Firewall Throughput ได้ไม่น้อยกว่า ๑ Gbps จำนวนเซสชัน สูงสุด (Max Sessions) ได้ไม่น้อยกว่า ๑๒๘,๐๐๐ sessions และรองรับการสร้างเซสชันใหม่ได้ไม่น้อยกว่า ๘,๓๐๐ sessions ต่อวินาที

๕.๖. มี Disk drive แบบ SSD สำหรับการเก็บ log ขนาดไม่ต่ำกว่า ๒๔๐GB

๕.๗. สามารถติดตั้งในรูปแบบ Transparent Inline, Non-Inline Monitoring (Tap), L๒ และ L๓ ได้หรือเทียบเท่า รวมทั้งสามารถติดตั้งทั้ง ๔ รูปแบบดังกล่าวได้พร้อมกัน โดยไม่ต้องแบ่ง Virtual system หรือ Virtual domain

๕.๘. รับ Syslog จากระบบอื่นเพื่อใช้ในการยืนยันตัวตน ของ User ภายในองค์กร โดยรองรับทั้ง User Log-in และ User Log-out

๕.๙. สามารถทำการตรวจสอบทราฟฟิคที่เข้ารหัส SSL ด้วยการทำ SSL decryption (ทั้งแบบ Inbound และ Outbound) รวมทั้งการทำ SSH Decryption ได้

๕.๑๐. สามารถทำงานร่วมกับระบบการพิสูจน์ตัวตน (Authentication Systems) ได้แก่ Active Directory, LDAP เพื่อทำการติดตามผู้ใช้ได้เป็นอย่างน้อย

๕.๑๑. สามารถกำหนด Policy แบบ Multi-Factor Authentication โดยการทำงานร่วมกับระบบพิสูจน์ตัวตน เช่น RADIUS, DUO และ OKTA ได้ รวมทั้งสามารถทำ SAML single sign-on (SSO) เพื่อทำการเข้าสู่ services และ applications ต่างๆผ่านการ logon ในครั้งเดียวได้

๕.๑๒. มีความสามารถในการป้องกันการรั่วไหลของชื่อผู้ใช้และรหัสผ่านขององค์กร (Credential Prevention) ผ่านการใช้งาน web site

๕.๑๓. สามารถควบคุมประเภทของไฟล์ที่อนุญาตให้ดาวน์โหลดและอัพโหลดบนแต่ละ Applications ได้ รวมทั้งสามารถป้องกันการ รั่วไหลของข้อมูล (Data Filtering) ออกจากระบบเครือข่าย เช่น หมายเลขบัตรเครดิต และสามารถสร้างรูปแบบได้ตามความ ต้องการ

๕.๑๔. มีระบบป้องกันภัยคุกคาม (Threat Prevention) โดยเมื่อเปิดการใช้งาน IPS, Antispyware และ Antivirus พร้อมกัน จะต้องรองรับ Throughput ไม่น้อยกว่า ๖๒๐ Mbps และมีคุณสมบัติอย่างน้อยดังต่อไปนี้

๕.๑๔.๑. สามารถป้องกัน Malware ประเภทต่างๆ แบบ Stream-Based ได้แก่ Virus, Spyware download, Spyware phone home, Trojan และ Botnet ได้เป็นอย่างน้อย

๕.๑๔.๒. สามารถตรวจจับและป้องกัน Vulnerability Exploits, Buffer Overflow, DoS/DDoS, Non-RFC compliant protocol, Port scans, Host sweeps, Malformed Packets, IP defragmentation และ TCP reassembly ได้เป็นอย่างน้อย รวมทั้งสามารถปรับแต่งรูปแบบของภัยคุกคาม (Custom signatures) ได้ตามความต้องการ

๕.๑๔.๓. สามารถตรวจจับและป้องกัน Virus บนโปรโตคอล HTTP, FTP, IMAP, POP๓, SMTP, SMB และ SSL รวมถึง Virus ที่ฝังตัวมากับ PDF, HTML, JavaScript และ Compressed Files ได้

๕.๑๔.๔. สามารถทำ DNS Sinkhole เพื่อป้องกันการเข้าถึง malicious domain และเฝ้าระวังผู้ใช้ที่มีการเรียกใช้งานไปยัง malicious domain

๕.๑๕. มีระบบตรวจจับ Advanced Malware แบบ Cloud-Based และใช้เทคโนโลยีแบบ Sandbox เพื่อใช้ระบุ Malware ประเภทใหม่ (Zero-day Malware) ซึ่งไม่มีในฐานข้อมูลการบุกรุกโจมตีได้ รวมถึงสามารถสร้างรูปแบบการโจมตี (Signature) ดังกล่าวขึ้นมาเพื่อใช้ป้องกันระบบเครือข่ายได้โดยอัตโนมัติ โดยมีคุณสมบัติอย่างน้อยดังนี้

๕.๑๕.๑. สามารถทำ Static Analysis, Dynamic Analysis, Machine Learning และ Bare metal Analysis ได้

๕.๑๕.๒. สามารถตรวจจับได้ทุก applications เช่น FTP, email (SMTP, IMAP, POP), web traffic และ encrypted (SSL) content

๕.๑๕.๓. สามารถตรวจสอบและป้องกัน zero-day malware จากไฟล์ชนิดต่างๆอย่างน้อยดังนี้ PDF, Java Applet (jar and class), PE file, Microsoft Office (.doc/.docx, .xls/.xlsx, .ppt/.pptx), Flash, HTTP/HTTPS Links contained in email, MacOS binaries (mach-O, DMG, PKG) และ APK ไฟล์

๕.๑๕.๔. มี report แสดงรายละเอียดการทำงานของ malware ที่ตรวจจับได้

๕.๑๕.๕. สามารถสร้าง signature ขึ้นมาเพื่อป้องกันได้หลังจากตรวจพบ malware

๕.๑๖. สามารถทำ NAT ในรูปแบบการวางแบบ Transparent Inline ได้

๕.๑๗. สามารถกำหนดนโยบายการเข้าถึง website (URL Filtering) สามารถติดตามและควบคุมการเข้าถึงเว็บได้ตาม Category และกำหนด Black list, White list รวมทั้งสามารถปรับแต่ง Custom Category ได้ตามต้องการ

๕.๑๘. อุปกรณ์ที่นำเสนอต้องสามารถทำ IPsec VPN (Site to Site) โดยมี IPSec VPN Throughput ได้ไม่น้อยกว่า ๔๐๐ Mbps

๕.๑๙. อุปกรณ์ที่นำเสนอต้องสามารถทำ Client VPN (Remote Access) บนโปรโตคอล IPSec และ SSL ได้ โดยรองรับจำนวนผู้ใช้ได้ ไม่น้อยกว่า ๑,๐๐๐ ผู้ใช้ รวมทั้งสามารถทำงานกับระบบปฏิบัติการ Windows (ทั้ง ๓๒ และ ๖๔ bits) และ Mac OS X ได้เป็น อย่างน้อย

๕.๒๐. สามารถทำการคัดกรอง log (log filtering) และส่ง log ผ่าน HTTP-based API ไปยังอุปกรณ์ ๓rd party ได้

๕.๒๑. สามารถเรียกดูสรุปข้อมูลของ Applications, URL Categories, Threats และ Data ในรูปแบบของกราฟฟิคได้

๕.๒๒. สามารถสร้างรายงาน (Report) ต่างๆอย่างน้อยดังต่อไปนี้ได้

๕.๒๒.๑. User Activity Report แสดงการใช้งานของ User แต่ละคน

๕.๒๒.๒. Top Application, Application Category และ HTTP Application

๕.๒๒.๓. Top Source, User, Destination และ Connection

๕.๒๒.๔. Top Threat, Vulnerabilities, Viruss, Spywares, Attackers และ Victims

๕.๒๒.๕. Botnet Report แสดงเครื่องที่มีพฤติกรรมติด Botnet

๕.๒๒.๖. Top URL categories

๕.๒๓. โดยสามารถ ปรับแต่งรายงานตามความต้องการ (Custom Report) และส่งออก (Export) ให้อยู่ในรูปแบบ CSV, PDF และ XML ได้เป็นอย่างน้อย พร้อมทั้งตั้งเวลา ส่งรายงานผ่านทาง Email แบบอัตโนมัติได้

๕.๒๔. สามารถจัดเก็บบันทึกข้อมูลโดยส่ง Syslog, SNMP และ NetFlow ไปยังระบบจัดการเครือข่ายที่รองรับคุณสมบัติดังกล่าวได้

๕.๒๕. ในกรณีที่มีอุปกรณ์ ๒ units สามารถรองรับการติดตั้งเพื่อทำ High Availability (HA) แบบ Active/Passive และ Active/Active ได้

๕.๒๖. ผลิตภัณฑ์ที่นำเสนอจะต้องอยู่ใน Leader Quadrant ของ Gartner Magic Quadrant ด้าน Enterprise Network Firewalls ปีล่าสุด อย่างน้อย ๔ ปี

๕.๒๗. ต้องรับประกันอุปกรณ์เป็นเวลาอย่างน้อย ๑ ปี

๕.๒๘. ผู้เสนอราคาต้องแสดงหลักฐานการมีสิทธิ์เสนอราคาสำหรับโครงการนี้ โดยต้องได้รับการแต่งตั้งเป็นตัวแทนจำหน่ายจาก บริษัทเจ้าของผลิตภัณฑ์

๖. อุปกรณ์กระจายการทำงานสำหรับเครือข่าย (Link Load Balancer) โดยมีคุณสมบัติอย่างน้อย ดังนี้

๖.๑. เป็นอุปกรณ์ (Hardware Appliance) ที่ออกแบบมาเพื่อใช้กระจายการทำงานสำหรับเครือข่ายโดยเฉพาะ

๖.๒. มี Router Throughput สูงสุดไม่น้อยกว่า ๑ Gbps

๖.๓. มีช่องเชื่อมต่อระบบเครือข่าย Ethernet WAN Ports แบบ ๑๐/๑๐๐/๑๐๐๐ Base-T หรือดีกว่า จำนวนไม่น้อยกว่า ๓ ช่องและมีช่องเชื่อมต่อระบบเครือข่าย LAN Port แบบ ๑๐/๑๐๐/๑๐๐๐ Base-T หรือดีกว่าจำนวนไม่น้อยกว่า ๓ ช่อง

๖.๔. สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS ได้เป็นอย่างน้อย

๖.๕. สามารถใช้งานตามมาตรฐาน IPv๖ ได้ และรองรับการเข้าใช้งานเครือข่ายได้ถึง ๕๐๐ user

๗. อุปกรณ์กระจายสัญญาณชนิดไร้สาย (Access point) ที่มีความปลอดภัยและระบบบริหารจัดการจากส่วนกลาง (Instant Access Point) โดยมีคุณสมบัติอย่างน้อยดังต่อไปนี้

๗.๑. อุปกรณ์ทำหน้าที่กระจายสัญญาณเครือข่ายไร้สาย (Wireless Access Point) เพื่อให้บริการสัญญาณ Wi-Fi ที่มีประสิทธิภาพสูงในระดับ Gigabit Wi-Fi ตามมาตรฐาน IEEE ๘๐๒.๑๑ac ได้เป็นอย่างน้อย

๗.๒. สามารถทำงานในแบบ Dual Radio คือกระจายสัญญาณทั้งย่านความถี่ ๒.๔GHz และ ๕GHz ได้พร้อมๆกัน ในระดับ ๒๐/๔๐ high-throughput (HT) และ ๒๐/๔๐/๘๐ very high throughput (VHT) ได้เป็นอย่างน้อย

๗.๓. รองรับการทำงานทั้งในรูปแบบ Instant Access Point (หรือ Standalone) และแบบ Virtual Controller เพื่อสามารถกระจายค่า Configuration ไปยัง Instant Access Point ตัวอื่นๆ ในระบบเครือข่ายไร้สายนั้นได้โดยอัตโนมัติ และในกรณี Virtual Controller ไม่สามารถทำงานได้ อุปกรณ์ Instant Access Point ตัวอื่นในระบบจะเปลี่ยนมาทำหน้าที่เป็น Virtual Controller แทนตัวเดิมที่เกิดปัญหาไปได้แบบอัตโนมัติ

๗.๔. สามารถเลือกที่จะตั้งค่าให้ทำงานในโหมดใดโหมดหนึ่งระหว่าง Controller-managed mode (ทำงานร่วมกับคอนโทรลเลอร์) และ Instant mode (ทำงานแบบ Standalone) ได้

๗.๕. มีพอร์ท Network Interface ชนิด ๑๐/๑๐๐/๑๐๐๐Based-T จำนวนไม่น้อยกว่า ๒ พอร์ท โดยรองรับมาตรฐาน ๘๐๒.๓a z Energy Efficient Ethernet (EEE) และรองรับการเพิ่ม Throughput ให้ได้มากถึง ๑.๙ Gbps ด้วยการทำพอร์ท Ether Channel link aggregation ได้เป็นอย่างน้อย

๗.๖. รองรับการส่งเฟรมข้อมูลขนาดใหญ่ (Jumbo frame) ในการเชื่อมต่อแบบ Uplink ได้เป็นอย่างน้อย

๗.๗. มีเสาอากาศแบบติดตั้งภายในชนิด Down-tilt Omni-directional ๓x๓ MIMO ที่มีกำลังขยาย (Gain) ๓.๕dBi สำหรับคลื่นความถี่ ๒.๔GHz และ ๔.๕dBi สำหรับคลื่นความถี่ ๕GHz เป็นอย่างน้อย โดยมีอัตราการส่งข้อมูลสูงสุด (Max Data Rate) ไม่น้อยกว่า ๑.๓ Gbps บนย่านความถี่ ๕GHz

๗.๘. สามารถบริหารจัดการ Radio Channel และ Transmit Power ได้โดยอัตโนมัติตามความเหมาะสมของสภาวะแวดล้อม

๗.๙. รองรับการทำงานใน Radio mode ต่างๆ ได้ ดังนี้

๗.๙.๑. Access mode: สำหรับกระจายสัญญาณให้บริการ Client

๗.๙.๒. Monitor mode: จะทำตัวเป็น Air Monitor สำหรับตรวจสอบหา Rogue AP และ Client ในทุกๆ ช่องสัญญาณ

๗.๙.๓. Spectrum Monitor mode: สำหรับตรวจสอบแบบ Full-spectrum RF โดยทำการตรวจสอบระบุที่มาของสัญญาณรบกวน (Interference) ในทุกๆ ช่องสัญญาณที่อาจเกิดจาก Access Point บริเวณข้างเคียง หรือสัญญาณรบกวนที่เกิดจากอุปกรณ์ประเภท non Wi-Fi devices เช่น Microwave และ Cordless phone เป็นต้น

๗.๑๐. รองรับการทำงานแบบ Hybrid AP เพื่อทำงานในโหมด Access Point กระจายสัญญาณ และทำงานในโหมด Air-Monitor (เพื่อทำงานเป็น Wireless intrusion protection) ได้พร้อมกัน และยังสามารถเลือกให้ทำงานในโหมดใดโหมดหนึ่งได้ ในกรณีทำงานร่วมกับคอนโทรลเลอร์ (Controller-managed AP)

๗.๑๑. รองรับการทำงานแบบ Remote AP (RAP) ในกรณีทำงานร่วมกับคอนโทรลเลอร์ (Controller-managed AP) โดยการเชื่อมต่อความปลอดภัย VPN tunnel จากอุปกรณ์ Access Point ไปยังคอนโทรลเลอร์โดยอัตโนมัติเพื่อทำงานในลักษณะศูนย์กลางในการกระจายค่า Configuration, Data encryption, Policy enforcement และ Network services ได้เป็นอย่างน้อย

๗.๑๒. รองรับการทำ RF Security/Spectrum scan ในทุกๆช่องสัญญาณ หรือ Off-Channel Scanning ในกรณีทำงานร่วมกับคอนโทรลเลอร์ในอนาคต

๗.๑๓. อุปกรณ์ทำงานบนมาตรฐานเทคโนโลยีการมอดูเลตดังต่อไปนี้

๗.๑๓.๑. ๘๐๒.๑๑b: Direct-Sequence Spread-Spectrum (DSSS)

๗.๑๓.๒. .๑๑a/g/n/ac: Orthogonal Frequency Division Multiplexing (OFDM)

๗.๑๓.๓. ๘๐๒.๑๑n/ac: ๓x๓ MIMO with ๓ Spatial streams

๗.๑๔. อุปกรณ์รองรับประเภทการ Modulation type ได้ดังนี้

๗.๑๔.๑. ๘๐๒.๑๑b: BPSK, QPSK, CCK

๗.๑๔.๒. ๘๐๒.๑๑a/g/n/ac: BPSK, QPSK, ๑๖-QAM, ๖๔-QAM, ๒๕๖-QAM

๗.๑๕. รองรับการทำงานตามคุณสมบัติของ Advanced cellular coexistence (ACC) เพื่อลดทอนสัญญาณรบกวนจากระบบเซลลูลาร์ เช่น ๓G / ๔G LTE, Femtocell ได้เป็นอย่างน้อย

๗.๑๖. สามารถให้บริการ Guest เข้าใช้งานผ่าน Captive Portal authentication บนตัวอุปกรณ์ และต้องสามารถเก็บ User name และ Password บน Internal Database ของอุปกรณ์ได้

๗.๑๗. มีคุณสมบัติ OS Fingerprinting และ DHCP Fingerprinting เพื่อระบุประเภท Operating Systems ของอุปกรณ์ที่มีการเชื่อมต่อกับระบบเครือข่ายไร้สาย เช่น iPhone, iPAD, OS-X, Android, Blackberry, Linux ได้เป็นอย่างน้อย

๗.๑๘. มีคุณสมบัติในการกำหนดนโยบายการเข้าถึงตามสิทธิของแต่ละบุคคลแบบ Role-based Access Control ได้เป็นอย่างน้อย

๗.๑๙. รองรับการเข้ารหัสความปลอดภัยแบบ WEP, TKIP และ AES รวมถึงต้องรองรับการพิสูจน์ตัวตนแบบ ๘๐๒.๑x, WPA, WPA๒, MAC authentication และ Captive Portal authentication ได้เป็นอย่างน้อย

๗.๒๐. รองรับการทำ VLAN Pooling และ DHCP Relay ได้เป็นอย่างน้อย

๗.๒๑. สามารถบริหารจัดการผ่านพอร์ท Serial Console Interface (RJ-๔๕) และมีพอร์ทแบบ USB ๒.๐ (A connector) เป็นอย่างน้อย

๗.๒๒. ผ่านการรับรองตาม Regulatory กำหนด เช่น FCC, UL/IEC/EN ๖๐๙๕๐, R&TTE Directive ๑๙๙๕/๕/EC, Low Voltage Directive ๗๒/๒๓/EEC และ CE Marked รวมถึงต้องมี Certifications ตามมาตรฐานสากลประเภท Wi-Fi Alliance (WFA) certified ๘๐๒.๑๑a/b/g/n/ac เป็นอย่างน้อย

๗.๒๓. อุปกรณ์กระจายสัญญาณเครือข่ายไร้สายที่เสนอนี้ต้องรับประกันอุปกรณ์แบบ Limited Lifetime warrant

๗.๒๔. อุปกรณ์ Power Injector มีรายละเอียดดังต่อไปนี้

๗.๒๔.๑. สามารถจ่ายกระแสไฟฟ้าตรงไปในสายสัญญาณ UTP Cat ๕ หรือดีกว่าได้ เพื่อเป็นแหล่งไฟฟ้าให้กับอุปกรณ์ Wireless Access Point

๗.๒๔.๒. สามารถทำงานได้ตามมาตรฐาน IEEE ๘๐๒.๓af และ IEEE ๘๐๒.๓at

๗.๒๔.๓. สามารถจ่ายไฟได้ไม่น้อยกว่า ๓๐Watt

๗.๒๔.๔. รองรับการทำงานที่ความเร็ว ๑๐/๑๐๐/๑๐๐๐Base-T LAN ได้เป็นอย่างน้อย

๘. อุปกรณ์เครื่องคอมพิวเตอร์แม่ข่ายและระบบปฏิบัติการ

๘.๑. เครื่องคอมพิวเตอร์แม่ข่าย แบบที่ ๑ คุณลักษณะพื้นฐาน มีรายละเอียดดังต่อไปนี้

๘.๑.๑. มีหน่วยประมวลผลกลาง (CPU) แบบ 8 แกนหลัก (8 core) หรือดีกว่า สาหรับคอมพิวเตอร์แม่ข่าย (Server) โดยเฉพาะและมีความเร็วสัญญาณนาฬิกาพื้นฐานไม่น้อยกว่า 2.1 GHz จานวนไม่น้อยกว่า 1 หน่วย

๘.๑.๒. หน่วยประมวลผลกลาง (CPU) รองรับการประมวลผลแบบ ๖๔ bit มีหน่วยความจาแบบ Cache Memory รวมในระดับ (Level) เดียวกันไม่น้อยกว่า ๑๑ MB

๘.๑.๓. มีหน่วยความจาหลัก (RAM) ชนิด ECC DDR๔ หรือดีกว่า มีขนาดไม่น้อยกว่า ๑๖ GB

๘.๑.๔. สนับสนุนการทางาน RAID ไม่น้อยกว่า RAID ๐, ๑, ๕

๘.๑.๕. มีหน่วยจัดเก็บข้อมูล ชนิด SCSI หรือ SAS หรือ SATA ที่มีความเร็วรอบไม่น้อยกว่า ๗,๒๐๐ รอบต่อนาที หรือ ชนิด Solid State Drive หรือดีกว่า ขนาดความจุไม่น้อยกว่า ๒๐๐ GB จานวนไม่น้อยกว่า ๒ หน่วย

๘.๑.๖. มี DVD-ROM หรือดีกว่า แบบติดตั้งภายใน (Internal) หรือภายนอก (External) จำนวน ๑ หน่วย

๘.๑.๗. มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ ๑๐/๑๐๐/๑๐๐๐ Base-T หรือดีกว่า จานวนไม่น้อยกว่า ๒ ช่อง

๘.๑.๘. มีจอแสดงภาพขนาดไม่น้อยกว่า ๑๗ นิ้ว จานวน ๑ หน่วย

๘.๑.๙. มี Power Supply แบบ Redundant หรือ Hot Swap จานวน ๒ หน่วย

๘.๑.๑๐. ชุดโปรแกรมระบบปฏิบัติการสำหรับเครื่องคอมพิวเตอร์แม่ข่าย (Server) สำหรับรองรับ ประมวลผลกลาง (CPU) ไม่น้อยกว่า 16 แกนหลัก (16 core) ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย

๙. เลขที่อยู่ไอ พี (Public IP)

๙.๑ เลขที่อยู่ไอ พี (Public IP) คุณลักษณะพื้นฐาน มีรายละเอียดดังต่อไปนี้

๙.๑.๑. ไอพีแอดเดรสเป็นหมายเลขประจำเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ที่เชื่อมต่ออยู่ในเครือข่ายเพื่อใช้ระบุที่อยู่หรือตำแหน่งของคอมพิวเตอร์และอุปกรณ์โดยไม่ซ้ำกัน

๙.๑.๒. คอมพิวเตอร์และอุปกรณ์สามารถติดต่อสื่อสารหรือรับส่งข้อมูลได้

๙.๑.๓ Public IP จะต้องไม่ซ้ำกัน และจะต้องมีคุณสมบัติอย่างน้อยตามมาตรฐานที่เกี่ยวข้องกำหนด

๙.๑.๔ รองรับมาตรฐานของหน่วยงานกลางคือ InterNIC (Inter Network Information Center) ทำหน้าที่ จัดสรรไอพีแอดเดรสให้กับผู้ใช้ทั่วโลก

๙.๑.๕ ไอพีแอดเดรสรองรับเวอร์ชั่น 4 (Ipv4) หรือ Ipv6 รวมทั้งสามารถรองรับการใช้งานตามมาตรฐานที่กำหนดในอนาคตได้

๙.๑.๖ รองรับการใช้งานระบบสื่อสารองค์กรขนาดกลางขึ้นไปที่มีการเชื่อมต่อไปยังผู้ให้บริการอินเทอร์เน็ตโดยใช้ Leased Line หรือ ADSL

๙.๑.๗ สามารถรองรับสำหรับเครือข่ายอินทราเน็ต โดยจะกำหนดไอพีแอดเดรสได้ตามต้องการ โดยใช้ไอพีแอดเดรสแบบ ภายใน (Private IP Address) และการกำหนดจากผู้ดูแลระบบเครือข่ายในองค์กร

๙.๑.๘ Public IP ประกอบด้วย ๒ ส่วนหลัก คือ Network ID กับ Host ID สำหรับ Network ID เป็นตัวบอกขอบเขตของเครือข่าย

ผู้เสนอราคาต้องแสดงแสดงเอกสารทางด้านเทคนิคเพื่อแสดงความเข้าใจในระบบสื่อสารข้อมูลและการให้บริการสัญญาณอินเตอร์เน็ต อย่างน้อยดังนี้

ลำดับที่	รายการ
๑.	**ความเข้าใจในการให้บริการ** ๑.๑ ความเข้าใจในระบบ เพื่อบริหารจัดการวงจรสำหรับการสื่อสารข้อมูลเฉพาะส่วน (Private Network) และวงจรสำหรับการให้บริการสัญญาณอินเตอร์เน็ตรองรับการใช้งานหน่วยงานภายในกองทางหลวงพิเศษระหว่างเมือง
๒.	**รูปแบบและแผนงาน วิธีการ บริหารจัดการใช้ทรัพยากร**อย่างมีประสิทธิภาพ ให้สอดคล้องและรองรับนโยบายการทำงานของหน่วยงานภายในกองทางหลวงพิเศษระหว่างเมือง ๒.๑ เสนอแนวทางในการปรับเปลี่ยนบริหารจัดการทรัพยากรใช้งานแบนด์วิของผู้ใช้งานอินเตอร์เน็ตในหน่วยงาน ติดตามพฤติกรรมการใช้งานให้เกิดความปลอดภัยสูงสุด ๒.๒ เสนอแนวทาง นโยบายบริหารจัดการใช้งาน (Service) ของสัญญาณอินเตอร์เน็ตและแบ่งกลุ่มผู้ใช้งานตามความต้องการของหน่วยงาน ๒.๓ เสนอแนวทาง นโยบาย การบริหารจัดการและจัดสรรช่องสัญญาณสื่อสารข้อมูลทั้งภายในและภายนอกรวมถึงการใช้งานทรัพยากรระบบเครือข่าย ๒.๔ เสนอแนวทาง นโยบาย ระบบการป้องกันเครือข่ายให้มีความปลอดภัยอย่างสูงสุดสำหรับองค์กร ๒.๕ เสนอแนวทาง นโยบาย ระบบเพิ่มประสิทธิภาพการเข้าถึงระบบเครือข่ายเพื่อการใช้งานอย่างสะดวก รวดเร็ว ทันการณ์ ๒.๖ เสนอแนวทาง รูปแบบ วิธีการ การให้บริการสัญญาณอินเตอร์เน็ตผ่านอุปกรณ์กระจายสัญญาณ (Access Point) เพื่อให้การใช้งานเกิดประสิทธิภาพสูงสุด ๒.๗ เสนอแนวทาง รูปแบบ วิธีการการเชื่อมต่อระบบสื่อสารข้อมูลระหว่างอาคารกองทางหลวงพิเศษระหว่างเมือง อาคารศูนย์ควบคุมฯ (CCB) ลาดกระบัง เพื่อให้การสื่อสารข้อมูลเป็นไปอย่างมีประสิทธิภาพ
๓.	**ความเข้าใจ แผนงาน และแนวทางการบำรุงรักษาระบบและอุปกรณ์** ๓.๑ ความเข้าใจ และแนวทางในการบำรุงรักษาระบบและอุปกรณ์ ๓.๒ แผนการดำเนินงานและวิธีการบำรุงรักษาระบบและอุปกรณ์
๔.	**ความพร้อมและคุณภาพของบุคลากรผู้ปฏิบัติงาน** ๔.๑ แสดงความพร้อมในการเข้าปฏิบัติงาน วุฒิการศึกษา ประสบการณ์ เพื่อรองรับการปฏิบัติงานได้อย่างมีประสิทธิภาพ

ลำดับที่	รายการ
๕.	**ความน่าเชื่อถือของผู้ประสงค์จะเสนอราคา** ๕.๑ ต้องแสดงผลงานและประสบการณ์ของผู้ประสงค์จะเสนอราคา รวมถึงการสนับสนุนด้านเทคโนโลยีของอุปกรณ์ต่างๆที่เกี่ยวข้อง
๖.	**ข้อเสนออื่นๆ เพื่อประโยชน์ต่อทางราชการ**

ภาคผนวก ข

การบริหารจัดการบริการสัญญาณ Internet

๑. การบริหารจัดการบริการสัญญาณ Internet โดยต้องมีข้อกำหนดอย่างน้อยดังนี้

๑.๑. ระบบให้บริการตรวจสอบสภาพวงจรและรายงานผลการใช้งานระบบอินเตอร์เน็ต ของผู้ว่าจ้างแบบออนไลน์และ real-time สามารถเข้าถึงได้จาก web browser พร้อมจัดหา user และ password จำนวนอย่างน้อย ๔ ชุด เพื่อให้เจ้าหน้าที่ของผู้ว่าจ้างสามารถตรวจสอบสภาพการใช้งานวงจร โดยต้องมีข้อมูลอย่างน้อยดังนี้

๑.๑.๑. รายงานแสดงความเร็วการดาวน์โหลดและอัพโหลดของการใช้งานระบบสื่อสารข้อมูลในแต่ละช่วงเวลาโดยแสดงเป็นกราฟ ที่ความเร็วเฉลี่ยทุก ทุก ๕ นาที, ๓๐ นาที ๒ ชั่วโมง ,๑ วัน แยกเป็นความเร็วในประเทศและต่างประเทศ

๑.๑.๒. รายงานความขัดข้องของสัญญาในแต่ละเดือน โดยแจ้งข้อมูลช่วง วัน เวลา และเหตุที่เกิดความขัดข้อง

๑.๒. ระบบบริหารจัดการทรัพยากร (Bandwidth Management)ของผู้ใช้งานแบบออนไลน์และ real-time สามารถเข้าถึงได้จาก web browser เพื่อให้เจ้าหน้าที่ของผู้ว่าจ้างสามารถตรวจสอบได้ โดยต้องมีข้อมูลอย่างน้อยดังนี้

๑.๒.๑. แสดงปริมาณการใช้งาน (Service) ของหน่วยงานได้แบบรายสัปดาห์และรายเดือน

๑.๒.๒.แสดงอันดับผู้ใช้งานทรัพยากรสูงสุดจำนวนอย่างน้อย ๑๐ อันดับ โดยสุ่มจากผู้ใช้งานเป็นรายสัปดาห์หรือรายเดือนทั้งในส่วนของอาคารกองทางหลวงพิเศษระหว่างเมือง และอาคารศูนย์ควบคุม (CCB) ลาดกระบัง, อาคารศูนย์ควบคุมพัทยา หรือจุดอื่นๆตามผู้ว่าจ้างกำหนด

๑.๓. ผู้รับจ้างจะต้องบริการให้คำปรึกษาและแก้ไขปัญหาต่างๆ ที่อาจเกิดขึ้นจากการใช้งาน ทันทีที่มีปัญหาหรือตามที่ผู้ว่าจ้างร้องขอ ทางโทรศัพท์ หรือแฟกซ์ หรือจดหมาย อิเล็กทรอนิกส์ (e-mail) ตามความเหมาะสมตลอด ๒๔ ชั่วโมง