

ขอบเขตของงาน (Terms of Reference : TOR)
โครงการทดแทนและเพิ่มประสิทธิภาพระบบรักษาความมั่นคงปลอดภัย
ระบบคอมพิวเตอร์และระบบเครือข่าย

๑. ความเป็นมา

ศูนย์คอมพิวเตอร์ของสำนักงานปลัดกระทรวงการคลัง มีภารกิจสำคัญในการให้บริการระบบคอมพิวเตอร์ ระบบเครือข่าย และระบบสารสนเทศรองรับภารกิจของกระทรวงการคลังและหน่วยงานในสังกัด อีกทั้งยังรองรับระบบระบบบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ใหม่ (New GFMS Thai) ซึ่งเป็นระบบโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) ซึ่งต้องปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ การให้บริการดังกล่าวจำเป็นต้องพึ่งพาระบบรักษาความมั่นคงปลอดภัยเครือข่ายที่มีเสถียรภาพและเชื่อถือได้ โดยเฉพาะอุปกรณ์ Internet Firewall และ Web Application Firewall ซึ่งทำหน้าที่เป็นด่านแรกในการควบคุมและป้องกันการเข้าถึงระบบจากภายนอก ซึ่งปัจจุบันได้ติดตั้งใช้งานมาแล้วไม่น้อยกว่า ๗ ปี อุปกรณ์เริ่มมีข้อจำกัดด้านสมรรถนะและเทคโนโลยี เนื่องจากสิ้นสุดการสนับสนุนจากผู้ผลิต (End of Support) ทำให้ไม่สามารถดำเนินการปรับปรุงฐานข้อมูลภัยคุกคามได้อย่างเพียงพอ ขณะที่สภาพแวดล้อมภัยคุกคามทางไซเบอร์มีความรุนแรงและซับซ้อนมากขึ้น ทั้งการโจมตีแบบ Ransomware การเจาะระบบผ่านช่องโหว่เว็บแอปพลิเคชัน และการโจมตีแบบปฏิเสธการให้บริการ (DDoS) ซึ่งล้วนส่งผลกระทบต่อความเสี่ยงในการหยุดชะงักของการให้บริการการรั่วไหลของข้อมูล และภาพลักษณ์ของกระทรวงการคลังโดยรวม

การทดแทนและยกระดับอุปกรณ์ป้องกันเครือข่ายและระบบป้องกันการโจมตีดังกล่าวจึงเป็นมาตรการที่มีความจำเป็นในการเสริมสร้างความมั่นคงปลอดภัยของโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศของหน่วยงาน ให้สอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ จึงมีความจำเป็นต้องดำเนินการ โครงการทดแทนและเพิ่มประสิทธิภาพระบบรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์และระบบเครือข่าย เพื่อให้ระบบมีความมั่นคงปลอดภัย ทันท่วงที และรองรับการให้บริการของหน่วยงานได้อย่างต่อเนื่องและมีประสิทธิภาพยิ่งขึ้น

๒. วัตถุประสงค์

- ๒.๑ เพื่อดำเนินการเปลี่ยนทดแทนอุปกรณ์ Internet Firewall และ Web Application Firewall ที่ติดตั้งใช้งานมาแล้วไม่น้อยกว่า ๗ ปี และใกล้หมดอายุการสนับสนุนจากผู้ผลิต ด้วยอุปกรณ์และระบบที่มีเทคโนโลยีด้านความมั่นคงปลอดภัยที่ทันสมัยยิ่งขึ้น
- ๒.๒ เพื่อเพิ่มระดับความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และระบบเครือข่ายของศูนย์คอมพิวเตอร์ถนนพระราม ๖ ศูนย์คอมพิวเตอร์ปทุมธานี และศูนย์คอมพิวเตอร์พิษณุโลก ให้สามารถป้องกัน ตรวจสอบ และตอบสนองต่อภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ
- ๒.๓ เพื่อเพิ่มประสิทธิภาพและเสถียรภาพในการให้บริการของระบบคอมพิวเตอร์และระบบเครือข่าย ให้รองรับปริมาณการใช้งานที่เพิ่มขึ้น และลดโอกาสการหยุดชะงักของการให้บริการที่เกิดจากข้อจำกัดของอุปกรณ์ป้องกันเครือข่ายเดิม
- ๒.๔ เพื่อจัดให้มีระบบบริหารจัดการอุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall Management System) แบบศูนย์กลาง สำหรับการกำหนดนโยบาย ฝ้าระวังเหตุการณ์และจัดทำรายงานด้านความมั่นคงปลอดภัยสารสนเทศได้อย่างเป็นระบบและตรวจสอบได้

๒.๕ เพื่อรองรับการปฏิบัติตามกฎหมาย นโยบาย และมาตรการด้านความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง ตลอดจนแนวนโยบายด้านการรักษาความมั่นคงปลอดภัยสารสนเทศของกระทรวงการคลัง

๓. เป้าหมาย

มีระบบรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์และระบบเครือข่ายที่ทันสมัยและมีประสิทธิภาพ โดยมีการติดตั้งอุปกรณ์ป้องกันเครือข่ายแบบ Next Generation Firewall ทดแทนอุปกรณ์เดิมที่ศูนย์คอมพิวเตอร์กระทรวงการคลัง จังหวัดปทุมธานี และศูนย์คอมพิวเตอร์พิบูลสงคราม พร้อมระบบบริหารจัดการอุปกรณ์ป้องกันเครือข่ายแบบศูนย์กลาง มีระบบ Web Application Firewall และ DDoS Protection บนระบบ Cloud ครอบคลุมการให้บริการเว็บไซต์ภายในทั้งหมดของกระทรวงการคลังจากศูนย์คอมพิวเตอร์ทั้ง ๓ แห่ง สามารถจัดเก็บและจัดทำรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยเพื่อใช้ในการบริหารจัดการความเสี่ยง และมีการถ่ายทอดความรู้ จัดทำคู่มือ และพัฒนาศักยภาพเจ้าหน้าที่ที่เกี่ยวข้องให้สามารถบริหารจัดการระบบดังกล่าวได้อย่างมีประสิทธิภาพ

๔. คุณสมบัติผู้ยื่นข้อเสนอ

๔.๑ มีความสามารถตามกฎหมาย

๔.๒ ไม่เป็นบุคคลล้มละลาย

๔.๓ ไม่อยู่ระหว่างเลิกกิจการ

๔.๔ ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

๔.๕ ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทำงานและได้แจ้งเวียนชื่อให้เป็นผู้ทำงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทำงานเป็นหุ้นส่วน ผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

๔.๖ มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

๔.๗ เป็นนิติบุคคล ผู้มีอาชีพขายพัสดุที่ประกวดราคาซื้อด้วยวิธีการทางอิเล็กทรอนิกส์

๔.๘ ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่สำนักงานปลัดกระทรวงการคลัง ณ วันยื่นข้อเสนอ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในครั้งนั้น

๔.๙ ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์ความคุ้มกันเช่นนั้น

๔.๑๐ ผู้ยื่นข้อเสนอต้องลงทะเบียนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement : e - GP) ของกรมบัญชีกลาง

๔.๑๑ ผู้ยื่นข้อเสนอต้องมีผลงานในการขายและติดตั้ง ระบบเครื่องคอมพิวเตอร์ หรือ ระบบเครือข่าย หรือ ระบบรักษาความมั่นคงปลอดภัย หรือ ระบบสนับสนุนศูนย์คอมพิวเตอร์ โดยมีผลงานในการขายและติดตั้งสำเร็จมาแล้วให้กับหน่วยงานของรัฐ ภายในระยะเวลา ๕ ปี นับจากวันแล้วเสร็จจนถึงวันยื่นข้อเสนอ ซึ่งมีมูลค่าไม่น้อยกว่า ๑๕,๐๐๐,๐๐๐.- บาท (สิบห้าล้านบาทถ้วน) ต่อหนึ่งสัญญา ทั้งนี้ ให้แนบสำเนาสัญญาและสำเนาหนังสือรับรองผลงาน มาพร้อมการยื่นข้อเสนอทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์

- ๔.๑๒ ผู้ยื่นข้อเสนอซึ่งเป็นผู้ประกอบการ SMEs แสดงสำเนาใบขึ้นทะเบียนผู้ประกอบการวิสาหกิจขนาดกลาง และขนาดย่อม (SMEs) เป็น SME-GP (ถ้ามี) มาพร้อมการยื่นข้อเสนอทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์
- ๔.๑๓ ผู้ยื่นข้อเสนอที่เป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยซึ่งได้จดทะเบียนเกินกว่า ๑ ปี ต้องมีมูลค่าสุทธิ ของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิที่ปรากฏในงบแสดงฐานะการเงินที่ มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก ๑ ปีสุดท้ายก่อนวันยื่นข้อเสนอ โดยแสดงสำเนา เอกสารหรือหลักฐานมาพร้อมการยื่นข้อเสนอทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์
- ๔.๑๔ ผู้ยื่นข้อเสนอที่เป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีงบแสดงฐานะการเงิน กับกรมพัฒนาธุรกิจการค้า จะต้องมียุทธศาสตร์ที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอ ไม่ต่ำกว่า ๘ ล้านบาท โดยแสดงสำเนาเอกสารหรือหลักฐานมาพร้อมการยื่นข้อเสนอทางระบบจัดซื้อ จัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์
- ๔.๑๕ กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียนหรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ ๑ ใน ๔ ของมูลค่างบประมาณของโครงการ หรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง (สินเชื่อที่ธนาคารภายในประเทศหรือบริษัทเงินทุนหรือบริษัท เงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้าประกัน ตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรองหรือที่สำนักงานสาขา รับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอนับถึงวันยื่นข้อเสนอไม่ เกิน ๙๐ วัน) โดยแสดงสำเนาแบบหนังสือรับรองวงเงินสินเชื่อ (ตามแบบที่กรมบัญชีกลางกำหนด) มา พร้อมการยื่นข้อเสนอทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์
- ๔.๑๖ กรณีที่ผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐ หรือ เป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่าง การฟื้นฟูกิจการตามพระราชบัญญัติล้มละลาย (ฉบับที่ ๑๐) พ.ศ. ๒๕๖๑ ไม่ต้องยื่นเอกสารข้อเสนอ ตามข้อ ๔.๑๓ - ๔.๑๕

๕. แบบรูปรายการหรือคุณลักษณะเฉพาะ

สำนักงานปลัดกระทรวงการคลังมีความต้องการจัดซื้ออุปกรณ์ในโครงการทดแทนและเพิ่ม ประสิทธิภาพระบบรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์และระบบเครือข่าย โดยต้องมีคุณลักษณะ เฉพาะอย่างน้อยตามเอกสารแนบท้าย แบบรูปรายการหรือคุณลักษณะเฉพาะ ประกอบด้วยรายการ ดังต่อไปนี้

- | | | |
|-----|---|-----------------|
| ๕.๑ | อุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall) | จำนวน ๔ เครื่อง |
| ๕.๒ | ระบบบริหารจัดการอุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall) | จำนวน ๒ ระบบ |
| ๕.๓ | ระบบป้องกันการโจมตีระบบเครือข่ายหรือบริการ (Web Application Firewall และ DDoS Protection) | จำนวน ๑ ระบบ |

๖. ระยะเวลาดำเนินการ

ภายในระยะเวลา ๒๔๐ วัน นับถัดจากวันลงนามในสัญญา

๗. ระยะเวลาส่งมอบงาน

ผู้ชนะการประกวดราคาจะต้องส่งมอบงาน ดังต่อไปนี้

งวดที่ ๑ ภายใน ๓๐ วัน นับถัดจากวันลงนามในสัญญา

๑. แผนการดำเนินงานโครงการ และโครงสร้างการบริหารโครงการ
๒. ร่างแผนผังระบบเครือข่าย (Network Diagram)
๓. ร่างแผนผังแสดงอุปกรณ์ในตู้ Rack (Rack Layout)
๔. แผนการฝึกอบรม ตามเอกสารแนบท้าย รายละเอียดการฝึกอบรม
๕. เอกสารจำนวน ๒ ชุด และในรูปแบบอิเล็กทรอนิกส์ซึ่งบันทึกลงใน Thumb Drive ๑ ชุด

งวดที่ ๒ ภายใน ๖๐ วัน นับถัดจากวันลงนามในสัญญา

๑. ส่งมอบระบบป้องกันการโจมตีระบบเครือข่ายหรือบริการ (Web Application Firewall และ DDoS Protection) (รายการตามข้อ ๕.๓) และผลการทดสอบตามคุณลักษณะที่กำหนด
๒. เอกสารจำนวน ๒ ชุด และในรูปแบบอิเล็กทรอนิกส์ซึ่งบันทึกลงใน Thumb Drive ๑ ชุด

งวดที่ ๓ ภายใน ๑๕๐ วัน นับถัดจากวันลงนามในสัญญา

๑. ส่งมอบครุภัณฑ์ รายการตามข้อ ๕.๑ และ ข้อ ๕.๒ และผลการทดสอบตามคุณลักษณะที่กำหนด
๒. เอกสารจำนวน ๒ ชุด และในรูปแบบอิเล็กทรอนิกส์ซึ่งบันทึกลงใน Thumb Drive ๑ ชุด

งวดสุดท้าย ภายใน ๒๔๐ วัน นับถัดจากวันลงนามในสัญญา

๑. ส่งมอบงานติดตั้งครุภัณฑ์ทั้งหมดในโครงการ
๒. แผนผังระบบเครือข่าย (Network Diagram) และแผนผังแสดงอุปกรณ์ในตู้ Rack (Rack Layout)
๓. เอกสารสรุปการติดตั้งและรายงานผลการทดสอบอุปกรณ์ทั้งหมดในโครงการ
๔. คู่มือการใช้งานของอุปกรณ์ในโครงการ
๕. ส่งมอบผลการฝึกอบรมในลักษณะ On The Job Training ในโครงการทั้งหมด
๖. ส่งมอบงานอื่น ๆ ทั้งหมดในโครงการ
๗. เอกสารจำนวน ๒ ชุด (ยกเว้น คู่มือการใช้งานตามข้อ ๔) และในรูปแบบอิเล็กทรอนิกส์ซึ่งบันทึกลงใน Portable Hard disk จำนวน ๖ ชุด

๘. เงื่อนไขการชำระเงิน

งวดที่ ๑ ชำระเงินในอัตราร้อยละ ๕ ของจำนวนเงินตามสัญญา เมื่อคณะกรรมการตรวจรับพัสดุได้ตรวจรับ การส่งมอบงานงวดที่ ๑ เรียบร้อยแล้ว

งวดที่ ๒ ชำระเงินในอัตราร้อยละ ๓๕ ของจำนวนเงินตามสัญญา เมื่อคณะกรรมการตรวจรับพัสดุได้ตรวจรับ การส่งมอบงานงวดที่ ๒ เรียบร้อยแล้ว

งวดที่ ๓ ชำระเงินในอัตราร้อยละ ๔๐ ของจำนวนเงินตามสัญญา เมื่อคณะกรรมการตรวจรับพัสดุได้ตรวจรับ การส่งมอบงานงวดที่ ๓ เรียบร้อยแล้ว

งวดสุดท้าย ชำระเงินในอัตราร้อยละ ๒๐ ของจำนวนเงินตามสัญญา เมื่อคณะกรรมการตรวจรับพัสดุ ได้ตรวจรับการส่งมอบงานงวดสุดท้าย เรียบร้อยแล้ว

๙. อัตราค่าปรับ

ผู้ชนะการประกวดราคาหรือผู้ขายต้องดำเนินการตามขอบเขตของงานที่กำหนดให้มีความถูกต้องครบถ้วน และหากไม่สามารถดำเนินการได้ครบถ้วนหรือถูกต้อง ผู้ชนะการประกวดราคาหรือผู้ขายยินยอมให้สำนักงานปลัดกระทรวงการคลังปรับเป็นรายวันในอัตราร้อยละ ๐.๒๐ (ศูนย์จุดสองศูนย์) ของราคาส่งของที่ยังไม่ได้ส่งมอบ จนกว่าจะดำเนินการแล้วเสร็จ หรือสำนักงานปลัดกระทรวงการคลังใช้สิทธิบอกเลิกสัญญา

๑๐. การรับประกันความชำรุดบกพร่อง

ผู้ชนะการประกวดราคาหรือผู้ขายต้องรับประกันความชำรุดบกพร่องของอุปกรณ์และระบบทั้งหมด ที่ส่งมอบในโครงการทดแทนและเพิ่มประสิทธิภาพการเชื่อมโยงเครือข่ายกลางกระทรวงการคลัง เป็นระยะเวลา ๑ ปี นับถัดจากวันที่คณะกรรมการตรวจรับพัสดุได้ตรวจรับการส่งมอบพัสดุงวดสุดท้ายเรียบร้อยแล้ว โดยมีรายละเอียดตามขอบเขตของงานที่กำหนด

๑๑. วงเงินในการจัดหา

วงเงินในการจัดหาเป็นเงินทั้งสิ้น ๓๗,๔๕๐,๐๐๐.- บาท (สามสิบล้านสี่แสนห้าหมื่นบาทถ้วน) ซึ่งเป็นวงเงินที่รวมภาษีมูลค่าเพิ่ม และค่าใช้จ่ายอื่นใดที่พึงประสงค์แล้ว โดยเบิกจ่ายจากเงินงบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. ๒๕๖๐

๑๒. หลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอ

ใช้เกณฑ์ราคาในการคัดเลือกผู้เสนอราคาต่ำสุดเป็นผู้ชนะการซื้อหรือจ้างหรือเป็นผู้ได้รับการคัดเลือก โดยกรณีดำเนินการจัดซื้อโดยวิธีประกวดราคาอิเล็กทรอนิกส์ (Electronic Bidding : e - Bidding) และใช้เกณฑ์ราคาในการพิจารณาคัดเลือกผู้ชนะ ให้พิจารณาให้แต้มต่อการยื่นข้อเสนอ ดังนี้

(๑) หากผู้ยื่นข้อเสนอซึ่งเป็นผู้ประกอบการ SMEs เสนอราคาสูงกว่าราคาต่ำสุดของผู้ยื่นข้อเสนอรายอื่นที่ไม่เกินร้อยละ ๑๐ ให้จัดซื้อจากผู้ประกอบการ SMEs ดังกล่าว โดยจัดเรียงลำดับผู้ยื่นข้อเสนอซึ่งเป็นผู้ประกอบการ SMEs ซึ่งเสนอราคาสูงกว่าราคาต่ำสุดของผู้ยื่นข้อเสนอรายอื่นไม่เกินร้อยละ ๑๐ ที่จะเรียกมาทำสัญญาไม่เกิน ๓ ราย

(๒) หากผู้ยื่นข้อเสนอได้เสนอพัสดุที่เป็นพัสดุที่ผลิตภายในประเทศ ที่ได้รับการรับรองและออกเครื่องหมายสินค้าที่ผลิตภายในประเทศไทย (Made in Thailand) จากสภาอุตสาหกรรมแห่งประเทศไทย เสนอราคาสูงกว่าราคาต่ำสุดของผู้ยื่นข้อเสนอรายอื่นไม่เกินร้อยละ ๕ ให้จัดซื้อจัดจ้างจากผู้ยื่นข้อเสนอที่เสนอพัสดุที่เป็นพัสดุที่ผลิตภายในประเทศที่ได้รับการรับรองและออกเครื่องหมายสินค้าที่ผลิตภายในประเทศไทย

สำหรับการประกวดราคาอิเล็กทรอนิกส์ ที่มีการเสนอราคาหลายรายการและกำหนดเงื่อนไขเป็นกรณีการพิจารณาราคารวม หากผู้ยื่นข้อเสนอได้เสนอพัสดุที่เป็นพัสดุที่ผลิตภายในประเทศ ที่ได้รับการรับรองและออกเครื่องหมายสินค้าที่ผลิตภายในประเทศไทย มีสัดส่วนมูลค่าตั้งแต่ร้อยละ ๖๐ ขึ้นไป ให้ได้แต้มต่อการเสนอราคาตามวรรคหนึ่ง

อนึ่ง หากในการเสนอราคาครั้งนั้น ผู้ยื่นข้อเสนอรายใดมีคุณสมบัติทั้ง (๑) และ (๒) ให้ผู้ยื่นข้อเสนอรายนั้นได้แต้มต่อการเสนอราคาสูงกว่าผู้ประกอบการรายอื่นไม่เกินร้อยละ ๑๕

(๓) หากผู้ยื่นข้อเสนอซึ่งมิใช่ผู้ประกอบการ SMEs แต่เป็นบุคคลธรรมดาที่ถือสัญชาติไทยหรือนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยเสนอราคาสูงกว่าราคาต่ำสุดของผู้ยื่นข้อเสนอซึ่งเป็นบุคคลธรรมดาที่มีได้ถือสัญชาติไทย

หรือนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายของต่างประเทศไม่เกินร้อยละ ๓ ให้จัดซื้อหรือจัดจ้างจากผู้ยื่นข้อเสนอ ซึ่งเป็นบุคคลธรรมดาที่ถือสัญชาติไทยหรือนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย

๑๓. ข้อมูลส่วนบุคคล

๑๓.๑ นโยบายคุ้มครองข้อมูลส่วนบุคคล

ผู้รับจ้างได้รับทราบและตกลงจะปฏิบัติตามประกาศสำนักงานปลัดกระทรวงการคลัง เรื่อง นโยบายคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) สำนักงานปลัดกระทรวงการคลัง ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ประกาศ ณ วันที่ ๔ กุมภาพันธ์ ๒๕๖๔ หรือตามประกาศฉบับที่ปรับปรุงล่าสุด รวมถึงนโยบายและประกาศอื่นใดที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลของสำนักงานปลัดกระทรวงการคลัง

๑๓.๒ การประมวลผลข้อมูลส่วนบุคคลในนามของสำนักงานปลัดกระทรวงการคลัง

การดำเนินงานของโครงการนี้ ผู้รับจ้างไม่มีการประมวลผลข้อมูลส่วนบุคคลในนามของสำนักงานปลัดกระทรวงการคลัง

๑๔. การเก็บรักษาข้อมูลไว้เป็นความลับ

๑๔.๑ เอกสารทั้งหมดที่จัดทำขึ้น ถือเป็นลิขสิทธิ์ของสำนักงานปลัดกระทรวงการคลัง ผู้ขายหรือผู้รับจ้างจะต้องไม่เผยแพร่เอกสาร และ/หรือข้อมูลใด ๆ ที่จัดทำขึ้นทั้งหมด โดยไม่ได้รับความเห็นชอบอย่างเป็นทางการเป็นลายลักษณ์อักษรจากสำนักงานปลัดกระทรวงการคลัง รวมทั้งจะต้องไม่แสวงหา หรือยินยอมให้บุคคลอื่นแสวงหาประโยชน์ใด ๆ จากข้อมูลและ/หรือ เอกสารดังกล่าวทั้งในทางพาณิชย์ หรือในกรณีอื่นอันอาจก่อให้เกิดความเสียหายแก่สำนักงานปลัดกระทรวงการคลังด้วยประการใดทั้งสิ้น

๑๔.๒ ข้อตกลงนี้ให้ถือเป็นส่วนหนึ่งของสัญญา อันเป็นเงื่อนไขที่สำนักงานปลัดกระทรวงการคลัง บอกเลิกสัญญาเรียกค่าเสียหายหรือปรับสินไหม รวมทั้งการดำเนินคดีทั้งในทางแพ่งและอาญาทุกประเภท

๑๔.๓ ข้อมูลต่าง ๆ ที่ผู้ขายหรือผู้รับจ้างได้รับทราบจากสำนักงานปลัดกระทรวงการคลังให้ถือเป็นความลับและลิขสิทธิ์ในเอกสารทุกฉบับและผลงานทุกชิ้น ซึ่งผู้ขายหรือผู้รับจ้างได้จัดทำขึ้น ให้ตกเป็นกรรมสิทธิ์ของสำนักงานปลัดกระทรวงการคลัง ผู้ขายหรือผู้รับจ้างจะนำไปเผยแพร่ไม่ได้ โดยจะต้องปฏิบัติตามข้อกำหนดดังกล่าวในชั้นข้อมูลลับของทางสำนักงานปลัดกระทรวงการคลัง เว้นแต่นำไปใช้เพื่อการศึกษาหรือขอผลงานทางวิชาการ (กรณีเป็นสถาบันการศึกษา)

๑๔.๔ ในการเก็บรักษาความลับของสำนักงานปลัดกระทรวงการคลัง ผู้ขายหรือผู้รับจ้างต้องระมัดระวังในการดูแลรักษาและปกป้องมิให้บุคคลอื่นที่ไม่เกี่ยวข้องกับการปฏิบัติงานตามสัญญาซื้อหรือจ้างได้ล่วงรู้ถึงข้อมูล หรือนำข้อมูลไปใช้หาประโยชน์ในการใด ๆ รวมถึงการเผยแพร่ต่อสาธารณะโดยมิได้รับอนุญาตจากสำนักงานปลัดกระทรวงการคลัง ยกเว้นในกรณีดังต่อไปนี้ ให้แจ้งสำนักงานปลัดกระทรวงการคลังทุกครั้ง กล่าวคือ

๑) เป็นการเปิดเผยเพื่อประโยชน์ หรือความจำเป็นในการทำหน้าที่ตามสัญญาซื้อหรือจ้าง

๒) เป็นกรณีจำเป็นต้องเปิดเผยตามกฎหมายหรือคำสั่งศาล

๑๔.๕ ผู้ขายหรือผู้รับจ้างต้องส่งมอบข้อมูล พร้อมทั้งข้อมูลที่ได้ทำซ้ำซึ่งสำเนาในทุกรูปแบบที่อาจสื่อความหมายถึงข้อมูลได้คืนแก่สำนักงานปลัดกระทรวงการคลังเมื่อเสร็จสิ้นงานซื้อหรือจ้าง หรือทำลายสำเนาข้อมูลเหล่านั้นเพื่อมิให้สามารถสื่อข้อความต่อไปได้อีก

๑๔.๖ ผู้ขายหรือผู้รับจ้างต้องรับผิดชอบในการดูแลรักษาความมั่นคงปลอดภัยข้อมูลให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และกฎหมายที่เกี่ยวข้องอย่างเคร่งครัด

๑๔.๗ ผู้ขาย/ผู้รับจ้าง พนักงาน ลูกจ้าง ตัวแทน หรือบุคคลอื่นใดที่ได้รับมอบหมายจากผู้ขาย/ผู้รับจ้าง ต้องเก็บรักษาข้อมูลและรายละเอียดต่าง ๆ ที่เกิดขึ้นจากการทำงานตามสัญญาหรือข้อตกลง ทั้งใน

- ระหว่างระยะเวลาในสัญญาและหลังสิ้นสุดสัญญาไว้เป็นความลับ ไม่มอบหรือเปิดเผยข้อมูลแก่ผู้อื่น โดยไม่ได้รับอนุญาตจาก สป.กค. และ/หรือเอาไปเพื่อประโยชน์อื่นใดแก่ตนเอง โดยหากมีการนำไปใช้หรือเปิดเผย หรือเผยแพร่ ข้อมูลดังกล่าวอันจะก่อให้เกิดความเสียหายแก่ สป.กค. ผู้ขาย/ผู้รับจ้าง จะต้องรับผิดชอบต่อการกระทำดังกล่าว และ สป.กค. มีสิทธิดำเนินการตามกฎหมายกับผู้ขาย/ผู้รับจ้าง
- ๑๔.๘ ข้อมูลที่เป็นความลับทั้งที่อยู่ในรูปของเอกสาร โปรแกรมคอมพิวเตอร์ ข้อมูลอิเล็กทรอนิกส์ที่บันทึกลงในสื่อต่าง ๆ หรือสิ่งอื่นใดที่เป็นรูปธรรมที่ สป.กค. เปิดเผยแก่ผู้ขาย/ผู้รับจ้าง ผู้ขาย/ผู้รับจ้าง ต้องทำเครื่องหมาย “ลับ” ไว้กับสิ่งนั้นอย่างชัดเจน ส่วนการเปิดเผยข้อมูลที่เป็นความลับด้วยวาจาหรือด้วยวิธีการอื่นใดที่ไม่เป็นรูปธรรม ซึ่ง สป.กค. ได้แจ้งให้ผู้ขาย/ผู้รับจ้าง ทราบ ณ เวลาเปิดเผยนั้นว่าเป็นการเปิดเผยข้อมูลที่เป็นความลับ ผู้ขาย/ผู้รับจ้าง จะต้องสรุปสาระสำคัญของข้อมูลที่เป็นความลับดังกล่าวเป็นลายลักษณ์อักษร พร้อมทั้งทำเครื่องหมาย “ลับ” หรือเครื่องหมายที่มีความหมายทำนองเดียวกันนี้ไว้กับข้อความสรุปนั้นอย่างชัดเจน พร้อมทั้งส่งมอบข้อความสรุปดังกล่าวให้แก่ สป.กค. ภายใน ๑๕ วัน นับตั้งแต่วันที่ สป.กค. เปิดเผยข้อมูลที่เป็นความลับนั้น
- ๑๔.๙ ผู้ขาย/ผู้รับจ้างตกลงจะเก็บรักษาข้อมูลที่เป็นความลับที่ สป.กค. ได้เปิดเผยแก่ผู้ขาย/ผู้รับจ้าง รวมถึงจะจัดให้มีมาตรการที่เหมาะสมตามมาตรฐานของการรักษาความมั่นคงปลอดภัยของข้อมูลที่เป็นความลับนั้นเพื่อป้องกันมิให้บุคคลภายนอกเข้าถึงข้อมูลที่เป็นความลับได้

๑๔. หน่วยงานผู้รับผิดชอบดำเนินการ

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง

๑๕. ข้อสงวนสิทธิในการยื่นข้อเสนอและอื่น ๆ

- ๑๕.๑ การจัดซื้อหรือการจัดจ้างครั้งนี้จะมีการลงนามในสัญญาหรือข้อตกลงเป็นหนังสือได้ต่อเมื่อพระราชบัญญัติงบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. ๒๕๗๐ มีผลใช้บังคับ และได้รับจัดสรรงบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. ๒๕๗๐ จากสำนักงบประมาณแล้ว สำหรับกรณีที่ไม่ได้รับการจัดสรรงบประมาณรายจ่ายเพื่อการจัดหาในครั้งนี้ ส่วนราชการสามารถยกเลิกจัดหาได้
- ๑๕.๒ หากข้อความใดในขอบเขตของงานมีความขัดแย้งกัน ให้ยึดถือตามข้อกำหนดที่เป็นประโยชน์กับสำนักงานปลัดกระทรวงการคลัง

ท่านสามารถเสนอแนะวิจารณ์ หรือแสดงความคิดเห็นโดยเปิดเผย

๑. ทางไปรษณีย์ ส่ง คณะกรรมการจัดทำร่างขอบเขตของงานหรือรายละเอียดคุณลักษณะเฉพาะของพัสดุที่จะซื้อ
และกำหนดราคากลาง โครงการทดแทนและเพิ่มประสิทธิภาพระบบรักษาความมั่นคง
ปลอดภัยระบบคอมพิวเตอร์และระบบเครือข่าย
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง
ถนนพระรามที่ ๖ แขวงพญาไท เขตพญาไท กรุงเทพมหานคร ๑๐๕๐๐

๒. ทาง e-Mail tor-mof-sec๗๐@mof.go.th

๓. ทางโทรศัพท์ หมายเลข ๐ ๒๑๒๖ ๕๙๐๐ ต่อ ๓๐๓๐๐, ๓๐๓๐๓

ทั้งนี้ โปรดแจ้ง ชื่อ ที่อยู่ พร้อมหมายเลขโทรศัพท์ติดต่อกลับด้วย

แบบรูปรายการหรือคุณลักษณะเฉพาะ

๑. ข้อกำหนดและเงื่อนไขในการยื่นข้อเสนอ

ผู้ยื่นข้อเสนอจะต้องปฏิบัติตามข้อกำหนดและเงื่อนไขในการยื่นข้อเสนอให้ครบถ้วนถูกต้อง รวมทั้งต้องปฏิบัติตามดังต่อไปนี้

- ๑.๑ ผู้ยื่นข้อเสนอต้องเป็นผู้ได้รับการแต่งตั้งให้เป็นตัวแทนจำหน่ายอุปกรณ์ที่เสนอจากผู้ผลิต หรือสาขาของผู้ผลิต หรือตัวแทนจำหน่ายในประเทศไทย และได้รับการแต่งตั้งให้การสนับสนุนและรับรองการให้บริการหลังการขาย จากเจ้าของผลิตภัณฑ์หรือสาขาของเจ้าของผลิตภัณฑ์ในประเทศไทย โดยเป็นหนังสือที่แต่งตั้งที่ออกให้สำหรับ โครงการที่เสนอโดยเฉพาะ ยื่นมาพร้อมกับการยื่นข้อเสนอของอุปกรณ์ดังต่อไปนี้
 - ๑) อุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall)
 - ๒) ระบบบริหารจัดการอุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall)
 - ๓) ระบบป้องกันการโจมตีระบบเครือข่ายหรือบริการ (Web Application Firewall และ DDoS Protection)
- ๑.๒ อุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall) และ ระบบบริหารจัดการอุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall) แต่ละชุด ต้องเป็นผลิตภัณฑ์ต่างยี่ห้อกัน
- ๑.๓ ผู้ยื่นข้อเสนอต้องระบุยี่ห้อ หรือ รุ่น (Model) อุปกรณ์หรือระบบที่เสนอทุกรายการในเอกสารรายการ พัสตุ หรือเอกสารข้อกำหนดทางเทคนิค (Technical Proposal) ให้ชัดเจน พร้อมแคตตาล็อกของอุปกรณ์ ที่เสนอ โดยต้องทำตารางเปรียบเทียบคุณลักษณะเฉพาะพร้อมอ้างอิงแคตตาล็อก มาพร้อมการยื่นข้อเสนอ
- ๑.๔ อุปกรณ์ทุกชิ้นที่เสนอต้องเป็นของแท้ ของใหม่ไม่เคยใช้งานมาก่อน ไม่เป็นของเก่าเก็บ ต้องอยู่ในสภาพที่ใช้งานได้ทันทีและต้องมีคุณสมบัติเฉพาะตรงตามที่กำหนดไว้ หรือดีกว่าข้อกำหนด

๒. คุณลักษณะเฉพาะของอุปกรณ์หรือระบบของโครงการทดแทนและเพิ่มประสิทธิภาพระบบรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์และระบบเครือข่าย ประกอบด้วยรายละเอียดดังต่อไปนี้

- ๒.๑ อุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall) จำนวน ๒ ชุด (๔ เครื่อง) สำหรับติดตั้งที่ศูนย์คอมพิวเตอร์ จังหวัดปทุมธานี และศูนย์คอมพิวเตอร์ถนนพิบูลสงคราม หรือศูนย์คอมพิวเตอร์ถนนพระราม ๖ โดยแต่ละชุดมีคุณลักษณะเฉพาะอย่างน้อยดังต่อไปนี้
 - ๒.๑.๑ อุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall) ชุดที่ ๑ จำนวน ๒ เครื่อง ที่ทำงานรวมกันในลักษณะ Redundant Firewall หรือดีกว่า แต่ละเครื่องมีคุณลักษณะเฉพาะอย่างน้อยดังต่อไปนี้
 - ๒.๑.๑.๑ เป็นอุปกรณ์ Firewall ชนิด Next Generation Firewall แบบ Appliance
 - ๒.๑.๑.๒ สามารถทำงานแบบ Active-Standby หรือ Active/Passive หรือ HA clustering ที่สามารถทำ High Availability หรือ Failover ได้
 - ๒.๑.๑.๓ มี Stateful Throughput หรือ Firewall Throughput ไม่น้อยกว่า ๓๕๐ Gbps หรือมี Application Firewall Throughput (appmix) ไม่น้อยกว่า ๕๐ Gbps หรือมี NGFW Throughput ไม่น้อยกว่า ๑๓๐ Gbps หรือมี Threat Prevention throughput (appmix) ไม่น้อยกว่า 35 Gbps
 - ๒.๑.๑.๔ มีช่องสำหรับรองรับการเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ ๑๐ Gbps (SFP+) จำนวนไม่น้อยกว่า ๘ ช่อง เสนอพร้อม Transceiver แบบ ๑๐GBASE-SR จำนวนไม่น้อยกว่า ๘ โมดูล

- ๒.๑.๑.๕ มีช่องสำหรับรองรับการเชื่อมต่อระบบเครือข่าย (Network Interface) ๒๕ Gbps (SFP๒๘) จำนวนไม่น้อยกว่า ๔ ช่อง เสนอพร้อม Transceiver แบบ ๒๕ GBASE-SR จำนวนไม่น้อยกว่า ๔ โมดูล
- ๒.๑.๑.๖ มีช่องสำหรับรองรับการเชื่อมต่อระบบเครือข่าย (Network Interface) ๔๐/๑๐๐ Gbps (QSFP๒๘) จำนวนไม่น้อยกว่า ๔ ช่อง เสนอพร้อม Transceiver แบบ ๑๐๐GBASE-SRBD หรือ ๑๐๐GBASE-BIDI หรือ QSFP-๑๐๐G-SRBD จำนวนไม่น้อยกว่า ๒ โมดูล
- ๒.๑.๑.๗ มีช่องเชื่อมต่อ HA แบบ ๑๐ Gigabit หรือดีกว่า ไม่น้อยกว่า ๑ ช่อง หรือสามารถกำหนด Network Interface ให้ทำหน้าที่เป็น HA Heartbeat Interface ได้ และต้องเสนออุปกรณ์มาพร้อมสำหรับการทำ HA หรือ Stacked management
- ๒.๑.๑.๘ มีช่องเชื่อมต่อสำหรับบริหารจัดการโดยเฉพาะ (Out of Band Management หรือ Management) ไม่น้อยกว่า ๑ ช่อง
- ๒.๑.๑.๙ สามารถตรวจสอบและป้องกันการบุกรุกรูปแบบต่าง ๆ อย่างน้อยดังนี้ Syn Flood, UDP Flood, ICMP Flood, IP Address Spoofing, Port Scan, DoS or DDoS, Teardrop Attack, Land Attack, IP Fragment, ICMP Fragment ได้
- ๒.๑.๑.๑๐ สามารถทำการกำหนด IP Address และ Service Port แบบ Network Address Translation (NAT) และ Port Address Translation (PAT) ได้
- ๒.๑.๑.๑๑ สามารถทำงานลักษณะ Transparent Mode ได้
- ๒.๑.๑.๑๒ สามารถ Routing แบบ Static, Dynamic Routing ได้
- ๒.๑.๑.๑๓ สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS หรือ SSH ได้เป็นอย่างน้อย
- ๒.๑.๑.๑๔ สามารถเก็บและส่งรายละเอียดและตรวจสอบการใช้งาน (Logging/Monitoring) ในรูปแบบ Syslog ได้
- ๒.๑.๑.๑๕ สามารถตรวจจับและควบคุม Application, User, Content ได้
- ๒.๑.๑.๑๖ สามารถใช้งานตามมาตรฐานทั้ง IPv๔ และ IPv๖ ได้
- ๒.๑.๑.๑๗ มี Power Supply แบบ Redundant หรือ Hot Swap จำนวน ๒ หน่วย
- ๒.๑.๑.๑๘ มีลิขสิทธิ์สำหรับการใช้งาน Threat Protection และ Intrusion Prevention System (IPS) จำนวนไม่น้อยกว่า ๒ ปี
- ๒.๑.๑.๑๙ รองรับการทำ Software-Defined Wan (SD-WAN) โดยตรวจสอบ WAN SLA ตาม latency, jitter และ packet loss และรองรับการทำ Forward Error Correction (FEC) สำหรับการรับส่งข้อมูลผ่าน SD-WAN VPN Overlay หรือ Packet Duplication ได้ด้วยอุปกรณ์ Firewall ที่เสนอ
- ๒.๑.๑.๒๐ ผลิตภัณฑ์ที่นำเสนอ จะต้องมีประสิทธิภาพในการทำงานเป็นอย่างดี โดยได้รับการจัดลำดับอยู่ใน Leaders ในการจัดลำดับของ Gartner Magic Quadrant เรื่องของ Hybrid Mesh Firewalls ปี ๒๐๒๕ เป็นอย่างน้อย
- ๒.๑.๒ ระบบบริหารจัดการอุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall) ชุดที่ ๑ จำนวน ๑ ระบบ มีคุณลักษณะเฉพาะอย่างน้อยดังต่อไปนี้
 - ๒.๑.๒.๑ สามารถเสนอระบบเป็น Hardware Appliance หรือ Virtual Appliance ได้
 - กรณีเป็น Hardware Appliance ต้องมี Power Supply แบบ Redundant หรือ Hot Swap จำนวน ๒ หน่วย และมีช่องเชื่อมต่อระบบเครือข่าย แบบ ๑/๑๐GbE RJ๔๕ หรือดีกว่า จำนวน ไม่น้อยกว่า ๒ ช่อง

- กรณีเป็น Virtual Appliance ต้องสามารถทำงานร่วมกับระบบเครื่องคอมพิวเตอร์เสมือน (Hypervisor) รุ่น VMware VSphere ของสำนักงานปลัดกระทรวงการคลังได้
- ๒.๑.๒.๒ สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS หรือ SSH ได้เป็นอย่างน้อย
- ๒.๑.๒.๓ สามารถบริหารจัดการอุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall) ได้อย่างน้อย ๒ เครื่อง
- ๒.๑.๒.๔ สามารถบริหารจัดการ Policy, Object, Backup configuration รวมถึง Update firmware หรือ software ของ Firewall ที่ถูกบริหารได้เป็นอย่างน้อย
- ๒.๑.๒.๕ สามารถตรวจสอบสถานะของ Firewall ที่ถูกบริหารได้
- ๒.๑.๒.๖ สามารถเป็นศูนย์กลางกระจาย signature update ให้กับอุปกรณ์ Firewall ที่ถูกบริหารได้
- ๒.๑.๒.๗ สามารถพิสูจน์ตัวตนของผู้ดูแลระบบด้วย Local หรือ LDAP หรือ RADIUS ได้
- ๒.๑.๒.๘ สามารถกำหนดสิทธิให้ผู้ดูแลระบบได้หลายระดับตาม Role หรือตาม Profile ของผู้ดูแลระบบ
- ๒.๑.๒.๙ รองรับการทำงานร่วมกับระบบ Software Defined Networking (SDN) โดยใช้ Connector หรือ Plugin หรือ Device package ได้
- ๒.๑.๒.๑๐ เป็นระบบบริหารจัดการ Next Generation Firewall ภายใต้เครื่องหมายการค้าเดียวกันกับอุปกรณ์ Next Generation Firewall ชุดที่ ๑
- ๒.๑.๓ อุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall) ชุดที่ ๒ จำนวน ๒ เครื่อง ที่ทำงานรวมกันในลักษณะ Redundant Firewall หรือดีกว่า แต่ละเครื่องมีคุณลักษณะเฉพาะอย่างน้อยดังต่อไปนี้
 - ๒.๑.๓.๑ เป็นอุปกรณ์ Firewall ชนิด Next Generation Firewall แบบ Appliance
 - ๒.๑.๓.๒ สามารถทำงานแบบ Active-Standby หรือ Active/Passive หรือ HA clustering ที่สามารถทำ High Availability หรือ Failover ได้
 - ๒.๑.๓.๓ มี Stateful Throughput หรือ Firewall Throughput ไม่น้อยกว่า ๓๕๐ Gbps หรือมี Application Firewall Throughput (appmix) ไม่น้อยกว่า ๕๐ Gbps หรือมี NGFW Throughput ไม่น้อยกว่า ๑๓๐ Gbps หรือมี Threat Prevention throughput (appmix) ไม่น้อยกว่า 35 Gbps
 - ๒.๑.๓.๔ มีช่องสำหรับรองรับการเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ ๑๐ Gbps (SFP+) จำนวนไม่น้อยกว่า ๘ ช่อง เสนอพร้อม Transceiver แบบ ๑๐GBASE-SR จำนวนไม่น้อยกว่า ๘ โมดูล
 - ๒.๑.๓.๕ มีช่องสำหรับรองรับการเชื่อมต่อระบบเครือข่าย (Network Interface) ๒๕ Gbps (SFP๒๘) จำนวนไม่น้อยกว่า ๔ ช่อง เสนอพร้อม Transceiver แบบ ๒๕ GBASE-SR จำนวนไม่น้อยกว่า ๔ โมดูล
 - ๒.๑.๓.๖ มีช่องสำหรับรองรับการเชื่อมต่อระบบเครือข่าย (Network Interface) ๔๐/๑๐๐ Gbps (QSFP๒๘) จำนวนไม่น้อยกว่า ๔ ช่อง เสนอพร้อม Transceiver แบบ ๑๐๐ GBASE-SRBD หรือ ๑๐๐GBASE-BIDI หรือ QSFP-๑๐๐G-SRBD จำนวนไม่น้อยกว่า ๒ โมดูล

- ๒.๑.๓.๗ มีช่องเชื่อมต่อ HA แบบ ๑๐ Gigabit หรือดีกว่า ไม่น้อยกว่า ๑ ช่อง หรือสามารถกำหนด Network Interface ให้ทำหน้าที่เป็น HA Heartbeat Interface ได้ และต้องเสนออุปกรณ์มาพร้อมสำหรับการทำ HA หรือ Stacked management
 - ๒.๑.๓.๘ มีช่องเชื่อมต่อสำหรับบริหารจัดการโดยเฉพาะ (Out of Band Management หรือ Management) ไม่น้อยกว่า ๑ ช่อง
 - ๒.๑.๓.๙ สามารถตรวจสอบและป้องกันการบุกรุกรูปแบบต่าง ๆ อย่างน้อยดังนี้ Syn Flood, UDP Flood, ICMP Flood, IP Address Spoofing, Port Scan, DoS or DDoS, Teardrop Attack, Land Attack, IP Fragment, ICMP Fragment ได้
 - ๒.๑.๓.๑๐ สามารถทำการกำหนด IP Address และ Service Port แบบ Network Address Translation (NAT) และ Port Address Translation (PAT) ได้
 - ๒.๑.๓.๑๑ สามารถทำงานลักษณะ Transparent Mode ได้
 - ๒.๑.๓.๑๒ สามารถ Routing แบบ Static, Dynamic Routing ได้
 - ๒.๑.๓.๑๓ สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS หรือ SSH ได้เป็นอย่างดี
 - ๒.๑.๓.๑๔ สามารถเก็บและส่งรายละเอียดและตรวจสอบการใช้งาน (Logging/Monitoring) ในรูปแบบ Syslog ได้
 - ๒.๑.๓.๑๕ สามารถตรวจจับและควบคุม Application, User, Content ได้
 - ๒.๑.๓.๑๖ สามารถใช้งานตามมาตรฐานทั้ง IPv๔ และ IPv๖ ได้
 - ๒.๑.๓.๑๗ มี Power Supply แบบ Redundant หรือ Hot Swap จำนวน ๒ หน่วย
 - ๒.๑.๓.๑๘ มีลิขสิทธิ์สำหรับการใช้งาน Threat Protection และ Intrusion Prevention System (IPS) จำนวนไม่น้อยกว่า ๒ ปี
 - ๒.๑.๓.๑๙ รองรับการทำ Software-Defined Wan (SD-WAN) โดยตรวจสอบ WAN SLA ตาม latency, jitter และ packet loss และรองรับการทำ Forward Error Correction (FEC) สำหรับการรับส่งข้อมูลผ่าน SD-WAN VPN Overlay หรือ Packet Duplication ได้ ด้วยอุปกรณ์ Firewall ที่เสนอ
 - ๒.๑.๓.๒๐ ผลิตภัณฑ์ที่นำเสนอ จะต้องมีประสิทธิภาพในการทำงานเป็นอย่างดี โดยได้รับการจัดลำดับอยู่ใน Leaders ในการจัดลำดับของ Gartner Magic Quadrant เรื่องของ Hybrid Mesh Firewalls ปี ๒๐๒๕ เป็นอย่างน้อย
- ๒.๑.๑ ระบบบริหารจัดการอุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall) ชุดที่ ๒ จำนวน ๑ ระบบ มีคุณลักษณะเฉพาะอย่างน้อยดังต่อไปนี้
- ๒.๑.๑.๑ สามารถเสนอระบบเป็น Hardware Appliance หรือ Virtual Appliance ได้
 - กรณีเป็น Hardware Appliance ต้องมี Power Supply แบบ Redundant หรือ Hot Swap จำนวน ๒ หน่วย และมีช่องเชื่อมต่อระบบเครือข่าย แบบ ๑/๑๐GbE RJ๔๕ หรือดีกว่า จำนวน ไม่น้อยกว่า ๒ ช่อง
 - กรณีเป็น Virtual Appliance ต้องสามารถทำงานร่วมกับระบบเครื่องคอมพิวเตอร์เสมือน (Hypervisor) รุ่น VMware VSphere ของสำนักงานปลัดกระทรวงการคลังได้
 - ๒.๑.๑.๒ สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS หรือ SSH ได้เป็นอย่างดี
 - ๒.๑.๑.๓ สามารถบริหารจัดการอุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall) ได้อย่างน้อย ๒ เครื่อง

- ๒.๑.๑.๔ สามารถบริหารจัดการ Policy, Object, Backup configuration รวมถึง Update firmware หรือ software ของ Firewall ที่ถูกบริหารได้เป็นอย่างดี
 - ๒.๑.๑.๕ สามารถตรวจสอบสถานะของ Firewall ที่ถูกบริหารได้
 - ๒.๑.๑.๖ สามารถเป็นศูนย์กลางกระจาย signature update ให้กับอุปกรณ์ Firewall ที่ถูกบริหารได้
 - ๒.๑.๑.๗ สามารถพิสูจน์ตัวตนของผู้ดูแลระบบด้วย Local หรือ LDAP หรือ RADIUS ได้
 - ๒.๑.๑.๘ สามารถกำหนดสิทธิให้ผู้ดูแลระบบได้หลายระดับตาม Role หรือตาม Profile ของผู้ดูแลระบบ
 - ๒.๑.๑.๙ รองรับการทำงานร่วมกับระบบ Software Defined Networking (SDN) โดยใช้ Connector หรือ Plugin หรือ Device package ได้
 - ๒.๑.๑.๑๐ เป็นระบบบริหารจัดการ Next Generation Firewall ภายใต้เครื่องหมายการค้าเดียวกันกับอุปกรณ์ Next Generation Firewall ชุดที่ ๒
- ๒.๒ ระบบป้องกันการโจมตีระบบเครือข่ายหรือบริการ (Web Application Firewall และ DDoS Protection) จำนวน ๑ ระบบ โดยมีคุณลักษณะเฉพาะอย่างน้อยดังต่อไปนี้
- ๒.๒.๑ บริการป้องกันการโจมตีระบบเครือข่ายหรือบริการ มีคุณลักษณะเฉพาะอย่างน้อยดังต่อไปนี้
 - ๒.๒.๑.๑ เป็นระบบที่ให้บริการ Web Application Firewall (WAF) และ DDoS Protection รวมถึงบริการ Content Delivery Network (CDN) ในรูปแบบ Global Cloud Platform เพื่อป้องกันการโจมตี Web Application และ DDoS ไปยังเครือข่ายหรือบริการโดยเฉพาะ โดยมีลักษณะเป็นโครงข่าย Globally Distributed Network และสามารถป้องกันการโจมตีอัตโนมัติได้ตลอด ๒๔ ชั่วโมง ไม่จำกัดจำนวนครั้ง และขนาดของการโจมตี
 - ๒.๒.๑.๒ ผู้ให้บริการต้องมี node หรือ Point of Presence (PoP) จำนวนไม่น้อยกว่า ๑๒๐ จุดทั่วโลก หรือมี Scrubbing Center ไม่น้อยกว่า ๖๐ แห่งทั่วโลก และมีจำนวนไม่น้อยกว่า ๑ จุด ในประเทศไทยที่มีการเชื่อมต่อกับโครงข่ายอินเทอร์เน็ตระหว่างประเทศ (International Internet Gateway: IIG)
 - ๒.๒.๑.๓ ผู้ให้บริการต้องมีบริการ authoritative DNS services สำหรับโดเมนสาธารณะ และต้องมี Host Domains ทุกภูมิภาคทั่วโลก โดยต้องมี node ในประเทศไทย ไม่น้อยกว่า ๑ จุด
 - ๒.๒.๑.๔ Scrubbing Center หรือ Point of Presence (PoP) ที่อยู่ในประเทศไทยจะต้องมีความสามารถในการป้องกัน DDoS หรือ Web Application Firewall (WAF) หรือ Content Delivery Network (CDN) ได้
 - ๒.๒.๑.๕ มีระยะเวลาการให้บริการป้องกันการโจมตีระบบเครือข่ายหรือบริการไม่น้อยกว่า ๒ ปี
 - ๒.๒.๑.๖ สามารถป้องกันการโจมตีระบบเครือข่ายจำนวน ๓ Domain เป็นอย่างน้อย
 - ๒.๒.๑.๗ เป็นผลิตภัณฑ์ที่จัดอยู่ในกลุ่ม Leader ของ The Forrester Wave Q๑ ๒๐๒๕ ในหัวข้อ Web Application Firewall Solution เป็นอย่างน้อย
 - ๒.๒.๒ ความสามารถในการป้องกันการโจมตีประเภท DDoS (DDoS Protections) โดยมี คุณลักษณะเฉพาะอย่างน้อยดังต่อไปนี้
 - ๒.๒.๒.๑ สามารถป้องกันการโจมตีจากในระดับเครือข่าย (DDoS attack) ที่ระดับ Network layer ๓, ๔ และ ๗ ได้

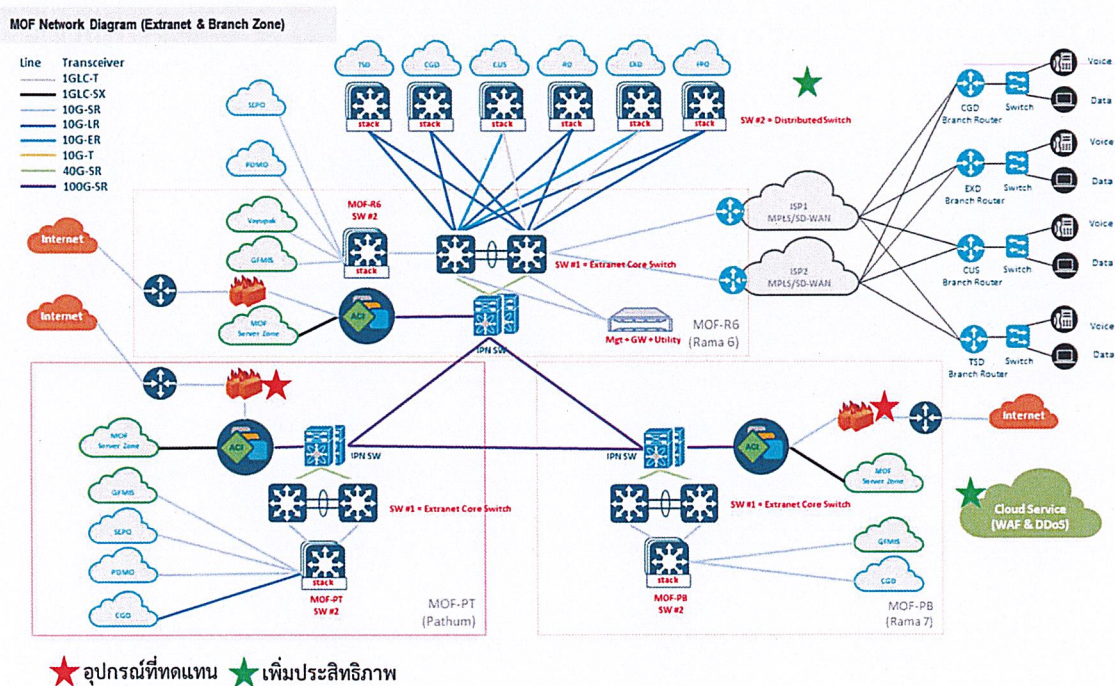
- ๒.๒.๒.๒ ผู้ให้บริการต้องให้บริการป้องกันการโจมตีในระดับเครือข่าย (DDoS attack) แบบไม่จำกัดจำนวนครั้ง
- ๒.๒.๒.๓ ผู้ให้บริการต้องมีเครือข่ายที่มีความสามารถในการป้องกันการโจมตีจากประเภท DDoS ขนาด ๑๓ Tbps เป็นอย่างน้อย
- ๒.๒.๒.๔ รองรับการทำ Adaptive DDoS Protection โดยสามารถทำการตรวจสอบ Traffic Pattern และป้องกันการโจมตี DDoS แบบไม่จำกัดจำนวนครั้งและขนาดการโจมตี โดยไม่มีค่าใช้จ่ายเพิ่มเติม โดยมีคุณสมบัติเทียบเท่าดังนี้
 - Adaptive DDoS Protection for Origins
 - Adaptive DDoS Protection for User-Agents
 - Adaptive DDoS Protection for Locations
- ๒.๒.๓ มีความสามารถในการป้องกันเว็บแอปพลิเคชัน (Web Security Functions) โดยมีคุณลักษณะเฉพาะอย่างน้อยดังต่อไปนี้
 - ๒.๒.๓.๑ สามารถป้องกันการโจมตีผ่านทาง Website ตามเงื่อนไข ดังนี้
 - Broken Access Control
 - Cryptographic Failures
 - Injection
 - Insecure Design
 - Security Misconfiguration
 - Vulnerable and Outdated Component
 - Identification and Authentication Failures
 - Software and Data Integrity Failures
 - Security Logging and Monitoring Failures
 - Server-Side Request Forgery
 - ๒.๒.๓.๒ สามารถกำหนดค่าของ Web Application Firewall (WAF) ได้แบบไม่น้อยกว่า ๑,๐๐๐ Custom WAF rules
 - ๒.๒.๓.๓ สามารถกำหนดค่า IP Firewall ด้วยเงื่อนไข Source IP address, Source IP address range, Autonomous System Number (ASN) และประเทศได้
 - ๒.๒.๓.๔ สามารถทำการตรวจสอบการออกใบรับรอง SSL โดยสามารถแจ้งเตือนเมื่อมีผู้ทำการออกใบรับรองภายใต้ชื่อโดเมนเดียวกันกับของกระทรวงการคลัง
 - ๒.๒.๓.๕ สามารถตรวจจับและระบุการใช้งาน Javascript ได้ ด้วยเงื่อนไขว่ามีการใช้งาน Javascript นั้นๆ ครั้งแรกและครั้งสุดท้ายเมื่อใด และทำการแจ้งเตือนได้ ดังนี้
 - มีการเรียกใช้งาน Javascript ใหม่เกิดขึ้น
 - Javascript ที่ใช้งานอยู่มีการเปลี่ยนแปลง (Page attribution)
 - มีการเรียกใช้งาน Javascript จากโดเมนใหม่
 - ๒.๒.๓.๖ ระบบต้องมีความสามารถในการตรวจสอบเนื้อหาภายใน Request Body/Payload เพื่อตรวจจับและป้องกันการโจมตีที่แฝงมากับข้อมูลได้
 - ๒.๒.๓.๗ ระบบต้องมีความสามารถในระดับ Account-Level WAF ในการกำหนด WAF Custom Rule กับแต่ละ Zone ภายใต้บัญชีเดียวกันได้
 - ๒.๒.๓.๘ รองรับการตรวจสอบ Sensitive Data Detection ได้เป็นอย่างดี

- ๒.๒.๓.๙ ระบบต้องมีความสามารถ Managed Lists ในการจัดกลุ่มข้อมูล โดยสามารถใช้งานร่วมกับ ๒๘ Threat Intelligence ได้ ดังนี้
- Open Proxies
 - Anonymizer
 - VPNs
 - Malware
 - Botnet, Command and Control Server
- ๒.๒.๓.๑๐ รองรับการทำ Bot Score ในรูปแบบตัวเลข เพื่อแสดงระดับความเป็นไปได้ว่า Request ดังกล่าวเกิดจาก Human หรือ Automated เพื่อนำค่าดังกล่าวมาใช้กำหนด Security Policy เช่น Allow, Block, Challenge หรือ Rate Limit ได้เป็นอย่างดี หรือ รองรับการทำการวิเคราะห์โดย Client Interrogation, Behavior Analysis และ Machine Learning ร่วมกันได้
- ๒.๒.๔ ความสามารถในการเพิ่มประสิทธิภาพเว็บแอปพลิเคชัน (Content Delivery Network : CDN & Optimization) โดยมีคุณลักษณะเฉพาะอย่างน้อยดังต่อไปนี้
- ๒.๒.๔.๑ สามารถทำการลบ Cache ทั้งหมดได้ทันที หรือกำหนดเงื่อนไขการลบ Cache เฉพาะ URL, Host name และ Tag ได้
- ๒.๒.๔.๒ สามารถใช้ API ในการอัปเดต Cache ในกรณีที่มีการอัปเดต Content ใหม่
- ๒.๒.๔.๓ บริการต้องรองรับการใช้ Bandwidth Consumption ได้ไม่น้อยกว่า ๕ TB ต่อเดือน
- ๒.๒.๔.๔ มีระบบ Always-on ที่สามารถทำการแสดง Static content ในกรณีที่ Server ดันทางไม่สามารถใช้งานได้
- ๒.๒.๔.๕ สามารถลด Latency time ให้กับ Dynamic content และแสดงผลในรูปแบบของประสิทธิภาพที่เพิ่มขึ้น และเวลาที่ตอบสนองได้
- ๒.๒.๔.๖ ระบบต้องมีความสามารถ Rate Limiting ในการจำกัดจำนวน Request ต่อ IP/Session ภายในช่วงเวลาที่กำหนดได้
- ๒.๒.๕ ความสามารถในการแสดงรายงาน (Dashboard Functions) โดยมีคุณลักษณะเฉพาะอย่างน้อยดังต่อไปนี้
- ๒.๒.๕.๑ มี Dashboard แสดงรายงานประเภท Security แบบ Real-time หรือ Near Real-time โดยสามารถแสดงถึงข้อมูลแหล่งที่มาของการโจมตี เช่น IP Address, Browser, Country และ Autonomous System Number (ASN) ได้อย่างน้อย ๓๐ วัน หรือเทียบเท่า
- ๒.๒.๕.๒ มี Dashboard แสดงรายงานประเภท Analytic แบบ Real-time หรือ Near Real-time โดยมีรายละเอียด Total Requests, Cached Request, Bandwidth Saved, Threat Sources, Top Threat Origin และ Top Traffic Origin ได้ อย่างน้อย ๓๐ วัน หรือเทียบเท่า
- ๒.๒.๕.๓ มี Dashboard ที่ช่วยผู้ใช้วิเคราะห์ Traffic ว่ามีความเป็นมนุษย์หรือมีความเป็นบอท ด้วยวิธีการ Machine learning หรือ Heuristic ได้
- ๒.๒.๕.๔ สามารถแสดง Activity Log การวิเคราะห์ Event ที่เกิดขึ้นได้
- ๒.๒.๕.๕ รองรับการส่ง Raw log ผ่านทาง Logpull REST API หรือ Logpush ได้

- ๒.๒.๕.๖ สามารถกำหนดสิทธิผู้ใช้งาน (Role-based access control) และยืนยันตัวตนด้วยวิธี Two-Factor Authentication ได้
- ๒.๒.๕.๗ มี Storage โดยสามารถเชื่อมต่อไปยัง Dashboard ที่ใช้งานเพื่อสามารถทำการจัดเก็บ log โดยมีขนาดรวมไม่น้อยกว่า ๑ TB
- ๒.๒.๕.๘ ระบบต้องมีความสามารถ Advanced Certificate Manager ในการออกและจัดการใบรับรอง SSL/TLS แบบกำหนดเองได้
- ๒.๒.๕.๙ สามารถแสดงการแจ้งเตือนไปยัง Email ที่ระบุไว้ได้ในกรณีที่ เว็บไซต์ของกระทรวงการคลังไม่สามารถใช้งานได้ โดยสามารถรองรับการตั้งค่าในการ Monitor ได้ในระดับ Type, Method, Port และ Path รวมถึงสามารถระบุ Expected codes ที่ต้องการได้

๓. แบบร่างแผนผังของระบบเครือข่ายสำหรับใช้ประกอบการออกแบบหรือการติดตั้งอุปกรณ์หรือระบบของโครงการทดแทนและเพิ่มประสิทธิภาพระบบรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์และระบบเครือข่าย

๓.๑ แบบร่าง System Diagram Architecture ที่เป็นการแสดงความต้องการเบื้องต้นสำหรับให้ผู้ชนะการประกวดราคาใช้ประกอบการพิจารณาปรับปรุงหรือนำไปออกแบบให้เหมาะสมกับอุปกรณ์ที่เสนอเพื่อให้ระบบสามารถใช้งานได้โดยมีประสิทธิภาพ



แผนภาพแสดง แนวทางการเชื่อมโยงระบบเครือข่ายสื่อสารข้อมูลกลางกระทรวงการคลัง

รายละเอียดการดำเนินงาน การติดตั้งและการทดสอบ

๑. การติดตั้งและสถานที่ติดตั้งอุปกรณ์ระบบคอมพิวเตอร์และเครือข่ายสื่อสาร

- ๑.๑ ต้องดำเนินการส่งมอบอุปกรณ์และติดตั้งพร้อมเดินสายสัญญาณหรือระบบไฟฟ้าในโครงการทดแทน และเพิ่มประสิทธิภาพระบบรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์และระบบเครือข่าย
- ๑.๒ ต้องส่งมอบอุปกรณ์หรืองานทั้งหมดตามโครงการ ณ อาคาร ๑๕๐ ปี กระทรวงการคลัง และนำไปติดตั้งที่อาคาร ๑๕๐ ปี กระทรวงการคลัง หรือศูนย์คอมพิวเตอร์กระทรวงการคลังที่เกี่ยวข้อง หรือตามที่คณะกรรมการตรวจรับพัสดุกำหนด
- ๑.๓ การเดินสายสัญญาณหรือสายไฟฟ้า (Cabling) ณ สถานที่ติดตั้ง ผู้ชนะการประกวดราคาต้องจัดหาวาง หรือท่อ หรือเฟล็กซ์ หรืออุปกรณ์อื่น ๆ ตามความจำเป็น สำหรับใช้ติดตั้งสายสัญญาณหรือสายไฟฟ้าตามโครงการและจัดให้เป็นระเบียบเรียบร้อย หรือเป็นไปตามมาตรฐานสากล
- ๑.๔ ผู้ชนะการประกวดราคาต้องติดตั้งและต่อเชื่อมระบบเครือข่ายตามการออกแบบที่คณะกรรมการตรวจรับพัสดุพิจารณา รวมทั้งต้อง Configuration และทดสอบให้ระบบทำงานได้ตามที่กำหนด หรือออกแบบ

๒. การบริหารจัดการและเงื่อนไขในการดำเนินงาน

- ๒.๑ ผู้ชนะการประกวดราคาต้องเสนอโครงสร้างการบริหารโครงการและแผนการดำเนินงาน เพื่อให้คณะกรรมการตรวจรับพัสดุพิจารณาก่อนดำเนินงาน โดยแผนการดำเนินงานต้องระบุความรับผิดชอบในส่วนของผู้ชนะการประกวดราคา หรือบริษัทเจ้าของผลิตภัณฑ์ หรือส่วนของศูนย์เทคโนโลยีสารสนเทศ และการสื่อสาร สำนักงานปลัดกระทรวงการคลัง
- ๒.๒ ผู้ชนะการประกวดราคา ต้องจัดทำแผนการดำเนินงานหลัก (Master Plan) และแผนการดำเนินงานในรายละเอียด (Action Plan) และแผนการดำเนินงานอื่นๆ ที่ประกอบด้วยตารางการปฏิบัติงาน ขั้นตอนในการดำเนินการ /ขั้นตอนในการปฏิบัติงาน ผู้รับผิดชอบงานแต่ละขั้นตอน ผลงานที่จะส่งมอบ ระยะเวลาที่ใช้ในแต่ละขั้นตอนเพื่อใช้ในการบริหารและติดตามผลการดำเนินงานให้ครอบคลุมการดำเนินงานทั้งหมด
- ๒.๓ ผู้ชนะการประกวดราคาต้องจัดให้มีบุคลากรผู้เชี่ยวชาญที่มีประสบการณ์ในการทำงาน ประกอบด้วย
 - ๑) ผู้บริหารโครงการ (Project Manager) จำนวน ๑ คน มีความชำนาญและประสบการณ์ในการควบคุม และบริหารโครงการมาแล้วไม่น้อยกว่า ๕ ปี
 - ๒) ผู้เชี่ยวชาญที่มีประสบการณ์ในด้านการออกแบบและติดตั้งระบบและอุปกรณ์ระบบเครือข่ายสื่อสาร ข้อมูลที่เสนอ จำนวนอย่างน้อย ๓ คน โดยผ่านการรับรอง (Certified) เรื่อง Routing หรือ Switching ในระดับ Professional หรือ Expert เป็นอย่างน้อย พร้อมเสนอเอกสารหรือวุฒิบัตร (Certification)
 - ๓) Administrative Officer จำนวนไม่น้อยกว่า ๑ คน โดยมีประสบการณ์การทำงาน ๑ - ๕ ปี เป็นอย่างน้อย
 - ๔) บุคลากรด้านอื่นๆ ที่เห็นว่าจำเป็นต่อการดำเนินโครงการ
- ๒.๔ จำนวนบุคลากรตามกำหนดต้องเสนอให้เพียงพอที่จะทำงานในด้านต่าง ๆ ได้ และต้องเป็นผู้รับผิดชอบทำงานตามข้อกำหนดนี้ ทั้งนี้ให้ระบุหน้าที่ความรับผิดชอบ ประวัติการศึกษา ประวัติการทำงาน ประสบการณ์ ตำแหน่งหน้าที่ และผลงานของบุคลากรแต่ละคนไว้ในประวัติบุคลากร พร้อมสำเนาหลักฐานที่แสดงว่า ได้ผ่านการฝึกอบรมเกี่ยวกับระบบที่เสนอ หรือการพัฒนาในระบบในลักษณะเดียวกับระบบที่เสนอมาแล้วจากผู้ผลิตโดยตรง หรือสถาบันการฝึกอบรมที่ได้รับการรับรองจากบริษัทผู้ผลิต

- ๒.๕ ในกรณีที่คณะกรรมการตรวจรับพัสดุและ/หรือผู้แทนของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง เห็นว่าบุคลากรตามเสนอมามีคุณสมบัติไม่เหมาะสมหรือทำงานไม่มีประสิทธิภาพ ผู้ชนะการประกวดราคาต้องดำเนินการปรับเปลี่ยนโดยทันทีที่ได้รับแจ้ง ทั้งนี้ ผู้ชนะการประกวดราคาจะอ้างการปรับเปลี่ยนนี้เข้ามาเป็นเหตุของการล่าช้าของงานไม่ได้
- ๒.๖ ผู้ชนะการประกวดราคาต้องเสนอรายงานความก้าวหน้าการดำเนินงานให้คณะกรรมการตรวจรับพัสดุ และ/หรือผู้แทน ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลังทราบ อย่างน้อยเดือนละครั้ง จนกว่างานจะแล้วเสร็จ

๓. การทดสอบและตรวจรับ

- ๓.๑ ผู้ชนะการประกวดราคาต้องส่งมอบอุปกรณ์ให้คณะกรรมการตรวจรับพัสดุ ณ สถานที่ติดตั้งที่คณะกรรมการตรวจรับพัสดุกำหนด โดยส่งมอบให้สำนักงานปลัดกระทรวงการคลังตามงวดงานที่กำหนดในเอกสาร ขอบเขตของงาน (TOR)
- ๓.๒ ผู้ชนะการประกวดราคาต้องติดตั้งและทดสอบการทำงานของอุปกรณ์และระบบทุกอย่างที่เสนอได้อย่างถูกต้องครบถ้วนสมบูรณ์
- ๓.๓ ผู้ชนะการประกวดราคาต้องเสนอเอกสารซึ่งประกอบด้วย รายละเอียดของอุปกรณ์ Configuration Diagram ทั้งหมด ข้อมูลวิธีการและขั้นตอนการตรวจรับของแต่ละอุปกรณ์โดยละเอียด
- ๓.๔ ผู้ชนะการประกวดราคาต้องจัดเตรียมอุปกรณ์สำหรับใช้งานหรือสนับสนุนการ Configuration และทดสอบระบบ ในช่วงระยะเวลาของการติดตั้ง ทดสอบ ฝึกอบรม บำรุงรักษา และนำกลับคืนเมื่อเสร็จสิ้นการใช้งาน โดยต้องเสนอรายละเอียดของอุปกรณ์ให้คณะกรรมการตรวจรับพัสดรร่วมพิจารณาก่อนนำมาใช้
- ๓.๕ คณะกรรมการตรวจรับพัสดุและ/หรือผู้แทนของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และ/หรือผู้แทนสำนักงานปลัดกระทรวงการคลัง ที่เข้าร่วมดูแลการติดตั้งจะดำเนินการตรวจรับงานเฉพาะในเวลาทำการปกติ คือ ๐๘.๓๐ - ๑๖.๓๐ น. เว้นวันเสาร์ - อาทิตย์ และวันหยุดราชการ ในกรณีที่ผู้ชนะการประกวดราคามีความจำเป็นต้องตรวจรับงานนอกเหนือจากเวลาดังกล่าวจะต้องแจ้งให้สำนักงานปลัดกระทรวงการคลังทราบ พร้อมทั้งจะต้องรับผิดชอบค่าใช้จ่ายในการปฏิบัติงาน (ถ้ามี)
- ๓.๖ คณะกรรมการตรวจรับพัสดุและ/หรือผู้แทนของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และ/หรือผู้แทนสำนักงานปลัดกระทรวงการคลัง สงวนสิทธิที่จะเข้าทดสอบและตรวจสอบการทำงานของอุปกรณ์หรือระบบที่ติดตั้ง ตามสถานที่ที่กำหนด เพื่อดำเนินการตรวจรับงาน โดยผู้ชนะการประกวดราคาจะต้องอำนวยความสะดวกในการเดินทางหรือรับผิดชอบในค่าใช้จ่ายในการปฏิบัติงาน (ถ้ามี)
- ๓.๗ สำนักงานปลัดกระทรวงการคลัง สามารถที่จะนำอุปกรณ์ และ/หรือ งานในส่วนที่ส่งมอบแล้วไปใช้งานตามที่สำนักงานปลัดกระทรวงการคลังเห็นสมควร โดยที่ไม่กระทบกระเทือนหรือเป็นอุปสรรคในการทำงานของผู้ชนะการประกวดราคา โดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง เพียงแต่แจ้งให้ผู้ชนะการประกวดราคาทราบ แต่หากการทดสอบอุปกรณ์/ระบบ ไม่ผ่านเงื่อนไขและเป็นเหตุให้ต้องเลิกสัญญาอันเนื่องมาจากความผิดพลาดของผู้ชนะการประกวดราคา ผู้ชนะการประกวดราคาไม่มีสิทธิเรียกร้องค่าใช้จ่ายหรือค่าเสียหายใดๆ จากสำนักงานปลัดกระทรวงการคลัง
- ๓.๘ หากมีข้อความใดในข้อกำหนดฉบับนี้ที่มีความขัดแย้งกัน ให้ยึดถือตามข้อกำหนดที่เป็นประโยชน์กับสำนักงานปลัดกระทรวงการคลัง

รายละเอียดการฝึกอบรมและคู่มือการใช้งาน

๑. รายละเอียดการฝึกอบรม

ผู้ชนะการประกวดราคาจะต้องจัดให้มีการฝึกอบรมทั้งภาคทฤษฎีและภาคปฏิบัติให้กับบุคลากรด้านต่าง ๆ ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง เพื่อรองรับการปฏิบัติงานได้อย่างมีประสิทธิภาพ โดยต้องทำตามข้อกำหนดอย่างน้อย ดังนี้

- ๑.๑ ผู้ชนะการประกวดราคาต้องจัดฝึกอบรม เกี่ยวกับอุปกรณ์ที่ส่งมอบตามโครงการ และการบริหารระบบ สำหรับผู้ดูแลระบบ โดยมีผู้เข้าอบรมอย่างน้อย ๕ คน ให้ผู้เข้าอบรมได้ใช้อุปกรณ์แบบ Hands on และมีเนื้อหาในด้านการทำงานของระบบ การใช้งาน การบำรุงรักษา เพื่อให้ผู้เข้าอบรมสามารถใช้งานอุปกรณ์ได้เป็นอย่างดี ดังนี้
 - ๑) หลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์ เช่น CompTIA Security+ หรือตามที่คณะกรรมการตรวจรับพัสดุพิจารณา
 - ๒) หลักสูตรอื่น ๆ ที่เกี่ยวเนื่องกับอุปกรณ์หรือซอฟต์แวร์ที่ส่งมอบตามโครงการ โดยรูปแบบการอบรม ในลักษณะ On The Job Training
- ๑.๒ ผู้ชนะการประกวดราคาต้องจัดทำแผนการฝึกอบรมเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร พร้อมหัวข้อการฝึกอบรมแต่ละหลักสูตร ให้คณะกรรมการตรวจรับพัสดุพิจารณา ก่อนดำเนินการ โดยที่หัวข้อการฝึกอบรมต้องครอบคลุมเนื้อหาทั้งหมดที่เกี่ยวกับการใช้งานระบบและการดูแลรักษาอย่างละเอียด ซึ่งผู้เข้าอบรมจะสามารถใช้งานระบบดังกล่าวได้เป็นอย่างดี และเนื้อหาในเอกสารการฝึกอบรมต้องเป็นของอุปกรณ์ที่ส่งมอบตามโครงการ
- ๑.๓ คณะกรรมการตรวจรับพัสดุขอสงวนสิทธิ์ที่จะเลือกหรือปรับปรุงเนื้อหา หัวข้อการฝึกอบรมแต่ละหลักสูตร และกำหนดการที่จัดอบรม โดยจะหารือกับผู้ชนะการประกวดราคาก่อนการอบรม
- ๑.๔ ผู้ชนะการประกวดราคาต้องจัดเตรียมอุปกรณ์ อาหารและเครื่องดื่ม พาหนะรับส่ง อุปกรณ์สำหรับการสาธิต และภาคปฏิบัติ และเอกสารฝึกอบรม
- ๑.๕ ผู้ชนะการประกวดราคาต้องรับผิดชอบในการจัดการฝึกอบรมในหลักสูตรเดิมหรือหลักสูตรใหม่ ทั้งหมดหรือบางส่วนของหลักสูตรอีกครั้ง หากคณะกรรมการตรวจรับพัสดุ หรือผู้แทนจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง เห็นว่าผลการฝึกอบรมที่ผ่านมา นั้นมีเนื้อหาไม่ครอบคลุมเพียงพอหรือการถ่ายทอดไม่ครบถ้วนตรงตามหลักสูตรที่ได้ตกลงไว้
- ๑.๖ การจัดฝึกอบรมต้องดำเนินการให้แล้วเสร็จภายในระยะเวลาส่งมอบงานหรือระยะเวลาการรับประกันผลงาน ตามความเหมาะสมที่คณะกรรมการตรวจรับพัสดุพิจารณา

๒. คู่มือการใช้งาน

- ๒.๑ ผู้ชนะการประกวดราคาต้องจัดหาหรือจัดทำและส่งมอบคู่มือการใช้งานอุปกรณ์หรือระบบที่มีการติดตั้ง และใช้งานในโครงการทั้งหมด ให้กับผู้ใช้ในวันที่ยื่นมอบโครงการหรืองานงวดสุดท้าย
- ๒.๒ ผู้ชนะการประกวดราคาต้องปรับปรุงเอกสารหรือคู่มือการใช้งานอุปกรณ์หรือระบบ ในกรณีที่ระบบ มีการปรับปรุงหรือปรับเปลี่ยนการทำงานของอุปกรณ์หรือระบบ เพื่อให้ได้เอกสารหรือคู่มือการใช้งาน อุปกรณ์หรือระบบ ที่มีความทันสมัยและเป็นปัจจุบัน โดยไม่คิดค่าใช้จ่ายเพิ่มจากผู้ซื้อ

เงื่อนไขการรับประกันผลงานและความชำรุดบกพร่องและการบำรุงรักษาและซ่อมแซมแก้ไข

ผู้ชนะการประกวดราคาต้องบำรุงรักษา ซ่อมแซมแก้ไขหรือเปลี่ยนทดแทนอุปกรณ์ที่ส่งมอบในโครงการทั้งหมด เป็นระยะเวลา ๑ ปี นับตั้งแต่คณะกรรมการตรวจรับพัสดุได้ตรวจรับงานงวดสุดท้ายเสร็จสมบูรณ์ โดยต้องปฏิบัติตามเงื่อนไขดังต่อไปนี้

๑. การบำรุงรักษาแบบป้องกัน (Preventive Maintenance)

ผู้ชนะการประกวดราคาต้องเสนอแผน และทำการบำรุงรักษา (Preventive Maintenance) ดังนี้

- ๑.๑. ผู้ชนะการประกวดราคาต้องทำการบำรุงรักษา (Preventive Maintenance) อุปกรณ์และระบบที่ส่งมอบในโครงการ อย่างน้อย ๓ ครั้ง ตลอดระยะเวลาประกัน เพื่อให้ระบบอยู่ในสภาพที่ใช้งานได้อย่างมีประสิทธิภาพตลอดเวลา โดยทำการบำรุงรักษาในช่วงระยะเวลาที่ไม่ส่งผลกระทบต่อการทำงานของสำนักงานปลัดกระทรวงการคลัง และจะต้องแจ้งให้ทราบล่วงหน้าอย่างน้อย ๕ วันทำการ ในทุกครั้ง ที่เข้าดำเนินการบำรุงรักษา
- ๑.๒. เมื่อมีการเปลี่ยนแปลง แก้ไข ปรับปรุงเพิ่มเติม Software ในลักษณะการ Upgrade หรือออก Version ใหม่ของอุปกรณ์ในโครงการให้ทันสมัยขึ้น ผู้ชนะการประกวดราคาต้องแจ้งให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลังทราบ และทำการปรับปรุงเมื่อสำนักงานปลัดกระทรวงการคลังร้องขอให้มาติดตั้ง โดยไม่คิดค่าใช้จ่ายใด ๆ พร้อมทั้งนำเอกสารและคู่มือประกอบการใช้งาน (ถ้ามี) มามอบให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และต้องทำการอบรมให้เจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ถ้าเป็นสิ่งที่กระทบกับสภาพการดำเนินงานหรือมีผลให้การทำงานเปลี่ยนแปลงไป

๒. การซ่อมแซมแก้ไข

- ๒.๑. หากอุปกรณ์หรือระบบชำรุด บกพร่อง หรือใช้งานไม่ได้ ถึงแม้ว่าจะติดตั้งอยู่ ณ สถานที่ใดตามที่กำหนดในสัญญา และความชำรุดนี้มิได้เกิดจากความผิดของสำนักงานปลัดกระทรวงการคลัง ผู้ชนะการประกวดราคาต้องเริ่มดำเนินการซ่อมแซมแก้ไขให้อยู่ในสภาพดีได้ดังเดิมโดยไม่คิดค่าใช้จ่ายใด ๆ จากสำนักงานปลัดกระทรวงการคลัง โดยต้องเข้าดำเนินการแก้ไขภายใน ๔ ชั่วโมง (ในเวลาทำการ ๘.๓๐-๑๖.๓๐) นับตั้งแต่ได้รับแจ้ง
- ๒.๒. ในการซ่อมแซมแก้ไข หากผู้ชนะการประกวดราคาคาดว่าไม่สามารถดำเนินการได้แล้วเสร็จภายใน ๑๒ ชั่วโมง (ในเวลาทำการ ๘.๓๐-๑๖.๓๐) นับแต่เริ่มทำการซ่อมแซมแก้ไข ผู้ชนะการประกวดราคาสามารถนำเครื่องหรืออุปกรณ์สำรองที่มีประสิทธิภาพทัดเทียมกัน ที่สามารถทำให้การใช้งานเป็นปกติดังเดิม ซึ่งจะไม่ถือว่าเป็นเวลาที่เกิดเหตุขัดข้อง แต่ผู้ชนะการประกวดราคาต้องเร่งดำเนินการแก้ไขเครื่องหรืออุปกรณ์ให้สามารถใช้งานได้ตามปกติ และนำมาเปลี่ยนทดแทน โดยเร็ว
- ๒.๓. สำนักงานปลัดกระทรวงการคลังยอมให้อุปกรณ์และระบบที่ส่งมอบในโครงการขัดข้องได้ไม่เกินเดือนละ ๔๘ ชั่วโมง (ในเวลาทำการ ๘.๓๐-๑๖.๓๐) โดยเริ่มนับเวลาตั้งแต่ที่เริ่มซ่อมแซมแก้ไขจนถึงเวลาที่ทำการซ่อมแซมแล้วเสร็จสมบูรณ์หรือเวลาที่ทำให้ระบบสามารถกลับมาทำงานได้ตามปกติ ถ้าการขัดข้องดังกล่าวมีระยะเวลาเกินเกณฑ์ที่กำหนด ผู้ชนะการประกวดราคาต้องถูกปรับในอัตราร้อยละ ๐.๐๒๕ ของราคาตามสัญญาต่อชั่วโมง เศษของชั่วโมง ให้นับเป็น ๑ ชั่วโมง

๓. การบริการและการสนับสนุน

ผู้ชนะการประกวดราคาจะต้องดำเนินการบริการและการสนับสนุน ตลอดระยะเวลารับประกัน โดยต้องปฏิบัติดังต่อไปนี้

- ๓.๑. จัดเจ้าหน้าที่ของผู้ชนะการประกวดราคามาปฏิบัติงานที่สำนักงานปลัดกระทรวงการคลังตามที่สำนักงานปลัดกระทรวงการคลังร้องขอ (On call) โดยไม่คิดค่าใช้จ่ายใด ๆ
- ๓.๒. ให้ความช่วยเหลือแก่ผู้บริหารจัดการระบบ (Administrator) และเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศ และการสื่อสาร ตามที่สำนักงานปลัดกระทรวงการคลังร้องขอ (On call) โดยไม่คิดค่าใช้จ่ายใด ๆ
- ๓.๓. ให้คำปรึกษาแนะนำความรู้ในลักษณะของการถ่ายทอดเทคนิคและวิธีการปฏิบัติงานของระบบ ที่มีรายละเอียดเพิ่มเติมตามความต้องการของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อให้สามารถบริหารจัดการระบบเครือข่ายต่อไปได้ภายหลังติดตั้ง

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและรายละเอียดค่าใช้จ่าย
การจัดซื้อจัดจ้างที่มีใช้งานก่อสร้าง

๑. ชื่อโครงการ ...โครงการทดแทนและเพิ่มประสิทธิภาพระบบรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์และระบบเครือข่าย
๒. หน่วยงานเจ้าของโครงการ...ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง...
๓. วงเงินงบประมาณที่ได้รับจัดสรร ...๓๗,๕๕๐,๐๐๐.- บาท (สามสิบเจ็ดล้านสี่แสนห้าหมื่นบาทถ้วน)
๔. วันที่กำหนดราคากลาง (ราคาอ้างอิง) ณ วันที่.....
เป็นเงิน ...๓๗,๕๕๐,๐๐๐.- บาท (สามสิบเจ็ดล้านสี่แสนห้าหมื่นบาทถ้วน)
ราคา/หน่วย (ถ้ามี).....บาท
๕. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)
 - ๕.๑ ...บริษัท แอ็ดวานซ์อินฟอร์เมชันเทคโนโลยี จำกัด (มหาชน).....
 - ๕.๒ ...บริษัท เดอะแพรคทีเคิลโซลูชัน จำกัด (มหาชน).....
 - ๕.๓ ...บริษัท เน็กซ์เทค เอเชีย จำกัด.....
๖. รายชื่อผู้รับผิดชอบกำหนดราคากลาง
 - ๖.๑ นายบุญลือ จิตตคาม
เจ้าพนักงานเครื่องคอมพิวเตอร์อาวุโส
 - ๖.๒ นางสาววิชุดา ด้านพรประเสริฐ
นักวิชาการคอมพิวเตอร์ชำนาญการ
 - ๖.๓ นายประทีป สร้อยนาค
นักวิชาการคอมพิวเตอร์ชำนาญการ
 - ๖.๔ นายรังสฤษฎ์ เพศยนาวิน
นักวิชาการคอมพิวเตอร์ปฏิบัติการ
 - ๖.๕ นายจิรวัฒน์ อิมณุกุลกิจ
นักวิชาการคอมพิวเตอร์ชำนาญการ