ขอบเขตของงาน (Terms of Reference: TOR)
โครงการพัฒนาระบบความมั่นคงปลอดภัยของกระทรวงการคลัง

๑ เหตุผลความจำเป็น

การบริหารจัดการด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารของกระทรวงการคลัง ถือเป็นหนึ่งในหน้าที่หลักที่สำคัญของ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารของกระทรวงการคลัง โดยในปัจจุบัน การบริหารความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารของกระทรวงการคลัง ได้มีการดำเนินการอย่างจริงจังและต่อเนื่อง เพื่อให้การปฏิบัติงานและการให้บริการของกระทรวงการคลังทั้งภายในและภายนอกเป็นไปอย่างราบรื่น ไม่ขาดตอน และปลอดภัย อันจะช่วยสร้างความมั่นใจในการนำเอาเทคโนโลยีดิจิทัลมาใช้งานในยุคเศรษฐกิจและสังคมดิจิทัล

ด้วยระบบสารสนเทศและการสื่อสารที่มีการขยายตัวอย่างต่อเนื่อง ความเชื่อมโยงของระบบที่มีความซับซ้อนมากขึ้น และเทคโนโลยีใหม่ ๆ ที่มีความหลากหลายและเปลี่ยนแปลงไปอย่างรวดเร็ว ทำให้การบริหารความมั่นคงปลอดภัยของกระทรวงการคลังเป็นไปด้วยความยากลำบาก นอกจากนี้ปัญหาภัยคุกคามต่อระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีรูปแบบที่หลากหลาย ทวีความรุนแรงและเพิ่มขึ้นเป็นอย่างมากในช่วงที่มา ประกอบกับอุปกรณ์ตรวจสอบและป้องกันภัยคุกคามในปัจจุบันที่ไม่ทันสมัย และไม่มีประสิทธิภาพเพียงพอ ทั้งหลายเหล่านี้ส่งผลให้ การตอบสนองกับภัยคุกคาม ไม่สามารถดำเนินการได้อย่างทันท่วงที อันอาจจะส่งผลกระทบถึงประสิทธิภาพการปฏิบัติงานและการให้บริการของกระทรวงการคลังได้

๒ วัตถุประสงค์

๒.๑ มีอุปกรณ์บริหารจัดการข้อมูลและเหตุการณ์ด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร ที่สามารถรวบรวมข้อมูลและวิเคราะห์ภัยคุกคามได้แบบรวมศูนย์

๒.๒ มีอุปกรณ์ป้องกันภัยคุกคามต่อระบบเทคโนโลยีสารสนเทศและการสื่อสารที่ทันสมัยและมีประสิทธิภาพ

๒.๓ มีการปรับปรุงระบบเทคโนโลยีสารสนเทศและการสื่อสารกระทรวงการคลังให้มีความมั่นคงปลอดภัย

๒.๔ มีกิจกรรมให้ความรู้ เพื่อสร้างความตระหนักและความรู้ความเข้าใจในเรื่องการบริหารความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร และในเรื่องความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ให้แก่บุคลากรของกระทรวงการคลัง

๓ เป้าหมาย

๓.๑ สามารถบริหารความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารของกระทรวงการคลังได้อย่างเป็นระบบ เป็นแบบรวมศูนย์ เพื่อให้สามารถเฝ้าระวัง ติดตาม และแก้ไขปัญหาภัยคุกคามต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร ได้อย่างมีประสิทธิภาพ รวดเร็ว และทันต่อสถานการณ์

๓.๒ เสริมสมรรถนะการบริหารความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารของกระทรวงการคลังให้มีความทันสมัย และแข็งแรง อย่างต่อเนื่อง พร้อมรับมือกับสถานการณ์ภัยคุกคามรูปแบบใหม่ ๆ ที่เปลี่ยนแปลงอยู่ตลอดเวลา

๓.๓ เสริมสร้างบุคลากรกระทรวงการคลังให้มีความตระหนักและรอบรู้ในเรื่องความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๔ คุณสมบัติผู้เสนอราคา

๔.๑ มีความสามารถตามกฎหมาย

๔.๒ ไม่เป็นบุคคลล้มละลาย

๔.๓ ไม่อยู่ระหว่างเลิกกิจการ

๔.๔ ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

๔.๕ ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วน ผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

๔.๖ มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

๔.๗ เป็นบุคคลธรรมดาหรือนิติบุคคล ผู้มีอาชีพขายพัสดุที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

๔.๘ ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่สำนักงาน ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

๔.๙ ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

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

๔.๑๑ ผู้ยื่นข้อเสนอซึ่งได้รับคัดเลือกเป็นคู่สัญญาต้องลงทะเบียนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement : e - GP) ของกรมบัญชีกลาง ตามที่คณะกรรมการ ป.ป.ช. กำหนด

๔.๑๒ ผู้ยื่นข้อเสนอต้องไม่อยู่ในฐานะเป็นผู้ไม่แสดงบัญชีรายรับรายจ่าย หรือแสดงบัญชีรายรับรายจ่ายไม่ถูกต้องครบถ้วนในสาระสำคัญ ตามที่คณะกรรมการ ป.ป.ช. กำหนด

๔.๑๓ ผู้ยื่นข้อเสนอซึ่งได้รับคัดเลือกเป็นคู่สัญญาต้องรับและจ่ายเงินผ่านบัญชีธนาคาร เว้นแต่ การจ่ายเงินแต่ละครั้งซึ่งมีมูลค่าไม่เกินสามหมื่นบาทคู่สัญญาอาจจ่ายเป็นเงินสดก็ได้ ตามที่คณะกรรมการ ป.ป.ช. กำหนด

๔.๑๔ ผู้ยื่นข้อเสนอต้องเคยมีผลงานการขายและติดตั้งระบบเครื่องคอมพิวเตอร์หรือระบบเครือข่ายหรือระบบรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ให้กับหน่วยงานราชการหรือรัฐวิสาหกิจที่มีสัญญาย้อนหลังไม่เกิน ๕ ปี นับจนถึงวันยื่นข้อเสนอราคา ซึ่งมีมูลค่าของสัญญาไม่น้อยกว่า ๑๕,๐๐๐,๐๐๐.- บาท (สิบห้าล้านบาทถ้วน) ต่อสัญญา ทั้งนี้ให้แนบสำเนาหนังสือรับรองผลงานและสำเนาสัญญาดังกล่าวมาพร้อมการยื่นข้อเสนอทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์

๕ ขอบเขตของงาน

โครงการพัฒนาระบบความมั่นคงปลอดภัยของกระทรวงการคลัง ประกอบไปด้วย

๕.๑ อุปกรณ์บริหารจัดการข้อมูลและเหตุการณ์ด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Security Information and Event Management – SIEM) จำนวน ๑ ชุด

๕.๒ อุปกรณ์ป้องกันเครือข่าย (Firewall) สำหรับ Intranet/DMZ Zone จำนวน ๒ ชุด

๕.๓ อุปกรณ์ป้องกันภัยคุกคามขั้นสูง (Advanced Persistent Threat) จำนวน ๑ ชุด

๕.๔ อุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall) จำนวน ๒ ชุด

๕.๕ ระบบสนับสนุนการติดตามเฝ้าระวังเหตุการณ์ผิดปรกติ/ภัยคุกคาม จำนวน ๑ ระบบ

๕.๖ การพัฒนาระบบความมั่นคงปลอดภัยของกระทรวงการคลัง จำนวน ๑ ระบบ

ทั้งนี้ ระบบคอมพิวเตอร์และอุปกรณ์ทั้งหมดในโครงการระบบความมั่นคงปลอดภัยของกระทรวงการคลัง ต้องมีคุณลักษณะเฉพาะและรายละเอียดอื่น ๆ ตรงตามที่กำหนดไว้ หรือดีกว่า ตามภาคผนวกที่ ๑ ถึง ๔ โดยผู้ยื่นข้อเสนอต้องจัดทำตารางเปรียบเทียบคุณลักษณะเฉพาะและรายละเอียดอื่น ๆ ทุกรายการ ตามภาคผนวก ๑ ถึง ๔ มาพร้อมการยื่นข้อเสนอทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ โดยมีรายละเอียดอย่างน้อย ดังนี้

๑) รายละเอียดคุณลักษณะเฉพาะและรายละเอียดอื่น ๆ ของโครงการ

๒) รายละเอียดคุณลักษณะเฉพาะและรายละเอียดอื่น ๆ ที่เสนอ

๓) การอ้างอิงถึงเอกสารแคตตาล็อก (ถ้ามี)

๖ ระยะเวลาดำเนินงาน

ส่งมอบงานทั้งหมดภายใน ๒๗๐ วัน นับถัดจากวันลงนามในสัญญา

๗ ระยะเวลาส่งมอบงาน

ผู้ชนะการประกวดราคาต้องส่งมอบงาน ดังต่อไปนี้

งานงวดที่ ๑ ส่งมอบงาน ภายใน ๓๐ วัน นับถัดจากวันลงนามในสัญญา ดังนี้

๑. ส่งมอบแผนการดำเนินงาน และรายชื่อทีมงาน

๒. เอกสารส่งมอบงาน จำนวน ๒ ชุด และสำเนาอิเล็กทรอนิกส์ใน Thumb Drive จำนวน ๕ ชุด

งานงวดที่ ๒ ส่งมอบงาน ภายใน ๑๒๐ วัน นับถัดจากวันลงนามในสัญญา ดังนี้

๑. ส่งมอบรายงานการออกแบบระบบ

๒. ส่งมอบแผนและรูปแบบการติดตั้งระบบ

๓. ส่งมอบการพัฒนาระบบความมั่นคงปลอดภัยกระทรวงการคลัง ตามภาคผนวก ๑ ข้อ ๖.๑-๖.๕

๔. ส่งมอบรายละเอียดคู่มือและเอกสารต่าง ๆ ตามภาคผนวก ๓ ข้อ ๑.๑

๕. เอกสารส่งมอบงาน จำนวน ๒ ชุด และสำเนาอิเล็กทรอนิกส์ใน Thumb Drive จำนวน ๕ ชุด

งานงวดที่ ๓ ส่งมอบงาน ภายใน ๑๕๐ วัน นับถัดจากวันลงนามในสัญญา ดังนี้

๑. ส่งมอบอุปกรณ์ทั้งหมดในโครงการ

๒. เอกสารส่งมอบงาน จำนวน ๒ ชุด และสำเนาอิเล็กทรอนิกส์ใน Thumb Drive จำนวน ๕ ชุด

งานงวดสุดท้าย ส่งมอบงาน ภายใน ๒๗๐ วัน นับถัดจากวันลงนามในสัญญา ดังนี้

๑. ส่งมอบการติดตั้งอุปกรณ์ทั้งหมดในโครงการ

๒. ส่งมอบการพัฒนาระบบความมั่นคงปลอดภัยของกระทรวงการคลัง ตามภาคผนวก ๑ ข้อ ๖.๖ - ๖.๑๓

๓. ส่งมอบรายละเอียดคู่มือและเอกสารต่าง ๆ ตามภาคผนวก ๓ ข้อ ๑.๒ – ๑.๗

๔. ส่งมอบเอกสารการฝึกอบรม ตามภาคผนวก ๓ ข้อ ๒

๕. เอกสารส่งมอบงาน จำนวน ๒ ชุด และสำเนาอิเล็กทรอนิกส์ใน Thumb Drive จำนวน ๕ ชุด

๘ เงื่อนไขการชำระเงิน

เงื่อนไขการชำระเงิน จะแบ่งการชำระเงินเป็น ๔ งวด ดังนี้

งวดที่ ๑ ชำระเงินในอัตราร้อยละ ๑๐ ของจำนวนเงินตามสัญญา เมื่อคณะกรรมการตรวจรับได้ตรวจรับการส่งมอบงานงวดที่ ๑ เรียบร้อยแล้ว

งวดที่ ๒ ชำระเงินในอัตราร้อยละ ๓๐ ของจำนวนเงินตามสัญญา เมื่อคณะกรรมการตรวจรับได้ตรวจรับการส่งมอบงานงวดที่ ๒ เรียบร้อยแล้ว

งวดที่ ๓ ชำระเงินในอัตราร้อยละ ๔๐ ของจำนวนเงินตามสัญญา เมื่อคณะกรรมการตรวจรับได้ตรวจรับการส่งมอบงานงวดที่ ๓ เรียบร้อยแล้ว

งวดสุดท้าย ชำระเงินในอัตราร้อยละ ๒๐ ของจำนวนเงินตามสัญญา เมื่อคณะกรรมการตรวจรับได้ตรวจรับการส่งมอบงานงวดสุดท้าย เรียบร้อยแล้ว

๙ วงเงินในการจัดหา

วงเงินในการจัดหาเป็นเงินทั้งสิ้น ๓๒,๕๑๙,๓๐๐.- บาท (สามสิบสองล้านห้าแสนหนึ่งหมื่นเก้าพันสามร้อยบาทถ้วน) ซึ่งเป็นวงเงินที่รวมภาษีมูลค่าเพิ่ม และค่าใช้จ่ายอื่นใดทั้งปวงไว้ด้วยแล้ว โดยเบิกจ่ายจากเงินงบประมาณประจำปีงบประมาณ พ.ศ. ๒๕๖๒

๑๐ หลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอ

ใช้เกณฑ์ราคา

๑๑ หน่วยงานผู้รับผิดชอบดำเนินการ

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง

ท่านสามารถเสนอแนะวิจารณ์ หรือแสดงความคิดเห็นโดยเปิดเผย

๑. ทางไปรษณีย์ โครงการพัฒนาระบบความมั่นคงปลอดภัยของกระทรวงการคลัง
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานปลัดกระทรวงการคลัง
ถนนพระราม ๖ แขวงพญาไท เขตพญาไท
กรุงเทพมหานคร ๑๐๔๐๐

๒. ทางอีเมล์ tor-mofsecurity@mof.go.th

๓. ทางโทรศัพท์ หมายเลข ๐๒-๑๒๖-๕๙๐๐ ต่อ ๓๓๐๖, ๓๓๑๒

๔. ทางโทรสาร หมายเลข ๐๒-๒๗๓-๙๗๙๐
ทั้งนี้โปรดแจ้ง ชื่อ ที่อยู่ พร้อมหมายเลขโทรศัพท์ติดต่อกลับด้วย

ภาคผนวก ๑
รายละเอียดคุณลักษณะเฉพาะ
โครงการพัฒนาระบบความมั่นคงปลอดภัยของกระทรวงการคลัง

ข้อกำหนดและเงื่อนไขในการยื่นข้อเสนอ

๑. ระบบคอมพิวเตอร์และอุปกรณ์ที่เสนอในโครงการต้องเป็นของแท้ ของใหม่ ไม่เคยผ่านการใช้งานมาก่อน ไม่เป็นของเก่าเก็บ ต้องอยู่ในสภาพที่ใช้งานได้ทันที และต้องมีคุณลักษณะเฉพาะตรงตามที่กำหนดไว้ หรือดีกว่า

๒. ผู้ยื่นข้อเสนอต้องได้รับการแต่งตั้งอย่างเป็นทางการจากเจ้าของผลิตภัณฑ์ หรือตัวแทนจำหน่ายอย่างเป็นทางการในประเทศไทยที่ได้รับการแต่งตั้งจากเจ้าของผลิตภัณฑ์ ในอุปกรณ์บริหารจัดการข้อมูลและเหตุการณ์ด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Security Information and Event Management - SIEM) อุปกรณ์ป้องกันเครือข่าย (Firewall) อุปกรณ์ป้องกันภัยคุกคามขั้นสูง (Advanced Persistent Threat) และอุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall) ที่เสนอในโครงการ ทั้งนี้ให้แนบสำเนาหนังสือแต่งตั้งดังกล่าวมาพร้อมการยื่นข้อเสนอทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์

รายละเอียดคุณลักษณะเฉพาะ

๑. **อุปกรณ์บริหารจัดการข้อมูลและเหตุการณ์ด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Security Information and Event Management - SIEM) จำนวน ๑ ชุด มีคุณลักษณะเฉพาะอย่างน้อย ดังนี้**

๑.๑ เป็นอุปกรณ์ Appliance ที่ออกแบบมาเพื่อใช้งานในลักษณะ SIEM โดยเฉพาะ

๑.๒ สามารถวิเคราะห์หาความสัมพันธ์ของข้อมูล Log หรือ Event เพื่อการเฝ้าระวังและเตือนภัยเหตุการณ์ภัยคุกคามได้ในแบบ Real Time หรือ Near Real Time

๑.๓ สามารถรับเหตุการณ์ที่เกิดขึ้นอย่างต่อเนื่องได้ไม่น้อยกว่า ๑,๐๐๐ เหตุการณ์ต่อวินาที (Event Per Second: EPS) หรือ ข้อความต่อวินาที (Message Per Second: MPS)

๑.๔ มีพื้นที่ในการเก็บบันทึกข้อมูลไม่น้อยกว่า ๑๒ TB หรือ เสนออุปกรณ์จัดเก็บข้อมูลภายนอกซึ่งสามารถใช้งานร่วมกับอุปกรณ์บริหารจัดการข้อมูลและเหตุการณ์ด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารที่เสนอในโครงการ โดยมีพื้นที่ในการจัดเก็บบันทึกข้อมูลได้ไม่น้อยกว่า ๑๒ TB

๑.๕ มีพอร์ต Ethernet สำหรับเชื่อมต่อที่ความเร็ว ๑ Gbps จำนวนไม่น้อยกว่า ๔ พอร์ต

๑.๖ มี Power Supply แบบ Redundant หรือ Hot Swap จำนวน ๒ หน่วย

๑.๗ สามารถใช้งานตามมาตรฐาน IPv๖ ได้

๑.๘ สามารถติดตั้งในตู้ Rack มาตรฐานขนาด ๑๙ นิ้วได้

๑.๙ สามารถแสดงรายงานในลักษณะ Dashboard และสามารถเพิ่มและปรับแต่งได้

๑.๑๐ สามารถจัดทำรายงานในรูปแบบตาราง และ Graphic ได้ในรูปแบบ Line Chart, Bar Chart, Pie Chart ได้เป็นอย่างน้อย

๑.๑๑ สามารถส่งออก (Export) รายงาน ในรูปแบบ Excel หรือ Pdf ได้เป็นอย่างน้อย

๑.๑๒ สามารถกำหนดสิทธิผู้ใช้งานในการเข้าถึงข้อมูลในระดับต่าง ๆ ได้

๑.๑๓ มีหน้าจอบริหารจัดการระบบได้ในรูปแบบ GUI (Graphical User Interface) ในลักษณะ Web-based และในรูปแบบ Command Line Interface (CLI)

๑.๑๔ สามารถบริหารจัดการและปรับตั้งค่าการจัดเก็บ Log ของอุปกรณ์ได้จากส่วนกลาง (Centralized Management) ในรูปแบบ GUI (Graphical User Interface) ในลักษณะ Web-based

๑.๑๕ สามารถแจ้งเตือน (Alert) ไปยังผู้ดูแลระบบได้ เมื่อตรวจพบเหตุการณ์ภัยคุกคาม

๑.๑๖ สามารถรับข้อมูลภัยคุกคาม (Threat Intelligence) เพื่อนำมาใช้วิเคราะห์ภัยคุกคามได้

๑.๑๗ สามารถบริหารจัดการเหตุการณ์ภัยคุกคามในลักษณะ Workflow ได้

๑.๑๘ สามารถทำงานร่วมกับอุปกรณ์เครือข่ายสื่อสารข้อมูล เพื่อตอบสนอง (Response) เมื่อตรวจพบข้อมูลที่สอดคล้องกับเงื่อนไขหรือเหตุการณ์ที่กำหนดไว้ (Correlation) ได้

๒. อุปกรณ์ป้องกันเครือข่าย (Firewall) สำหรับ Intranet/DMZ Zone จำนวน ๒ ชุด มีคุณลักษณะเฉพาะอย่างน้อย ดังนี้

๒.๑ เป็นอุปกรณ์ Appliance ที่ออกแบบมาเพื่อใช้งานในลักษณะ Firewall โดยเฉพาะ โดยทำงานแบบ Stateful Inspection Firewall และสามารถวิเคราะห์ข้อมูลได้ถึงระดับ Application Layer

๒.๒ มีประสิทธิภาพในการทำงาน Firewall (Firewall Throughput) ความเร็วไม่น้อยกว่า ๓๐ Gbps หรือความเร็วไม่น้อยกว่า ๗๖ Gbps ในสภาวะการใช้งานกับ UDP Packet ขนาด ๑,๕๑๘ bytes

๒.๓ สามารถรับจำนวน Connection ได้อย่างน้อย ๑๘๕,๐๐๐ connections per second และ ๒๕,๐๐๐,๐๐๐ concurrent connections

๒.๔ มีประสิทธิภาพในการทำงาน VPN Throughput ไม่น้อยกว่า ๑๐ Gbps

๒.๕ มีประสิทธิภาพในการทำงาน IPS Throughput หรือ Threat Prevention Throughput ไม่น้อยกว่า ๑๔ Gbps

๒.๖ สามารถบริหารจัดการอุปกรณ์ด้วย Command Line Interface (CLI) และ Graphical User Interface (GUI) ได้เป็นอย่างน้อย

๒.๗ สามารถตรวจสอบและป้องกันการบุกรุกรูปแบบต่าง ๆ อย่างน้อย ดังนี้ Sync Flood, UDP Flood หรือ Non-TCP Flood, ICMP Flood, IP Address Spoofing, IP Address Sweep, Port Scan, Dos หรือ DDos, Teardrop Attack, Land Attack, IP Fragment, ICMP Fragment ได้

๒.๘ สามารถตรวจสอบและกำหนดนโยบาย (Policy) การใช้งานในระดับ Application (Application Control) ได้

๒.๙ มีข้อมูลของ Application ไม่น้อยกว่า ๒,๐๐๐ Applications และมีการจัดระดับความเสี่ยง (Risk Level) ของ Application

๒.๑๐ สามารถตรวจจับ Virus ที่มาในรูปแบบของ HTTP, HTTPS และ SMTP Protocol ได้

๒.๑๑ สามารถทำ URL Filtering ได้ และมีข้อมูล URL Category ไม่น้อยกว่า ๕๐ Categories

๒.๑๒ สามารถตรวจจับพฤติกรรมที่ไม่ประสงค์ดีด้วยการส่งไฟล์ต้องสงสัยไปตรวจสอบบนระบบ Cloud (Cloud-Based) ซึ่งใช้เทคโนโลยี Sandbox เพื่อระบุ Malware ประเภท Zero-day Malware ได้

๒.๑๓ สามารถบริหารจัดการอุปกรณ์จากส่วนกลางได้ (Centralized Management)

๒.๑๔ มีระบบบริหารจัดการส่วนกลาง (Centralized Management) เพื่อบริหารจัดการอุปกรณ์ป้องกันเครือข่ายทั้งหมดที่เสนอในโครงการ จำนวนรวมทั้งหมด ๑ ชุด โดยมีคุณลักษณะเฉพาะอย่างน้อย ดังนี้

๑) เป็นอุปกรณ์ Appliance หรือ Virtual Appliance หรือ Virtual Management Server โดยไม่จำเป็นต้องเป็นยี่ห้อเดียวกับอุปกรณ์ป้องกันเครือข่ายที่เสนอในโครงการ ที่สามารถบริหารจัดการอุปกรณ์ป้องกันเครือข่าย ได้ไม่น้อยกว่า ๕ อุปกรณ์

๒) สามารถบริหารจัดการ Security Policy ได้

๓) สามารถควบคุมอุปกรณ์ป้องกันเครือข่าย (Firewall) ที่เสนอในโครงการได้

๔) สามารถกำหนดช่วงเวลาที่ต้องการให้สร้างและแสดงผลรายงาน (Schedule report) และกำหนดให้ส่งรายงานผ่านทาง Email ได้

๒.๑๕ สามารถทำการกำหนด IP Address และ Service Port แบบ Network Address Translation (NAT) และ Port Address Translation (PAT) ได้

๒.๑๖ สามารถ Routing แบบ Static, Dynamic Routing ได้

๒.๑๗ สามารถทำ High Availability ในแบบ Active/Passive หรือ Active/Active ได้

๒.๑๘ มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ ๑๐Gbps พร้อมโมดูล จำนวนไม่น้อยกว่า ๖ Ports และรองรับการขยายช่องเชื่อมต่อระบบเครือข่าย แบบ ๑๐๐Gbps ได้ จำนวนไม่น้อยกว่า ๒ Ports

๒.๑๙ มีหน่วยจัดเก็บข้อมูล (Hard drive) ขนาดไม่น้อยกว่า ๘๐๐ GB

๒.๒๐ มี Power Supply แบบ Redundant หรือ Hot Swap จำนวน ๒ หน่วย

๒.๒๑ สามารถใช้งานตามมาตรฐาน IPv๖ ได้

๒.๒๒ สามารถติดตั้งในตู้ Rack มาตรฐานขนาด ๑๙ นิ้วได้

๒.๒๓ มีการปรับปรุงข้อมูลรูปแบบการบุกรุก (Signature) เป็นระยะเวลาไม่น้อยกว่า ๒ ปี

๓. อุปกรณ์ป้องกันภัยคุกคามขั้นสูง (Advanced Persistent Threat) จำนวน ๑ ชุด มีคุณลักษณะเฉพาะอย่างน้อย ดังนี้

๓.๑ เป็นอุปกรณ์ Appliance ที่ออกแบบมาใช้งานป้องกันภัยคุกคามขั้นสูง (Advanced Persistent Threat) โดยเฉพาะ และสามารถป้องกันภัยคุกคามแบบ Zero-day Attacks ในขณะที่ยังไม่มีการกำหนด Signature ในระบบได้ และไม่มีลักษณะเป็นคุณสมบัติส่วนหนึ่งของอุปกรณ์ Next Generation Firewall หรือ Firewall หรือ อุปกรณ์ IPS

๓.๒ มีประสิทธิภาพในการทำงาน Throughput ความเร็วไม่น้อยกว่า ๗๐๐ Mbps

๓.๓ มีพื้นที่ในการเก็บบันทึกข้อมูลไม่น้อยกว่า ๑ TB

๓.๔ สามารถตรวจจับพฤติกรรมที่ไม่ประสงค์ดีโดยใช้เทคโนโลยี Sandbox ซึ่งความสามารถในการตรวจสอบไฟล์ไม่น้อยกว่า ๒๕๐,๐๐๐ files ต่อเดือน หรือเสนออุปกรณ์ป้องกันภัยคุกคามขั้นสูงมากกว่า ๑ ชุด เพื่อให้สามารถตรวจจับพฤติกรรมที่ไม่ประสงค์ดีโดยใช้เทคโนโลยี Sandbox ซึ่งความสามารถในการตรวจสอบไฟล์รวมไม่น้อยกว่า ๒๕๐,๐๐๐ files ต่อเดือน

๓.๕ มี Network Interface ต่ออุปกรณ์ป้องกันภัยคุกคามขั้นสูง ๑ ชุด หรือ มี Network Interface รวมอุปกรณ์ป้องกันภัยคุกคามขั้นสูงทุกชุด ในกรณีเสนออุปกรณ์ป้องกันภัยคุกคามขั้นสูงมากกว่า ๑ ชุด โดยมีคุณลักษณะแบบใดแบบหนึ่ง หรือดีกว่า ดังนี้

แบบที่ ๑ มี Network Interface แบบ ๑๐/๑๐๐/๑๐๐๐Base-T RJ๔๕ จำนวนอย่างน้อย ๘ พอร์ต หรือ

แบบที่ ๒ มี Network Interface แบบ ๑๐๐๐Base-T RJ๔๕ จำนวนอย่างน้อย ๒ พอร์ต และแบบ ๑๐Gbps พร้อมโมดูล จำนวนอย่างน้อย ๒ พอร์ต

๓.๖ สามารถตรวจสอบและป้องกันภัยคุกคามแบบ Zero Day attacks โดยสามารถทำผ่าน HTTP, HTTPS และ SMTP เป็นอย่างน้อย

๓.๗ สามารถวิเคราะห์และตรวจจับ Malware ในเอกสารและ File ต่างๆ ได้แก่ Adobe PDF, Microsoft Office, Java, Flash, EXE (Executable) file และ Archives file เช่น zip, rar, tar ได้เป็นอย่างน้อย

๓.๘ สามารถตรวจสอบและป้องกันภัยคุกคามสำหรับ Traffic ขาเข้า (Inbound) ที่มีการเข้ารหัสผ่านโปรโตคอล SSL ได้

๓.๙ สามารถป้องกันไฟล์ต้องสงสัยที่เป็น Zero-day ได้บนอุปกรณ์ป้องกันภัยคุกคามขั้นสูงที่เสนอในโครงการ โดยใช้เทคโนโลยี Sandbox หรือ สามารถป้องกันไฟล์ต้องสงสัยที่เป็น Zero-day ได้โดยทำงานร่วมกับซอฟต์แวร์ Agent ที่เครื่องผู้ใช้งาน ในกรณีที่ต้องมีการติดตั้งซอฟต์แวร์ Agent ที่เครื่องผู้ใช้งาน ต้องมีสิทธิ์การใช้งานของซอฟต์แวร์ Agent จำนวนไม่น้อยกว่า ๑,๐๐๐ ผู้ใช้งาน

๓.๑๐ สามารถบริหารจัดการอุปกรณ์ด้วย Command Line Interface (CLI) และ Graphical User Interface (GUI) ได้เป็นอย่างน้อย

๓.๑๑ สามารถใช้งานตามมาตรฐาน IPv๖ ได้

๓.๑๒ สามารถติดตั้งในตู้ Rack มาตรฐานขนาด ๑๙ นิ้วได้

๓.๑๓ มี Power Supply แบบ Redundant หรือ Hot Swap จำนวน ๒ หน่วย

๓.๑๔ มีการปรับปรุงข้อมูลรูปแบบการบุกรุก (Signature) เป็นระยะเวลาไม่น้อยกว่า ๒ ปี

๔. อุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall) จำนวน ๒ ชุด มีคุณลักษณะเฉพาะอย่างน้อย ดังนี้

๔.๑ เป็นอุปกรณ์ Appliance ที่ออกแบบมาเพื่อใช้งานในลักษณะ Web Application Firewall โดยเฉพาะ

๔.๒ มีประสิทธิภาพในการทำงาน (Throughput) ความเร็วไม่น้อยกว่า ๑ Gbps

๔.๓ สามารถป้องกันการโจมตีระบบ Application ในแบบ Brute Force Login, Buffer Overflow, Cross Site Request Forgery (CSRF), Cross Site Scripting (XSS), Session Hijacking, Site Reconnaissance, SQL Injection ได้เป็นอย่างน้อย

๔.๔ สามารถเลือกใช้งานในรูปแบบ Reverse Proxy, In-Line (Bridge หรือ Transparent Proxy) และ Non-inline (Reverse Proxy หรือ Span หรือ Offline หรือ Sniffer) ได้เป็นอย่างน้อย

๔.๕ สามารถทำงานในลักษณะ SSL Offloading ได้

๔.๖ สามารถป้องการรั่วไหลของข้อมูล (Data Theft Protection/Data Loss Prevention)

๔.๗ สามารถป้องกันการโจมตีเว็บไซต์ตาม OWASP Top ๑๐ ปี ๒๐๑๗ หรือเวอร์ชั่นล่าสุด ได้เป็นอย่างน้อย

๔.๘ สามารถทำ URL Rewrite/Redirect ได้

๔.๙ สามารถแจ้งเตือนในกรณีที่เกิดเหตุการณ์ต่างๆ ผ่านทางอีเมล์ ได้เป็นอย่างน้อย

๔.๑๐ สามารถเรียนรู้การใช้งานปกติของ Web Application เพื่อใช้ป้องกันการใช้งานที่ผิดปกติจากเดิมได้

๔.๑๑ สามารถทำ High Availability ในแบบ Active/Passive หรือ Active/Active ได้

๔.๑๒ สามารถบริหารจัดการอุปกรณ์ได้ในรูปแบบ GUI (Graphical User Interface) ในลักษณะ Web-based

๔.๑๓ มีพอร์ต Ethernet ความเร็ว ๑๐/๑๐๐/๑๐๐๐ จำนวนไม่น้อยกว่า ๔ พอร์ต

๔.๑๔ มี Power Supply แบบ Redundant หรือ Hot Swap จำนวน ๒ หน่วย

๔.๑๕ สามารถติดตั้งในตู้ Rack มาตรฐานขนาด ๑๙ นิ้วได้

๔.๑๖ ได้รับการรับรองมาตรฐานด้าน Web Application Firewall จาก ICSA เป็นอย่างน้อย

๔.๑๗ สามารถใช้งานตามมาตรฐาน IPv๖ ได้

๔.๑๘ มีการปรับปรุงข้อมูลรูปแบบการบุกรุก (Signature) เป็นระยะเวลาไม่น้อยกว่า ๒ ปี

๕. ระบบสนับสนุนการติดตามเฝ้าระวังเหตุการณ์ผิดปรกติ/ภัยคุกคาม ๑ ระบบ ประกอบไปด้วย

๕.๑ ระบบแสดงผลสำหรับการเฝ้าระวังเหตุการณ์ผิดปรกติ/ภัยคุกคาม จำนวน ๔ ชุด มีคุณลักษณะอย่างน้อย ดังนี้

๕.๑.๑ เป็นจอภาพที่ออกแบบมาเพื่อเปิดใช้งานในต่อเนื่องตลอดเวลาในลักษณะ ๒๔x๗ โดยเฉพาะ

๕.๑.๒ เป็นจอภาพชนิดแอลซีดี หรือ แอลอีดี หรือดีกว่า ขนาดไม่น้อยกว่า ๕๕ นิ้ว

๕.๑.๓ มีความหนาของขอบด้านบนและด้านซ้าย ไม่เกิน ๓.๔ มิลลิเมตร และมีความหนาของขอบด้านล่างและด้านขวา ไม่เกิน ๒.๐ มิลลิเมตร

๕.๑.๔ สามารถแสดงผลความละเอียดแบบ Full HD (๑๙๒๐x๑๐๘๐)

๕.๑.๕ มีค่าความสว่าง (Brightness) สูงสุด ไม่น้อยกว่า ๗๐๐ cd/m^2

๕.๑.๖ มีค่า Contrast Ratio ไม่น้อยกว่า ๔,๐๐๐:๑

๕.๑.๗ มีค่า Aspect Ratio ที่ ๑๖:๙

๕.๑.๘ มีมุมมองภาพไม่น้อยกว่า ๑๗๘ องศา ทั้งในแนบราบ (Horizontal) และแนวดิ่ง (Vertical)

๕.๑.๙ มีช่องรับสัญญาณเข้า HDMI จำนวนไม่น้อยกว่า ๑ ช่อง

๕.๑.๑๐ ได้รับรองมาตรฐานจาก UL และ FCC เป็นอย่างน้อย

๕.๒ อุปกรณ์ Video Controller จำนวน ๑ ชุด มีคุณลักษณะอย่างน้อย ดังนี้

๕.๒.๑ มีช่องเชื่อมต่อ Input ในแบบ HDMI และ IP Streaming ได้เป็นอย่างน้อย

๕.๒.๒ สามารถเชื่อมต่อและแสดงผลร่วมกับระบบจอภาพแสดงผลสำหรับการเฝ้าระวังเหตุการณ์ผิดปรกติ/ภัยคุกคามที่เสนอในโครงการได้

๕.๒.๓ สามารถสร้างโซน เพื่อใช้แสดงผลได้ไม่น้อยกว่า ๔ โซน ใน ๑ หน้าจอ

๕.๒.๔ สามารถ Drag&Drop เพื่อกำหนดตำแหน่ง และขยายหน้าจอได้

๕.๒.๕ สามารถสร้าง, คัดลอก, ลบ, บันทึก Layout ได้

๕.๒.๖ สามารถสร้าง Shortcut สำหรับ Layout ได้

๕.๒.๗ สามารถตั้ง Layout Looping ได้

๕.๒.๘ มี Power Supply แบบ Redundant หรือ Hot Swap จำนวน ๒ หน่วย

๕.๒.๙ สามารถติดตั้งในตู้ Rack มาตรฐานขนาด ๑๙ นิ้วได้

๕.๒.๑๐ ได้รับรองมาตรฐานจาก UL และ FCC เป็นอย่างน้อย

๕.๓ เครื่องคอมพิวเตอร์ตั้งโต๊ะ จำนวน ๔ ชุด มีคุณลักษณะอย่างน้อย ดังนี้

๕.๓.๑ มีหน่วยประมวลผลกลาง (CPU) ไม่น้อยกว่า ๔ แกนหลัก (๔ Core) หรือ ๘ แกนเสมือน (๘ Thread) โดยมีความเร็วสัญญาณนาฬิกาไม่น้อยกว่า ๓.๒ GHz จำนวน ๑ หน่วย

๕.๓.๒ หน่วยประมวลผลกลาง (CPU) มีหน่วยความจำแบบ Cache Memory ขนาดไม่น้อยกว่า ๘ MB

๕.๓.๓ มีหน่วยประมวลผลเพื่อแสดงภาพ ที่มีแผงวงจรเพื่อแสดงภาพแยกจากแผงวงจรหลักที่มีหน่วยความจำขนาดไม่น้อยกว่า ๒ GB

๕.๓.๔ มีหน่วยความจำหลัก (RAM) ชนิด DDR๔ หรือดีกว่า ขนาดไม่น้อยกว่า ๘ GB

๕.๓.๕ มีหน่วยจัดเก็บข้อมูล (Hard Disk) ชนิด SATA หรือดีกว่า ขนาดความจุไม่น้อยกว่า ๒ TB จำนวน ๑ หน่วย หรือ Solid State Drive ขนาดความจุไม่น้อยกว่า ๒๔๐ GB จำนวน ๑ หน่วย

๕.๓.๖ มี DVD-RW หรือดีกว่า จำนวน ๑ หน่วย

๕.๓.๗ มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ ๑๐/๑๐๐/๑๐๐๐ Base-T หรือดีกว่า จำนวนไม่น้อยกว่า ๑ ช่อง

๕.๓.๘ มีช่องเชื่อมต่อ (Interface) แบบ USB ๒.๐ หรือดีกว่า ไม่น้อยกว่า ๓ ช่อง

๕.๓.๙ มีแป้นพิมพ์และเมาส์

๕.๓.๑๐ มีจอภาพแบบ LED หรือดีกว่า มี Contrast Ratio ไม่น้อยกว่า ๖๐๐:๑ และมีขนาดไม่น้อยกว่า ๑๙ นิ้ว จำนวน ๑ หน่วย

๕.๔ เครื่องคอมพิวเตอร์โน้ตบุ๊ก จำนวน ๔ ชุด มีคุณลักษณะอย่างน้อย ดังนี้

๕.๔.๑ มีหน่วยประมวลผลกลาง (CPU) ซึ่งมีเทคโนโลยีเพิ่มสัญญาณนาฬิกาได้ในกรณีที่ต้องใช้ความสามารถในการประมวลผลสูง จำนวน ๑ หน่วย โดยมีคุณลักษณะเฉพาะอย่างใดอย่างหนึ่ง หรือดีกว่า ดังนี้

๑) มีขนาดไม่น้อยกว่า ๒ แกนหลัก (๒ Core) โดยมีความเร็วสัญญาณนาฬิกาไม่น้อยกว่า ๓.๒ GHz

๒) มีขนาดไม่น้อยกว่า ๔ แกนหลัก (๔ Core) โดยมีความเร็วสัญญาณนาฬิกาไม่น้อยกว่า ๑.๖ GHz

๕.๔.๒ มีหน่วยความจำแบบ Cache Memory ขนาดไม่น้อยกว่า ๓ MB

๕.๔.๓ มีหน่วยความจำหลัก (RAM) ชนิด DDR๔ หรือดีกว่า ขนาดไม่น้อยกว่า ๘ GB

๕.๔.๔ มีหน่วยจัดเก็บข้อมูล (Hard Disk) ขนาดความจุไม่น้อยกว่า ๑ TB จำนวน ๑ หน่วย หรือ Solid State Drive ขนาดความจุไม่น้อยกว่า ๑๒๐ GB จำนวน ๑ หน่วย

๕.๔.๕ มีจอภาพที่รองรับความละเอียดไม่น้อยกว่า ๑,๓๖๖x๗๖๘ Pixel และมีขนาดไม่น้อยกว่า ๑๒ นิ้ว

๕.๔.๖ มี DVD-RW หรือดีกว่า แบบติดตั้งภายใน (Internal) หรือภายนอก (External) จำนวน ๑ หน่วย

๕.๔.๗ มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ ๑๐/๑๐๐/๑๐๐๐ Base-T หรือดีกว่า จำนวนไม่น้อยกว่า ๑ ช่อง

๕.๔.๘ มีช่องเชื่อมต่อ (Interface) แบบ USB ๒.๐ หรือดีกว่า ไม่น้อยกว่า ๓ ช่อง

๕.๔.๙ มีช่องเชื่อมต่อแบบ HDMI หรือ VGA จำนวนไม่น้อยกว่า ๑ ช่อง

๕.๔.๑๐ สามารถใช้งาน Wi-Fi (๘๐๒.๑๑b, g, n, ac) และ Bluetooth ได้เป็นอย่างน้อย

๕.๔.๑๑ มีเมาส์แบบไร้สาย

๕.๔.๑๒ มีกระเป๋าพร้อมสายสะพายสำหรับใส่เครื่องคอมพิวเตอร์โน้ตบุ๊กที่เสนอในโครงการ

๕.๕ ชุดโปรแกรมระบบปฏิบัติการ จำนวน ๘ ชุด มีคุณลักษณะอย่างน้อย ดังนี้

๕.๕.๑ เป็นระบบปฏิบัติการ Windows ๑๐ Pro เวอร์ชั่นล่าสุด หรือดีกว่า

๕.๕.๒ เป็นสิทธิการใช้งานประเภทติดตั้งมาจากโรงงาน (OEM) หรือแบบ Full Package Product (FPP)

๕.๕.๓ สามารถใช้งานได้กับเครื่องคอมพิวเตอร์ตั้งโต๊ะ และเครื่องคอมพิวเตอร์โน้ตบุ๊ก ที่เสนอในโครงการ

๕.๕.๔ มีลิขสิทธิ์ที่ถูกต้องตามกฎหมาย

๕.๖ ชุดโปรแกรมสำนักงาน จำนวน ๘ ชุด มีคุณลักษณะอย่างน้อย ดังนี้

๕.๖.๑ เป็น Microsoft Office ๒๐๑๙ หรือเวอร์ชั่นล่าสุด หรือดีกว่า

๕.๖.๒ ประกอบไปด้วย Microsoft Word, Microsoft Excel และ Microsoft PowerPoint เป็นอย่างน้อย

๕.๖.๓ สามารถใช้งานได้กับเครื่องคอมพิวเตอร์ตั้งโต๊ะ และเครื่องคอมพิวเตอร์โน้ตบุ๊ก ที่เสนอในโครงการ

๕.๖.๔ มีลิขสิทธิ์ที่ถูกต้องตามกฎหมาย

๕.๗ ซอฟต์แวร์ Vulnerability Assessment ประเภทที่ ๑ จำนวน ๑ ชุด มีคุณลักษณะอย่างน้อย ดังนี้

๕.๗.๑ สามารถตรวจสอบช่องโหว่ของเว็บแอพพลิเคชันได้

๕.๗.๒ สามารถตรวจสอบช่องโหว่จาก URL หรือ IP ของเว็บไซต์ผ่านทางมาตรฐาน HTTP/HTTPS (SSL/TLS)

๕.๗.๓ สามารถตรวจสอบช่องโหว่ของ Web Application ตามมาตรฐาน OWASP

๕.๗.๔ สามารถประเมินความรุนแรงของช่องโหว่ที่ได้จากการตรวจสอบได้

๕.๗.๕ สามารถตั้งเวลาในการตรวจสอบช่องโหว่ได้

๕.๗.๖ สามารถตรวจสอบช่องโหว่ได้พร้อมกันไม่น้อยกว่า ๕ URL หรือ IP

๕.๗.๗ มีคำแนะนำวิธีในการแก้ไขปัญหาในเบื้องต้นของช่องโหว่ที่ได้จากการตรวจสอบได้

๕.๗.๘ สามารถออกรายงานในรูปแบบ XML, PDF, HTML และ CSV ได้

๕.๗.๙ สามารถออกรายงานตามมาตรฐาน ISO/IEC ๒๗๐๐๑ ได้

๕.๗.๑๐ มีลิขสิทธิ์การใช้งานที่ถูกต้องตามกฎหมาย และสามารถปรับปรุงข้อมูลช่องโหว่ เป็นระยะเวลาไม่น้อยกว่า ๒ ปี

๕.๘ ซอฟต์แวร์ Vulnerability Assessment ประเภทที่ ๒ จำนวน ๑ ชุด มีคุณลักษณะอย่างน้อย ดังนี้

๕.๘.๑ สามารถตรวจสอบช่องโหว่ได้อย่างน้อย ดังนี้

๑) อุปกรณ์เครือข่าย ได้แก่ Firewall, Router, Switch, Wireless Controller

๒) ระบบ Virtualization ได้แก่ VMware ESX, VMware ESXi, Vmware vSphere, Vmware vCenter

๓) ระบบปฏิบัติการ ได้แก่ Windows, OS X, Linux, Solaris

๔) ระบบฐานข้อมูล ได้แก่ Oracle, SQL Server, MySQL, DB๒

๕.๘.๒ สามารถตรวจสอบช่องโหว่ของเครื่องคอมพิวเตอร์ลูกข่ายได้

๕.๘.๓ สามารถจัดลำดับคะแนนความเสี่ยงของช่องโหว่ได้จากการตรวจสอบ ตามมาตรฐาน CVSS (Common Vulnerability Scoring System) ได้

๕.๘.๔ สามารถประเมินความรุนแรงของช่องโหว่ที่ได้จากการตรวจสอบได้

๕.๘.๕ สามารถตรวจสอบช่องโหว่แบบไม่จำกัดจำนวนเครื่อง

๕.๘.๖ สามารถตรวจสอบช่องโหว่ภายในระบบเครือข่ายผ่าน IPv๔ และ IPv๖

๕.๘.๗ สามารถตั้งเวลาในการตรวจสอบช่องโหว่ได้

๕.๘.๘ มีคำแนะนำวิธีในการแก้ไขปัญหาในเบื้องต้นของช่องโหว่ที่ได้จากการตรวจสอบได้

๕.๘.๙ สามารถออกรายงานในรูปแบบ XML, PDF, HTML และ CSV ได้

๕.๘.๑๐ สามารถติดตั้งบนระบบปฏิบัติการได้อย่างน้อย ดังนี้

๑) ระบบปฏิบัติการ Linux เช่น Red Hat, CentOS

๒) ระบบปฏิบัติการ Windows

๓) ระบบ Virtualization ได้แก่ Microsoft HyperV, VMware ESX ในแบบติดตั้งโดยตรง หรือแบบติดตั้งผ่านระบบปฏิบัติการในข้อ ๕.๘.๑๐ ๑) และ ๕.๘.๑๐ ๒)

๕.๘.๑๑ มีลิขสิทธิ์การใช้งานที่ถูกต้องตามกฎหมาย และสามารถปรับปรุงข้อมูลช่องโหว่ เป็นระยะเวลาไม่น้อยกว่า ๒ ปี

๖. การพัฒนาระบบความมั่นคงปลอดภัยของกระทรวงการคลัง จำนวน ๑ ระบบ มีรายละเอียดอย่างน้อย ดังนี้

๖.๑ ออกแบบและจัดทำสื่อวีดิทัศน์ ในรูปแบบเอนิเมชั่น ที่แสดงเนื้อหาที่เกี่ยวข้องกับการสร้างความตระหนักการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างปลอดภัย ความยาวไม่น้อยกว่า ๑ นาที ๓๐ วินาที จำนวนไม่น้อยกว่า ๑๒ ชิ้นงาน ทั้งนี้ต้องนำเสนอหัวข้อและร่าง Storyboard ให้คณะกรรมการตรวจรับพิจารณาก่อนดำเนินงาน โดยชิ้นงานดังกล่าวทั้งหมดถือเป็นลิขสิทธิ์เป็นของสำนักงานปลัดกระทรวงการคลัง

๖.๒ ออกแบบและจัดทำโปสเตอร์ประชาสัมพันธ์ในรูปแบบ Infographic ขนาดไม่น้อยกว่า A๓ ที่แสดงเนื้อหาที่เกี่ยวข้องกับการสร้างความตระหนักการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างปลอดภัย จำนวนไม่น้อยกว่า ๑๒ ชิ้นงาน พร้อมส่งชิ้นงานดังกล่าวทั้งหมดในรูปแบบอิเล็กทรอนิกส์ ทั้งนี้ต้องนำเสนอหัวข้อและร่างออกแบบ ให้คณะกรรมการตรวจรับพิจารณาก่อนดำเนินงาน โดยชิ้นงานดังกล่าวทั้งหมดถือเป็นลิขสิทธิ์ของสำนักงานปลัดกระทรวงการคลัง

๖.๓ จัดทำข้อเสนอแนะในเอกสารแนวนโยบายด้านความมั่นคงปลอดภัยของสำนักงานปลัดกระทรวงการคลัง และปรับปรุงเอกสารร่างแนวนโยบายด้านความมั่นคงปลอดภัยของสำนักงานปลัดกระทรวงการคลัง โดยอ้างอิงตามข้อกำหนดมาตรฐาน ISO/IEC ๒๗๐๐๑

๖.๔ จัดทำร่างนโยบายคุ้มครองข้อมูลส่วนบุคคลของสำนักงานปลัดกระทรวงการคลัง ประกอบไปด้วย

๑) จัดทำร่างนโยบายคุ้มครองข้อมูลส่วนบุคคลของสำนักงานปลัดกระทรวงการคลัง เพื่อให้เป็นไปตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ฉบับปัจจุบัน

๒) จัดทำร่างแผนผังการไหลของข้อมูลส่วนบุคคล

๓) จัดทำเอกสารและแบบฟอร์มต่าง ๆ เพื่อใช้ประกอบการดำเนินงานตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

๔) ดำเนินการร่างกระบวนการตรวจสอบ Data Processor ที่สำนักงานปลัดกระทรวงการคลังมีการส่งต่อข้อมูลส่วนบุคคลต่าง ๆ

๖.๕ ดำเนินการวิเคราะห์ Gap Analysis ตามมาตรฐาน ISO/IEC ๒๗๐๐๑ โดยดำเนินการพัฒนาร่างระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System) ตามมาตรฐาน ISO/IEC ๒๗๐๐๑:๒๐๑๓ สำหรับห้อง Data Center ประกอบไปด้วย

๑) จัดทำร่างเอกสารบริบทขององค์กร (Context of the Organization) โดยต้องระบุประเด็นภายใน (Internal issues) และประเด็นภายนอก (External issues)

๒) วิเคราะห์ช่องว่างมาตรการควบคุมความมั่นคงปลอดภัยของสารสนเทศตามมาตรฐาน ISO/IEC ๒๗๐๐๑:๒๐๑๓ (Gap Analysis of Information Security Controls) พร้อมจัดทำรายงานผลการวิเคราะห์ช่องว่างมาตรการควบคุมความมั่นคงปลอดภัยสารสนเทศ

๓) จัดทำร่างกรอบการบริหารจัดความมั่นคงปลอดภัยสารสนเทศ (ISMS Framework)

๔) จัดทำร่างนโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Policy)

๕) จัดทำร่างขั้นตอนการประเมินความเสี่ยงความมั่นคงปลอดภัยของสารสนเทศ (Information Security Risk Assessment Methodology) ให้สอดคล้องข้อกำหนดตามมาตรฐาน ISO/IEC ๒๗๐๐๑:๒๐๑๓

๖) ประเมินความเสี่ยงความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Assessing) และจัดทำผลการประเมินความเสี่ยงความมั่นคงปลอดภัยสารสนเทศ

๗) จัดทำร่างแผนลดความเสี่ยงความมั่นคงปลอดภัยของสารสนเทศ (Risk Treatment Plan)

๘) นำเสนอผลการดำเนินการวิเคราะห์ Gap Analysis ตามมาตรฐาน ISO/IEC ๒๗๐๐๑

๖.๖ การพัฒนาระบบเฝ้าระวังภัยคุกคามต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร ประกอบด้วย

๑) ดำเนินการประเมินความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร ของอุปกรณ์ และระบบงาน ของสำนักงานปลัดกระทรวงการคลัง

๒) ออกแบบ และพัฒนา Use-Case จำนวนไม่น้อยกว่า ๑๐ Use-Case

๓) ทำการรวบรวมข้อมูล Log หรือ Event ของอุปกรณ์ และระบบงาน ที่เกี่ยวข้องในการทำ Use-Case จำนวนไม่น้อยกว่า ๒๐ อุปกรณ์

๔) ออกแบบ และพัฒนา Security Dashboard สำหรับการเฝ้าระวังภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๕) ออกแบบ และพัฒนาระบบการแจ้งเตือนกรณีตรวจพบเหตุการณ์ผิดปรกติ/ภัยคุกคามตามระดับความสำคัญหรือความรุนแรง ผ่านทางช่องทางอีเมล์

๖) ออกแบบ และพัฒนากระบวนการปฏิบัติงาน กระบวนการตอบสนองต่อเหตุการณ์ผิดปรกติ/ภัยคุกคาม

๖.๗ ดำเนินการตรวจสอบช่องโหว่ด้วยการทำ Vulnerability Assessment พร้อมรายงานผลและข้อเสนอในการแก้ไขช่องโหว่ จำนวนไม่น้อยกว่า ๕๐ อุปกรณ์ หรือ IP Address อย่างน้อย ๑ ครั้ง และต้องจัดทำแผนการตรวจสอบช่องโหว่ ก่อนดำเนินงานทุกครั้ง

๖.๘ ดำเนินการเจาะระบบ Web Penetration Testing จำนวนไม่น้อยกว่า ๕ URLs อย่างน้อย ๑ ครั้ง และต้องจัดทำแผนการเจาะระบบ ก่อนดำเนินงานทุกครั้ง

๖.๙ ดำเนินการเจาะระบบภายในองค์กร (Internal Penetration Testing) พร้อมรายงานผล จำนวนไม่น้อยกว่า ๑๐ อุปกรณ์ หรือ IP Address อย่างน้อย ๑ ครั้ง และต้องจัดทำแผนการเจาะระบบ ก่อนดำเนินงานทุกครั้ง

๖.๑๐ จัดการฝึกซ้อมรับมือภัยคุกคามต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Security Drill) จำนวนไม่น้อยกว่า ๔ ครั้ง ด้วยการทำ E-Mail Phishing หรือรูปแบบอื่นตามที่คณะกรรมการตรวจรับกำหนด ในกรณีที่ดำเนินการทำ E-mail Phishing ผู้เสนอราคาต้องทำ E-Mail Phishing ภายในเครือข่ายของกระทรวงการคลัง และห้ามส่งผลการวิเคราะห์การตกเป็นเหยื่อออกนอกเครือข่าย

๖.๑๑ จัดอบรม หลักสูตรการสร้างความตระหนักในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างปลอดภัย (Security Awareness) จำนวนไม่น้อยกว่า ๒ หลักสูตร โดยในแต่ละหลักสูตร มีผู้เข้าอบรมจำนวนไม่น้อยกว่า ๕๐ คน และมีระยะเวลาไม่น้อยกว่า ๐.๕ วัน

๖.๑๒ จัดให้มีบุคลากรหรือเจ้าหน้าที่ปฏิบัติงานเฝ้าระวังภัยคุกคาม (Security Monitoring Officer) ซึ่งมีวุฒิการศึกษาขั้นต่ำระดับปริญญาตรี สาขาวิทยาการคอมพิวเตอร์ หรือสาขาอื่น ๆ ที่มีความเกี่ยวข้อง และมีประสบการณ์ด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร อย่างน้อย ๒ ปี และมีใบรับรองที่เกี่ยวข้องกับด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร อย่างน้อย ๑ ใบรับรอง มาประจำที่สำนักงานปลัดกระทรวงการคลัง จำนวนไม่น้อยกว่า ๑ คน เป็นระยะเวลาอย่างน้อย ๑ ปี โดยปฏิบัติงานในวันและเวลาราชการ ดังต่อไปนี้

๑) ติดตามเฝ้าระวังและแจ้งเหตุภัยคุกคามต่อระบบเทคโนโลยีสารสนเทศและการสื่อสารของกระทรวงการคลัง

๒) ให้คำปรึกษา คำแนะนำ ข้อเสนอแนะ และร่วมหารือกับเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง ในการบริหารจัดการเหตุการณ์ผิดปรกติ/ภัยคุกคาม

๓) จัดทำรายงานสรุปเหตุการณ์ผิดปรกติ/ภัยคุกคาม รายเดือน พร้อมจำแนกตามความระดับความสำคัญหรือความรุนแรง

๔) จัดทำรายงานประจำเดือนของสถานะของระบบเฝ้าระวังภัยคุกคาม

๕) ร่วมประชุมเพื่อรายงานสถานการณ์ด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารของกระทรวงการคลัง และรายงานข่าวสารสรุปสถานการณ์ด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๖.๑๓ จัดให้มีบุคลากรหรือเจ้าหน้าที่วิเคราะห์ภัยคุกคาม (Security Incident Analyst) ซึ่งมีวุฒิการศึกษาขั้นต่ำระดับปริญญาตรี สาขาวิทยาการคอมพิวเตอร์ หรือสาขาอื่น ๆ ที่มีความเกี่ยวข้อง และมีประสบการณ์เคยปฏิบัติงานในศูนย์เฝ้าระวังภัยคุกคามทางคอมพิวเตอร์ หรือ Security Operation Center (SOC) อย่างน้อย ๓ ปี และมีใบรับรองที่เกี่ยวข้องกับด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรือด้าน SIEM อย่างน้อย ๑ ใบรับรอง มาประจำที่สำนักงานปลัดกระทรวงการคลัง จำนวนไม่น้อยกว่า ๑ คน เป็นระยะเวลาอย่างน้อย ๑ ปี โดยปฏิบัติงาน ๑ วันต่อสัปดาห์ในวันและเวลาราชการ ดังต่อไปนี้

....

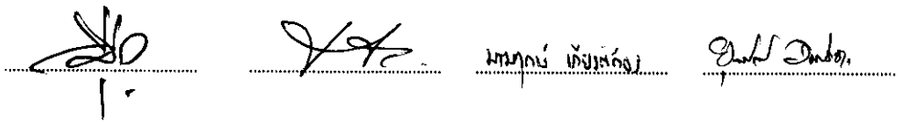
๑๐

๑) ติดตามเฝ้าระวังและแจ้งเหตุภัยคุกคามต่อระบบเทคโนโลยีสารสนเทศและการสื่อสารของกระทรวงการคลัง

๒) ให้คำปรึกษา คำแนะนำ ข้อเสนอแนะ และร่วมหารือกับเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง ในการบริหารจัดการเหตุการณ์ผิดปรกติ/ภัยคุกคาม

๓) ร่วมประชุมเพื่อรายงานสถานการณ์ด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารของกระทรวงการคลัง และรายงานข่าวสารสรุปสถานการณ์ด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๔) ตรวจสอบการปฏิบัติงานของ บุคลากรหรือเจ้าหน้าที่ปฏิบัติงานเฝ้าระวังภัยคุกคาม (Security Monitoring



ภาคผนวก ๒
รายละเอียดการติดตั้งและทดสอบ
โครงการพัฒนาระบบความมั่นคงปลอดภัยของกระทรวงการคลัง

ผู้ชนะการประกวดราคาต้องทำการติดตั้งระบบคอมพิวเตอร์และอุปกรณ์ทั้งหมดของโครงการพัฒนาระบบความมั่นคงปลอดภัยของกระทรวงการคลัง ณ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือศูนย์คอมพิวเตอร์กระทรวงการคลัง หรือสถานที่ที่คณะกรรมการตรวจรับกำหนด โดยต้องทำตามข้อกำหนดอย่างน้อยดังนี้

๑. การติดตั้ง

๑.๑ เสนอแผนและรูปแบบการติดตั้งระบบคอมพิวเตอร์และอุปกรณ์ ให้คณะกรรมการตรวจรับเห็นชอบ และดำเนินการติดตั้งตามแผนการติดตั้งที่ได้รับความเห็นชอบ

๑.๒ เดินสายไฟฟ้า เดินสายสัญญาณที่เชื่อมโยงระหว่างอุปกรณ์ที่ทำการติดตั้งเข้ากับอุปกรณ์เดิมที่มีอยู่ โดยรับผิดชอบค่าใช้จ่ายทั้งหมด เพื่อให้สามารถใช้งานได้อย่างเพียงพอครบถ้วน

๑.๓ ดำเนินการติดตั้ง และรับผิดชอบค่าใช้จ่ายทั้งหมดในการติดตั้งระบบคอมพิวเตอร์และอุปกรณ์ที่จัดซื้อตามโครงการนี้ทั้งหมด เพื่อให้ระบบคอมพิวเตอร์และอุปกรณ์สามารถทำงานได้ตามฟังก์ชั่น และมีประสิทธิภาพ

๑.๔ จัดหา ดำเนินการติดตั้ง และรับผิดชอบค่าใช้จ่ายทั้งหมดในการติดตั้งฮาร์ดแวร์ หรือซอฟต์แวร์ เพิ่มเติมเพื่อให้ระบบคอมพิวเตอร์และอุปกรณ์ที่จัดซื้อตามโครงการนี้ทั้งหมด สามารถทำงานได้ตามฟังก์ชั่น และมีประสิทธิภาพ

๑.๕ จัดทำ Label ที่มีรูปแบบและข้อความตามที่คณะกรรมการตรวจรับกำหนด สำหรับติดที่เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ ในตำแหน่งที่มองเห็นได้ชัดเจน

๑.๖ ในการดำเนินโครงการ ต้องประกอบไปด้วยผู้ปฏิบัติงานอย่างน้อย ดังต่อไปนี้

๑.๖.๑ ผู้จัดการโครงการ Project Manager จำนวนไม่น้อยกว่า ๑ คน
๑.๖.๒ IT Security Consultant จำนวนไม่น้อยกว่า ๑ คน
๑.๖.๓ IT Security Risk Analyst จำนวนไม่น้อยกว่า ๑ คน
๑.๖.๔ IT Security Architect จำนวนไม่น้อยกว่า ๑ คน
๑.๖.๕ IT Security Analyst จำนวนไม่น้อยกว่า ๒ คน
๑.๖.๖ IT Security Engineer จำนวนไม่น้อยกว่า ๒ คน
๑.๖.๗ Network Engineer จำนวนไม่น้อยกว่า ๑ คน
๑.๖.๘ System Engineer จำนวนไม่น้อยกว่า ๑ คน
๑.๖.๙ Graphic Designer จำนวนไม่น้อยกว่า ๒ คน
๑.๖.๑๐ Graphic Animator จำนวนไม่น้อยกว่า ๒ คน
๑.๖.๑๑ Administrative Officer จำนวนไม่น้อยกว่า ๑ คน

๑.๗ ในการเข้ามาปฏิบัติงาน ณ สำนักงานปลัดกระทรวงการคลัง ผู้ปฏิบัติงานในโครงการต้องติดบัตรสำหรับผู้มาติดต่อ โดยผู้ชนะการประกวดราคาต้องจัดหาบัตรดังกล่าวให้เพียงพอในการปฏิบัติงาน

๑๐

๒. การทดสอบและการตรวจรับ

๒.๑ ผู้ชนะการประกวดราคาต้องออกแบบ และวางแผนการทดสอบทั้งหมด โดยครอบคลุมหัวข้อการทดสอบดังต่อไปนี้

๒.๑.๑ การทดสอบการทำงานระหว่างระบบ (Integration Test)

๒.๑.๒ การทดสอบเพื่อการตรวจรับระบบ (User Acceptance Test)

ทั้งนี้ การทดสอบสามารถเปลี่ยนแปลงได้ตามที่คณะกรรมการตรวจรับกำหนด

๒.๒ ผู้ชนะการประกวดราคาต้องเป็นผู้รับผิดชอบค่าใช้จ่ายทั้งหมดที่เกิดขึ้นหากมีติดตั้งฮาร์ดแวร์ หรือซอฟต์แวร์ เพิ่มเติมที่เกี่ยวข้องกับการทดสอบทั้งหมด

๒.๓ ผู้ชนะการประกวดราคาต้องเป็นผู้รับผิดชอบค่าใช้จ่ายทั้งหมดที่เกิดขึ้นในการตรวจสอบการติดตั้งและการทดสอบของคณะกรรมการตรวจรับ

๑๐

ภาคผนวก ๓
รายละเอียดเอกสารและการฝึกอบรม
โครงการพัฒนาระบบความมั่นคงปลอดภัยของกระทรวงการคลัง

๑. เอกสารต่าง ๆ

ผู้ชนะการประกวดราคา ต้องจัดทำคู่มือและเอกสาร จำนวน ๒ ชุด และสำเนาในรูปแบบอิเล็กทรอนิกส์ลงใน Thumb Drive จำนวน ๕ ชุด โดยแต่ละชุดมีเนื้อหาอย่างน้อย ดังนี้

๑.๑ เอกสารการพัฒนาระบบความมั่นคงปลอดภัยของกระทรวงการคลังด้านการสร้างความตระหนักและการบริหารจัดการความมั่นคงปลอดภัย ประกอบด้วยเอกสารอย่างน้อยดังนี้

๑) รายงานการจัดทำสื่อวีดิทัศน์ ในรูปแบบเอนิเมชั่น
๒) รายงานการจัดทำโปสเตอร์ประชาสัมพันธ์ในรูปแบบ Infographic
๓) รายงานข้อเสนอแนะในเอกสารแนวนโยบายด้านความมั่นคงปลอดภัยของสำนักงานปลัดกระทรวงการคลัง และเอกสารร่างแนวนโยบายด้านความมั่นคงปลอดภัยของสำนักงานปลัดกระทรวงการคลังที่ได้ปรับปรุงแล้ว
๔) เอกสารร่างนโยบายคุ้มครองข้อมูลส่วนบุคคลของสำนักงานปลัดกระทรวงการคลัง
๕) เอกสารรายงานผลการวิเคราะห์ Gap Analysis ตามมาตรฐาน ISO ๒๗๐๐๑

๑.๒ เอกสาร System, Network & Security Architecture ประกอบด้วยเอกสารอย่างน้อยดังนี้

๑) System Architecture/Configuration Diagram
๒) Network & Security Architecture/Configuration Diagram
๓) Rack Layout/Installation Diagram
๔) Software and Application Configuration

๑.๓ รายการผลการทดสอบตามภาคผนวก ๒ ข้อ ๒.๑

๑.๔ รายการระบบคอมพิวเตอร์และอุปกรณ์ และสิทธิ์การใช้งานที่ส่งมอบพร้อมรายละเอียดโดยสังเขป

๑.๕ คู่มือและเอกสาร Operation Procedure ซึ่งมีรายละเอียดอย่างน้อยดังนี้

๑) การเปิด-ปิด การใช้งาน และ Routine Job/House Keeping Job ที่ใช้งานในระบบ
๒) การ Monitor ระบบ และการใช้งาน Monitoring Tool (ถ้ามี)

๑.๖ วิธีการและแผนการบำรุงรักษา Preventive Maintenance

๑.๗ เอกสารการตรวจสอบและเฝ้าระวังความมั่นคงปลอดภัย ประกอบด้วยเอกสารอย่างน้อยดังนี้

๑) รายงานผลการตรวจหาช่องโหว่ (Vulnerability Assessment)
๒) รายงานผลการเจาะระบบ (Web Penetration Testing)
๓) รายงานผลการเจาะระบบภายในองค์กร (Internal Penetration Testing)
๔) รายงานผลการฝึกซ้อมรับมือภัยคุกคามต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Security Drill)
๕) เอกสารการพัฒนา Use-Case/Security Dashboard สำหรับการเฝ้าระวังภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร
๖) เอกสารการพัฒนาระบบการแจ้งเตือนกรณีตรวจพบเหตุการณ์ผิดปรกติ/ภัยคุกคาม
๗) เอกสารกระบวนการปฏิบัติงาน กระบวนการตอบสนองต่อเหตุการณ์ผิดปรกติ/ภัยคุกคาม

๒. การฝึกอบรม

ผู้ชนะการประกวดราคา ต้องจัดให้มีการฝึกอบรมให้กับบุคลากรของสำนักงานปลัดกระทรวงการคลัง โดยต้องทำตามข้อกำหนดอย่างน้อยดังนี้

๒.๑ ผู้ชนะการประกวดราคา ต้องเสนอแผนการฝึกอบรมบุคลากรของสำนักงานปลัดกระทรวงการคลังที่เกี่ยวข้องกับการใช้และดูแลระบบ โดยต้องเสนอหลักสูตรฝึกอบรมให้เหมาะสม โดยระบุรายละเอียดอย่างน้อยดังนี้

๑) ประสบการณ์การทำงานของผู้สอน

๒) ภาพรวมและเค้าโครงหลักสูตร

๓) ระดับผู้เข้ารับการอบรม

๔) จำนวนผู้รับเข้าอบรม

๕) ระยะเวลาการฝึกอบรม

๖) ช่วงเวลาที่จะดำเนินการฝึกอบรม

๗) สถานที่ฝึกอบรม

๒.๒ ผู้สอนจะต้องมีความรู้ ความเชี่ยวชาญ และความชำนาญในหลักสูตรฝึกอบรม

๒.๓ ผู้ชนะการประกวดราคาต้องจัดเตรียม หนังสือ, เอกสารประกอบการฝึกอบรม, อาหารว่าง, ซอฟต์แวร์ (ถ้ามี) ให้เพียงพอกับผู้เข้าฝึกอบรม

๒.๔ ผู้ชนะการประกวดราคาต้องรับผิดชอบค่าใช้จ่ายทั้งหมดในการฝึกอบรม ซึ่งประกอบไปด้วยหลักสูตรอย่างน้อยดังต่อไปนี้

หัวข้อฝึกอบรม	บุคคลเข้ารับการฝึกอบรม	จำนวน (อย่างน้อย)	ระยะเวลา (อย่างน้อย)
อุปกรณ์บริหารจัดการข้อมูลและเหตุการณ์ด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร (SIEM)	ผู้ดูแลระบบ	๓ คน	๒ วัน
อุปกรณ์ Firewall	ผู้ดูแลระบบ	๓ คน	๒ วัน
อุปกรณ์ Advanced Persistent Threat	ผู้ดูแลระบบ	๓ คน	๒ วัน
อุปกรณ์ Web Application Firewall	ผู้ดูแลระบบ	๓ คน	๒ วัน
ระบบแสดงผลสำหรับการเฝ้าระวังเหตุการณ์ผิดปรกติ/ภัยคุกคาม และอุปกรณ์ Video Controller	ผู้ดูแลระบบ	๓ คน	๑ วัน
ซอฟต์แวร์ที่ใช้ดำเนินการ Vulnerability Assessment	ผู้ดูแลระบบ	๓ คน	๑ วัน
ระบบเฝ้าระวังภัยคุกคามต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร	ผู้ดูแลระบบ	๕ คน	๑ วัน
หลักสูตรการสร้างความตระหนักในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างปลอดภัย (Security Awareness) จำนวน ๒ หลักสูตร	บุคลากรของสำนักงานปลัดกระทรวงการคลัง	๕๐ คน/หลักสูตร	๓ ชั่วโมง/หลักสูตร

ภาคผนวก ๔
รายละเอียดการบริการบำรุงรักษาและซ่อมแซมแก้ไข
โครงการพัฒนาระบบความมั่นคงปลอดภัยของกระทรวงการคลัง

ผู้ชนะการประกวดราคา ต้องบริการบำรุงรักษา ซ่อมแซม แก้ไข หรือเปลี่ยนแทน ระบบคอมพิวเตอร์และอุปกรณ์ทุกรายการของโครงการ นับตั้งแต่ตรวจรับงานสุดท้ายเสร็จสมบูรณ์ เป็นระยะเวลารับประกัน ๑ ปี โดยต้องปฏิบัติตามเงื่อนไขดังต่อไปนี้

๑. การบริการและการสนับสนุน

ผู้ชนะการประกวดราคาต้องสนับสนุนและให้คำปรึกษาแนะนำเกี่ยวกับการใช้งานระบบคอมพิวเตอร์และอุปกรณ์ที่เสนอทั้งหมดภายหลังติดตั้ง

๒. การบำรุงรักษาและซ่อมแซมแก้ไข

ผู้ชนะการประกวดราคา มีหน้าที่บำรุงรักษาและซ่อมแซมแก้ไขระบบคอมพิวเตอร์และอุปกรณ์สำหรับโครงการพัฒนาระบบความมั่นคงปลอดภัยของกระทรวงการคลัง ไม่ว่าจะติดตั้ง ณ สถานที่ใด ๆ ตามที่กำหนดในสัญญาให้อยู่ในสภาพใช้งานได้ดีอยู่เสมอตลอดระยะเวลารับประกันด้วยค่าใช้จ่ายของผู้ชนะการประกวดราคา หากระบบคอมพิวเตอร์และอุปกรณ์บกพร่องหรือใช้งานไม่ได้ และความชำรุดนี้มิได้เกิดจากความผิดของสำนักงานปลัดกระทรวงการคลัง ผู้ชนะการประกวดราคาต้องจัดการซ่อมแซมแก้ไขให้อยู่ในสภาพดีได้ดังเดิมโดยไม่คิดค่าใช้จ่ายใดๆ จากสำนักงานปลัดกระทรวงการคลัง ทั้งนี้ต้องเริ่มจัดการซ่อมแซมแก้ไขหลังจากที่ได้รับแจ้งจากสำนักงานปลัดกระทรวงการคลังหรือผู้ที่ได้รับมอบหมายจากสำนักงานปลัดกระทรวงการคลัง

๒.๑ สำหรับเครื่องคอมพิวเตอร์และอุปกรณ์ ต้องเริ่มจัดการซ่อมแซมแก้ไขภายใน ๓ ชั่วโมง หลังจากที่ได้รับแจ้งจากสำนักงานปลัดกระทรวงการคลังหรือผู้ที่ได้รับมอบหมายจากสำนักงานปลัดกระทรวงการคลัง หากไม่สามารถเริ่มจัดการซ่อมแซมแก้ไขภายในเวลาดังกล่าว ผู้ชนะการประกวดราคาต้องถูกปรับ ในอัตราชั่วโมงละ ๓,๐๐๐.- บาท (สามพันบาทถ้วน) เศษของชั่วโมงให้นับเป็น ๑ ชั่วโมง ถ้าการซ่อมแซมแก้ไขไม่แล้วเสร็จภายใน ๑๒ ชั่วโมง นับแต่เริ่มทำการซ่อมแซมแก้ไข ผู้ชนะการประกวดราคา ต้องนำเครื่องหรืออุปกรณ์สำรองที่มีประสิทธิภาพทัดเทียมกัน ที่สามารถใช้งานได้เป็นปรกติดังเดิม มาให้ใช้แทนไปจนกว่าจะซ่อมแซมแล้วเสร็จสมบูรณ์ หากไม่สามารถติดตั้งเครื่องหรืออุปกรณ์ที่มาให้ใช้แทนดังกล่าว ให้สามารถใช้งานได้เป็นปรกติดังเดิมได้ ผู้ชนะการประกวดราคาต้องถูกปรับ ในอัตราชั่วโมงละ ๑๐,๐๐๐.- บาท (หนึ่งหมื่นบาทถ้วน) นับตั้งแต่ชั่วโมงที่ ๑๒ เป็นต้นไป เศษของชั่วโมงให้นับเป็น ๑ ชั่วโมง

สำนักงานปลัดกระทรวงการคลังยอมให้เครื่องคอมพิวเตอร์และอุปกรณ์ ขัดข้องได้ไม่เกินเดือนละ ๑๒ ชั่วโมง โดยเริ่มนับเวลาตั้งแต่ที่ซ่อมแซมแก้ไขไม่แล้วเสร็จภายใน ๑๒ ชั่วโมง และไม่สามารถนำเครื่องหรืออุปกรณ์สำรองที่มีประสิทธิภาพทัดเทียมกันมาให้ใช้แทนไปจนกว่าจะซ่อมแซมแล้วเสร็จสมบูรณ์ ผู้ชนะการประกวดราคาต้องถูกปรับ ในอัตราชั่วโมงละ ๑๐,๐๐๐.- บาท (หนึ่งหมื่นบาทถ้วน) นับตั้งแต่ชั่วโมงที่ ๑๒ เป็นต้นไป เศษของชั่วโมงให้นับเป็น ๑ ชั่วโมง

๒.๒ ผู้ชนะการประกวดราคาต้องทำการบำรุงรักษาระบบและซอฟต์แวร์ทั้งหมดในโครงการนี้ ตลอดระยะเวลารับประกัน โดยไม่คิดค่าใช้จ่ายใดๆ ในกรณีที่มีข้อผิดพลาดอันเนื่องมาจากการทำงานของระบบ และซอฟต์แวร์ ผู้ชนะการประกวดราคาต้องทำการแก้ไข และปรับปรุงระบบและซอฟต์แวร์ ให้ถูกต้องแล้วเสร็จ โดยไม่คิดค่าใช้จ่าย ใดๆ จากสำนักงานปลัดกระทรวงการคลัง ทั้งนี้ต้องเริ่มทำการแก้ไขหลังจากที่ได้รับแจ้งจาก

สำนักงานปลัดกระทรวงการคลังหรือผู้ที่ได้รับมอบหมายจากสำนักงานปลัดกระทรวงการคลังภายใน ๑๒ ชั่วโมง หากไม่สามารถเริ่มทำการแก้ไขภายในเวลาดังกล่าว ผู้ชนะการประกวดราคาต้องถูกปรับ ในอัตราชั่วโมงละ ๑๐,๐๐๐.- บาท (หนึ่งหมื่นบาทถ้วน) เศษของชั่วโมงนับเป็น ๑ ชั่วโมง

๒.๓ ผู้ชนะการประกวดราคาต้องจัดหาบุคลากรหรือเจ้าหน้าที่ปฏิบัติงานเฝ้าระวังภัยคุกคาม (Security Monitoring Officer) และบุคลากรหรือเจ้าหน้าที่วิเคราะห์ภัยคุกคาม (Security Incident Analyst) มาประจำที่สำนักงานปลัดกระทรวงการคลัง รายละเอียดตามภาคผนวก ๑ ข้อ ๖.๑๒ และข้อ ๖.๑๓ ในกรณีที่เจ้าหน้าที่ไม่มาปฏิบัติงาน ต้องหาเจ้าหน้าที่ที่มีคุณสมบัติตามที่กำหนดมาปฏิบัติหน้าที่แทน มิฉะนั้นผู้ชนะการประกวดราคาต้องถูกปรับ ในอัตราวันละ ๒,๐๐๐.- บาท (สองพันบาทถ้วน) ทั้งนี้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ขอสงวนสิทธิ์ในการเปลี่ยนตัวเจ้าหน้าที่ได้

๒.๔ ในกรณีที่มีการเปลี่ยนแปลง แก้ไขปรับปรุง เพิ่มเติมซอฟต์แวร์ในลักษณะ Upgrade Release หรือ Version ใหม่ให้ทันสมัยขึ้น ผู้ชนะการประกวดราคาต้องมาติดตั้งให้โดยไม่คิดค่าใช้จ่ายใดๆ ทั้งสิ้น ทั้งนี้การติดตั้งดังกล่าวต้องได้รับเห็นชอบจากสำนักงานปลัดกระทรวงการคลังหรือผู้ที่ได้รับมอบหมายจากสำนักงานปลัดกระทรวงการคลังก่อน

๓. การบำรุงรักษาแบบป้องกัน (Preventive Maintenance)

ผู้ชนะการประกวดราคาต้องเสนอแผน และทำการบำรุงรักษา (Preventive Maintenance) ระบบคอมพิวเตอร์และอุปกรณ์สำหรับโครงการพัฒนาและปรับปรุงระบบความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร กระทรวงการคลัง อย่างน้อย ๓ เดือนต่อ ๑ ครั้ง นับจากวันตรวจรับงวดสุดท้ายเสร็จสมบูรณ์ เพื่อให้อยู่ในสภาพที่ใช้งานได้อย่างมีประสิทธิภาพตลอดเวลา อย่างน้อยดังต่อไปนี้

(ก) ตรวจสอบการทำงาน และทำความสะอาด

(ข) ตรวจสอบค่า Configuration และทำการสำรองข้อมูล Configuration

หากผู้ชนะการประกวดราคาไม่สามารถทำการบำรุงรักษา (Preventive Maintenance) ดังกล่าวได้ ผู้ชนะการประกวดราคาต้องถูกปรับในอัตราครั้งละ ๒๐,๐๐๐.- บาท (สองหมื่นบาทถ้วน)