ขอบเขตของงาน

โครงการศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ระยะที่ ๑

---

๑. <u>ความเป็นมา</u>

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงมหาดไทย ได้จัดทำโครงการศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ระยะที่ ๑ ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงมหาดไทย โดยจัดให้มีระบบวิเคราะห์ระบบเฝ้าระวังและป้องกันภัยคุกคามไซเบอร์อัจฉริยะ, อุปกรณ์ตรวจจับ, วิเคราะห์ และเฝ้าระวังภัยคุกคามบนระบบเครือข่าย ที่มีลิขสิทธิ์ถูกต้อง ทำการติดตั้งที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารสำนักงานปลัดกระทรวงมหาดไทย และศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเขต ๑ – ๑๒ รวมทั้งศาลากลางจังหวัดจำนวน ๗๖ จังหวัด เพื่อให้ครอบคลุมการใช้งานป้องกันภัยคุกคามกับหน่วยงานในสังกัดสำนักงานปลัดกระทรวงมหาดไทยทั้งหมด โดยปัจจุบันระบบเทคโนโลยีสารสนเทศใหม่ ๆ ซึ่งมีการพัฒนาเพิ่มขึ้นหลายรูปแบบ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงมหาดไทย จึงได้จัดทำโครงการศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ระยะที่ ๑ ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงมหาดไทย

เพื่อทำให้ระบบรักษาความปลอดภัยด้านสารสนเทศที่ใช้งานอยู่ในปัจจุบันตอบสนองต่อการให้บริการ รวมถึงปริมาณการใช้งานที่เพิ่มขึ้นในปัจจุบัน และสามารถรองรับการทำงานได้อย่างมีประสิทธิภาพ ให้ทันสมัย ครอบคลุมการทำงาน รองรับระบบงาน และเทคโนโลยีสารสนเทศรูปแบบใหม่ ประกอบกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และพระราชบัญญัติที่เกี่ยวข้องได้มีข้อกำหนดเพิ่มเติม จึงจำเป็นที่จะต้องปรับปรุงระบบให้สามารถป้องกันภัยคุกคามไซเบอร์ใหม่ๆ ได้อย่างทันท่วงที

๒. <u>วัตถุประสงค์</u>

๒.๑ เพื่อให้หน่วยงานในสำนักงานปลัดกระทรวงมหาดไทย มีความคล่องตัวในการเข้าถึงระบบงานต่าง ๆ ของสำนักงานปลัดกระทรวงมหาดไทยที่ใช้งานในปัจจุบัน และการเข้าถึงข้อมูลข่าวสารภายนอกได้อย่างสะดวกและรวดเร็ว ก่อให้เกิดประสิทธิภาพในการทำงาน และเพิ่มศักยภาพในการป้องกันคุกคามไซเบอร์

๒.๒ เพื่อเพิ่มประสิทธิภาพ ระบบวิเคราะห์ระบบเฝ้าระวังและป้องกันภัยคุกคามไซเบอร์อัจฉริยะ, อุปกรณ์ตรวจจับ, วิเคราะห์และเฝ้าระวังภัยคุกคามบนระบบเครือข่ายให้มีความมั่นคงปลอดภัย และรองรับเทคโนโลยีสารสนเทศใหม่ ๆ

๒.๓ เพื่อให้การเชื่อมโยงเครือข่ายในระบบเป็นแนวทางเดียวกัน ถูกต้องตามข้อกฎหมาย ระเบียบ และไม่เกิดปัญหากับเครือข่ายของสำนักงานปลัดกระทรวงมหาดไทย

๒.๔ เพื่อเพิ่มประสิทธิภาพและอำนวยความสะดวกในการให้บริการแก่ประชาชน และหน่วยงานที่มาขอรับบริการได้อย่างทั่วถึง และรวดเร็ว

๒.๕ เพื่อเพิ่มประสิทธิภาพระบบวิเคราะห์ระบบเฝ้าระวังและป้องกันภัยคุกคามไซเบอร์อัจฉริยะ, อุปกรณ์ตรวจจับ, วิเคราะห์และเฝ้าระวังภัยคุกคามบนระบบเครือข่ายให้ทันต่อเทคโนโลยีเพื่อต่อต้านภัยคุกคามทาง Cyber รูปแบบใหม่ ๆ

/๓. คุณสมบัติ...

ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....

๓. <u>คุณสมบัติผู้ยื่นเสนอ</u>

๓.๑ มีความสามารถตามกฎหมาย

๓.๒ ไม่เป็นบุคคลล้มละลาย

๓.๓ ไม่อยู่ระหว่างเลิกกิจการ

๓.๔ ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

๓.๕ ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

๓.๖ มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

๓.๗ เป็นนิติบุคคล ผู้มีอาชีพรับจ้างงานที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

๓.๘ ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่สำนักงานปลัดกระทรวงมหาดไทย ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

๓.๙ ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์ความคุ้มกันเช่นว่านั้น

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

๓.๑๑ ผู้ยื่นข้อเสนอสามารถเสนอในรูปแบบกิจการค้าร่วม/ร่วมค้า ดังนี้

๓.๑๑.๑ กรณีที่กิจการร่วมค้าได้จดทะเบียนเป็นนิติบุคลใหม่ กิจการร่วมค้าจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารประกวดราคา และการเสนอราคาให้เสนอในนาม “กิจการร่วมค้า” ส่วนคุณสมบัติด้านผลงาน กิจการส่วนร่วมค้าดังกล่าวสามารถนำผลงานของผู้ร่วมค้ามาใช้แสดงเป็นผลงานของกิจการร่วมค้าที่เข้าประกวดราคาได้

๓.๑๑.๒ กรณีที่กิจการร่วมค้าไม่ได้จดทะเบียนเป็นนิติบุคคลใหม่ นิติบุคคลแต่ละนิติบุคคลที่เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารประกวดราคา เว้นแต่ในกรณีที่กิจการร่วมค้าได้มีข้อตกลงระหว่างผู้เข้าร่วมค้าเป็นลายลักษณ์อักษรกำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้รับผิดชอบหลักในการเข้าเสนอราคากับหน่วยงานของรัฐ และแสดงหลักฐานดังกล่าวมาพร้อมการยื่นข้อเสนอประกวดราคาทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ กิจการร่วมค้านั้นสามารถใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

สำหรับข้อตกลงฯ ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมค้าหลัก ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน

๓.๑๑.๓ กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงฯ จะต้องมีการกำหนดสัดส่วนหน้าที่ และความรับผิดชอบในปริมาณงาน สิ่งของ หรือ มูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกรายการ

๓.๑๑.๔ กรณีที่ข้อตกลงฯ กำหนดให้มีการมอบหมายให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า การยื่นข้อเสนอดังกล่าวไม่ต้องมีหนังสือมอบอำนาจสำหรับข้อตกลงฯ

/ที่ไม่ได้กำหนด...

ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....

ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้ยื่นข้อเสนอ ผู้เข้าร่วมค้าทุกรายจะต้องลงลายมือชื่อในหนังสือมอบอำนาจให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า

๓.๑๑.๕ ให้ผู้เข้าร่วมค้าที่ได้รับมอบหมาย หรือมอบอำนาจตามข้อ ๓.๑๑.๔ ดำเนินการซื้อและดาวน์โหลดเอกสารประกวดราคาอิเล็กทรอนิกส์ กรณีที่มีการจำหน่ายเอกสารซื้อหรือจ้างหรือดาวน์โหลดเอกสารประกวดราคาอิเล็กทรอนิกส์ กรณีที่ไม่มีการจำหน่ายเอกสารซื้อหรือจ้าง จึงจะมีสิทธิ์ในการยื่นข้อเสนอในนามกิจการร่วมค้าได้

ทั้งนี้ "กิจการร่วมค้าที่จดทะเบียนเป็นนิติบุคคลใหม่" หมายความว่า กิจการร่วมค้าที่จดทะเบียนเป็นนิติบุคคลต่อกรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์

๓.๑๒ ผู้ยื่นเสนอต้องมีผลงานประเภทเดียวกันกับงานที่จะประกวดราคา เช่น เกี่ยวข้องกับระบบรักษาความปลอดภัยด้านสารสนเทศและการสื่อสาร เป็นต้น ให้กับส่วนราชการ รัฐวิสาหกิจ หรือบริษัทเอกชนที่เชื่อถือได้ มีมูลค่ารวมไม่น้อยกว่า ๒๐,๐๐๐,๐๐๐.-บาท (ยี่สิบล้านบาทถ้วน) ซึ่งผลงานดังกล่าวของผู้ยื่นข้อเสนอต้องเป็นผลงานในสัญญาเดียวกันเท่านั้น และเป็นสัญญาที่ผู้ยื่นเสนอได้ทำงานเสร็จตามสัญญา ซึ่งได้มีการส่งมอบงานและตรวจรับเรียบร้อยแล้ว หากยื่นข้อเสนอในรูปแบบกิจการค้าร่วม/ร่วมค้า ผู้ยื่นข้อเสนอต้องมีคุณสมบัติตามรายละเอียดคุณลักษณะเฉพาะฯ ข้อ ๓.๑๑ โดยต้องมีสำเนาสัญญาจ้างและหนังสือรับรองผลงานพร้อมเอกสารประกอบที่เชื่อถือได้ มาแสดงเพื่อประกอบการพิจารณา

๓.๑๓ ผู้ยื่นข้อเสนอจะต้องจัดทำตารางเปรียบเทียบรายละเอียดข้อกำหนดและรายละเอียด (Specification) เป็นรายข้อทุกข้อ (Statement of Compliance) ของเอกสารเสนอราคา (อุปกรณ์ที่ระบุในข้อกำหนดขอบเขตของงานและการดำเนินการทุกข้อระบุยี่ห้อ/รุ่นชัดเจนพร้อมแนบเอกสารแสดงคุณลักษณะ) โดยใช้ตัวอย่างแบบฟอร์มการเปรียบเทียบตามตารางที่ ๑ ในการเปรียบเทียบรายการดังกล่าว หากมีกรณีที่ต้องมีการอ้างอิงข้อความหรือเอกสารในส่วนอื่นที่จัดทำเสนอมา ผู้ยื่นข้อเสนอจะต้องระบุให้เห็นอย่างชัดเจนสามารถตรวจสอบได้ง่ายไว้ในเอกสารเปรียบเทียบด้วยว่า สิ่งที่ต้องการอ้างอิงถึงนั้นอยู่ในส่วนตำแหน่งใดของเอกสารอื่น ๆ ที่จัดทำเสนอมา สำหรับเอกสารที่อ้างอิงถึงให้ขีดเส้นใต้หรือระบายสีพร้อมเขียนหัวข้อกำกับไว้เพื่อให้สามารถไปตรวจสอบกับเอกสารเปรียบเทียบได้ง่ายและตรงกัน หากผู้ยื่นข้อเสนอไม่ดำเนินการตามข้อนี้ สำนักงานปลัดกระทรวงมหาดไทย จะขอสงวนสิทธิ์ในการไม่พิจารณาข้อเสนอของผู้ยื่นข้อเสนอรายนั้น เว้นแต่เป็นข้อผิดพลาด หรือผิดหลงเพียงเล็กน้อย หรือผิดแผกไปจากเงื่อนไขของเอกสารประกวดราคาในส่วนที่มิใช่สาระสำคัญ ทั้งนี้เฉพาะในกรณีที่พิจารณาเห็นว่าจะเป็นประโยชน์ต่อหน่วยงาน

ตารางที่ ๑ ตารางเปรียบเทียบคุณสมบัติข้อกำหนดและรายละเอียดข้อเสนอโครงการ

อ้างถึง	ข้อกำหนด/ที่ต้องการ	ข้อกำหนด/ที่เสนอ	เอกสารอ้างอิง
ระบุหัวข้อให้ตรงกับหัวข้อที่ระบุในเอกสารเสนอราคา	ให้คัดลอกคุณลักษณะเฉพาะที่กำหนดมากรอกในช่องนี้	ให้ระบุคุณลักษณะเฉพาะที่เสนอ	ระบุบทที่ และหมายเลขหน้าของเอกสารอ้างอิง

๓.๑๔ ผู้ยื่นข้อเสนอต้องทำการสาธิตและทดสอบการใช้งานจริง (Proof of concept : POC) ระบบวิเคราะห์ระบบเฝ้าระวังและป้องกันภัยคุกคามไซเบอร์อัจฉริยะ, อุปกรณ์ตรวจจับ, วิเคราะห์และเฝ้าระวังภัยคุกคามบนระบบเครือข่ายกับอุปกรณ์เครือข่ายของสำนักงานปลัดกระทรวงมหาดไทย เพื่อแสดงว่าระบบสามารถใช้งานร่วมกันได้อย่างมีประสิทธิภาพ ผู้ยื่นข้อเสนอจะต้องเป็นผู้จัดหา และนำอุปกรณ์เข้าร่วมในการทดสอบโดยมีรายละเอียด ดังนี้

๓.๑๔.๑ การทดสอบการใช้งานจริง (POC) โดยการจำลองการเชื่อมต่อเครือข่ายของสำนักงานปลัดกระทรวงมหาดไทย **มีรายละเอียดตามภาคผนวก ค**

/๓.๑๔.๒ ระบบวิเคราะห์...

๓.๑๔.๒ ระบบวิเคราะห์ระบบเฝ้าระวังและป้องกันภัยคุกคามไซเบอร์อัจฉริยะ, อุปกรณ์ตรวจจับ, วิเคราะห์และเฝ้าระวังภัยคุกคามบนระบบเครือข่ายที่นำมาทำการทดสอบการใช้งานจริง (POC) จะต้องเป็นยี่ห้อเดียวกันกับอุปกรณ์ที่ยื่นในเอกสารเสนอราคา และมีความสามารถด้านฟังก์ชันการทำงานของอุปกรณ์ไม่น้อยกว่าระบบที่จะเสนอจริง

๓.๑๔.๓ หากทดสอบการใช้งานจริง (POC) แล้ว ไม่สามารถทำได้ตามที่เสนอ หรือไม่มาทำการสาธิต และทดสอบ สำนักงานปลัดกระทรวงมหาดไทยจะถือว่าข้อเสนอทางเทคนิคของผู้ยื่นข้อเสนอไม่ถูกต้อง และจะไม่พิจารณาราคาของผู้ยื่นข้อเสนอรายนั้น

๓.๑๔.๔ ผู้ยื่นข้อเสนอต้องเป็นผู้รับผิดชอบค่าใช้จ่ายในการทดสอบระบบและอุปกรณ์ที่เกี่ยวข้องในการทดสอบ รวมทั้งหากเกิดความเสียหายที่เกี่ยวข้องกับการทดสอบผู้ยื่นข้อเสนอต้องเป็นผู้รับผิดชอบค่าใช้จ่าย

๓.๑๔.๕ กำหนดการทดสอบภายใน ๕ วันทำการ (นับถัดจากวันที่เสนอราคา)

๔. <u>ขอบเขตการดำเนินงาน</u>

ผู้ชนะการเสนอราคาจะต้องติดตั้งระบบวิเคราะห์ระบบเฝ้าระวังและป้องกันภัยคุกคามไซเบอร์อัจฉริยะ, อุปกรณ์ตรวจจับ, วิเคราะห์และเฝ้าระวังภัยคุกคามบนระบบเครือข่ายใหม่ที่จัดซื้อในครั้งนี้พร้อมทั้งติดตั้งค่าอุปกรณ์ (Configuration) ให้สามารถใช้งานได้

๔.๑ จัดหาพร้อมติดตั้งระบบวิเคราะห์ ระบบเฝ้าระวัง และป้องกันภัยคุกคามไซเบอร์อัจฉริยะ, อุปกรณ์ตรวจจับ, วิเคราะห์ และเฝ้าระวังภัยคุกคามบนระบบเครือข่ายตามสถานที่ดำเนินการที่ระบุไว้ใน**ภาคผนวก ข**

๔.๒ ระบบวิเคราะห์ ระบบเฝ้าระวัง และป้องกันภัยคุกคามไซเบอร์อัจฉริยะ, อุปกรณ์ตรวจจับ, วิเคราะห์ และเฝ้าระวังภัยคุกคามบนระบบเครือข่ายที่จัดหาใหม่ต้องใช้งานร่วมกันกับระบบรักษาความปลอดภัยเดิม (ที่ได้ดำเนินการติดตั้งใช้งานอยู่ในปัจจุบัน) ได้อย่างสมบูรณ์ และเป็นไปตามวัตถุประสงค์ มีดังนี้

๔.๒.๑ ระบบวิเคราะห์ ระบบเฝ้าระวัง และป้องกันภัยคุกคามไซเบอร์อัจฉริยะ จำนวน ๑ ระบบ

๔.๒.๒ อุปกรณ์ตรวจจับ, วิเคราะห์และเฝ้าระวังภัยคุกคามบนระบบเครือข่าย จำนวน ๑ ระบบ

๔.๒.๓ บริการเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cybersecurity Operations Center: CSOC) และตอบสนองต่อเหตุการณ์ที่อยู่ในข่ายเป็นภัยคุกคามทางไซเบอร์ (Managed Detection & Response: MDR) จำนวน ๑ งาน

๕. <u>วิธีการดำเนินการ</u>

๕.๑ ผู้ชนะการเสนอราคาจะต้องติดตั้งระบบวิเคราะห์ระบบเฝ้าระวังและป้องกันภัยคุกคามไซเบอร์อัจฉริยะ, อุปกรณ์ตรวจจับ, วิเคราะห์ และเฝ้าระวังภัยคุกคามบนระบบเครือข่ายตามคุณลักษณะเฉพาะทางเทคนิคใน **ภาคผนวก ก** และสถานที่ที่กำหนดใน **ภาคผนวก ข** พร้อมส่งมอบอุปกรณ์ทั้งหมดที่อยู่ในโครงการนี้ทั้งหมด

๕.๒ ผู้ชนะการเสนอราคาจะต้องส่งมอบผังการเชื่อมโยงอุปกรณ์ คู่มือการใช้งาน และวิธีดูแลรักษาระบบวิเคราะห์ ระบบเฝ้าระวัง และป้องกันภัยคุกคามไซเบอร์อัจฉริยะ, อุปกรณ์ตรวจจับ, วิเคราะห์ และเฝ้าระวังภัยคุกคามบนระบบเครือข่ายในโครงการนี้ โดยมอบให้สำนักงานปลัดกระทรวงมหาดไทย จำนวน ๒ ชุด

๕.๓ ผู้ชนะการเสนอราคาจะต้องทดสอบการทำงานของระบบวิเคราะห์ระบบเฝ้าระวังและป้องกันภัยคุกคามไซเบอร์อัจฉริยะ, อุปกรณ์ตรวจจับ, วิเคราะห์และเฝ้าระวังภัยคุกคามบนระบบเครือข่ายให้สามารถใช้งานได้อย่างสมบูรณ์

/๕.๔ ผู้ชนะ...

ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....

๕.๔ ผู้ชนะการเสนอราคาต้องจัดทำแผนการติดตั้งค่าอุปกรณ์ (Configuration) เช่น Secure Policy เบื้องต้นร่วมกับผู้ซื้อก่อนดำเนินงาน

๕.๕ ผู้ชนะการเสนอราคาจะต้องส่งแผนและขั้นตอนการดำเนินการ และออกแบบการติดตั้ง และจัดทำแผนผังการเชื่อมโยงระบบ อุปกรณ์ (Network Diagram) ส่งให้คณะกรรมการตรวจรับพัสดุพิจารณาทราบก่อนดำเนินการไม่น้อยกว่า ๖๐ วันทำการ นับถัดจากวันที่ลงนามในสัญญา และผู้ชนะการเสนอราคาจะเข้าดำเนินการได้ต่อเมื่อได้รับความยินยอมจากสำนักงานปลัดกระทรวงมหาดไทย โดยเป็นไปตามข้อกำหนดระยะเวลาดำเนินการและส่งมอบงาน

๕.๖ ผู้ชนะการเสนอราคาต้องให้คำปรึกษา แนะนำ ด้านระบบและอุปกรณ์ที่ติดตั้งตามโครงการนี้แก่บุคลากรของสำนักงานปลัดกระทรวงมหาดไทย เมื่อมีการร้องขอโดยไม่คิดค่าใช้จ่ายตลอดอายุสัญญา

๕.๗ ผู้ชนะการเสนอราคาจะต้องรับผิดชอบค่าใช้จ่ายติดตั้งอุปกรณ์ในโครงการนี้พร้อมทั้งค่าใช้จ่ายที่เกิดขึ้นทั้งหมด

๕.๘ ในกรณีที่ผู้ชนะการเสนอราคาประสงค์จะนำอุปกรณ์รายการใดแตกต่างไปจากรายละเอียดที่กำหนดไว้ในสัญญามาติดตั้งให้สำนักงานปลัดกระทรวงมหาดไทย ผู้ชนะการเสนอราคาจะต้องได้รับความเห็นชอบจากคณะกรรมการตรวจรับพัสดุ และอุปกรณ์ที่จะนำมาติดตั้งดังกล่าวจะต้องมีคุณสมบัติไม่ต่ำกว่าที่กำหนดไว้ในสัญญา ทั้งนี้ ผู้ชนะการเสนอราคาจะต้องไม่คิดค่าใช้จ่ายเพิ่มเติม ไม่ว่ากรณีใด ๆ

๖. <u>การจัดฝึกอบรม</u>

ผู้ชนะการเสนอราคาจะต้องทำการจัดอบรม การใช้งานระบบวิเคราะห์ ระบบเฝ้าระวังและป้องกันภัยคุกคามไซเบอร์อัจฉริยะ, อุปกรณ์ตรวจจับ, วิเคราะห์และเฝ้าระวังภัยคุกคามบนระบบเครือข่ายทั้งหมด รวมทั้งให้ความรู้อื่น ๆ ที่เกี่ยวข้องให้กับผู้ที่เกี่ยวข้อง โดยให้จัดอบรมครั้งเดียวเป็นเวลาไม่น้อยกว่า ๒ วันทำการ ผู้เข้าร่วมอบรมไม่น้อยกว่า ๑๐ คน โดยดำเนินการดังนี้

๖.๑ ผู้ชนะการเสนอราคาจะต้องส่งหลักสูตร สถานที่และวันเวลา ที่จัดอบรมให้คณะกรรมการตรวจรับพัสดุพิจารณาก่อนวันอบรม ๑๕ วันทำการ

๖.๒ ผู้ชนะการเสนอราคาจะต้องจัด สถานที่ อุปกรณ์ ตามโครงการที่จัดหาพร้อมบุคลากรที่ใช้ในการอบรม โดยไม่คิดค่าใช้จ่ายเพิ่มจากสำนักงานปลัดกระทรวงมหาดไทย

๖.๓ ผู้ชนะการเสนอราคาต้องให้คำปรึกษา แนะนำ ด้านระบบรักษาความปลอดภัยตามโครงการนี้แก่บุคลากรของสำนักงานปลัดกระทรวงมหาดไทย เมื่อมีการร้องขอโดยไม่มีค่าใช้จ่ายใด ๆ ตลอดอายุสัญญา

๖.๔ ในกรณีที่เกิดสถานการณ์ฉุกเฉิน หรือการแพร่ระบาดของโรคติดต่ออันตราย ผู้เข้ารับการฝึกอบรมไม่สามารถเดินทางเข้ารับการฝึกอบรม ณ สถานที่ฝึกอบรมได้ ผู้ชนะการเสนอราคาจะต้องจัดให้มีการอบรมในรูปแบบ Online และจะต้องจัดทำคู่มือการใช้งานระบบสำหรับเจ้าหน้าที่ผู้ดูแลระบบ (Admin) ในรูปแบบสื่อมัลติมีเดีย เพื่อเผยแพร่ให้แก่ส่วนราชการในสังกัดสำนักงานปลัดกระทรวงมหาดไทย ทั้งในส่วนกลางและส่วนภูมิภาค

/๗. ระยะเวลาดำเนินการ...

ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....

๗. <u>ระยะเวลาดำเนินการและส่งมอบงาน</u>

กำหนดระยะเวลาส่งมอบทั้งโครงการ ภายใน ๑๒๐ วัน นับถัดจากวันที่ลงนามในสัญญา โดยแบ่งเป็นงวดงาน และมีการดำเนินงานดังนี้

๗.๑ **งวดงานที่ ๑** ภายใน ๖๐ วันนับถัดจากวันที่ลงนามในสัญญา ผู้รับจ้างจะต้องส่งแผนและขั้นตอนการดำเนินการ ออกแบบการติดตั้ง และจัดทำแผนผังการเชื่อมโยงระบบ อุปกรณ์ (Network Diagram) ส่งให้คณะกรรมการตรวจรับพัสดุพิจารณาทราบ โดยผู้รับจ้างจะต้องส่งมอบอุปกรณ์พร้อมติดตั้งในข้อ ๑ ตาม ภาคผนวก ก ให้แล้วเสร็จ โดยดำเนินการติดตั้ง ที่ส่วนกลาง และจังหวัด จำนวน ๒๓ จังหวัด ตามที่สำนักงานปลัดกระทรวงมหาดไทยกำหนด

๗.๒ **งวดงานที่ ๒** ภายใน ๙๐ วันนับถัดจากวันที่ลงนามในสัญญา โดยผู้รับจ้างจะต้องส่งมอบอุปกรณ์พร้อมติดตั้งในข้อ ๑ ตาม ภาคผนวก ก ให้แล้วเสร็จโดยดำเนินการติดตั้งจังหวัด จำนวน ๕๓ จังหวัด ตามที่สำนักงานปลัดกระทรวงมหาดไทยกำหนด และข้อ ๒ ตาม ภาคผนวก ก โดยดำเนินการติดตั้งที่ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงมหาดไทยให้แล้วเสร็จ

๗.๓ **งวดงานที่ ๓** ภายใน ๑๒๐ วันนับถัดจากวันที่ลงนามในสัญญา ผู้รับจ้างจะต้องให้บริการเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cybersecurity Operations Center: CSOC) และตอบสนองต่อเหตุการณ์ที่อยู่ในข่ายเป็นภัยคุกคามทางไซเบอร์ (Managed Detection & Response: MDR) ตาม ภาคผนวก ก

๗.๔ คู่มือการใช้งานและวิธีดูแลรักษาระบบวิเคราะห์ระบบเฝ้าระวังและป้องกันภัยคุกคามไซเบอร์อัจฉริยะ, อุปกรณ์ตรวจจับ, วิเคราะห์และเฝ้าระวังภัยคุกคามบนระบบเครือข่าย สำหรับศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.มท ๒ ชุด

๗.๕ การจัดอบรม การใช้งานระบบวิเคราะห์ระบบเฝ้าระวังและป้องกันภัยคุกคามไซเบอร์อัจฉริยะ, อุปกรณ์ตรวจจับ, วิเคราะห์และเฝ้าระวังภัยคุกคามบนระบบเครือข่าย รวมทั้งให้ความรู้อื่น ๆ ที่เกี่ยวข้อง

๗.๖ คณะกรรมการตรวจรับพัสดุพร้อมอุปกรณ์ทั้งระบบ ณ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.มท ตามรายละเอียดการทดสอบการใช้งานในสัญญาฯ เมื่อสำนักงานปลัดกระทรวงมหาดไทยได้รับหนังสือแจ้งจากผู้รับจ้างว่าได้ติดตั้ง เสร็จเรียบร้อยแล้ว พร้อมที่จะส่งมอบระบบรักษาความปลอดภัยฯ

๘. <u>เงื่อนไขการชำระเงิน</u>

กำหนดการจ่ายเงินแบ่งเป็นเงินจ่ายล่วงหน้า และตามการส่งมอบงาน ดังนี้

๘.๑ เงินจ่ายล่วงหน้า ผู้ว่าจ้างจะจ่ายเงินล่วงหน้าให้แก่ผู้รับจ้างหลังจากวันลงนามในสัญญาฯ เป็นจำนวนเงินร้อยละ ๑๕ ของวงเงินตามสัญญาฯ โดยผู้รับจ้างนำพันธบัตรรัฐบาลไทย หรือหนังสือค้ำประกันธนาคารในประเทศมาค้ำประกันเงินที่รับล่วงหน้าเต็มตามจำนวนที่รับไป และจะหักคืนค่าจ้างในแต่ละงวดจนกว่าจำนวนเงินที่หักไว้จะครบตามจำนวนเงินค่าจ้างล่วงหน้าที่ผู้รับจ้างได้รับไปแล้ว ยกเว้นค่าจ้างงวดสุดท้ายจะหักไว้เป็นจำนวนเท่ากับจำนวนเงินค่าจ้างล่วงหน้าที่เหลือทั้งหมด

๘.๒ เงินจ่ายตามการส่งมอบงาน **แบ่งเป็น ๓ งวด**

งวดที่ ๑ ผู้ว่าจ้างจะจ่ายเงินให้หลังจากผู้รับจ้างส่งมอบงานงวดที่ ๑ และคณะกรรมการตรวจรับพัสดุฯ ดำเนินการตรวจรับถูกต้อง ครบถ้วนแล้ว เป็นจำนวนเงิน ร้อยละ ๓๐ ของวงเงินตามสัญญาฯ

งวดที่ ๒ ผู้ว่าจ้างจะจ่ายเงินให้หลังจากผู้รับจ้างส่งมอบงานงวดที่ ๒ และคณะกรรมการตรวจรับพัสดุฯ ดำเนินการตรวจรับถูกต้อง ครบถ้วนแล้ว เป็นจำนวนเงิน ร้อยละ ๓๐ ของวงเงินตามสัญญาฯ

/งวดสุดท้าย...

ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....

งวดสุดท้าย ผู้ว่าจ้างจะจ่ายเงินให้หลังจากผู้รับจ้างส่งมอบงานงวดสุดท้าย และคณะกรรมการตรวจรับพัสดุฯ ดำเนินการตรวจรับถูกต้อง ครบถ้วนแล้ว เป็นจำนวนเงิน ร้อยละ ๔๐ ของวงเงินตามสัญญาฯ

๙. <u>การสนับสนุนของสำนักงานปลัดกระทรวงมหาดไทย</u>

สำนักงานปลัดกระทรวงมหาดไทยจะอำนวยความสะดวกให้กับผู้ยื่นข้อเสนอเพื่อให้การดำเนินงานเรียบร้อยและมีประสิทธิภาพ ดังนี้

๙.๑ ดำเนินการจัดเจ้าหน้าที่อำนวยความสะดวกและให้ข้อมูลเกี่ยวระบบคอมพิวเตอร์

๙.๒ อนุญาตให้ผู้ยื่นข้อเสนอใช้ และสามารถส่งข้อมูลผ่านระบบเครือข่ายสื่อสารของสำนักงานปลัดกระทรวงมหาดไทยตามความเหมาะสม

๑๐. <u>การรับประกันความชำรุดบกพร่อง</u>

๑๐.๑ ผู้รับจ้างต้องรับประกันความชำรุดบกพร่องของอุปกรณ์ที่เสนอเป็นระยะเวลาไม่น้อยกว่า ๑ ปี นับถัดจากวันที่ได้ส่งมอบงานงวดสุดท้ายเป็นที่เรียบร้อย และคณะกรรมการฯ ตรวจรับถูกต้อง ครบถ้วนเรียบร้อยแล้ว

๑๐.๒ ในระหว่างการดำเนินการและระหว่างเวลาการรับประกันตามสัญญาฯ หากมีอุปกรณ์ชำรุดขัดข้องจากการใช้งานตามปกติ ผู้รับจ้างจะต้องเดินทางมาถึงที่เกิดเหตุภายใน ๒๔ ชั่วโมง นับตั้งแต่เวลาที่ได้รับแจ้งจากผู้ว่าจ้าง หรือผู้ดูแลระบบ และดำเนินการซ่อมแซมแก้ไข/หาทดแทนให้แล้วเสร็จภายใน ๒๔ ชั่วโมง และถ้าผู้รับจ้างไม่สามารถดำเนินการได้ ผู้ว่าจ้างมีสิทธิว่าจ้างผู้อื่นมาดำเนินการซ่อมแซมแก้ไข โดยผู้รับจ้างจะต้องรับผิดชอบค่าใช้จ่ายที่เกิดขึ้นทั้งสิ้น

๑๐.๓ ผู้รับจ้างต้องมีศูนย์บริการรับแจ้ง (Help Desk Center) ณ ที่ทำการของผู้รับจ้าง และให้บริการรับแจ้งปัญหาจากผู้ใช้งานตลอดเวลาการปฏิบัติงานในวันเวลาราชการ โดยแจ้งหมายเลขโทรศัพท์และระบบสื่อสารอื่นที่สามารถติดต่อได้

๑๑. <u>อัตราค่าปรับ</u>

ผู้ชนะการเสนอราคาไม่ปฏิบัติตามสัญญาหรือผิดสัญญาข้อหนึ่งข้อใด และสำนักงานปลัดกระทรวงมหาดไทยยังไม่บอกเลิกสัญญา ผู้ชนะการเสนอราคาจะต้องถูกปรับเป็นรายวันในอัตราร้อยละ ๐.๑ ของงานจ้าง

๑๒. <u>การจ้างช่วง</u>

ผู้รับจ้างจะต้องไม่เอางานทั้งหมดหรือบางส่วนนี้ไปจ้างช่วงอีกทอดหนึ่ง เว้นแต่การจ้างช่วงงานแต่บางส่วนที่ได้รับอนุญาตเป็นหนังสือจากผู้ว่าจ้างแล้ว การที่ผู้ว่าจ้างได้อนุญาตให้จ้างช่วงงานแต่บางส่วนดังกล่าวนั้นไม่เป็นเหตุให้ผู้รับจ้างหลุดพ้นจากความรับผิดหรือพันธะหน้าที่ตามสัญญานี้ และผู้รับจ้างจะยังคงต้องรับผิดในความผิดและความประมาทของผู้รับจ้างช่วงหรือของตัวแทนหรือลูกจ้างของผู้รับจ้างช่วงนั้นทุกประการ

กรณีผู้รับจ้างไปจ้างช่วงงานแต่บางส่วนโดยฝ่าฝืนความในวรรคหนึ่ง ผู้รับจ้างต้องชำระค่าปรับให้แก่ผู้ว่าจ้างเป็นจำนวนเงินในอัตราร้อยละสิบ ของวงเงินของงานที่จ้างช่วงตามสัญญา ทั้งนี้ไม่ตัดสิทธิผู้ว่าจ้างในการบอกเลิกสัญญา

/๑๓. หลักเกณฑ์...

ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....

๑๓. <u>หลักเกณฑ์การพิจารณาผู้ชนะการเสนอราคา</u>

สำนักงานปลัดกระทรวงมหาดไทย จะพิจารณาคัดเลือกข้อเสนอโดยใช้เกณฑ์ราคาในการคัดเลือกผู้ที่เสนอราคาต่ำสุดจากราคารวมเป็นผู้ชนะการเสนอราคา ที่ผ่านการพิจารณาทั้งคุณสมบัติผู้ยื่นเสนอ และแบบรูปรายการหรือคุณลักษณะเฉพาะ ตามแนวทางปฏิบัติระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ.๒๕๖๐ ข้อ ๘๓ (๑)

๑๔. <u>งบประมาณในการจัดหา</u>

งบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. ๒๕๖๗ จำนวน ๘๐,๐๐๐,๐๐๐.๐๐- บาท (แปดสิบล้านบาทถ้วน) รวมภาษีมูลค่าเพิ่ม ภาษีอากรอื่น ๆ และค่าใช้จ่ายทั้งปวงด้วย

๑๕. <u>หน่วยงานผู้รับผิดชอบ</u>

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงมหาดไทย

ลงชื่อ.....(ประธานกรรมการ)
(นายณัฐกิตติ์ ตาวงษ์สา)
ผู้อำนวยการกลุ่มงานโครงสร้างพื้นฐานด้านสารสนเทศและการสื่อสาร

ลงชื่อ.....(กรรมการ)
(นายทศพล นิติมณฑล)
นักวิชาการคอมพิวเตอร์ชำนาญการ

ลงชื่อ.....(กรรมการ)
(นายบุญยง เรืองพงษ์)
นายช่างไฟฟ้าอาวุโส

ลงชื่อ.....(กรรมการ)
(นายชัชวาล ยอดคำตัน)
นายช่างไฟฟ้าชำนาญงาน

ลงชื่อ.....(กรรมการ)
(นายสมนึก โลสันเทียะ)
นายช่างไฟฟ้าชำนาญงาน

ภาคผนวก ก

คุณลักษณะเฉพาะทางเทคนิค (Technical Specification)

โครงการศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ระยะที่ ๑

---

๑. ระบบวิเคราะห์ระบบเฝ้าระวังและป้องกันภัยคุกคามไซเบอร์อัจฉริยะ จำนวน ๑ ระบบ โดยมีคุณลักษณะอย่างน้อย ดังนี้

๑.๑ เป็น Platform ที่มีความสามารถในการตรวจหาภัยคุกคามที่เกิดขึ้นในองค์กร (Threat Hunting) และหาข้อมูลความเกี่ยวโยงของภัยคุกคามที่เกิดขึ้น (Investigation) ของเครื่องคอมพิวเตอร์ลูกข่าย แม่ข่าย และ เครือข่าย ได้

๑.๒ Agent Software ต้องสามารถป้องกันภัยคุกคามที่เกิดขึ้นบนเครื่องคอมพิวเตอร์ลูกข่าย เครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เคลื่อนที่ (Mobile Device) **จำนวน ๑,๐๐๐ ลิขสิทธิ์** โดยมีความสามารถด้านการป้องกันภัยคุกคาม ดังนี้

๑.๑.๑ ป้องกันการโจมตีที่ช่องโหว่ของระบบ (Exploit Prevention)

๑.๑.๒ ป้องกันมัลแวร์ หรือไวรัส (Malware Prevention หรือ Antivirus)

๑.๑.๓ ป้องกันการโจมตีของมัลแวร์ระดับสูง ที่ใช้เทคนิคโจมตีแบบไม่ใช้ไฟล์ (Fileless Attacks)

๑.๑.๔ ป้องกันการโจมตีโดยใช้เทคนิคของ (AI-based local analysis engine) หรือ Machine Learning

๑.๑.๕ ป้องกันการโจมตีโดยใช้การวิเคราะห์พฤติกรรม (Behavior)

๑.๑.๖ ป้องกันมัลแวร์เรียกค่าไถ่ (Ransomware Protection)

๑.๓ Agent Software ต้องสามารถป้องกัน Exploit และ Malware ในกรณีที่ไม่สามารถติดต่อกับ Management Console ได้ (Offline)

๑.๔ สามารถค้นหาข้อมูลโดยรองรับการสร้าง Rule เพื่อตรวจจับภัยคุกคามเครื่องคอมพิวเตอร์ลูกข่ายจาก Indicators of compromise (IOCs) และ Behavioral indicators of compromise (BIOCs)

๑.๕ แสดงข้อมูลเหตุการณ์ภัยคุกคามทางไซเบอร์ โดยมีรายละเอียด อย่างน้อยดังนี้

๑.๕.๑ ระบุประเภทของภัยคุกคาม

๑.๕.๒ วัน-เวลา เริ่มต้นและสิ้นสุดของภัยคุกคาม

๑.๕.๓ ระบุต้นทาง (Source) ปลายทาง (Destination)

๑.๕.๔ ระบุระดับความรุนแรง (Severity)

๑.๕.๕ รายละเอียดเหตุการณ์และพฤติกรรม

๑.๕.๖ ค่าคะแนน (Scoring) ของภัยคุกคามเมื่อเกิดขึ้นกับ IP address, Host และ Username ที่มีความสำคัญสูง ได้เป็นอย่างน้อย

๑.๕.๗ สามารถแสดงเทคนิคของภัยคุกคามที่ตรวจพบ โดยเทียบเคียงกับ MITRE ATT&CK stage ต่าง ๆ

๑.๖ ระบบ Detection and Response ในการตรวจจับภัยคุกคาม และรวบรวมข้อมูลจากกิจกรรมต่างๆ ที่เกิดขึ้น โดย ทั้งระบบที่นำเสนอต้องมีความสามารถรวมกัน อย่างน้อยดังนี้

๑.๖.๑ Endpoint Detection and Response (EDR) (ตรวจจับและตอบสนองต่อเครื่องแม่ข่าย)

๑.๖.๒ Root Cause Analysis (วิเคราะห์หาต้นตอของปัญหาที่เกิดขึ้น)

๑.๖.๓ Timeline analysis of alerts (สามารถแสดง Timeline ของเหตุการณ์ที่เกิดขึ้น)

/๑.๖.๔ Threat Hunting...

๑.๖.๔ Threat Hunting (การตรวจหาภัยคุกคาม อาจเกิดขึ้นในองค์กร)

๑.๖.๕ Incident response and recovery (ตอบสนองและกู้คืนระบบจากเหตุการณ์ที่เกิด)

๑.๖.๖ User Behavior Analytics (UBA) หรือ User and Entity Behavior Analytics (UEBA) (ระบบวิเคราะห์สิ่งผิดปกติจากพฤติกรรมของผู้ใช้งาน)

๑.๗ มีวิธีการในการตอบสนองต่อภัยคุกคาม (Response) อย่างน้อยดังนี้

๑.๗.๑ แยกหรือตัดการเชื่อมต่อเครื่องคอมพิวเตอร์ลูกข่าย และแม่ข่าย (Isolate Endpoint) ได้หลายๆเครื่องพร้อมๆกัน (Multiple Selection) ผ่านหน้า management console

๑.๗.๒ ควบคุมเครื่องคอมพิวเตอร์ลูกข่ายผ่าน Terminal (Live Terminal) หรือ หยุดการทำงานของ Process บนเครื่องคอมพิวเตอร์ลูกข่าย (Terminate Process)

๑.๗.๓ เพิ่มค่า Hash ของไฟล์ที่ต้องการป้องกันได้ (Add to Block List)

๑.๘ สามารถทำงานร่วมกับ Cloud Sandbox หรือ On-Premise Sandbox เพื่อวิเคราะห์ภัยคุกคามและนำผลลัพธ์มาใช้ในการป้องกันได้ กรณีที่ต้องทำงานร่วมกับ On-Premise Sandbox ให้เสนอ On-Premise Sandbox เพิ่มเติมให้ครอบคลุม และเพียงพอต่อการทำงาน

๑.๙ สามารถกำหนด Password สำหรับถอดการติดตั้ง Agent จาก Management Console เพื่อป้องกันไม่ให้ User ถอนการติดตั้ง Agent software ได้

๑.๑๐สามารถทำงานร่วมกับอุปกรณ์ที่เสนอในข้อ ๒ ที่ทำงานเป็น Network Sensor ที่มี AI และ Machine Learning เพื่อให้สามารถทำ Log Stitching หรือ Data Stacking เพื่อทำให้ข้อมูลดังกล่าวเป็นภาพเดียวกันได้ กรณีที่ไม่สามารถทำงานร่วมได้ ให้เสนออุปกรณ์เพิ่มเติมเพื่อให้ครอบคลุม และเพียงพอต่อการทำงาน

๑.๑๑ สามารถตรวจสอบช่องโหว่ของระบบปฏิบัติการ (Vulnerability Assessment) บนระบบปฏิบัติการ Windows และ Linux โดยอ้างอิงช่องโหว่ตาม Common Vulnerabilities and Exposures (CVE) โดยไม่ต้องติดตั้ง Agent เพิ่มเติม หรือนำเสนอระบบอื่นๆเพิ่มเติม เพื่อสามารถทำได้ตามความต้องการดังกล่าว

๑.๑๒ มีสามารถแสดง Host Inventory เช่น User, Application, Services, Driver, Autorun, Share ของเครื่องคอมพิวเตอร์ได้ เพื่อสามารถตรวจสอบข้อมูลได้อย่างรวดเร็ว หรือนำเสนอระบบอื่นๆเพิ่มเติม เพื่อทำได้ตามความต้องการดังกล่าว

๑.๑๓ ระบบที่นำเสนอจะต้องสามารถรองรับเชื่อมต่อแบบ Single Sign-on เพื่อนำเข้าข้อมูลบัญชีผู้ใช้งานผ่านโปรโตคอล SAML ๒.๐ ได้

๑.๑๔ ระบบที่นำเสนอต้องมีความสามารถในการทำ Disk Encryption ได้ ทั้งบน Windows และ MAC OS

๑.๑๕ สามารถสร้างแดชบอร์ดโดยใช้ XQL หรือ KQL หรือเทียบเท่ามาเป็นเงื่อนไขในการ Filter ข้อมูล

๑.๑๖ สามารถวิเคราะห์ตรวจจับภัยคุกคามบนระบบเครือข่ายโดยใช้เทคโนโลยี Machine learning และ AI ในการวิเคราะห์พฤติกรรมที่เกิดขึ้นโดยการหาความสัมพันธ์ของข้อมูลที่ได้มาจากเครื่อง Endpoint, Log ของอุปกรณ์ตรวจจับภัยคุกคามเครือข่ายระดับแอพพลิเคชั่น (Network Sensor), Windows Event Log, AWS Audit Log, Azure Audit Log, GCP Audit Log เป็นต้น

/๑.๑๗.ระบบ...

ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....

๑.๑๗ ระบบที่นำเสนอต้องผ่านการประเมินทดสอบของ The Forrester New Wave™: Extended Detection And Response (XDR) Providers, Q๔ ๒๐๒๑ โดยถูกจัดให้อยู่ใน Leaders หรือ Strong Performers ได้เป็นอย่างน้อย

๑.๑๘ ระบบที่นำเสนอต้องผ่านการประเมินจาก MITRE ATT&CK Evaluations ปี ๒๐๒๒ (Wizard Spider + Sandworm) หรือล่าสุด โดยมีผลการตรวจจับล่าช้า (Delayed) ไม่มากกว่า ๒ ครั้ง และผลการตรวจจับโดยที่ไม่มีการเปลี่ยนแปลงค่า (Configuration Change) ไม่มากกว่า ๑ ครั้ง โดยอ้างอิงจากข้อมูลที่แสดงบนเว็บไซต์ MITRE ATT&CK Evaluations หรือผ่านการประเมินจาก Forrester New Wave ในหัวข้อ Extended Detection And Response (XDR) Providers Scorecard ปี ๒๐๒๑ หรือล่าสุด โดยได้รับผลการประเมิน Differentiated ไม่น้อยกว่า ๗ หัวข้อ

๑.๑๙ ต้องรับประกันระบบที่นำเสนอเป็นเวลาอย่างน้อย ๑ ปี

๑.๒๐ ผู้เสนอราคาต้องมีหนังสือสนับสนุนทางด้านเทคนิคจากผู้ผลิตหรือสาขาของผู้ผลิตในประเทศไทย และรับรองว่าอุปกรณ์ภายในโครงการนี้ อยู่ในสภาพที่ใช้งานได้ดี เป็นรุ่นที่ยังอยู่ในสายการผลิต และเป็นของใหม่ มิได้ถูกติดตั้งใช้งาน ณ ที่ใดมาก่อน

๒. อุปกรณ์ตรวจจับ, วิเคราะห์และเฝ้าระวังภัยคุกคามบนระบบเครือข่าย จำนวน ๑ ระบบ โดยมีคุณลักษณะอย่างน้อย ดังนี้

๒.๑ เป็นอุปกรณ์แบบ Appliance-Based ที่สามารถส่งข้อมูลการใช้งานไปใช้ในการวิเคราะห์พฤติกรรมการใช้งานของระบบเครือข่าย (Network Traffic Analysis) **โดยต้องติดตั้งในลักษณะ High Availability (HA)**

๒.๒ มี Network Interface อย่างน้อยดังนี้

๒.๒.๑ Interface แบบ RJ๔๕ (๑๐Mbps/๑๐๐Mbps/๑Gbps/๑๐Gbps) หรือดีกว่าไม่น้อยกว่า ๘ พอร์ท

๒.๒.๒ ช่องเชื่อมต่อแบบ ๑G/๑๐G SFP/SFP+ หรือดีกว่า ไม่น้อยกว่า ๑๒ ช่อง

๒.๒.๓ ช่องเชื่อมต่อแบบ ๑G/๑๐G/๒๕G SFP/SFP+/SFP๒๘ หรือดีกว่า ไม่น้อยกว่า ๔ ช่อง

๒.๒.๔ ช่องเชื่อมต่อแบบ ๔๐G/๑๐๐G QSFP+/QSFP๒๘ หรือดีกว่า ไม่น้อยกว่า ๔ ช่อง

๒.๓ มี Interface HA แบบ ๑๐/๑๐๐/๑๐๐๐ หรือดีกว่าไม่น้อยกว่า ๒ พอร์ท, ๔๐G QSFP+ ไม่น้อยกว่า ๑ พอร์ท และมี Interface แบบ ๑๐/๑๐๐/๑๐๐๐ หรือดีกว่าสำหรับบริหารจัดการโดยเฉพาะ (Out of Band Management) ไม่น้อยกว่า ๑ พอร์ท โดยทั้งหมดไม่นับรวมกับ interface จากข้อที่ ๒.๒

๒.๔ มี Threat prevention Throughput ไม่น้อยกว่า ๒๖ Gbps ในแบบ Appmix หรือ Enterprise testing condition หรือ Enterprise traffic mix

๒.๕ มี storage ชนิด SSD สำหรับจัดเก็บข้อมูลระบบ (System Storage) ขนาดไม่ต่ำกว่า ๔๘๐ GB หรือดีกว่า

๒.๖ มี Cloud Sandbox หรือ On-Premise Sandbox เพื่อวิเคราะห์ภัยคุกคาม **โดยรองรับปริมาณข้อมูล ๖๖๐ GB ต่อวัน เป็นอย่างน้อย** และนำผลลัพธ์มาใช้ในการป้องกันได้ กรณีที่ต้องทำงานร่วมกับ On-Premise Sandbox ให้เสนอ On-Premise Sandbox เพิ่มเติมให้ครอบคลุม และเพียงพอต่อการทำงาน

/๒.๗.สามารถ...

๒.๗ สามารถทำงานร่วมกับระบบที่เสนอในข้อ ๑ โดยทำงานเป็น Network Sensor ที่มี AI และ Machine Learning เพื่อให้สามารถทำ Log Stitching หรือ Data Stacking เพื่อทำให้ข้อมูลดังกล่าวเป็นภาพเดียวกันได้ กรณีที่ไม่สามารถทำงานร่วมได้ ให้เสนออุปกรณ์เพิ่มเติมเพื่อให้ครอบคลุม และเพียงพอต่อการทำงาน

๒.๘ สามารถติดตั้งในรูปแบบ Transparent Inline (Virtual Wire), Non-Inline Monitoring (Tap), L๒ และ L๓ หรือเทียบเท่าได้

๒.๙ สามารถทำ Routing แบบ Static, RIP, BGP, OSPF, Multicast และ Policy Based Forwarding หรือ Policy based Routing ได้เป็นอย่างน้อย

๒.๑๐ สามารถทำการตรวจสอบทราฟฟิคที่เข้ารหัส SSL ด้วยการทำ SSL decryption (ทั้งแบบ Inbound และ Outbound) รวมทั้งการทำ SSL Decryption Broker หรือ Network Packet Broker ได้ หรือเสนออุปกรณ์อื่นเพิ่มเติมเพื่อให้สามารถทำงานได้ตามข้อกำหนด โดยอุปกรณ์ที่นำเสนอเพิ่มเติม ต้องมี Throughput ไม่ต่ำกว่า Threat Prevention Throughput ของอุปกรณ์

๒.๑๑ สามารถทำงานร่วมกับระบบการพิสูจน์ตัวตน (Authentication Systems) ได้แก่ Active Directory, LDAP, Radius เพื่อทำการติดตามผู้ใช้ได้เป็นอย่างน้อย

๒.๑๒ สามารถรับ Syslog จากระบบที่มีอยู่ได้ เพื่อใช้ในการยืนยันตัวตน ของ User ที่ใช้งาน โดยรองรับทั้ง User Log-in และ User Log-out ได้ หรือเสนออุปกรณ์อื่นเพิ่มเติมเพื่อให้สามารถทำงานได้ตามข้อกำหนด

๒.๑๓ สามารถตรวจจับและป้องกันภัยคุกคามประเภท Vulnerability และ Spyware ได้ โดยสามารถมีการอัพเดท Signature ใหม่แบบอัตโนมัติได้

๒.๑๔ สามารถติดตาม และควบคุมการเข้าถึงเว็บได้ตาม Category, Block list, Allow list ที่กำหนดได้ และต้องมีการจัด category ให้กับแต่ละ website ไม่น้อยกว่า ๒ category (Multi-Category URL Filtering) โดยอัตโนมัติ หรือเสนออุปกรณ์อื่นเพิ่มเติมเพื่อให้สามารถทำงานได้ตามข้อกำหนด

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

๒.๑๖ สามารถตรวจจับ และ ป้องกัน การเข้าถึง Malicious Domain ภายในองค์กรได้ โดยต้องมีความสามารถอย่างน้อย ดังนี้

๒.๑๖.๑ มีระบบ Machine Learning ในการตรวจหาเทคนิคอัลกอริทึม Domain generation algorithms (DGA) เพื่อวิเคราะห์คาดการณ์ ป้องกัน Malicious Domain ที่ไม่เคยพบมาก่อนได้

๒.๑๖.๒ สามารถตรวจจับและป้องกัน DNS Tunneling ได้ทั้งในรูปแบบ Known และ unknown เพื่อป้องกันการขโมยข้อมูลในองค์กร ผ่านช่องทาง DNS

๒.๑๖.๓ ทำงานแบบ Real time และไม่มีข้อจำกัดรองรับปริมาณ Malicious Domain ที่เพิ่มขึ้นในอนาคต โดยตรวจจับผ่านทาง DNS และต้องไม่ส่งผลกระทบกับ Performance ของตัวอุปกรณ์

๒.๑๖.๔ สามารถนำเสนออุปกรณ์อื่นเพิ่มเติมเพื่อให้สามารถทำงานได้ตามข้อกำหนดในข้อ ๒.๑๖.๑ – ๒.๑๖.๓

/๒.๑๗ มีระบบตรวจจับ...

๒.๑๗ มีระบบตรวจจับ Advanced Malware แบบ Cloud-Based และใช้เทคโนโลยีแบบ Sandbox , Machine Learning เพื่อใช้ระบุ Malware ประเภทใหม่ (Zero-day Malware) ซึ่งไม่มีในฐานข้อมูลการบุกรุกโจมตีได้ รวมถึงสามารถสร้างรูปแบบการโจมตี (Signature) ดังกล่าวขึ้นมาเพื่อใช้ป้องกันระบบเครือข่ายได้โดยอัตโนมัติ

๒.๑๘ สามารถเรียกดูสรุปข้อมูลของ Data ในรูปแบบของกราฟฟิคได้ และสามารถทำรายงานต่างๆ ได้โดยไม่ต้องเสนออุปกรณ์อื่นเพิ่มเติมอย่างน้อยดังนี้

๒.๑๘.๑ Top Application, Application Category

๒.๑๘.๒ Top Source, User, Destination

๒.๑๘.๓ User activity report

๒.๑๙ สามารถทำรายงานรวมถึงปรับแต่งรายงานตามความต้องการ ในรูปแบบ PDF ได้เป็นอย่างน้อยพร้อมทั้งตั้งเวลาส่งรายงานผ่านทาง Email แบบอัตโนมัติได้

๒.๒๐ ระบบที่นำเสนอนั้นต้องติดตั้งแบบ High Availability ในโหมด Active-Passive

๒.๒๑ มีแหล่งจ่ายไฟฟ้า (Power Supply) แบบ redundant และมีพัดลมระบายความร้อน (Fan tray หรือ Cooling Fan หรือ Fan assembly) แยกจาก Power Supply แบบ hot swap

๒.๒๒ ต้องรับประกันอุปกรณ์เป็นเวลาอย่างน้อย ๑ ปี

๒.๒๓ ต้องได้รับการจัดอันดับให้อยู่ในกลุ่ม Leader ของ Gartner Magic Quadrant ในกลุ่มผลิตภัณฑ์ Enterprise Network Firewalls ปี ๒๐๒๒ หรือปีล่าสุด

๒.๒๔. ผู้เสนอราคาต้องมีหนังสือสนับสนุนทางด้านเทคนิคจากผู้ผลิตหรือสาขาของผู้ผลิตในประเทศไทย และรับรองว่าอุปกรณ์ภายในโครงการนี้ อยู่ในสภาพที่ใช้งานได้ดี เป็นรุ่นที่ยังอยู่ในสายการผลิต และเป็นของใหม่ มิได้ถูกติดตั้งใช้งาน ณ ที่ใดมาก่อน

๓. ผู้เสนอราคาต้องให้บริการเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cybersecurity Operations Center: CSOC) และตอบสนองต่อเหตุการณ์ที่อยู่ในข่ายเป็นภัยคุกคามทางไซเบอร์ (Managed Detection & Response: MDR) โดยจะต้องประกอบด้วยการทำงาน ดังต่อไปนี้

๓.๑ ผู้เสนอราคา ต้องได้รับมาตรฐานการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ISO/IEC ๒๗๐๐๑ : ๒๐๑๓ หรือ ISO/IEC ๒๗๐๐๑ : ๒๐๒๒ เป็นอย่างน้อย

๓.๒ เฝ้าระวัง วิเคราะห์ และแจ้งเตือนภัยคุกคามทางไซเบอร์ และตอบสนองต่อเหตุการณ์ภัยคุกคามที่ตรวจพบโดยใช้ระบบวิเคราะห์ระบบวิเคราะห์ระบบเฝ้าระวังและป้องกันภัยคุกคามไซเบอร์อัจฉริยะ, อุปกรณ์ตรวจจับ, วิเคราะห์และเฝ้าระวังภัยคุกคามบนระบบเครือข่ายตลอด ๒๔ ชั่วโมง ชั่วโมงของทุกวัน ไม่มีวันหยุด (๗ x ๒๔) ตลอดระยะเวลาของสัญญา

๓.๓ ผู้รับจ้างต้องจัดทำขั้นตอนการปฏิบัติงานต่างๆ (On-boarding process) โดยกระบวนการที่นำเสนอจะสอดคล้องกับระบบและอุปกรณ์ที่นำเสนอและมีใช้งานอยู่ในปัจจุบัน

๓.๔ ผู้รับจ้างต้องออกแบบรูปแบบการทำงานของระบบทั้งหมดให้มีความปลอดภัย และดำเนินปรับเปลี่ยนรูปแบบให้สอดคล้องกับสถานการณ์และลักษณะการทำงานของศูนย์เทคโนโลยีสารสนเทศและการ

/สื่อสาร...

ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....

สื่อสาร สำนักงานปลัดกระทรวงมหาดไทย รวมถึงให้คำแนะนำที่ทันต่อเหตุการณ์แก่หน่วยงานผู้ดูแลระบบอย่างต่อเนื่อง ตลอดระยะเวลาของสัญญา

๓.๕ เชื่อมโยง อุปกรณ์ตรวจจับ, วิเคราะห์และเฝ้าระวังภัยคุกคามบนระบบเครือข่าย และระบบวิเคราะห์ระบบวิเคราะห์ระบบเฝ้าระวังและป้องกันภัยคุกคามไซเบอร์อัจฉริยะ, อุปกรณ์ตรวจจับ, วิเคราะห์และเฝ้าระวังภัยคุกคามบนระบบเครือข่าย ที่นำเสนอเข้าด้วยกันเพื่อให้ระบบสามารถทำการวิเคราะห์ภาพรวมภัยคุกคามจากข้อมูล Network, Endpoint สามารถมองเห็นภัยคุกคามไซเบอร์ในภาพรวมขององค์กร

๓.๖ ต้องจัดให้มีทีมผู้เชี่ยวชาญคอยทำการค้นหาข้อมูล เชื่อมโยงพฤติกรรม หรือข้อมูลบ่งชี้สัญญาณภัยคุกคามไซเบอร์ต่าง ๆ ในกรณีที่มีเหตุการณ์ ข่าวสาร หรือลักษณะพฤติกรรมที่อยู่ในข่ายน่าสงสัย

๓.๗ ผู้รับจ้างต้องจัดให้มีทีมแจ้งเตือนและประสานงานไปยังเจ้าหน้าที่หรือหน่วยงานที่รับผิดชอบ (Triage & Event Prioritization)

๓.๘ ผู้รับจ้างต้องจัดให้มีการแจ้งเตือนภัยคุกคามด้านความมั่นคงปลอดภัยทางไซเบอร์ และการให้คำแนะนำรวมทั้งขั้นตอนการดำเนินการ ต้องครอบคลุมเนื้อหาดังนี้

๓.๘.๑ ระบุประเภทของภัยคุกคาม

๓.๘.๒ วัน-เวลา เริ่มต้นและสิ้นสุดของภัยคุกคาม

๓.๘.๓ ระบุต้นทาง (Attacker) และปลายทาง (Target)

๓.๘.๔ ระบุระดับความรุนแรง (Severity)

๓.๘.๕ รายละเอียดเหตุการณ์และพฤติกรรมทั้งหมด

๓.๘.๖ คำแนะนำและขั้นตอนการดำเนินการแก้ไขเชิงเทคนิค

๓.๘.๗ จัดทำรายงานการแจ้งเตือนโดยใช้ช่องทางอีเมลและโทรศัพท์ตามระดับความรุนแรงของเหตุการณ์ภัยคุกคาม

๓.๙ ผู้รับจ้างต้องจัดให้มีเจ้าหน้าที่เฝ้าระวังภัยและตอบสนองคุกคามทางไซเบอร์ (Cyber Security Analyst and Threat Hunting) เพื่อให้บริการเฝ้าระวังภัยคุกคามทางไซเบอร์และตอบสนองคุกคามทางไซเบอร์ที่เป็นภัยคุกคาม เพื่อนระงับ ยับยั้ง หรือยุติกระบวนการที่เป็นอันตรายต่อระบบ ที่เกิดขึ้นแบบ Off-site ตลอด ๒๔ ชั่วโมง โดยมีหน้าที่ดังนี้

๓.๙.๑ วิเคราะห์เหตุภัยคุกคามทางไซเบอร์ที่ได้รับการแจ้งเตือน

๓.๙.๒ ทำความเข้าใจเกี่ยวกับขอบเขตของผลกระทบที่อาจจะเกิดจากภัยคุกคามดังกล่าว

๓.๙.๓ ยืนยันความถูกต้องของเหตุการณ์

๓.๙.๔ จัดลำดับความสำคัญของเหตุการณ์

๓.๙.๕ ทำการการแยกเครื่อง (Endpoint) ที่เป็นอันตรายออกจากระบบ เพื่อหลีกเลี่ยงการแพร่กระจายไปสู่เครื่องอื่นๆ โดยผ่านการทำ Isolate จากระบบที่เสนอในโครงการ

๓.๙.๖ ทำการระงับ ยับยั้ง หรือ ยุติกระบวนการที่เป็นอันตรายต่อระบบโดยผ่านระบบที่เสนอในโครงการ

๓.๙.๗ บันทึกเหตุการณ์พร้อมสรุปข้อมูลเหตุการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้น (Threat Response Summary)

๓.๑๐ จัดทำสรุปรายงานภัยคุกคามประจำเดือนตามรูปแบบมาตรฐาน (Summary Monthly threat event and Incident Report) และเข้าร่วมประชุมพร้อมนำเสนอในรูปแบบออนไลน์หรือ ณ สถานที่ทำงานของผู้ใช้บริการ (Onsite or Online Quarterly meeting) และจัดส่งรายงานในรูปแบบ Softcopy

/ผ่านช่องทาง...

ผ่านช่องทางอีเมล โดยมีรูปแบบรายงานดังต่อไปนี้

- Endpoint and Malware block report
- Windows Firewall report
- Peripheral report
- Blocked/Allowed Application report
- Application Control Policy Violators report
- ทั้งนี้ข้อมูลและรูปแบบรายงานสามารถเปลี่ยนแปลงตามการตั้งค่านโยบายและลิขสิทธิ์การใช้งานระบบวิเคราะห์ระบบวิเคราะห์ระบบเฝ้าระวังและป้องกันภัยคุกคามไซเบอร์อัจฉริยะ, อุปกรณ์ตรวจจับ, วิเคราะห์และเฝ้าระวังภัยคุกคามบนระบบเครือข่าย

๓.๑๑ ตารางระยะเวลามาตรฐานการให้บริการวิเคราะห์ (Detect & Triage SLA)

ระดับความรุนแรง	เวลาที่เริ่มดำเนินการวิเคราะห์หลังได้รับการแจ้งเตือนจากระบบ (Mean Time to Detect)	เวลาที่ดำเนินการรวมรวมข้อมูลและยืนยันความรุนแรงของเหตุการณ์ (Mean Time to Triage)	ความถี่ในการติดตามความคืบหน้าการตอบสนองเหตุการณ์ของผู้ใช้บริการ
สูง	๓๐ นาที	๑ ชั่วโมง	๔ ชั่วโมง
กลาง	๑ ชั่วโมง	๒ ชั่วโมง	๑๒ ชั่วโมง
ต่ำ	๔ ชั่วโมง	๖ ชั่วโมง	๒๔ ชั่วโมง

๓.๑๒. ตารางระยะเวลามาตรฐานการแจ้งเตือนผู้ใช้บริการ (Customer Notification SLA)

ระดับความรุนแรง	ช่องทางการติดต่อ	แจ้งเตือนภายในระยะเวลา
สูง	โทรศัพท์	๓๐ นาที
	อีเมล	๑ ชั่วโมง
กลาง	อีเมล	๒ ชั่วโมง
ต่ำ	อีเมล	๖ ชั่วโมง

๓.๑๓. ตารางระยะเวลาดำเนินการปรับปรุงและปรับแต่งการตั้งค่า (Policy Change Request)

ประเภทการร้องขอ	ระยะเวลาตอบสนอง
ปรับปรุงและปรับแต่งการตั้งค่า	๔ ชั่วโมงในวันและเวลาทำการ

ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....

ภาคผนวก ข
สถานที่ติดตั้ง
โครงการศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ระยะที่ ๑

---

๑. ส่วนกลาง ได้แก่
   ๑.๑ ศาลาว่าการกระทรวงมหาดไทย
   ๑.๒ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.มท

๒. จังหวัด ๗๖ จังหวัด ได้แก่
   ๒.๑ จังหวัดพระนครศรีอยุธยา
   ๒.๒ จังหวัดอุดรธานี
   ๒.๓ จังหวัดชลบุรี
   ๒.๔ จังหวัดพิษณุโลก
   ๒.๕ จังหวัดเชียงใหม่
   ๒.๖ จังหวัดขอนแก่น
   ๒.๗ จังหวัดสุราษฎร์ธานี
   ๒.๘ จังหวัดสงขลา
   ๒.๙ จังหวัดเพชรบุรี
   ๒.๑๐ จังหวัดฉะเชิงเทรา
   ๒.๑๑ จังหวัดนครราชสีมา
   ๒.๑๒ จังหวัดอุบลราชธานี
   ๒.๑๓ จังหวัดสกลนคร
   ๒.๑๔ จังหวัดภูเก็ต
   ๒.๑๕ จังหวัดเชียงราย
   ๒.๑๖ จังหวัดนครสวรรค์
   ๒.๑๗ จังหวัดกระบี่
   ๒.๑๘ จังหวัดชุมพร
   ๒.๑๙ จังหวัดนครปฐม
   ๒.๒๐ จังหวัดกาญจนบุรี
   ๒.๒๑ จังหวัดเพชรบูรณ์
   ๒.๒๒ จังหวัดลพบุรี
   ๒.๒๓ จังหวัดสิงห์บุรี
   ๒.๒๔ จังหวัดกาฬสินธุ์
   ๒.๒๕ จังหวัดกำแพงเพชร
   ๒.๒๖ จังหวัดจันทบุรี
   ๒.๒๗ จังหวัดชัยนาท
   ๒.๒๘ จังหวัดชัยภูมิ
   ๒.๒๙ จังหวัดตรัง

ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....

๒.๓๐ จังหวัดตราด
๒.๓๑ จังหวัดตาก
๒.๓๒ จังหวัดนครนายก
๒.๓๓จังหวัดนครพนม
๒.๓๔ จังหวัดนครศรีธรรมราช
๒.๓๕ จังหวัดนนทบุรี
๒.๓๖ จังหวัดนราธิวาส
๒.๓๗ จังหวัดน่าน
๒.๓๘ จังหวัดบึงกาฬ
๒.๓๙ จังหวัดบุรีรัมย์
๒.๔๐ จังหวัดปทุมธานี
๒.๔๑ จังหวัดประจวบคีรีขันธ์
๒.๔๒ จังหวัดปราจีนบุรี
๒.๔๓ จังหวัดปัตตานี
๒.๔๔ จังหวัดพะเยา
๒.๔๕ จังหวัดพังงา
๒.๔๖ จังหวัดพัทลุง
๒.๔๗ จังหวัดพิจิตร
๒.๔๘ จังหวัดแพร่
๒.๔๙ จังหวัดมหาสารคาม
๒.๕๐ จังหวัดมุกดาหาร
๒.๕๑ จังหวัดแม่ฮ่องสอน
๒.๕๒ จังหวัดยโสธร
๒.๕๓ จังหวัดยะลา
๒.๕๔ จังหวัดร้อยเอ็ด
๒.๕๕ จังหวัดระนอง
๒.๕๖ จังหวัดระยอง
๒.๕๗ จังหวัดราชบุรี
๒.๕๘ จังหวัดลำปาง
๒.๕๙ จังหวัดลำพูน
๒.๖๐ จังหวัดเลย
๒.๖๑ จังหวัดศรีสะเกษ
๒.๖๒ จังหวัดสตูล
๒.๖๓ จังหวัดสมุทรปราการ
๒.๖๔ จังหวัดสมุทรสงคราม
๒.๖๕ จังหวัดสมุทรสาคร
๒.๖๖ จังหวัดสระแก้ว
๒.๖๗ จังหวัดสระบุรี
๒.๖๘ จังหวัดสุโขทัย

ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....

๒.๖๙จังหวัดสุพรรณบุรี
๒.๗๐จังหวัดสุรินทร์
๒.๗๑ จังหวัดหนองคาย
๒.๗๒ จังหวัดหนองบัวลำภู
๒.๗๓จังหวัดอ่างทอง
๒.๗๔ จังหวัดอำนาจเจริญ
๒.๗๕ จังหวัดอุตรดิตถ์
๒.๗๖ จังหวัดอุทัยธานี

ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....

ภาคผนวก ค

การสาธิตและทดสอบสมรรถนะของระบบ (Demonstration and Benchmark Test)

โครงการโครงการศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ระยะที่ ๑

ผู้เสนอราคาจะต้องนำอุปกรณ์ที่เกี่ยวข้องมาติดตั้งเพื่อการสาธิตและทดสอบสมรรถนะของระบบ ณ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป. โดยกำหนด รายละเอียดดังนี้

การทดสอบคุณสมบัติของอุปกรณ์ตามที่กำหนดในขอบเขตของงาน

เกณฑ์การตัดสิน	ผ่าน	ไม่ผ่าน	หมายเหตุ
ระบบมีการส่งข้อมูลทั้งหมดมาจัดเก็บบน Platforms โดยไม่จำเป็นต้องเป็น Alert (The solution must send all EDR data to the PLATFORM even if there are no alerts occurring)			
สามารถสร้าง IOC / BIOC ที่สามารถทำงานกับข้อมูลที่ได้รับมาจากระบบเครือข่ายและเครื่องคอมพิวเตอร์ลูกข่าย เพื่อสร้าง Alert กับข้อมูลย้อนหลัง ได้แบบอัตโนมัติ (The solution must support custom IOC/BIOC that work also in past data automatically across Network & Endpoints)			
ระบบที่นำเสนอต้องสามารถแนะนำวิธีการแก้ไขปัญหาเบื้องต้นได้ (The solution must provide remediation suggestion)			
ระบบสามารถแยกหรือตัดการเชื่อมต่อเครื่องคอมพิวเตอร์ลูกข่ายออกจากระบบเครือข่ายได้หลายๆเครื่องพร้อมๆกัน (Isolate multiple endpoints at the same time)			
ระบบสามารถส่งข้อมูลภัยคุกคามที่เป็น Unknown ไปทดสอบบน Sandbox ได้แบบอัตโนมัติ (The solution must automatically send all unknown executed files for sandbox analysis)			
ระบบสามารถเชื่อมโยงข้อมูลการโจมตีระหว่าง Network และ Endpoint ได้ โดยไม่ต้องมีการสร้าง ruleset หรือกำหนดความเชื่อมโยงไว้ล่วงหน้า (The solution must be able to stitch network data with endpoint data to provide complete end to end visibility of alerts with Predefined relation or rule)			
ระบบสามารถตรวจสอบช่องโหว่ที่มีอยู่บนเครื่องคอมพิวเตอร์ลูกข่ายได้ทั้ง Windows และ Linux (The solution must have Vulnerability Assessment where can detect the vulnerability on the host both Windows and Linux)			
ระบบต้องสามารถแสดงข้อมูลการติดตั้งแอพลิเคชั่นทั้งหมดที่ใช้งานอยู่บนเครื่องคอมพิวเตอร์ลูกข่ายได้ โดยไม่ต้องใช้ Agent อื่นๆ เพิ่มเติม (The solution must provide inventory of all installed			

ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....

เกณฑ์การตัดสิน	ผ่าน	ไม่ผ่าน	หมายเหตุ
applications on all major platforms: Windows and Linux without having to install additional agents.)			
ระบบสามารถวิเคราะห์ข้อมูลที่ได้รับมาจากระบบเครือข่ายเพื่อวิเคราะห์หาพฤติกรรมที่ผิดปกติได้ (The Solutions can analyze Network Traffic to identify abnormal behavior)			
ระบบที่นำเสนอต้องมีความสามารถในการส่งข้อมูลไปยัง Network Devices เพื่อทำงานร่วมกันกับ เช่นการส่ง IP Address List หรือ External Domain Names เป็นต้น (The solution must have the capability to respond to network devices that allows integration of your defined external Domain Names and IP Address lists with a firewall)			

หมายเหตุ :

๑. สถานที่ทดสอบ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงมหาดไทย ห้องประชุมวิสุทธิกษัตริย์ ชั้น ๓

๒. ติดต่อเพื่อขอทราบข้อมูลเพิ่มเติมได้ที่

๒.๑ ทางไปรษณีย์ ส่งถึง กองคลัง สำนักงานปลัดกระทรวงมหาดไทย ถนนอัษฎางค์ แขวงราชบพิตร เขตพระนคร กรุงเทพฯ ๑๐๒๐๐

๒.๒ ทางโทรศัพท์หมายเลข ๐๒ ๒๘๒ ๖๕๖๐ ต่อ ๕๐๖๕๗ หรือ ๕๐๓๖๘ กองคลัง สำนักงานปลัดกระทรวงมหาดไทย

๒.๓ ทางจดหมายอิเล็กทรอนิกส์ (E-Mail) ส่งถึง moi๐๒๐๓.๔@moi.go.th

ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....