ขอบเขตของงาน
โครงการศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ระยะที่ ๒
สำนักงานปลัดกระทรวงมหาดไทย

---

๑. <u>ความเป็นมา</u>

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงมหาดไทย ได้จัดทำโครงการศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ระยะที่ ๒ ของ สป.มท. ในการนี้สำนักงานปลัดกระทรวงมหาดไทยได้ดำเนินการส่วนต่อขยายเพื่อครอบคลุมส่วนงานอื่น ๆ ที่เกี่ยวข้องและเป็นไปตามกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ จากสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) โดยจัดให้มีการขยายกรอบการทำงาน เพื่อให้มีการพัฒนานโยบาย มาตรฐาน และกระบวนการด้านความมั่นคงปลอดภัยไซเบอร์ ระบบวิเคราะห์ระบบเฝ้าระวังและป้องกันภัยคุกคามไซเบอร์อัจฉริยะ ระบบตอบสนองและแก้ไขปัญหาแบบอัตโนมัติ ระบบตรวจสอบช่องโหว่ของระบบจากมุมมองของบุคคลภายนอก และระบบป้องกันข้อมูลรั่วไหลผ่านทางระบบเครือข่ายที่มีลิขสิทธิ์ถูกต้อง ทำการติดตั้งที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงมหาดไทย รองรับการป้องกันระบบต่าง ๆ ภายในศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป. และอุปกรณ์ตามโครงการระบบบริการสารสนเทศของกระทรวงมหาดไทยด้วยโครงข่ายเสมือน เพื่อให้ครอบคลุมการใช้งานป้องกันภัยคุกคามกับหน่วยงานในสังกัดสำนักงานปลัดกระทรวงมหาดไทยทั้งหมด โดยปัจจุบันระบบเทคโนโลยีสารสนเทศใหม่ ๆ ซึ่งมีการพัฒนาเพิ่มขึ้นหลายรูปแบบ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงมหาดไทย จึงได้จัดทำโครงการศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ระยะที่ ๒

เพื่อทำให้ระบบรักษาความปลอดภัยด้านสารสนเทศที่ใช้งานอยู่ในปัจจุบันตอบสนองต่อการให้บริการรวมถึงปริมาณการใช้งานที่เพิ่มขึ้นในปัจจุบัน และสามารถรองรับการทำงานได้อย่างมีประสิทธิภาพ ให้ทันสมัยครอบคลุมการทำงาน รองรับระบบงาน และเทคโนโลยีสารสนเทศรูปแบบใหม่ ประกอบกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และพระราชบัญญัติที่เกี่ยวข้องได้มีข้อกำหนดเพิ่มเติม จึงจำเป็นที่จะต้องปรับปรุงระบบให้สามารถป้องกันภัยคุกคามไซเบอร์ใหม่ ๆ ได้อย่างทันท่วงที

๒. <u>วัตถุประสงค์</u>

๒.๑ เพื่อให้หน่วยงานในสำนักงานปลัดกระทรวงมหาดไทย มีความคล่องตัวในการเข้าถึงระบบงานต่าง ๆ ของสำนักงานปลัดกระทรวงมหาดไทยที่ใช้งานในปัจจุบัน และการเข้าถึงข้อมูลข่าวสารภายนอกได้อย่างสะดวกและรวดเร็ว ก่อให้เกิดประสิทธิภาพในการทำงาน และเพิ่มศักยภาพในการป้องกันภัยคุกคามไซเบอร์

๒.๒ เพื่อเพิ่มประสิทธิภาพระบบวิเคราะห์ระบบเฝ้าระวังและป้องกันภัยคุกคามไซเบอร์อัจฉริยะ อุปกรณ์ตรวจจับ ให้มีความมั่นคงปลอดภัยและรองรับเทคโนโลยีสารสนเทศใหม่ ๆ

๒.๓ เพื่อให้การเชื่อมโยงเครือข่ายในระบบเป็นแนวทางเดียวกัน ถูกต้องตามข้อกฎหมาย ระเบียบ และไม่เกิดปัญหากับเครือข่ายของสำนักงานปลัดกระทรวงมหาดไทย

๒.๔ เพื่อเพิ่มประสิทธิภาพและอำนวยความสะดวกในการให้บริการแก่ประชาชน และหน่วยงานที่มาขอรับบริการได้อย่างทั่วถึงและรวดเร็ว

๒.๕ เพื่อเพิ่มประสิทธิภาพระบบวิเคราะห์ระบบเฝ้าระวังและป้องกันภัยคุกคามไซเบอร์อัจฉริยะ อุปกรณ์ตรวจจับ ให้ทันต่อเทคโนโลยีเพื่อต่อต้านภัยคุกคามทางไซเบอร์รูปแบบใหม่ ๆ รวมทั้งสามารถแก้ไขปัญหาที่เกิดขึ้นได้แบบอัตโนมัติ เพื่อเพิ่มความรวดเร็วและต่อเนื่องในการให้บริการ

/๓. <u>คุณสมบัติ</u>...

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 กิจการร่วมค้าดังกล่าวสามารถนำผลงานของผู้ร่วมค้ามาใช้แสดงเป็นผลงานของกิจการร่วมค้าที่เข้าประกวดราคาได้

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 กรณีที่...

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

๓.๑๑.๔ กรณีที่ข้อตกลงฯ กำหนดให้มีการมอบหมายให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า การยื่นข้อเสนอดังกล่าวไม่ต้องมีหนังสือมอบอำนาจสำหรับข้อตกลงฯ 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 ผู้ยื่นข้อเสนอจะต้องระบุให้เห็นอย่างชัดเจน สามารถตรวจสอบได้ง่ายไว้ในเอกสารเปรียบเทียบด้วยว่า สิ่งที่ต้องการอ้างอิงถึงนั้นอยู่ในส่วนตำแหน่งใดของเอกสารอื่น ๆ ที่จัดทำเสนอมา สำหรับเอกสารที่อ้างอิงถึงให้ขีดเส้นใต้หรือระบายสีพร้อมเขียนหัวข้อกำกับไว้ เพื่อให้สามารถไปตรวจสอบกับเอกสารเปรียบเทียบได้ง่ายและตรงกัน 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 กับอุปกรณ์เครือข่ายของสำนักงานปลัดกระทรวงมหาดไทย เพื่อแสดงว่าระบบสามารถใช้งานร่วมกันได้อย่างมีประสิทธิภาพ ผู้ยื่นข้อเสนอจะต้องเป็นผู้จัดหา และนำอุปกรณ์เข้าร่วมในการทดสอบโดยมีรายละเอียด ดังนี้

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

/๓.๑๔.๒ ระบบวิเคราะห์...

๓.๑๔.๒ ระบบวิเคราะห์ระบบเฝ้าระวังและป้องกันภัยคุกคามไซเบอร์อัจฉริยะ, ระบบตอบสนองและแก้ไขปัญหาแบบอัตโนมัติ (SOAR), ระบบตรวจสอบช่องโหว่ของระบบจากมุมมองของบุคคลภายนอก (Attack Surfaces Management) ระบบป้องกันเว็บแอปพลิเคชันด้วยเครื่องมือป้องกันการโจมตีเว็บไซต์ ระบบป้องกันการรั่วไหลของข้อมูลสารสนเทศผ่านทางระบบเครือข่าย (Network Data Leak Prevention) ระบบที่นำมาทำการทดสอบการใช้งานจริง (POC) จะต้องเป็นยี่ห้อเดียวกันกับอุปกรณ์ที่ยื่นในเอกสารเสนอราคา และมีความสามารถด้านฟังก์ชันการทำงานของอุปกรณ์ไม่น้อยกว่าระบบที่จะเสนอจริง

๓.๑๔.๓ หากทดสอบการใช้งานจริง (POC) แล้ว ไม่สามารถทำได้ตามที่เสนอ หรือไม่มาทำการสาธิต และทดสอบ สำนักงานปลัดกระทรวงมหาดไทยจะถือว่าข้อเสนอทางเทคนิคของผู้ยื่นข้อเสนอไม่ถูกต้องและจะไม่พิจารณาราคาของผู้ยื่นข้อเสนอรายนั้น

๓.๑๔.๔ ผู้ยื่นข้อเสนอต้องเป็นผู้รับผิดชอบค่าใช้จ่ายในการทดสอบระบบและอุปกรณ์ที่เกี่ยวข้องในการทดสอบ รวมทั้งหากเกิดความเสียหายที่เกี่ยวข้องกับการทดสอบผู้ยื่นข้อเสนอต้องเป็นผู้รับผิดชอบค่าใช้จ่าย

๓.๑๔.๕ กำหนดการทดสอบภายใน ๕ วันทำการ (นับถัดจากวันที่เสนอราคา)

๔. <u>ขอบเขตการดำเนินงาน</u>

ผู้ชนะการเสนอราคาจะต้องติดตั้งระบบวิเคราะห์ระบบเฝ้าระวังและป้องกันภัยคุกคามไซเบอร์อัจฉริยะ อุปกรณ์ตรวจจับใหม่ที่จัดซื้อในครั้งนี้พร้อมทั้งติดตั้งค่าอุปกรณ์ (Configuration) ให้สามารถใช้งานได้

๔.๑ จัดหาพร้อมติดตั้งระบบวิเคราะห์ระบบเฝ้าระวังและป้องกันภัยคุกคามไซเบอร์ ระบบตอบสนองและแก้ไขปัญหาแบบอัตโนมัติ (SOAR) และอุปกรณ์ตรวจจับวิเคราะห์และเฝ้าระวังภัยคุกคามบนระบบเครือข่ายตามสถานที่ดำเนินการที่ระบุไว้ในภาคผนวก ข

๔.๒ ระบบวิเคราะห์ระบบเฝ้าระวังและป้องกันภัยคุกคามไซเบอร์อัจฉริยะ, อุปกรณ์ตรวจจับ, วิเคราะห์ และเฝ้าระวังภัยคุกคามบนระบบเครือข่ายที่จัดหาใหม่ต้องใช้งานร่วมกันกับระบบรักษาความปลอดภัยเดิม (ที่ได้ดำเนินการติดตั้งใช้งานอยู่ในปัจจุบัน) ได้อย่างสมบูรณ์ และเป็นไปตามวัตถุประสงค์ มีดังนี้

๔.๒.๑ พัฒนานโยบาย มาตรฐาน และกระบวนการด้านความมั่นคงปลอดภัยไซเบอร์สำหรับศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงมหาดไทย จำนวน ๑ งาน

๔.๒.๒ ระบบวิเคราะห์ระบบเฝ้าระวังและป้องกันภัยคุกคามไซเบอร์อัจฉริยะ จำนวน ๑ ระบบ

๔.๒.๓ ระบบตอบสนองและแก้ไขปัญหาแบบอัตโนมัติ (SOAR) จำนวน ๑ ระบบ

๔.๒.๔ ระบบตรวจสอบช่องโหว่ของระบบจากมุมมองของบุคคลภายนอก (Attack Surfaces Management) จำนวน ๑ ระบบ

๔.๒.๕ ระบบป้องกันเว็บแอปพลิเคชันด้วยเครื่องมือป้องกันการโจมตีเว็บ Web Application Firewall และ API Protection จำนวน ๑ ระบบ

๔.๒.๖ ระบบป้องกันการรั่วไหลของข้อมูลสารสนเทศผ่านทางระบบเครือข่าย (Network Data Leak Prevention) จำนวน ๑ ระบบ

/๕. วิธีการดำเนินการ...

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

๕. <u>วิธีการดำเนินการ</u>

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

๕.๒ ผู้ชนะการเสนอราคาจะต้องส่งมอบผังการเชื่อมโยงอุปกรณ์ คู่มือการใช้งาน และวิธีดูแลรักษาระบบวิเคราะห์ระบบเฝ้าระวังและป้องกันภัยคุกคามไซเบอร์อัจฉริยะ, อุปกรณ์ตรวจจับ, วิเคราะห์ และเฝ้าระวังภัยคุกคามบนระบบเครือข่ายในโครงการนี้ โดยมอบให้สำนักงานปลัดกระทรวงมหาดไทย จำนวน ๒ ชุด

๕.๓ ผู้ชนะการเสนอราคาจะต้องทดสอบการทำงานของระบบวิเคราะห์ระบบเฝ้าระวังและป้องกันภัยคุกคามไซเบอร์อัจฉริยะ, อุปกรณ์ตรวจจับ ให้สามารถใช้งานได้อย่างสมบูรณ์

๕.๔ ผู้ชนะการเสนอราคาต้องจัดทำแผนการติดตั้งค่าอุปกรณ์ (Configuration) เช่น Secure Policy เบื้องต้นร่วมกับผู้ซื้อก่อนดำเนินงาน

๕.๕ ผู้ชนะการเสนอราคาจะต้องส่งแผนและขั้นตอนการดำเนินการ และออกแบบการติดตั้งและจัดทำแผนผังการเชื่อมโยงระบบ อุปกรณ์ (Network Diagram) ส่งให้คณะกรรมการตรวจรับพัสดุทราบภายใน ๓๐ วันทำการ นับถัดจากวันที่ลงนามในสัญญา

๕.๖ ผู้ชนะการเสนอราคาต้องให้คำปรึกษา แนะนำ ด้านระบบและอุปกรณ์ที่ติดตั้งตามโครงการนี้แก่บุคลากรของสำนักงานปลัดกระทรวงมหาดไทย เมื่อมีการร้องขอโดยไม่คิดค่าใช้จ่ายตลอดอายุสัญญา

๕.๗ ผู้ชนะการเสนอราคาจะต้องรับผิดชอบค่าใช้จ่ายติดตั้งอุปกรณ์ในโครงการนี้พร้อมทั้งค่าใช้จ่ายที่เกิดขึ้นทั้งหมด

๕.๘ ในกรณีที่ผู้ชนะการเสนอราคาประสงค์จะนำอุปกรณ์รายการใดแตกต่างไปจากรายละเอียดที่กำหนดไว้ในสัญญามาติดตั้งให้สำนักงานปลัดกระทรวงมหาดไทย ผู้ชนะการเสนอราคาจะต้องได้รับความเห็นชอบจากคณะกรรมการตรวจรับพัสดุ และอุปกรณ์ที่จะนำมาติดตั้งดังกล่าวจะต้องมีคุณสมบัติไม่ต่ำกว่าที่กำหนดไว้ในสัญญา ทั้งนี้ ผู้ชนะการเสนอราคาจะต้องไม่คิดค่าใช้จ่ายเพิ่มเติม ไม่ว่ากรณีใด ๆ

๖. <u>การจัดฝึกอบรม</u>

ผู้ชนะการเสนอราคาจะต้องทำการจัดอบรม การใช้งานระบบวิเคราะห์ระบบเฝ้าระวังและป้องกันภัยคุกคามไซเบอร์อัจฉริยะ, อุปกรณ์ตรวจจับ ทั้งหมด รวมทั้งให้ความรู้อื่น ๆ ที่เกี่ยวข้องให้กับผู้ที่เกี่ยวข้อง โดยให้จัดอบรมครั้งเดียวเป็นเวลาไม่น้อยกว่า ๒ วันทำการ ผู้เข้าร่วมอบรมไม่น้อยกว่า ๑๐ คน โดยดำเนินการ ดังนี้

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. <u>ระยะเวลา</u>...

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

๗. <u>ระยะเวลาดำเนินการและส่งมอบงาน</u>

กำหนดระยะเวลาส่งมอบทั้งโครงการ ภายใน ๑๘๐ วัน นับถัดจากวันที่ลงนามในสัญญา โดยแบ่งเป็นงวดงาน และมีการดำเนินงานดังนี้

๗.๑ **งวดงานที่ ๑** ภายใน ๖๐ วัน นับถัดจากวันที่ลงนามในสัญญา ผู้รับจ้างจะต้องส่งแผนและขั้นตอนการดำเนินการ ออกแบบการติดตั้ง และจัดทำแผนผังการเชื่อมโยงระบบอุปกรณ์ (Network Diagram) ส่งให้คณะกรรมการตรวจรับพัสดุทราบ และผู้รับจ้างจะต้องส่งมอบอุปกรณ์พร้อมติดตั้งในข้อ ๔ และข้อ ๖ ตามภาคผนวก ก ให้แล้วเสร็จ ตามที่สำนักงานปลัดกระทรวงมหาดไทยกำหนด

๗.๒ **งวดงานที่ ๒** ภายใน ๑๒๐ วัน นับถัดจากวันที่ลงนามในสัญญา โดยผู้รับจ้างจะต้องส่งมอบอุปกรณ์พร้อมติดตั้งในข้อ ๓ และข้อ ๕ ตามภาคผนวก ก ให้แล้วเสร็จ ตามที่สำนักงานปลัดกระทรวงมหาดไทยกำหนด

๗.๓ **งวดที่ ๓ (งวดสุดท้าย)** ภายใน ๑๘๐ วัน นับถัดจากวันที่ลงนามในสัญญาโดยผู้รับจ้างจะต้องส่งมอบอุปกรณ์พร้อมติดตั้งในข้อ ๑ และข้อ ๒ ตามภาคผนวก ก ให้แล้วเสร็จ ตามที่สำนักงานปลัดกระทรวงมหาดไทยกำหนด

๗.๔ คู่มือการใช้งานและวิธีดูแลรักษาระบบวิเคราะห์ระบบเฝ้าระวังและป้องกันภัยคุกคามไซเบอร์อัจฉริยะ อุปกรณ์ตรวจจับ สำหรับศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.มท. ๒ ชุด

๗.๕ การจัดอบรม การใช้งานระบบวิเคราะห์ระบบเฝ้าระวังและป้องกันภัยคุกคามไซเบอร์อัจฉริยะ อุปกรณ์ตรวจจับ รวมทั้งให้ความรู้อื่น ๆ ที่เกี่ยวข้อง

๗.๖ คณะกรรมการตรวจรับพัสดุ จะตรวจรับงานโดยการตรวจอุปกรณ์ทั้งระบบตามรายละเอียด การทดสอบการใช้งานในสัญญาฯ เมื่อสำนักงานปลัดกระทรวงมหาดไทยได้รับหนังสือแจ้งจากผู้รับจ้างว่าได้ติดตั้งเสร็จเรียบร้อยแล้ว 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 หักคืนเงินล่วงหน้าร้อยละ ๑๕

งวดที่ ๒ ผู้ว่าจ้างจะจ่ายเงินให้หลังจากผู้รับจ้างส่งมอบงานงวดที่ ๒ และคณะกรรมการตรวจรับพัสดุฯ ดำเนินการตรวจรับถูกต้อง ครบถ้วนแล้ว เป็นจำนวนเงิน ร้อยละ ๓๐ ของวงเงินตามสัญญาฯ หักคืนเงินล่วงหน้าร้อยละ ๑๕

/งวดสุดท้าย...

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

งวดสุดท้าย ผู้ว่าจ้างจะจ่ายเงินให้หลังจากผู้รับจ้างส่งมอบงานงวดสุดท้าย และคณะกรรมการตรวจรับพัสดุฯ ดำเนินการตรวจรับถูกต้อง ครบถ้วนแล้ว เป็นจำนวนเงิน ร้อยละ ๔๐ ของวงเงินตามสัญญาฯ หักคืนเงินล่วงหน้าร้อยละ ๑๕

๙. <u>การสนับสนุนของสำนักงานปลัดกระทรวงมหาดไทย</u>

สำนักงานปลัดกระทรวงมหาดไทยจะอำนวยความสะดวกให้กับผู้ยื่นข้อเสนอเพื่อให้การดำเนินงานเรียบร้อยและมีประสิทธิภาพ ดังนี้

๙.๑ ดำเนินการจัดเจ้าหน้าที่อำนวยความสะดวกและให้ข้อมูลเกี่ยวกับระบบคอมพิวเตอร์

๙.๒ อนุญาตให้ผู้ยื่นข้อเสนอใช้ และสามารถส่งข้อมูลผ่านระบบเครือข่ายสื่อสารของสำนักงานปลัดกระทรวงมหาดไทยตามความเหมาะสม

๑๐. <u>การรับประกันความชำรุดบกพร่อง</u>

๑๐.๑ ผู้รับจ้างต้องรับประกันความชำรุดบกพร่องของอุปกรณ์ที่เสนอเป็นระยะเวลาไม่น้อยกว่า ๓ ปี นับถัดจากวันที่ได้ส่งมอบงานงวดสุดท้ายเป็นที่เรียบร้อย และคณะกรรมการฯ ตรวจรับถูกต้อง ครบถ้วนเรียบร้อยแล้ว

๑๐.๒ ในระหว่างการดำเนินการและระหว่างเวลาการรับประกันตามสัญญาฯ หากมีอุปกรณ์ชำรุดขัดข้องจากการใช้งานตามปกติ ผู้รับจ้างจะต้องเดินทางมาถึงที่เกิดเหตุภายใน ๒๔ ชั่วโมง นับตั้งแต่เวลาที่ได้รับแจ้งจากผู้ว่าจ้าง หรือผู้ดูแลระบบ และดำเนินการซ่อมแซมแก้ไข/หาทดแทนให้แล้วเสร็จภายใน ๔๘ ชั่วโมง และถ้าผู้รับจ้างไม่สามารถดำเนินการได้ ผู้ว่าจ้างมีสิทธิว่าจ้างผู้อื่นมาดำเนินการซ่อมแซมแก้ไข โดยผู้รับจ้างจะต้องรับผิดชอบค่าใช้จ่ายที่เกิดขึ้นทั้งสิ้น

๑๐.๓ ผู้รับจ้างต้องมีศูนย์บริการรับแจ้ง (Help Desk Center) ณ ที่ทำการของผู้รับจ้าง และให้บริการรับแจ้งปัญหาจากผู้ใช้งานตลอดเวลาการปฏิบัติงานในวันเวลาราชการ โดยแจ้งหมายเลขโทรศัพท์และระบบสื่อสารอื่นที่สามารถติดต่อได้

๑๐.๔ ในระหว่างการดำเนินการและระหว่างเวลาการรับประกันตามสัญญาฯ ผู้รับจ้างต้องรายงานการตรวจพบการโจมตี และการแก้ไข ส่งเป็นรายเดือน รายไตรมาส รายปี

๑๑. <u>อัตราค่าปรับ</u>

หากผู้ชนะการเสนอราคาไม่ปฏิบัติตามสัญญาหรือผิดสัญญาข้อหนึ่งข้อใด และสำนักงานปลัดกระทรวงมหาดไทยยังไม่บอกเลิกสัญญา ผู้ชนะการเสนอราคาจะต้องถูกปรับเป็นรายวันในอัตราร้อยละ ๐.๑ ของงานจ้าง

๑๒. <u>การจ้างช่วง</u>

ผู้รับจ้างจะต้องไม่เอางานทั้งหมดหรือบางส่วนนี้ไปจ้างช่วงอีกทอดหนึ่ง เว้นแต่การจ้างช่วงงานแต่บางส่วนที่ได้รับอนุญาตเป็นหนังสือจากผู้ว่าจ้างแล้ว การที่ผู้ว่าจ้างได้อนุญาตให้จ้างช่วงงานแต่บางส่วนดังกล่าวนั้นไม่เป็นเหตุให้ผู้รับจ้างหลุดพ้นจากความรับผิดหรือพ้นธะหน้าที่ตามสัญญานี้ และผู้รับจ้างจะยังคงต้องรับผิดในความผิดและความประมาทของผู้รับจ้างช่วงหรือของตัวแทนหรือลูกจ้างของผู้รับจ้างช่วงนั้นทุกประการ

กรณีผู้รับจ้างไปจ้างช่วงงานแต่บางส่วนโดยฝ่าฝืนความในวรรคหนึ่ง ผู้รับจ้างต้องชำระค่าปรับให้แก่ผู้ว่าจ้างเป็นจำนวนเงินในอัตราร้อยละสิบ ของวงเงินของงานที่จ้างช่วงตามสัญญา ทั้งนี้ไม่ตัดสิทธิผู้ว่าจ้างในการบอกเลิกสัญญา

/๑๓. หลักเกณฑ์การ...

ประธานกรรมการ.....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. ๒๕๖๙ จำนวน ๙๘,๐๐๐,๐๐๐.๐๐.- บาท (เก้าสิบแปดล้าน-บาทถ้วน) รวมภาษีมูลค่าเพิ่ม ภาษีอากรอื่น ๆ และค่าใช้จ่ายทั้งปวงด้วย

๑๕. <u>หน่วยงานผู้รับผิดชอบ</u>

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงมหาดไทย

ลงชื่อ ..... ประธานกรรมการ
(นายเสรี กัณฑ์โรจน์)
ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.

ลงชื่อ ..... กรรมการ
(นายณัฐกิตติ์ ตาวงษ์สา)
ผู้อำนวยการกลุ่มงานโครงสร้างพื้นฐาน
ด้านสารสนเทศและการสื่อสาร

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

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

ลงชื่อ ..... กรรมการ
(นายธนวัฒน์ สังกระธาตุ)
นายช่างไฟฟ้าชำนาญงาน

ภาคผนวก ก

คุณลักษณะเฉพาะทางเทคนิค (Technical Specification)

โครงการศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ระยะที่ ๒

สำนักงานปลัดกระทรวงมหาดไทย

---

๑. พัฒนานโยบาย มาตรฐาน และกระบวนการด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงมหาดไทย จำนวน ๑ งาน โดยมีคุณลักษณะอย่างน้อย ดังนี้

๑.๑ ดำเนินการพัฒนานโยบาย ระบบรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ เพื่อปฏิบัติตามข้อกำหนดพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๑.๒ ดำเนินการศึกษา และวิเคราะห์ช่องโหว่ (GAP Analysis) สถานะในปัจจุบัน (As-IS) ด้านความมั่นคงปลอดภัยสารสนเทศ และเปรียบเทียบกับกรอบปฏิบัติ (Framework) ในระดับสากลที่ได้รับความน่าเชื่อถือ เช่น NIST Cybersecurity Framework ๒.๐ เป็นต้น หรือประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ประกาศตามข้อกำหนดพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ โดยจะต้องมีขอบเขตดังนี้

๑.๒.๑ ดำเนินการศึกษาในภาพรวมของการดำเนินการของหน่วยงาน หรือการใช้ระบบเทคโนโลยีสารสนเทศ เพื่อระบุระบบเทคโนโลยีสารสนเทศที่เกี่ยวข้อง

๑.๒.๒ ดำเนินการรวบรวมข้อมูลที่เกี่ยวข้องเพื่อดำเนินการทำ GAP & Risk Assessment โดยมีขอบเขตการรวบรวมอย่างน้อย ดังนี้

๑.๒.๒.๑ ดำเนินการสัมภาษณ์บุคลากรที่เกี่ยวข้อง

๑.๒.๒.๒ ดำเนินการตรวจสอบจากเอกสารรายงานที่เกี่ยวข้อง

๑.๒.๒.๓ ดำเนินการตรวจสอบขั้นตอนการปฏิบัติในด้านการตอบสนองต่ออุบัติการณ์และเอกสารประกอบอื่น ๆ

๑.๒.๓ ดำเนินการศึกษา และวิเคราะห์สถานภาพของการตรวจสอบความพร้อมในการตอบสนองต่ออุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กร (GAP Assessment) เปรียบเทียบกับข้อกำหนดของกรอบปฏิบัติที่ได้รับการยอมรับในระดับสากล NIST Cybersecurity Framework ๒.๐ โดยครอบคลุมหัวข้อ ดังนี้

๑.๒.๒.๑ การกำกับดูแล (Govern)

๑.๒.๒.๒ การระบุความเสี่ยง (Identify)

๑.๒.๒.๓ มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

๑.๒.๒.๔ มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

๑.๒.๒.๕ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

๑.๒.๒.๖ มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

๑.๒.๔ ดำเนินการประเมินความเสี่ยง (Risk Assessment) ที่จะส่งผลกระทบต่อการดำเนินงานของระบบเทคโนโลยีสารสนเทศ ซึ่งการประเมินความเสี่ยงจะประเมินในรูปแบบของ Scenario base approach ตามวิธีการประเมินความเสี่ยง ที่ออกแบบตามหลักของมาตรฐานสากล

๑.๒.๕ ดำเนินการสรุปผลการวิเคราะห์ และข้อเสนอแนะเพื่อการเตรียมพร้อมในการตอบสนองภัยคุกคามด้านไซเบอร์ ทั้งในด้านของบุคลากร (People) กระบวนการบริหารจัดการ (Process) และระบบเทคโนโลยีที่ใช้ในการป้องกันและตรวจจับภัยคุกคามด้านไซเบอร์ (Technology)

/๒. ระบบวิเคราะห์

๒. ระบบวิเคราะห์ระบบเฝ้าระวังและป้องกันภัยคุกคามไซเบอร์อัจฉริยะ จำนวน ๑ ระบบ โดยมีคุณลักษณะอย่างน้อย ดังนี้

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

๒.๒ Agent Software ต้องสามารถป้องกันภัยคุกคามที่เกิดขึ้นบนเครื่องคอมพิวเตอร์ลูกข่าย เครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เคลื่อนที่ (Mobile Device) จำนวน ๕๐๐ ลิขสิทธิ์ โดยมีความสามารถด้านการป้องกันภัยคุกคาม ดังนี้

๒.๒.๑ ป้องกันการโจมตีที่ช่องโหว่ของระบบ (Exploit Prevention)

๒.๒.๒ ป้องกันมัลแวร์ หรือไวรัส (Malware Prevention หรือ Antivirus)

๒.๒.๓ ป้องกันการโจมตีของมัลแวร์ระดับสูง ที่ใช้เทคนิคโจมตีแบบไม่ใช้ไฟล์ (Fileless Attacks)

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

๒.๒.๕ ป้องกันการโจมตีโดยใช้การวิเคราะห์พฤติกรรม (Behavior)

๒.๒.๖ ป้องกันมัลแวร์เรียกค่าไถ่ (Ransomware Protection)

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

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

๒.๕ แสดงข้อมูลเหตุการณ์ภัยคุกคามทางไซเบอร์ โดยมีรายละเอียดอย่างน้อย ดังนี้

๒.๕.๑ ระบุประเภทของภัยคุกคาม

๒.๕.๒ วัน-เวลา เริ่มต้นและสิ้นสุดของภัยคุกคาม

๒.๕.๓ ระบุต้นทาง (Source) ปลายทาง (Destination)

๒.๕.๔ ระบุระดับความรุนแรง (Severity)

๒.๕.๕ รายละเอียดเหตุการณ์และพฤติกรรม

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

๒.๕.๗ สามารถแสดงเทคนิคของภัยคุกคามที่ตรวจพบ โดยเทียบเคียงกับ MITRE ATT & CK stage ต่าง ๆ

๒.๖ ระบบ Detection and Response ในการตรวจจับภัยคุกคาม และรวบรวมข้อมูลจากกิจกรรมต่าง ๆ ที่เกิดขึ้น โดยทั้งระบบที่นำเสนอต้องมีความสามารถรวมกันอย่างน้อย ดังนี้

๒.๖.๑ Endpoint Detection and Response (EDR) (ตรวจจับและตอบสนองต่อเครื่องแม่ข่าย)

๒.๖.๒ Root Cause Analysis (วิเคราะห์หาต้นตอของปัญหาที่เกิดขึ้น)

๒.๖.๓ Timeline analysis of alerts (สามารถแสดง Timeline ของเหตุการณ์ที่เกิดขึ้น)

๒.๖.๔ Threat Hunting (การตรวจหาภัยคุกคาม อาจเกิดขึ้นในองค์กร)

๒.๖.๕ Incident response and recovery (ตอบสนองและกู้คืนระบบจากเหตุการณ์ที่เกิด)

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

/๒.๗ มีวิธีการ...

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

๒.๗ มีวิธีการในการตอบสนองต่อภัยคุกคาม (Response) อย่างน้อย ดังนี้

๒.๗.๑ แยกหรือตัดการเชื่อมต่อเครื่องคอมพิวเตอร์ลูกข่าย และแม่ข่าย (Isolate Endpoint) ได้หลาย ๆ เครื่องพร้อม ๆ กัน (Multiple Selection) ผ่านหน้า management console

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

๒.๗.๓ เพิ่มค่า Hash ของไฟล์ที่ต้องการป้องกันได้ (Add to Block List)

๒.๗.๔ สามารถสร้าง Automation Rule เพื่อกำหนดให้ระบบตอบสนองอัตโนมัติเมื่อมี Alert ที่ตรงเงื่อนไขเกิดขึ้น โดยสามารถเลือกจากเงื่อนไข (Attribute) ได้ไม่น้อยกว่า ๒ เงื่อนไขพร้อมกันได้ หรือเสนอระบบอื่นๆ เพิ่มเติมเพื่อให้สามารถทำงานได้ตามข้อกำหนด

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

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

๒.๑๐ สามารถทำงานร่วมกับอุปกรณ์ที่ทำหน้าที่เป็น Network Sensor ที่มี AI และ Machine Learning เพื่อให้สามารถทำ Log Stitching หรือ Data Stacking เพื่อทำให้ข้อมูลดังกล่าวเป็นภาพเดียวกันได้ กรณีที่ไม่สามารถทำงานร่วมได้ ให้เสนออุปกรณ์เพิ่มเติมเพื่อให้ครอบคลุม และเพียงพอต่อการทำงาน

๒.๑๑ สามารถตรวจสอบช่องโหว่ของระบบปฏิบัติการ (Vulnerability Assessment) บนระบบปฏิบัติการ Windows และ Linux โดยอ้างอิงช่องโหว่ตาม Common Vulnerabilities and Exposures (CVE) โดยไม่ต้องติดตั้ง Agent เพิ่มเติม หรือนำเสนอระบบอื่น ๆ เพิ่มเติม เพื่อสามารถทำได้ตามความต้องการดังกล่าว

๒.๑๒ สามารถแสดง Host Inventory เช่น User, Application, Services, Driver, Autorun, Share ของเครื่องคอมพิวเตอร์ได้ เพื่อสามารถตรวจสอบข้อมูลได้อย่างรวดเร็ว หรือนำเสนอระบบอื่น ๆ เพิ่มเติม เพื่อทำได้ตามความต้องการดังกล่าว

๒.๑๓ ระบบที่นำเสนอจะต้องสามารถรองรับเชื่อมต่อแบบ Single Sign-on เพื่อนำเข้าข้อมูลบัญชีผู้ใช้งานผ่านโปรโตคอล SAML ๒.๐ ได้

๒.๑๔ ระบบที่นำเสนอต้องมีความสามารถในการทำ Disk Encryption ได้ ทั้งบน Windows และ MAC OS

๒.๑๕ สามารถสร้างแดชบอร์ดโดยใช้ XQL หรือ KQL หรือเทียบเท่ามาเป็นเงื่อนไขในการ Filter ข้อมูล

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

๒.๑๗ มีความสามารถในการแจ้งเตือน (Alert) ผ่าน Email, Slack หรือ SYSLOG โดยสามารถเลือกจากเงื่อนไข (Attribute) ได้ไม่น้อยกว่า ๒ เงื่อนไขพร้อมกันได้ หรือเสนอระบบอื่น ๆ เพิ่มเติมเพื่อให้สามารถทำงานได้ตามข้อกำหนด

/๒.๑๘ สามารถสร้าง...

๒.๑๘ สามารถสร้างและแก้ไข Correlation rule เพื่อทำการตรวจสอบเหตุการณ์การโจมตีได้จากหลาย ๆ เหตุการณ์ (multi-events) จากหลาย ๆ อุปกรณ์ (multi-sources) ด้วย Query Language ได้ หรือนำเสนอระบบอื่น ๆ เพิ่มเติม เพื่อสามารถทำได้ตามความต้องการดังกล่าว

๒.๑๙ ระบบที่นำเสนอต้องอยู่ในกลุ่ม Leader ของ Gartner Magic Quadrant for EPP ๒๐๒๔ หรือใหม่กว่า และ The Forrester Wave™: Extended Detection And Response Platform, Q๒ ๒๐๒๔ หรือใหม่กว่า

๒.๒๐ ต้องรับประกันระบบที่นำเสนอเป็นเวลาอย่างน้อย ๓ ปี

๒.๒๑ ผู้เสนอราคาต้องมีหนังสือสนับสนุนทางด้านเทคนิคจากผู้ผลิตหรือสาขาของผู้ผลิตในประเทศไทย และรับรองว่าอุปกรณ์ภายในโครงการนี้ อยู่ในสภาพที่ใช้งานได้ดี เป็นรุ่นที่ยังอยู่ในสายการผลิต และเป็นของใหม่ มิได้ถูกติดตั้งใช้งาน ณ ที่ใดมาก่อน

๓. ระบบตอบสนองและแก้ไขปัญหาแบบอัตโนมัติ (SOAR) จำนวน ๑ ระบบ โดยมีคุณลักษณะอย่างน้อย ดังนี้

๓.๑ เป็นระบบที่ออกแบบมาเพื่อจัดการเรื่อง Security Orchestration, Automation and Response (SOAR) โดยเฉพาะและมีสำนักงานในประเทศไทย เพื่อให้มีประสิทธิภาพในการทำงานสูงสุด

๓.๒ เป็น Software ที่ออกแบบมาเพื่อช่วยในการบริหารจัดการสำหรับ Security Operation Team โดยเฉพาะ โดยมีเครื่องมือที่ช่วยในการทำ Accelerate Response โดยสามารถทำงานร่วมกับระบบต่าง ๆ ได้เป็นอย่างน้อย ดังนี้

๓.๒.๑ Security Information and Event Management (SIEM)

๓.๒.๒ Endpoint Detection and Response (EDR)

๓.๒.๓ Extended Detection and Response (XDR)

๓.๒.๔ Threats Intelligence (TI)

๓.๒.๕ Malware Analysis

๓.๒.๖ Data Loss Prevention (DLP)

๓.๒.๗ Email

๓.๒.๘ Ticketing Systems

๓.๒.๙ Users and Entity Behavior Analytic

๓.๓ มีรูปแบบการบริหารจัดการ Standardize Process และติดตามเหตุการณ์ที่เกิดขึ้น (incident) รวมไปถึงช่วยวิเคราะห์ (Analyst Metrics) เช่น Task-based workflows หรือ Visual playbook editor หรือ SLA and metric tracking เป็นอย่างน้อย

๓.๔ มีระบบช่วยให้ทีมผู้ดูแลระบบต่าง ๆ สามารถทำงานร่วมกัน ได้ลักษณะ Virtual War Room ที่สามารถสื่อสารข้อความ, เก็บข้อมูลเกี่ยวกับ Incident, Log การทำงานของ WorkFlow/Playbook ต่าง ๆ หรือนำเสนอระบบอื่น ๆ เพิ่มเติมเพื่อสามารถทำความต้องการดังกล่าว โดยระบบที่นำเสนอเพิ่มเติมจะต้องสามารถเชื่อมโยงข้อมูลการสนทนาที่เกี่ยวข้องกับ Incident นั้น ๆ จากระบบ SOAR ไปยังระบบ Collaborate and Learn ได้ทันที

/๓.๕ สามารถสร้าง...

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

๓.๕ สามารถสร้าง Work Plan หรือ WorkFlow หรือ Playbook และสามารถทำ Sub Playbook ได้ โดยมีความสามารถอย่างน้อย ดังนี้

๓.๕๑ สามารถ Enrichment ข้อมูล Indicator of Compromise (IOC) ที่ได้จาก Threat Intelligence (TI) ได้

๓.๕.๒ สามารถ Enrichment ข้อมูลร่วมกับระบบงานภายนอก เช่น Active Directory

๓.๖ สามารถทำ Case Management เพื่อบริหารจัดการ Incident ต่าง ๆ ที่เกิดขึ้น เช่น กำหนดระยะเวลาในการตอบสนองต่อ Incident type ประเภทต่าง ๆ ได้ รวมถึงแสดงผลการทำงานในภาพรวมลักษณะ SLA Dashboard ได้ หรือนำเสนอระบบอื่น ๆ เพิ่มเติม เพื่อสามารถทำงานลักษณะดังกล่าว

๓.๗ มีความสามารถในการบริหารจัดการความรับผิดชอบงาน (Shift Management) ของผู้ดูแลระบบความปลอดภัย และสามารถส่ง Incident ให้กับผู้ดูแลระบบความปลอดภัยตามความรับผิดชอบงานหรือภาระงาน (load) ได้เป็นอย่างน้อย

๓.๘ สามารถทำงานร่วมกับระบบรักษาความปลอดภัยเครือข่าย (Application Firewall) ที่มีอยู่เดิมได้ในลักษณะ WorkFlow/Playbook แบบพร้อมใช้งาน หรือทำการพัฒนาเพิ่มเติมให้ครบถ้วน โดยมีความสามารถอย่างน้อย ดังนี้

๓.๘.๑ สามารถ commit การแก้ไข configuration บนอุปกรณ์ได้

๓.๘.๒ สามารถดึงค่า, สร้าง และลบ Custom URL Category ได้

๓.๘.๓ สามารถดึงค่าของ URL Category ได้

๓.๘.๔ สามารถสร้าง, แก้ไข, ย้าย และลบ Policy rule ได้

๓.๘.๕ สามารถดึงค่า, สร้าง, อัพเดท และ ลบ EDL (External Dynamic List) ได้

๓.๘.๖ สามารถทำการค้นหา (Query) log จาก Traffic, Threat, URL log ได้

๓.๘.๗ สามารถทำการสั่งดาวน์โหลด และติดตั้ง content update ได้

๓.๙ สามารถบริหารแบบ GUI จัดการผ่าน Web Browser เช่น Chrome หรือ Firefox หรือ Microsoft Edge เป็นอย่างน้อย

๓.๑๐ มี Licenses สิทธิในการใช้งานที่สามารถรองรับผู้ใช้งานระดับ Security Analyst ได้ไม่น้อยกว่า ๒ ผู้ใช้งาน

๓.๑๑ สามารถพิสูจน์ตัวตนของผู้ใช้ระบบบน Local system หรือ สามารถทำ Single sign-on (SSO) ด้วย SAML

๓.๑๒ มี Playbook Marketplace ที่สามารถนำ Playbook ใหม่ ๆ มาติดตั้งใช้งานได้อย่างต่อเนื่อง หรือมี Playbook ที่พร้อมนำมาใช้งาน หรือพัฒนาเพิ่มเติมให้ครบตามจำนวน ไม่น้อยกว่า ๖๐๐ Playbook

๓.๑๓ ผู้เสนอราคาต้องมีหนังสือสนับสนุนทางด้านเทคนิคจากผู้ผลิตหรือสาขาของผู้ผลิตในประเทศไทย และรับรองว่าอุปกรณ์ภายในโครงการนี้ อยู่ในสภาพที่ใช้งานได้ดี เป็นรุ่นที่ยังอยู่ในสายการผลิต และเป็นของใหม่ มิได้ถูกติดตั้งใช้งาน ณ ที่ใดมาก่อน

๓.๑๔ ต้องรับประกันระบบที่นำเสนอเป็นเวลาอย่างน้อย ๓ ปี

/๓.๑๕ ต้องได้รับ...

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

๓.๑๕ ต้องได้รับการจัดอันดับให้อยู่ในกลุ่ม Leader ของ Gigaom Radar ในกลุ่มผลิตภัณฑ์ Security Orchestration, Automation & Response (SOAR) ปี ๒๐๒๔ หรือใหม่กว่า และ ได้รับการจัดอันดับให้อยู่ในกลุ่ม Leader ของ SOFTWARE REVIEWS Data Quadrant ในกลุ่มผลิตภัณฑ์ Security Orchestration, Automation, and Response ปี ๒๐๒๔ หรือใหม่กว่า

๔. ระบบตรวจสอบช่องโหว่ของระบบจากมุมมองของบุคคลภายนอก (Attack Surfaces Management) จำนวน ๑ ระบบ โดยมีคุณลักษณะอย่างน้อย ดังนี้

๔.๑ สามารถระบุทรัพย์สินทั้งหมดที่มีการสื่อสารบนอินเทอร์เน็ตต่อสาธารณะทั่วโลก (Asset Inventory) ที่เกี่ยวข้องกับการให้บริการของหน่วยงาน เช่น Domains, Responsive IP address หรือ IP ranges, Services, Websites, Certificates และ Cloud Inventory หรือ Cloud Resources ได้

๔.๒ มีนโยบายด้านความปลอดภัย (Rule) เพื่อแจ้งปัญหาที่พบได้ไม่น้อยกว่า ๘๕๐ แบบ ซึ่งจะต้องสามารถปรับความสำคัญของ Rule ได้

๔.๓ มี Compliance Dashboard กับมาตรฐาน NIST ๘๐๐-๕๓, NIST ๘๐๐-๑๗๑, CMMC L๑-L๓ และ CMMC L๑-L๕ เป็นอย่างน้อย เพื่อที่แสดงความเชื่อมโยงของปัญหากับ Compliance Frameworks

๔.๔ สามารถระบุการให้บริการของทรัพย์สินต่าง ๆ เช่น Services, Port ที่มีการใช้งาน และระบุช่องโหว่ในรูปแบบ CVE ของ Service นั้น ๆ ได้

๔.๕ สามารถ Integrate workflow เข้ากับระบบการบริหารจัดการด้าน Cyber Security workflow ได้อย่างมีประสิทธิภาพ เช่น การทำงานร่วมกับอุปกรณ์ต่าง ๆ ดังนี้

๔.๕.๑ Vulnerability Management ได้แก่ Rapid๗, Tenable, Qualys

๔.๕.๒ Ticketing Management ได้แก่ Service Now

๔.๕.๓ SIEM ได้แก่ Q-Radar, Splunk

๔.๕.๔ SOAR ที่เสนอในโครงการนี้

๔.๖ สามารถทำรายงานค่าคะแนนประเมินความเสี่ยงแบบเปรียบเทียบเกณฑ์มาตรฐาน Attack Surfaces Management ของอุตสาหกรรมประเภทเดียวกันได้

๔.๗ สามารถระบุปัญหา DNS dangling เพื่อป้องกันไม่ให้ผู้โจมตีทำ Domain take over ได้

๔.๘ สามารถระบุระดับความสำคัญของปัญหาที่พบ (Priority) เพื่อให้สอดคล้องกับนโยบายความปลอดภัยขององค์กร และระบุวิธีการแก้ไขปัญหาเพื่อลดทอนความเสี่ยงที่เกิดขึ้น

๔.๙ สามารถระบุ Certificate และ Domain ที่กำลังจะ Expire ในอีก ๓๐ วันได้

๔.๑๐ สามารถค้นหา Alerts ได้โดยการระบุ MITRE ATT & CK Techniques และ Tactics

๔.๑๑ สามารถค้นหาและติดตามข้อมูลเว็บไซต์ของหน่วยงานอย่างต่อเนื่อง

๔.๑๒ สามารถระบุเว็บไซต์ที่ไม่ปลอดภัยและการกำหนดค่าไม่ถูกต้อง (Misconfigured Website)

๔.๑๓ สามารถระบุเว็บไซต์ที่ให้บริการโดยมีเนื้อหาที่เกี่ยวข้องกับข้อมูลส่วนบุคคล (PII)

๔.๑๔ มี Dashboard แสดงภัยคุกคามที่เกิดขึ้นใหม่ ๆ ที่มีผลกระทบกับ Asset ที่เกี่ยวข้องกับหน่วยงาน

๔๑๕ ระบบที่นำเสนอสามารถแนะนำวิธีการแก้ไขเบื้องต้น (Remediation) สำหรับช่องโหว่หรือความเสี่ยงที่ตรวจพบได้

/๔.๑๖ ผู้เสนอราคา...

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

๔.๑๖ ผู้เสนอราคาต้องมีหนังสือสนับสนุนทางด้านเทคนิคจากผู้ผลิตหรือสาขาของผู้ผลิตในประเทศไทย และรับรองว่าอุปกรณ์ภายในโครงการนี้ อยู่ในสภาพที่ใช้งานได้ดี เป็นรุ่นที่ยังอยู่ในสายการผลิต และเป็นของใหม่ มิได้ถูกติดตั้งใช้งาน ณ ที่ใดมาก่อน

๔.๑๗ ต้องรับประกันระบบที่นำเสนอเป็นเวลาอย่างน้อย ๓ ปี

๕. ระบบรักษาความปลอดภัยสำหรับ Web Application จำนวน ๑ ระบบ โดยมีคุณลักษณะอย่างน้อย ดังนี้

๕.๑ อุปกรณ์รักษาความปลอดภัย Web Application Firewall จำนวน ๑ อุปกรณ์

๕.๑.๑ ผลิตภัณฑ์ที่นำเสนอจะต้องได้รับการจัดอันดับด้าน Web Application Firewall จาก Gartner Magic Quadrant ในกลุ่ม Leader หรือ Challenges ปี ๒๐๒๐ หรือใหม่กว่า

๕.๑.๒ เป็นอุปกรณ์ Hardware Appliance ที่ถูกออกแบบมาเพื่อทำหน้าที่รักษาความปลอดภัย และป้องกันระบบงานด้าน Web Application Firewall โดยเฉพาะ

๕.๑.๓ อุปกรณ์ต้องมีค่าความสามารถประมวลผลข้อมูล (WAF Throughput) เมื่อเปิดใช้ WAF Policy แบบ out-of-the-box จะต้องมีค่า WAF Throughput อย่างน้อย ๕๐๐ Mbps

๕.๑.๔ มี Interface แบบ ๑G Copper จำนวนไม่น้อยกว่า ๘ พอร์ต ที่สามารถทำ Inline Fail Open ได้อัตโนมัติ ในกรณีอุปกรณ์ WAF ไม่สามารถใช้งานได้ หรือเสนออุปกรณ์ต่อพ่วงที่มีความสามารถเทียบเท่าในการทำ Fail Open

๕.๑.๕ มี Interface แบบ ๑G Copper จำนวนไม่น้อยกว่า ๑ พอร์ต เพื่อใช้งานเป็น Out-of-band port management โดยเฉพาะ

๕.๑.๖ มี Hard drive แบบ Dual hot-swap หรือเทียบเท่า ขนาดไม่น้อยกว่า ๙๖๐ GB

๕.๑.๗ สามารถกำหนดให้ทำงานร่วมกับ Network Time Protocol (NTP) Server ได้

๕.๑.๘ สามารถใช้งานตามมาตรฐาน IPv๖ ได้

๕.๑.๙ สามารถติดตั้งและทำงานแบบ In-Line Bridge Transparent (Layer ๒) และ Reverse Proxy Mode (Layer ๓) ได้เป็นอย่างน้อย

๕.๑.๑๐ สามารถส่งข้อมูล Log แบบ Syslog ไปยังระบบ Centralized Log หรือ ระบบ SIEM ได้

๕.๑.๑๑ อุปกรณ์มี Power supply แบบ Dual hot-swap หรือเทียบเท่าเป็นอย่างน้อย

๕.๑.๑๒ สามารถป้องกันการโจมตีไปยัง API (Application Program Interface) ที่อยู่ในรูปแบบ JSON และ XML ได้เป็นอย่างน้อย

๕.๑.๑๓ สามารถเรียนรู้รูปแบบพฤติกรรมการใช้งาน (Learning Profile หรือ Structure) Web Application และ API เพื่อใช้สร้างเป็น Policy หรือ Whitelist หรือ Positive Security ได้

๕.๑.๑๔ สามารถกำหนด Custom Error Page ได้

๕.๑.๑๕ สามารถทำ Blacklist ตาม Geolocation และ Reputation Intelligence profile ได้

๕.๑.๑๖ สามารถกำหนดเงื่อนไข Security Rule โดยใช้ข้อมูล Actual Client IP ใน X-Forwarded-For (XFF) ได้

/๕.๑.๑๗ สามารถป้อง...

๕.๑.๑๗ สามารถป้องกันโดยใช้ Signature-based ที่ออกแบบมาสำหรับป้องกัน Web Application โดยเฉพาะ

๕.๑.๑๘ สามารถตรวจจับและป้องกัน Web Application ตามรูปแบบการถูกโจมตี ได้อย่างน้อย ดังนี้

๕.๑.๑๘.๑ OWASP Top ๑๐

๕.๑.๑๘.๒ Injection

๕.๑.๑๘.๓ Cross-Site Scripting

๕.๑.๑๘.๔ DoS

๕.๑.๑๘.๕ Data leakage

๕.๑.๑๘.๖ Bruteforce

๕.๑.๑๙ สามารถทำ Predefined Policy หรือ Signature สำหรับตรวจสอบและป้องกันภัยคุกคามและการโจมตีที่เป็นรู้จักกันอย่างดี (Well Known) หรือตามหมายเลข CVE ได้

๕.๒ อุปกรณ์บริหารจัดการอุปกรณ์รักษาความปลอดภัยสำหรับ Web Application Firewall จำนวน ๑ ลิขสิทธิ์

๕.๒.๑ เป็นอุปกรณ์ Hardware หรือ Virtual Appliance/Software ที่ออกแบบมาเพื่อทำหน้าที่บริหารจัดการ (Centralized Management หรือ Central Management) อุปกรณ์ Web Application Firewall ที่เสนอโดยเฉพาะ พร้อมสิทธิ์การใช้งานถูกต้องตามกฎหมาย

๕.๒.๒ สามารถบริหารจัดการ Configuration, Backup และ Restore อุปกรณ์ WAAP ได้

๕.๒.๓ สามารถกำหนดให้ทำงานร่วมกับ Network Time Protocol (NTP) Server ได้

๕.๒.๔ สามารถแจ้งเตือนในกรณีที่เกิดเหตุการณ์ผิดปกติกับอุปกรณ์ในระบบ ผ่านทาง อีเมล หรือ Syslog ได้

๕.๒.๕ สามารถบริหารจัดการผ่าน Web-Based หรือ GUI

๕.๒.๖ สามารถสร้าง Role Based Management กำหนดสิทธิ์ให้กับ User มี Role ที่แตกต่างกันได้

๕.๒.๗ สามารถแสดง Security Event หรือ Attack Log ได้ผ่าน GUI

๕.๒.๘ สามารถทำรายงานภัยคุกคามที่เกิดขึ้นได้

๕.๒.๙ สามารถอัปเดตฐานข้อมูลช่องโหว่รูปแบบการโจมตี (Attack Signature) แบบ Schedule หรือ Automatic ได้

๕.๒.๑๐ มีระบบ AI หรือ Machine Learning หรือ Analytic Dashboard สำหรับแสดงการโจมตีที่เกิดขึ้นเพื่อแสดงผลข้อมูลในเชิงวิเคราะห์จากอุปกรณ์ WAF โดยสามารถแสดงข้อมูล เช่น Attack target, Attack type, Country เป็นต้น

๕.๓ ระบบรักษาความปลอดภัยแบบ Cloud Web Application Firewall (Saas) จำนวน ๑ ระบบ

/๕.๓.๑ เป็นผลิตภัณฑ์...

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

๕.๓.๑ เป็นผลิตภัณฑ์ที่ถูกจัดให้อยู่ใน Leader Quadrant หรือ Visionaries ของ Gartner Magic Quadrant Web Application Firewall ปี ๒๐๒๒ หรือใหม่กว่า เป็นระบบ Cloud-WAF ที่ให้บริการในรูปแบบ Cloud Platform และสามารถใช้งานได้กับ Website จำนวน ๑ website

๕.๓.๒ สามารถใช้งานแบบ Data transfer ไม่น้อยกว่า ๒๐ TB ต่อเดือน หรือแบบ ๙๕ percentile cleaned-bandwidth ไม่น้อยกว่า ๒๐ Mbps ต่อเดือน

๕.๓.๓ ต้องมี Data center หรือ Scrubbing Center หรือ Point of Presence ทั่วโลก ไม่น้อยกว่า ๕๐ แห่ง และ อยู่ในประเทศไทยไม่น้อยกว่า ๑ แห่ง

๕.๓.๔ มีระบบ Bot Management โดยสามารถแยกกลุ่มของ Bots จาก User Agent String และ Headless browser หรือสามารถแยกแยะประเภทที่เป็นกลุ่ม Good bots และกลุ่ม Bad bots ได้

๕.๓.๕ มีระบบป้องกัน Web DDoS attacks ที่ทำงานแบบอัตโนมัติ ไม่จำกัดจำนวนครั้ง และสามารถรองรับการโจมตีแบบ DDoS Volumetric Attacks ได้อย่างน้อย ๖Tbps โดยไม่ส่งผลกระทบต่อผู้ใช้งานปกติขณะเปิดระบบป้องกัน และไม่มีการคิดค่าบริการจากปริมาณการรับ-ส่งข้อมูลที่เกิดขึ้นจากการโจมตี

๕.๓.๖ ระบบ Dashboard ต้องสามารถแสดงข้อมูล Traffic, Security และ Performance เช่น ประเทศต้นทางของผู้ใช้งาน และภัยคุกคามที่เกิดขึ้นกับเว็บไซต์ ได้อย่างน้อย ๓๐ วัน ย้อนหลัง

๕.๓.๗ มีระบบหรือเสนอบริการจัดเก็บ Audit Event หรือ Trail หรือ Admin Activity ได้ไม่น้อยกว่า ๗ ปี มีระบบหรือเสนอบริการวิเคราะห์การโจมตีที่เกิดขึ้นโดยอัตโนมัติ (Analytics) ที่แสดงผลข้อมูลในเชิงวิเคราะห์ได้อย่างน้อย ดังต่อไปนี้

๕.๓.๗.๑ แสดงการจัดกลุ่มและบ่งบอกถึงประเภทการโจมตีที่เกิดขึ้น (Correlated incidents) พร้อมระบุระดับความรุนแรงของเหตุการณ์ (Severity)

๕.๓.๗.๒ แสดงรูปแบบการโจมตี และเครื่องมือที่ใช้โจมตี Website (Violation and Attack tool types)

๕.๓.๗.๓ แสดงอัตราการป้องกันต่อการโจมตีที่เกิดขึ้น (Blocked rate)

๕.๓.๗.๔ แสดงแนวโน้มการโจมตีที่เกิดขึ้น (Event and Incident)

๕.๓.๗.๕ แสดงและจัดอันดับ Website ที่ถูกโจมตีสูงสุด (Top attacked websites)

๕.๓.๗.๖ แสดงและเลือกดูข้อมูลในช่วงเวลาที่กำหนด โดยต้องสามารถดูย้อนหลังได้ไม่ต่ำกว่า ๓๐ วัน

๕.๓.๘ มีระบบหรือเสนอบริการฐานข้อมูล IP Reputation สำหรับค้นหา ประวัติ อุตสาหกรรมเป้าหมาย และความเสี่ยงของ IP ที่ต้องสงสัยได้ และสามารถป้องกัน Bad reputation IP ตามระดับความเสี่ยง และประเภทของความเสี่ยงได้ เช่น TOR IP และ Anonymous Proxy IP

๕.๔ ผู้เสนอราคาต้องมีหนังสือสนับสนุนทางด้านเทคนิคจากผู้ผลิตหรือสาขาของผู้ผลิตในประเทศไทย และรับรองว่าอุปกรณ์ภายในโครงการนี้ อยู่ในสภาพที่ใช้งานได้ดี เป็นรุ่นที่ยังอยู่ในสายการผลิต และเป็นของใหม่ มิได้ถูกติดตั้งใช้งาน ณ ที่ใดมาก่อน

๕.๕ ต้องรับประกันระบบที่นำเสนอเป็นเวลาอย่างน้อย ๓ ปี

/๖. ระบบป้องกัน...

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

๖. ระบบป้องกันการรั่วไหลของข้อมูลสารสนเทศผ่านทางระบบเครือข่าย (Network Data Leak Prevention) จำนวน ๑ ระบบ โดยมีคุณลักษณะอย่างน้อย ดังนี้

๖.๑ เป็นระบบการทำงานที่สามารถทำงานร่วมกับอุปกรณ์ Next Generation Firewall หรือ Network Sensors เดิม หรือเทียบเท่า ที่ใช้งานอยู่ได้โดยไม่ต้องเสนออุปกรณ์ หรือปรับเปลี่ยนอุปกรณ์เพิ่มเติม

๖.๒ สามารถทำ DLP (Data Loss Prevention) เพื่อป้องกันข้อมูลรั่วไหลไปยังภายนอก โดยมีความสามารถอย่างน้อย ดังนี้

๖.๒.๑ ใช้ Machine Learning, AI models ในกระบวนการ Detection เพื่อเพิ่มความแม่นยำในการตรวจสอบข้อมูล

๖.๒.๒ มีความสามารถในการทำ Exact Data Matching (EDM) และ Optical Character Recognition (OCR) ในการตรวจจับข้อมูลทั้งในรูปแบบ structure และ unstructured data

๖.๒.๓ มี templates ของมาตรฐานต่าง ๆ เช่น GDPR, CCPA, GLBA, Financial regulations เป็นอย่างน้อย

๖.๒.๔ สามารถปรับแต่ง policy (Policy Tuning) โดยการใช้ Advance Boolean operators

๖.๓ สามารถกำหนดนโยบายหรือกฎระเบียบการป้องกันข้อมูลรั่วไหล เพื่อควบคุมกิจกรรม การรับส่งและการใช้งานข้อมูลผ่านทางระบบเครือข่าย โดยต้องทำงานร่วมกับ Network Security Policy ได้

๖.๔ สามารถตรวจสอบทำ DLP (Data Loss Prevention) เพื่อป้องกันข้อมูลรั่วไหลไปยังภายนอก โดยมีความสามารถอย่างน้อย ดังนี้

๖.๔.๑ สามารถปรับแต่ง policy (Policy Tuning) โดยการใช้ Advance Boolean operators

๖.๔.๒ สามารถตรวจสอบ File โดยสามารถตรวจสอบได้ทั้งการ Upload และ Download และรองรับ File Types ได้อย่างน้อยดังนี้

๖.๔.๒.๑ PDF files (.pdf), Java files (.java), Powershell (.ps๑, .ps๒)

๖.๔.๒.๒ Encrypted files (.๗z, .zip, .gz, .tgz)

๖.๔.๒.๓ MS office file (.docx, .pptx, .xlsx)

๖.๕ สามารถดำเนินการทำ Data classification แบบ Network inline เพื่อจำแนกประเภทของ Data ได้

๖.๖ สามารถแสดงรายงานของเหตุการณ์ที่ละเมิดนโยบาย โดยมีรายละเอียดอย่างน้อย ดังนี้ ผู้ใช้งาน (User), ชื่อเครื่องคอมพิวเตอร์ หรือชื่ออุปกรณ์ (Device) หรือ IP Address หรือ Destination IP หรือ ชื่อเอกสาร (Asset) เป็นอย่างน้อย

๖.๗ การกำหนดนโยบาย (Policy Rule) ต้องสามารถกำหนดการ Action เช่น Alert หรือ Block ได้เป็นอย่างน้อย

๖.๘ สามารถกำหนดนโยบายจากระบบบริหารจัดการส่วนกลางที่นำเสนอได้ (Centralized Management)

๖.๙ มีระบบการจัดการจากศูนย์กลางเป็นแบบ Web-Base Management หรือ Cloud Management

๖.๑๐ ผู้เสนอราคาต้องมีหนังสือสนับสนุนทางด้านเทคนิคจากผู้ผลิตหรือสาขาของผู้ผลิตในประเทศไทย และรับรองว่าอุปกรณ์ภายในโครงการนี้ อยู่ในสภาพที่ใช้งานได้ดี เป็นรุ่นที่ยังอยู่ในสายการผลิต และเป็นของใหม่ มิได้ถูกติดตั้งใช้งาน ณ ที่ใดมาก่อน

๖.๑๑ ต้องรับประกันระบบที่นำเสนอเป็นเวลาอย่างน้อย ๓ ปี

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

ภาคผนวก ข
สถานที่ติดตั้ง
โครงการศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ระยะที่ ๒
สำนักงานปลัดกระทรวงมหาดไทย

---

๑. ส่วนกลาง ได้แก่

๑.๑ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงมหาดไทย

๑.๒ อุปกรณ์ตามโครงการระบบบริการสารสนเทศของกระทรวงมหาดไทยด้วยโครงข่ายเสมือน

๒. จังหวัด ติดตั้งกับอุปกรณ์คอมพิวเตอร์โครงการป้ายประชาสัมพันธ์อัจฉริยะ

๓. เครื่องคอมพิวเตอร์แม่ข่ายหรือเครื่องคอมพิวเตอร์ สำหรับงานประมวลผล หรือเครื่องคอมพิวเตอร์โน้ตบุ๊ก ตามที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงมหาดไทยกำหนด

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

ภาคผนวก ค

การสาธิตและทดสอบการใช้งานจริง (Proof of Concept : POC)

โครงการศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ระยะที่ ๒

สำนักงานปลัดกระทรวงมหาดไทย

ผู้เสนอราคาจะต้องนำอุปกรณ์ที่เกี่ยวข้องมาติดตั้ง ณ สถานที่ ที่สำนักงานปลัดกระทรวงมหาดไทยกำหนด รายละเอียด ดังนี้ การทดสอบคุณสมบัติของอุปกรณ์ตามที่กำหนดในรายละเอียดคุณลักษณะเฉพาะ

เกณฑ์การตัดสิน	ผ่าน	ไม่ผ่าน	หมายเหตุ
๑. ระบบวิเคราะห์ระบบเฝ้าระวังและป้องกันภัยคุกคามไซเบอร์อัจฉริยะ			
๑.๑ ระบบมีการส่งข้อมูลทั้งหมดมาจัดเก็บบน Platforms โดยไม่จำเป็นต้องเป็น Alert (The solution must send all EDR data to the PLATFORM even if there are no alerts occurring)			
๑.๒ ระบบที่นำเสนอต้องสามารถแนะนำวิธีการแก้ไขปัญหาเบื้องต้นได้ (The solution must provide remediation suggestion)			
๑.๓ ระบบสามารถแยกหรือตัดการเชื่อมต่อเครื่องคอมพิวเตอร์ลูกข่ายออกจากระบบเครือข่ายได้หลาย ๆ เครื่องพร้อม ๆ กัน (Isolate multiple endpoints at the same time)			
๑.๔ ระบบสามารถตรวจสอบช่องโหว่ที่มีอยู่บนเครื่องคอมพิวเตอร์ลูกข่ายได้ทั้ง Windows และ Linux (The solution must have Vulnerability Assessment where can detect the vulnerability on the host both Windows and Linux)			
๑.๕ ระบบต้องสามารถแสดงข้อมูลการติดตั้งแอปพลิเคชันทั้งหมดที่ใช้งานอยู่บนเครื่องคอมพิวเตอร์ลูกข่ายได้ โดยไม่ต้องใช้ Agent อื่น ๆ เพิ่มเติม (The solution must provide inventory of all installed applications on all major platforms: Windows and Linux without having to install additional agents.)			
๑.๖ สามารถทำการตรวจสอบพฤติกรรมการโจมตีประเภท suspicious DNS traffic หรือ DNS tunneling ที่เครื่องแม่ข่ายหรือเครื่องลูกข่ายได้			
๑.๗ สามารถสร้าง Automation Rule เพื่อกำหนดให้ระบบตอบสนองอัตโนมัติเมื่อมี Alert ที่ตรงเงื่อนไขเกิดขึ้น โดยสามารถเลือกจากเงื่อนไข (Attribute) ได้ไม่น้อยกว่า ๒ เงื่อนไขพร้อมกันได้ หรือเสนอระบบอื่น ๆ เพิ่มเติมเพื่อให้สามารถทำงานได้ตามข้อกำหนด			
๑.๗ สามารถทำการค้นหาและทำลายไฟล์ต้องสงสัยบน Windows OS จากค่า hash หรือ File Path ได้			

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

เกณฑ์การตัดสิน	ผ่าน	ไม่ผ่าน	หมายเหตุ
๒. ระบบตอบสนองและแก้ไขปัญหาแบบอัตโนมัติ (SOAR)			
๒.๑ มีระบบช่วยให้ทีมผู้ดูแลระบบต่าง ๆ สามารถทำงานร่วมกันได้ ลักษณะ Virtual War Room ที่สามารถสื่อสารข้อความ, เก็บข้อมูลเกี่ยวกับ Incident, Log การทำงานของ WorkFlow/Playbook ต่าง ๆ หรือนำเสนอระบบอื่น ๆ เพิ่มเติมเพื่อรองรับความต้องการดังกล่าว โดยระบบที่นำเสนอเพิ่มเติม จะต้องสามารถเชื่อมโยงข้อมูลการสนทนาที่เกี่ยวข้องกับ Incident นั้น ๆ จากระบบ SOAR ไปยังระบบ Collaborate and Learn ได้ทันที			
๒.๒ สามารถสร้าง Work Plan หรือ WorkFlow หรือ Playbook และสามารถทำ Sub Playbook ได้ โดยมีความสามารถอย่างน้อยดังนี้ ๒.๒.๑ Manual action and Task ๒.๒.๒ การสร้างขั้นตอนในการตัดสินใจและอนุมัติ ๒.๒.๓ การเรียกใช้งาน Playbook ที่ซ้อนกันได้ ๒.๒.๔ การกำหนดเงื่อนไขและลูป ๒.๒.๕ การหยุดหรือดำเนินการต่อเมื่อเกิดข้อผิดพลาดใน Playbook ๒.๒.๖ สามารถทำการเก็บข้อมูลในรูปแบบ Snapshot เพื่อทำการย้อนกลับ (Roll back) ในกรณีที่ Playbook เกิดปัญหาได้ หรือการทำ Playbook Version History ๒.๒.๗ สามารถทำการจำลองขั้นตอนของ Playbook เพื่อทดสอบการทำงานได้			
๓. ระบบตรวจสอบช่องโหว่ของระบบจากมุมมองของบุคคลภายนอก (Attack Surfaces Management)			
๓.๑ สามารถระบุการให้บริการของทรัพย์สินต่าง ๆ เช่น Services, Port ที่มีการใช้งาน และระบุช่องโหว่ในรูปแบบ CVE ของ Service นั้น ๆ ได้			
๓.๒ สามารถ Integrate workflow เข้ากับระบบการบริหารจัดการด้าน Cyber Security workflow ได้แก่ SOAR ได้			
๔. ระบบป้องกันเว็บแอปพลิเคชันด้วยเครื่องมือป้องกันการโจมตีเว็บ Web Application Firewall และ API Protection			
๔.๑ ระบบต้องสามารถป้องการโจมตีเว็บแอปพลิเคชัน ตามมาตรฐาน OWASP Top ๑๐ ปีล่าสุด			
๔.๒ ระบบต้องสามารถส่งข้อมูล Log แบบ Syslog ไปยังระบบ Centralized Log หรือ ระบบ SIEM ได้			

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

เกณฑ์การตัดสิน	ผ่าน	ไม่ผ่าน	หมายเหตุ
๔.๓ ระบบต้องสามารถทำ Dynamic Profiling หรือ Auto Policy Generation เพื่อเรียนรู้ Parameter, Method, Cookie และ URL ของ Website ได้อัตโนมัติ และสามารถทำเป็น Profile Policy เพื่อป้องกันการใช้งานนอกเหนือพฤติกรรมที่เรียนรู้ได้ และมีระบบ Automatic Profile Update ที่สามารถตรวจจับการเปลี่ยนแปลงการใช้งาน Application ได้ เพื่อปรับการเรียนรู้ Profile โดยอัตโนมัติ			
๔.๔ ระบบต้องมี Attack Analytics Dashboard หรือบริการวิเคราะห์การโจมตีที่เกิดขึ้นเพื่อแสดงผลข้อมูลในเชิงวิเคราะห์จากอุปกรณ์ WAF ที่นำเสนอได้แบบอัตโนมัติ			
๕. ระบบป้องกันการรั่วไหลของข้อมูลสารสนเทศผ่านทางระบบเครือข่าย (Network Data Leak Prevention)			
๕.๑ สามารถกำหนดนโยบายหรือกฎระเบียบการป้องกันข้อมูลรั่วไหลเพื่อควบคุมกิจกรรมการรับส่งและการใช้งานข้อมูลผ่านทางระบบเครือข่ายโดยต้องทำงานร่วมกับ Network Security Policy ได้			
๕.๒ มีความสามารถในการทำ Exact Data Matching (EDM) โดยสามารถแจ้งเตือนหรือ Block เมื่อตรวจจับข้อมูลได้ หรือสามารถกำหนด Pattern แบบ Regex เพื่อหาคำเฉพาะ (Specific Word) ได้			
๕.๓ มีความสามารถในการทำ Optical Character Recognition (OCR) ได้			
๕.๔ สามารถ File blocking ได้ทั้ง upload และ download พร้อมทั้งรองรับ file format ได้อย่างน้อย ดังต่อไปนี้ .doc .docx .ppt .pptx .xls .xlsx .pdf			
๕.๕ สามารถสร้างรายงานการเฝ้าระวังและป้องกันข้อมูลรั่วไหลในรูปแบบ PDF หรือ CSV ได้			

หมายเหตุ :

๑. สถานที่ทดสอบ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงมหาดไทย ห้องประชุมวิสุทธิกษัตริย์ ชั้น ๓

๒. ติดต่อเพื่อขอทราบข้อมูลเพิ่มเติมได้ที่

๒.๑ ทางไปรษณีย์ ส่งถึง กองคลัง สำนักงานปลัดกระทรวงมหาดไทย ถนนอัษฎางค์ แขวงวัดราชบพิธ เขตพระนคร กรุงเทพฯ ๑๐๒๐๐

๒.๒ ทางโทรศัพท์หมายเลข ๐๒ ๒๘๒ ๖๕๖๐ ต่อ ๕๐๖๕๗ หรือ ๕๐๓๖๘ กองคลัง สำนักงานปลัดกระทรวงมหาดไทย

๒.๓ ทางจดหมายอิเล็กทรอนิกส์ (E-Mail) ส่งถึง moio๒๐๓.๑@moi.go.th

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

หลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอ

โครงการศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ระยะที่ ๒

สำนักงานปลัดกระทรวงมหาดไทย ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

คณะกรรมการกำหนดหลักเกณฑ์ที่ใช้ในการพิจารณาคัดเลือกข้อเสนอได้พิจารณา โครงการศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ระยะที่ ๒ สำนักงานปลัดกระทรวงมหาดไทย ประจำปีงบประมาณ พ.ศ. ๒๕๖๙ แล้วเห็นว่าการกำหนดคุณลักษณะเฉพาะ ของพัสดุเป็นมาตรฐาน และมีคุณภาพดีเพียงพอตามความต้องการใช้งาน และเป็นประโยชน์ต่อหน่วยงานของรัฐแล้ว จึงเห็นควรใช้หลักเกณฑ์ตามแนวทางปฏิบัติระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริการพัสดุภาครัฐ พ.ศ. ๒๕๖๐ ข้อ ๘๓(๑) โดยใช้เกณฑ์ราคาในการคัดเลือกผู้ที่เสนอราคาต่ำสุดเป็นผู้ชนะการซื้อหรือจ้าง หรือเป็นผู้ได้รับการคัดเลือก

คณะกรรมการกำหนดหลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอ จึงได้ลงลายมือชื่อไว้เป็นหลักฐาน

ลงชื่อ..... ประธานกรรมการ

(นายเสรี กัณฑ์โรจน์)

ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.

ลงชื่อ ..... กรรมการ

(นายณัฐกิตติ์ ตาวงษ์สา)

ผู้อำนวยการกลุ่มงานโครงสร้างพื้นฐาน

ด้านสารสนเทศและการสื่อสาร

ลงชื่อ..... กรรมการ

(นายบุญยง เรืองพงษ์)

นายช่างไฟฟ้าอาวุโส

ลงชื่อ..... กรรมการ

(นายสมนึก โลสันเทียะ)

นายช่างไฟฟ้าชำนาญงาน

ลงชื่อ ..... กรรมการ

(นายธนวัฒน์ สังกระธาตุ)

นายช่างไฟฟ้าชำนาญงาน