(ร่าง)

ขอบเขตของงาน (Terms of Reference : TOR)
โครงการพัฒนาโครงสร้างพื้นฐานศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ กระทรวงการคลัง

๑. ความเป็นมา

ในยุคที่เทคโนโลยีดิจิทัลมีบทบาทสำคัญต่อระบบเศรษฐกิจและการเงินการคลัง ภัยคุกคามทางไซเบอร์ได้ทวีความรุนแรงและซับซ้อนมากขึ้น โดยเฉพาะการโจมตีที่มุ่งเป้าไปยังสถาบันการเงินและหน่วยงานด้านการคลังของรัฐ ซึ่งหากถูกโจมตีสำเร็จจะส่งผลกระทบในวงกว้างต่อความมั่นคงทางการเงินของประเทศ โครงการนี้สอดคล้องกับนโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม (พ.ศ. ๒๕๖๑ – ๒๕๘๐) ในยุทธศาสตร์ที่ ๖ ด้านการสร้างความเชื่อมั่นในการใช้ เทคโนโลยีดิจิทัล และแผนแม่บทการส่งเสริมเศรษฐกิจดิจิทัล (พ.ศ. ๒๕๖๖ – ๒๕๗๐) ในประเด็นการพัฒนาโครงสร้างพื้นฐานด้านความมั่นคงปลอดภัยทางดิจิทัล

ปัจจุบันพบประเด็นปัญหาสำคัญ ดังนี้

๑. การแลกเปลี่ยนข้อมูลภัยคุกคามระหว่างหน่วยงานยังขาดความเป็นเอกภาพและไม่ทันต่อสถานการณ์
๒. ขาดกลไกกลางในการประสานงานและรับมือภัยคุกคามที่เข้าใจบริบทเฉพาะด้านการเงินการคลัง
๓. การตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยยังเป็นแบบแยกส่วนทำให้ขาดประสิทธิภาพในการรับมือภัยคุกคาม

หากไม่ดำเนินโครงการจะก่อให้เกิดผลกระทบ ดังนี้

๑. ความเสี่ยงต่อการถูกโจมตีทางไซเบอร์เพิ่มสูงขึ้นเนื่องจากขาดการเตรียมพร้อมและประสานงานที่มีประสิทธิภาพ
๒. การรับมือกับภัยคุกคามล่าช้า ส่งผลกระทบต่อความต่อเนื่องในการให้บริการทางการเงินการคลัง
๓. สูญเสียโอกาสในการป้องกันและลดความเสียหายจากภัยคุกคามที่อาจเกิดขึ้น

ทั้งนี้ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง มีความพร้อมในการดำเนินโครงการและรับผิดชอบโดยตรงพร้อมปฏิบัติตามระเบียบคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติว่าด้วยการบริหารกองทุนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ. ๒๕๖๑ อย่างเคร่งครัด

๒. วัตถุประสงค์

๒.๑. เพื่อสร้างความยั่งยืนและผลกระทบในระยะยาวให้กับระบบความปลอดภัยไซเบอร์ของกระทรวงการคลัง ตามแนวทางพัฒนาดิจิทัลที่มุ่งเน้นนวัตกรรมและการพัฒนาประสิทธิภาพอย่างแท้จริง

๒.๒. พัฒนาแพลตฟอร์มบริการและเทคโนโลยีสำหรับปฏิบัติการและสนับสนุนงานศูนย์ MOF-CSIRT แบบครบวงจร เพื่อเพิ่มขีดความสามารถในการเฝ้าระวังและรับมือภัยคุกคามทางไซเบอร์

๒.๓. เพื่อจัดตั้งและพัฒนาหน่วยปฏิบัติการ MOF-CSIRT ที่มีความเชี่ยวชาญในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ ครอบคลุมกระบวนการสืบสวน ตรวจสอบ ตอบสนอง และสนับสนุนการกู้คืนจากเหตุการณ์ รวมทั้งการบริหารจัดการช่องโหว่และความเสี่ยงของระบบสารสนเทศ

๒.๔. เพื่อให้บริการจากศูนย์ MOF-CSIRT แก่หน่วยงานในสังกัดและหน่วยงานในกำกับของกระทรวงการคลัง โดยเน้นการแลกเปลี่ยนข้อมูลข่าวกรองภัยคุกคาม การจัดการเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ การตรวจประเมินช่องโหว่และความเสี่ยง รวมทั้งการถ่ายทอดองค์ความรู้และฝึกอบรมเพื่อยกระดับศักยภาพด้านความมั่นคงปลอดภัยไซเบอร์ในภาพรวม

๓. เป้าหมาย

๓.๑. ยกระดับความมั่นคงปลอดภัยทางไซเบอร์ของระบบการเงินการคลังของประเทศ

๓.๒. ลดความเสี่ยงและความเสียหายจากภัยคุกคามทางไซเบอร์ผ่านการแลกเปลี่ยนข้อมูลและการรับมืออย่างทันท่วงที

๓.๓. เพิ่มขีดความสามารถในการปกป้องระบบสำคัญทางการเงินการคลังของประเทศ

๓.๔. สร้างความเชื่อมั่นต่อระบบการเงินการคลังดิจิทัลของประเทศ

๔. คุณสมบัติผู้ยื่นข้อเสนอ

๔.๑. มีความสามารถตามกฎหมาย

๔.๒. ไม่เป็นบุคคลล้มละลาย

๔.๓. ไม่อยู่ระหว่างเลิกกิจการ

๔.๔. ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

๔.๕. ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

๔.๖. มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

๔.๗. เป็นนิติบุคคล ผู้มีอาชีพขายพัสดุที่ประกวดราคาซื้อด้วยวิธีการทางอิเล็กทรอนิกส์

๔.๘. ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่สำนักงานปลัดกระทรวงการคลัง ณ วันยื่นข้อเสนอ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในครั้งนี้

๔.๙. ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์ความคุ้มกันเช่นว่านั้น

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

๔.๑๑. ผู้ยื่นข้อเสนอต้องมีผลงานในการขายและติดตั้ง ระบบเครื่องคอมพิวเตอร์ หรือ ระบบเครือข่าย หรือ ระบบรักษาความมั่นคงปลอดภัย หรือพัฒนาระบบงานด้านความมั่นคงปลอดภัย โดยมีผลงานในการขายและติดตั้งสำเร็จมาแล้วให้กับหน่วยงานของรัฐ ภายในระยะเวลา ๕ ปี นับจากวันแล้วเสร็จจนถึงวันยื่นข้อเสนอ ซึ่งมีมูลค่าไม่น้อยกว่า ๒๕,๐๐๐,๐๐๐.- บาท (ยี่สิบห้าล้านบาทถ้วน) ต่อหนึ่งสัญญา ทั้งนี้ ให้แนบสำเนาสัญญาและสำเนาหนังสือรับรองผลงาน มาพร้อมการยื่นข้อเสนอทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์

๔.๑๒. ผู้ยื่นข้อเสนอซึ่งเป็นผู้ประกอบการ SMEs แสดงสำเนาใบขึ้นทะเบียนผู้ประกอบการวิสาหกิจขนาดกลางและขนาดย่อม (SMEs) เป็น SME-GP (ถ้ามี) มาพร้อมการยื่นข้อเสนอทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์

๔.๑๓. ผู้ยื่นข้อเสนอที่เป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยซึ่งได้จดทะเบียนเกินกว่า ๑ ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิที่ปรากฏในงบแสดงฐานะการเงิน

ที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก ๑ ปีสุดท้ายก่อนวันยื่นข้อเสนอ โดยแสดงสำเนาเอกสารหรือหลักฐานมาพร้อมการยื่นข้อเสนอทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์

๔.๑๔. ผู้ยื่นข้อเสนอที่เป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า จะต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอไม่ต่ำกว่า ๘ ล้านบาท โดยแสดงสำเนาเอกสารหรือหลักฐานมาพร้อมการยื่นข้อเสนอทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์

๔.๑๕. กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียนหรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง (สินเชื่อที่ธนาคารภายในประเทศหรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้าประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรองหรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอนับถึงวันยื่นข้อเสนอไม่เกิน ๙๐ วัน) โดยแสดงสำเนาแบบหนังสือรับรองวงเงินสินเชื่อ (ตามแบบที่กรมบัญชีกลางกำหนด) มาพร้อมการยื่นข้อเสนอทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์

๔.๑๖. กรณีที่ผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐ หรือ เป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการตามพระราชบัญญัติล้มละลาย (ฉบับที่ ๑๐) พ.ศ. ๒๕๖๑ ไม่ต้องยื่นเอกสารข้อเสนอตามข้อ ๔.๑๓ – ๔.๑๕

๕. แบบรูปรายการหรือคุณลักษณะเฉพาะ

สำนักงานปลัดกระทรวงการคลังมีความต้องการจัดซื้อจัดจ้าง “โครงการพัฒนาโครงสร้างพื้นฐานศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์กระทรวงการคลัง” เพื่อพัฒนาเทคโนโลยีสำหรับปฏิบัติการและสนับสนุนงานศูนย์ MOF-CSIRT เพื่อเพิ่มขีดความสามารถในการเฝ้าระวังและรับมือภัยคุกคามทางไซเบอร์ให้แก่หน่วยงานในสังกัดกระทรวงการคลัง โดยต้องมีคุณลักษณะเฉพาะอย่างน้อยตามเอกสารแนบ ๑ (แบบรูปรายการหรือคุณลักษณะเฉพาะ) ประกอบด้วยรายการหลักดังต่อไปนี้

๕.๑. แพลตฟอร์มข่าวกรองภัยคุกคามไซเบอร์ (Cyber Threat Intelligence Platform) จำนวน ๑ ระบบ

๕.๒. แพลตฟอร์มตรวจประเมินช่องโหว่และความเสี่ยงระบบเทคโนโลยีสารสนเทศส่วนกลาง (Continuous Security Validation Platform) จำนวน ๑ ระบบ

๕.๓. แพลตฟอร์มเฝ้าระวังและตอบสนองต่อภัยคุกคามไซเบอร์แบบบูรณาการ (SecOps Platform) จำนวน ๑ ระบบ

๕.๔. แพลตฟอร์มตอบสนองต่อภัยคุกคามทางไซเบอร์ และการสืบสวนสอบสวนทางนิติวิทยาศาสตร์ดิจิทัล (Digital Forensics an d Incident Response Platform : DFIR) จำนวน ๑ ระบบ

๕.๕. บริการเพื่อสนับสนุนภารกิจ MOF-CSIRT ในระยะแรก (๑ ปี) จำนวน ๑ งาน

๕.๖. การพัฒนาศักยภาพบุคลากรและเจ้าหน้าที่ของ MOF-CSIRT เพื่อยกระดับองค์ความรู้และทักษะความเชี่ยวชาญสำหรับการปฏิบัติภารกิจในระยะยาวในรูปแบบการฝึกอบรมเชิงปฏิบัติการ (On the Job Training) จำนวน ๑ งาน

ผู้ชนะการประกวดราคาต้องส่งมอบระบบและดำเนินการติดตั้งทดสอบระบบตามคุณลักษณะที่กำหนดรวมทั้งต้องดำเนินอื่นๆ ตามที่กำหนดในเอกสารแนบ ๓-๔

.....ประธาน.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการและเลขานุการ

๖. ระยะเวลาดำเนินการ

ระยะเวลาดำเนินการ ๓๖๕ วัน นับถัดจากวันลงนามในสัญญา

๗. ระยะเวลาส่งมอบงาน

ผู้ชนะการประกวดราคาจะต้องส่งมอบงาน ดังต่อไปนี้

งวดที่ ๑ ภายใน ๖๐ วัน นับถัดจากวันลงนามในสัญญา

๑. รายงานสำรวจและออกแบบโครงการพัฒนาโครงสร้างพื้นฐานศูนย์ประสานการรักษาความปลอดภัยไซเบอร์กระทรวงการคลัง

๒. รายงานผลการติดตั้งและทดสอบการใช้งานแพลตฟอร์มข่าวกรองภัยคุกคามไซเบอร์ (Cyber Threat Intelligence Platform)

๓. รายงานผลการติดตั้งและทดสอบการใช้งานแพลตฟอร์มตรวจประเมินช่องโหว่และความเสี่ยงระบบเทคโนโลยีสารสนเทศส่วนกลาง (Continuous Security Validation Platform)

๔. รายงานผลการติดตั้งและทดสอบการใช้งานแพลตฟอร์มเฝ้าระวังและตอบสนองต่อภัยคุกคามไซเบอร์แบบบูรณาการ (SecOps Platform)

๕. รายงานผลการติดตั้งและทดสอบการใช้งานแพลตฟอร์มตอบสนองต่อภัยคุกคามทางไซเบอร์และการสืบสวนสอบสวนทางนิติวิทยาศาสตร์ดิจิทัล (Digital Forensics and Incident Response Platform : DFIR)

๖. เอกสารจำนวน ๒ ชุด และในรูปแบบอิเล็กทรอนิกส์บันทึกลงใน Thumb Drive หรือ Portable SSD จำนวน ๕ ชุด

งวดที่ ๒ ภายใน ๑๕๐ วัน นับถัดจากวันลงนามในสัญญา

๑. รายงานจัดตั้งหน่วยปฏิบัติการ เฝ้าระวัง และตอบสนองต่อภัยคุกคามไซเบอร์และผลการดำเนินงานของหน่วยงาน

๒. รายงานดำเนินงานพัฒนาศักยภาพบุคลากรและเจ้าหน้าที่ของ MOF-CSIRT ในรูปแบบการฝึกอบรมเชิงปฏิบัติการ (On the Job Training) ตามหลักสูตรที่กำหนด

๓. รายงานการให้บริการของศูนย์ MOF-CSIRT ที่ให้การสนับสนุนและช่วยเหลือหน่วยงานในสังกัด

๔. เอกสารจำนวน ๒ ชุด และในรูปแบบอิเล็กทรอนิกส์ซึ่งบันทึกลงใน Thumb Drive หรือ Portable SSD จำนวน ๕ ชุด

งวดสุดท้าย ภายใน ๓๖๕ วัน นับถัดจากวันลงนามในสัญญา

๑. รายงานการจัดกิจกรรมนำเสนอและฝึกอบรมระบบ ประกอบด้วย

๑.๑. รายงานผลการจัดกิจกรรมนำเสนอโครงการแก่หน่วยงานในสังกัดกระทรวงการคลัง

๑.๒. รายงานการจัดอบรมบุคลากรผู้ดูแลระบบ

๑.๓. รายงานสรุปผลการดำเนินงานของโครงการ

๒. รายงานฉบับสมบูรณ์

๓. เอกสารจำนวน ๒ ชุด และในรูปแบบอิเล็กทรอนิกส์ซึ่งบันทึกลงใน Thumb Drive หรือ Portable SSD จำนวน ๕ ชุด

.....ประธาน.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการและเลขานุการ

๘. เงื่อนไขการชำระเงิน

งวดที่ ๑ ชำระเงินในอัตราร้อยละ ๔๐ ของจำนวนเงินตามสัญญา เมื่อคณะกรรมการตรวจรับพัสดุได้ตรวจรับการส่งมอบงานงวดที่ ๑ เรียบร้อยแล้ว

งวดที่ ๒ ชำระเงินในอัตราร้อยละ ๔๐ ของจำนวนเงินตามสัญญา เมื่อคณะกรรมการตรวจรับพัสดุได้ตรวจรับการส่งมอบงานงวดที่ ๒ เรียบร้อยแล้ว

งวดสุดท้าย ชำระเงินในอัตราร้อยละ ๒๐ ของจำนวนเงินตามสัญญา เมื่อคณะกรรมการตรวจรับพัสดุได้ตรวจรับการส่งมอบงานงวดสุดท้าย เรียบร้อยแล้ว

สำนักงานปลัดกระทรวงการคลังขอสงวนสิทธิการจ่ายเงินแก่ผู้ชนะการประกวดราคาเมื่อได้รับเงินทุนอุดหนุนจากกองทุนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม เรียบร้อยแล้ว

๙. อัตราค่าปรับ

ผู้ชนะการประกวดราคาหรือผู้ขายต้องดำเนินการตามขอบเขตของงานที่กำหนดให้มีความถูกต้องครบถ้วน และหากไม่สามารถดำเนินการได้ครบถ้วนหรือถูกต้อง ผู้ชนะการประกวดราคาหรือผู้ขายยินยอมให้สำนักงานปลัดกระทรวงการคลังปรับเป็นรายวันในอัตราร้อยละ ๐.๒๐ (ศูนย์จุดสองศูนย์) ของราคาสิ่งของที่ยังไม่ได้ส่งมอบ จนกว่าจะดำเนินการแล้วเสร็จ หรือสำนักงานปลัดกระทรวงการคลังใช้สิทธิบอกเลิกสัญญา

๑๐.การรับประกันความชำรุดบกพร่อง

ผู้ชนะการประกวดราคาหรือผู้ขายต้องรับประกันความชำรุดบกพร่องของอุปกรณ์และระบบทั้งหมดที่ส่งมอบในโครงการพัฒนาโครงสร้างพื้นฐานศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์กระทรวงการคลัง เป็นระยะเวลา ๑ ปี นับถัดจากวันที่คณะกรรมการตรวจรับพัสดุได้ตรวจรับการส่งมอบพัสดุงวดสุดท้ายเรียบร้อยแล้ว โดยมีรายละเอียดตามขอบเขตของงานที่กำหนด

๑๑.วงเงินในการจัดหา

วงเงินในการจัดหาเป็นเงินทั้งสิ้น ๕๔,๖๘๙,๑๐๐.- บาท (ห้าสิบสี่ล้านหกแสนแปดหมื่นเก้าพันหนึ่งร้อยบาทถ้วน) ซึ่งเป็นวงเงินที่รวมภาษีมูลค่าเพิ่ม และค่าใช้จ่ายอื่นใดทั้งปวงไว้ด้วยแล้ว โดยเบิกจ่ายจากเงินกองทุนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม

๑๒.หลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอ

๑๒.๑. ในการพิจารณาผลการยื่นข้อเสนอประกวดราคาอิเล็กทรอนิกส์ (Electronic Bidding : e - Bidding) ครั้งนี้ ใช้หลักเกณฑ์การประเมินค่าประสิทธิภาพต่อราคา (Price Performance) และจะพิจารณาจากคะแนนรวม

๑๒.๒. ในการพิจารณาผู้ชนะการยื่นข้อเสนอ สำนักงานฯ จะใช้หลักเกณฑ์การประเมินค่าประสิทธิภาพต่อราคา (Price Performance) โดยพิจารณาให้คะแนนตามปัจจัยหลักและน้ำหนักร้อยละที่กำหนด โดยกำหนดให้น้ำหนักรวมทั้งหมดเท่ากับร้อยละ ๑๐๐ คะแนน รายละเอียดตาม เอกสารแนบ ๒

๑๒.๓. ในการพิจารณาสำนักงานฯ มีสิทธิให้ผู้ยื่นข้อเสนอชี้แจงข้อเท็จจริง สภาพ ฐานะ หรือข้อเท็จจริงอื่นใดที่เกี่ยวข้องกับผู้ยื่นข้อเสนอได้ โดยสำนักงานฯ มีสิทธิที่จะไม่รับราคาหรือไม่ทำสัญญาหากหลักฐานดังกล่าวไม่มีความเหมาะสมหรือไม่ถูกต้อง การให้คะแนนของคณะกรรมการให้เป็นสิทธิของคณะกรรมการโดยเด็ดขาด ผู้ยื่นข้อเสนอจะโต้แย้ง คัดค้านหรือเรียกร้องค่าเสียหายใด ๆ มิได้ สำนักงานฯ ทรงไว้ซึ่งสิทธิที่จะไม่รับราคาต่ำสุดหรือราคาหนึ่งราคาใดหรือราคาที่เสนอทั้งหมดได้

โดยไม่พิจารณาจัดจ้างเลยก็ได้สุดแต่จะพิจารณา ทั้งนี้เพื่อประโยชน์ของทางราชการเป็นสำคัญและให้ถือว่าการตัดสินของคณะกรรมการเป็นเด็ดขาด ผู้ยื่นข้อเสนอจะเรียกร้องค่าเสียหายใด ๆ มิได้ รวมทั้งสำนักงานฯ จะพิจารณายกเลิกการจัดซื้อจัดจ้างและลงโทษผู้ยื่นข้อเสนอเป็นผู้ทิ้งงาน ไม่ว่าจะเป็นผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกหรือไม่ก็ตาม หากมีเหตุที่เชื่อได้ว่าการเสนอราคากระทำการโดยไม่สุจริต เช่น การเสนอเอกสารอันเป็นเท็จ หรือใช้ชื่อนิติบุคคลอื่นมาเสนอราคาแทน เป็นต้น

๑๓. ข้อตกลงในการเก็บรักษาความลับข้อมูลหรือเอกสาร

๑๓.๑. เอกสารทั้งหมดที่จัดทำขึ้น ถือเป็นลิขสิทธิ์ของสำนักงานปลัดกระทรวงการคลัง ผู้ขายหรือผู้รับจ้างจะต้องไม่เผยแพร่เอกสาร และ/หรือข้อมูลใด ๆ ที่จัดทำขึ้นทั้งหมด โดยไม่ได้รับความเห็นชอบอย่างเป็นลายลักษณ์อักษรจากสำนักงานปลัดกระทรวงการคลัง รวมทั้งจะต้องไม่แสวงหา หรือยินยอมให้บุคคลอื่นแสวงหาประโยชน์ใด ๆ จากข้อมูลและ/หรือ เอกสารดังกล่าวทั้งในทางพาณิชย์ หรือในกรณีอื่นอันอาจก่อให้เกิดความเสียหายแก่สำนักงานปลัดกระทรวงการคลังด้วยประการใดทั้งสิ้น

๑๓.๒. ข้อตกลงนี้ให้ถือเป็นส่วนหนึ่งของสัญญา อันเป็นเงื่อนไขที่สำนักงานปลัดกระทรวงการคลัง บอกเลิกสัญญา เรียกค่าเสียหายหรือปรับสินไหม รวมทั้งการดำเนินคดีทั้งในทางแพ่งและอาญาทุกประเภท

๑๓.๓. ข้อมูลต่าง ๆ ที่ผู้ขายหรือผู้รับจ้างได้รับทราบจากสำนักงานปลัดกระทรวงการคลังให้ถือเป็นความลับและลิขสิทธิ์ในเอกสารทุกฉบับและผลงานทุกชิ้น ซึ่งผู้ขายหรือผู้รับจ้างได้จัดทำขึ้น ให้ตกเป็นกรรมสิทธิ์ของสำนักงานปลัดกระทรวงการคลัง ผู้ขายหรือผู้รับจ้างจะนำไปเผยแพร่มิได้ โดยจะต้องปฏิบัติต่อข้อมูลดังกล่าวในชั้นข้อมูลลับของทางสำนักงานปลัดกระทรวงการคลัง เว้นแต่นำไปใช้เพื่อการศึกษาหรือขอผลงานทางวิชาการ (กรณีเป็นสถาบันการศึกษา)

๑๓.๔. ในการเก็บรักษาความลับของสำนักงานปลัดกระทรวงการคลัง ผู้ขายหรือผู้รับจ้างต้องระมัดระวังในการดูแลรักษาและปกป้องมิให้บุคคลอื่นที่ไม่เกี่ยวข้องกับการปฏิบัติงานตามสัญญาซื้อหรือจ้างได้ล่วงรู้ถึงข้อมูล หรือนำข้อมูลไปใช้หาประโยชน์ในการใด ๆ รวมถึงการเผยแพร่ต่อสาธารณะโดยมิได้รับอนุญาตจากสำนักงานปลัดกระทรวงการคลัง ยกเว้นในกรณีดังต่อไปนี้ ให้แจ้งสำนักงานปลัดกระทรวงการคลังทุกครั้ง กล่าวคือ

(๑) เป็นการเปิดเผยเพื่อประโยชน์ หรือความจำเป็นในการทำหน้าที่ตามสัญญาซื้อหรือจ้าง

(๒) เป็นกรณีจำเป็นต้องเปิดเผยตามกฎหมายหรือคำสั่งศาล

๑๓.๕. ผู้ขายหรือผู้รับจ้างต้องส่งมอบข้อมูล พร้อมทั้งข้อมูลที่ได้ทำซ้ำซึ่งสำเนาในทุกรูปแบบที่อาจสื่อความหมาย ถึงข้อมูลได้คืนแก่สำนักงานปลัดกระทรวงการคลังเมื่อเสร็จสิ้นงานซื้อหรือจ้าง หรือทำลายสำเนาข้อมูลเหล่านั้นเพื่อไม่ให้สามารถสื่อข้อความต่อไปได้อีก

๑๓.๖. ผู้ขายหรือผู้รับจ้างต้องรับผิดชอบในการดูแลรักษาความมั่นคงปลอดภัยข้อมูลให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และกฎหมายที่เกี่ยวข้องอย่างเคร่งครัด

๑๔. หน่วยงานผู้รับผิดชอบดำเนินการ

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง

๑๕. ข้อสงวนสิทธิในการยื่นข้อเสนอและอื่น ๆ

หากข้อความใดในขอบเขตของงานมีความขัดแย้งกัน ให้ยึดถือตามข้อกำหนดที่เป็นประโยชน์กับสำนักงานปลัดกระทรวงการคลัง

ท่านสามารถเสนอแนะวิจารณ์ หรือแสดงความคิดเห็นโดยเปิดเผย

๑. ทางไปรษณีย์ ส่ง คณะกรรมการจัดทำร่างขอบเขตของงานหรือรายละเอียดคุณลักษณะเฉพาะของพัสดุที่จะจ้างและกำหนดราคากลาง โครงการพัฒนาโครงสร้างพื้นฐานศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์กระทรวงการคลัง
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง
ถนนพระรามที่ ๖ แขวงพญาไท เขตพญาไท กรุงเทพมหานคร ๑๐๔๐๐

๒. ทาง e-Mail tor-mofcsirt@mof.go.th

๓. ทางโทรศัพท์ **หมายเลข ๐ ๒๑๒๖ ๕๙๐๐ ต่อ ๓๐๓๐๑, ๓๐๓๐๓, ๓๐๓๐๔**

ทั้งนี้ โปรดแจ้ง ชื่อ ที่อยู่ พร้อมหมายเลขโทรศัพท์ติดต่อกลับด้วย

.....ประธาน.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการและเลขานุการ

แบบรูปรายการหรือคุณลักษณะเฉพาะ
โครงการพัฒนาโครงสร้างพื้นฐานศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ กระทรวงการคลัง

๑. ข้อกำหนดและเงื่อนไขในการยื่นข้อเสนอ

ผู้ยื่นข้อเสนอจะต้องปฏิบัติตามข้อกำหนดและเงื่อนไขในการยื่นข้อเสนอให้ครบถ้วนถูกต้อง รวมทั้งต้องศึกษารายงานขั้นต้น (Inception Report) รวมทั้งปรับปรุงให้เหมาะสมกับสภาพการณ์ปัจจุบัน ซึ่งประกอบด้วยหัวข้อและรายละเอียด ดังนี้

๑.๑. ทฤษฎี/แนวคิด

๑.๒. ขอบเขตการดำเนินงาน

๑.๓. แผนการดำเนินงาน

๑.๔. ผลที่คาดว่าจะได้รับ

๒. สำรวจและออกแบบโครงการพัฒนาโครงสร้างพื้นฐานศูนย์ประสานการรักษาความปลอดภัยไซเบอร์ กระทรวงการคลัง โดยต้องจัดทำเป็นเอกสารรายงานประกอบด้วยรายละเอียดอย่างน้อย ดังนี้

๒.๑. โครงสร้างการทำงานและภาพรวมของระบบ

๒.๒. รูปแบบการติดตั้งและการเชื่อมต่อระบบ

๒.๓. รูปแบบการปฏิบัติงานของหน่วยงานและทีมงานทั้งหมดที่เกี่ยวข้องในโครงการ

๓. พัฒนาแพลตฟอร์มข่าวกรองภัยคุกคามไซเบอร์ (Cyber Threat Intelligence Platform) จำนวน ๑ ระบบ โดยมีคุณลักษณะเฉพาะอย่างน้อยดังต่อไปนี้

๓.๑. เป็นระบบที่พัฒนาต่อยอดจาก MISP (Malware Information Sharing Platform) Open Source Software โดยสามารถติดตั้งและทำงานบนระบบปฏิบัติการ Linux Enterprise Grade และรองรับการทำงานในรูปแบบ Virtual Appliance

๓.๒. มีส่วนติดต่อผู้ใช้งานแบบ Web-based Interface ผ่าน HTTPS พร้อมระบบยืนยันตัวตนแบบ Multi-factor Authentication หรือรองรับการเชื่อมต่อกับ Active Directory/LDAP

๓.๓. ความสามารถด้านการจัดการข้อมูลข่าวกรองภัยคุกคาม

๓.๓.๑. สามารถจัดเก็บและแลกเปลี่ยนข้อมูลตามมาตรฐาน STIX/TAXII พร้อมระบบจัดการ Events, Attributes และ Indicators of Compromise (IoCs) ประเภทต่างๆ

๓.๔. ความสามารถด้านการแลกเปลี่ยนข้อมูล

๓.๔.๑. สามารถเชื่อมต่อและแลกเปลี่ยนข้อมูลกับ MISP Communities พร้อมระบบควบคุมการเผยแพร่ข้อมูลตามระดับชั้นความลับ

๓.๔.๒. สามารถแลกเปลี่ยนข้อมูลผ่าน REST API และ TAXII Server พร้อมระบบตรวจสอบและป้องกันการรั่วไหลของข้อมูล

๓.๕. ความสามารถด้านการวิเคราะห์และสืบค้น

๓.๕.๑. มีเครื่องมือสำหรับวิเคราะห์ความเชื่อมโยงของข้อมูลภัยคุกคาม พร้อมความสามารถในการสืบค้นข้อมูลแบบ Full-text Search และ Advanced Search

๓.๕.๒. สามารถสร้าง Custom Dashboard สำหรับการวิเคราะห์ข้อมูล พร้อมระบบแจ้งเตือนอัตโนมัติ

๓.๖. การบูรณาการกับระบบอื่น

๓.๖.๑. สามารถเชื่อมต่อกับระบบ SIEM หรือ XDR และระบบป้องกันภัยคุกคามต่างๆ ผ่าน API หรือ Integration Module

๓.๖.๒. รองรับการแลกเปลี่ยนข้อมูลกับแหล่งข้อมูลภัยคุกคามภายนอกผ่าน Plugin มาตรฐาน

๓.๗. การรายงานและการบริหารจัดการ

๓.๗.๑. มี Dashboard และระบบรายงานที่สามารถปรับแต่งได้พร้อมความสามารถในการส่งออกข้อมูลในรูปแบบมาตรฐาน

๓.๗.๒. มีระบบจัดการสิทธิ์ผู้ใช้งานแบบ Role-based Access Control และระบบบันทึก Audit Log

๓.๘. ประสิทธิภาพและความปลอดภัย

๓.๘.๑. สามารถทำงานแบบ High Availability และมีระบบรักษาความปลอดภัยของการสื่อสารระหว่างองค์กร

๓.๘.๒. มีระบบสำรองและกู้คืนข้อมูลพร้อมระบบป้องกันการโจมตีและการเข้าถึงที่ไม่ได้รับอนุญาต

๓.๙. จัดทำรายงานผลการติดตั้งและทดสอบการใช้งานแพลตฟอร์มข่าวกรองภัยคุกคามไซเบอร์ (Cyber Threat Intelligence Platform) จำนวน ๑ รายงาน

๔. พัฒนาแพลตฟอร์มตรวจประเมินช่องโหว่และความเสี่ยงระบบเทคโนโลยีสารสนเทศส่วนกลาง (Continuous Security Validation Platform) จำนวน ๑ ระบบ โดยมีคุณลักษณะเฉพาะอย่างน้อยดังต่อไปนี้

๔.๑. สามารถประเมินติดตามและรายงานผลการประเมินความเสี่ยง โดยอ้างอิงตามข้อกำหนดมาตรฐาน ISO ๒๗๐๐๑

๔.๒. สามารถกำหนดระดับความสำคัญจัดหมวดหมู่และบริหารจัดการรายการทรัพย์สินของระบบเทคโนโลยีสารทนเทศได้ (IT Asset Management)

๔.๓. สามารถวิเคราะห์ความเสี่ยงและภัยคุกคามที่อาจเกิดขึ้น (Threat Modeling)

๔.๔. สามารถตรวจสอบ ประเมิน ติดตามและบริหารจัดการช่องโหว่และความเสี่ยงทางเทคนิคของระบบเทคโนโลยีสารสนเทศ โดยครอบคลุมหัวข้อดังต่อไปนี้เป็นอย่างน้อย

๔.๕. สามารถตรวจสอบช่องโหว่เครื่องแม่ข่ายและช่องโหว่ของโครงสร้างพื้นฐานของระบบที่เกี่ยวข้อง (Vulnerability Assessment หรือ VA)

๔.๖. สามารถตรวจสอบความปลอดภัยด้านการออกแบบแอพพลิเคชันให้มีความปลอดภัย (Application Design Security)

๔.๗. สามารถตรวจสอบ ประเมิน และบริหารจัดการความปลอดภัยของระบบหรือแอปพลิเคชัน โดยใช้กระบวนการ Static Application Security Testing (SAST) เพื่อป้องกันความเสี่ยงที่เกิดจากการเขียนโปรแกรม

๔.๘. สามารถทดสอบ ประเมิน และบริหารจัดการความปลอดภัยของระบบหรือแอปพลิเคชันที่พัฒนา โดยใช้กระบวนการ Dynamic Application Security Testing (DAST) เพื่อป้องกันความเสี่ยงของระบบขณะทำงานจริง

๔.๙. สามารถตรวจสอบ ประเมิน และบริหารจัดการช่องโหว่ของ Open Source และ Third-Party Libraries ที่เกี่ยวข้องกับระบบเพื่อป้องกันความเสี่ยงจากซอฟต์แวร์ของบุคคลที่สาม (Software Composition Analysis หรือ SCA)

๔.๑๐. สามารถกำหนดบทบาทหน้าที่ ติดตามผล และบริหารจัดการช่องโหว่หรือความเสี่ยงที่ตรวจพบทั้งหมด (Vulnerability Management)

๔.๑๑. รองรับการนำเข้ารายงานผลการทดสอบเจาะระบบโดยทีมผู้เชี่ยวชาญ (Penetration Testing) เพื่อติดตามและตรวจสอบผลการปรับปรุงแก้ไขช่องโหว่ที่ตรวจพบได้

๔.๑๒. สามารถกำหนดให้ทำการเฝ้าระวังความปลอดภัยระบบอย่างต่อเนื่อง (Continuous Security Monitoring

๔.๑๓. สามารถแสดงรายงานสรุปผลตามมาตรฐานหรือข้อกำหนดด้าน Compliance ได้แก่ PDPA, NCSA NCRI, ISO๒๗๐๐๑, NIST CSF และ OWASP ASVS เป็นอย่างน้อย

๔.๑๔. สามารถบริหารจัดการจากส่วนกลาง (Centralize Management) และแสดงผลรายงานจากส่วนกลาง (Centralize Dashboard) เพื่อแสดงผลสรุปภาพรวมความปลอดภัยได้

๔.๑๕. จัดทำรายงานผลการติดตั้งและทดสอบการใช้งานแพลตฟอร์มตรวจประเมินช่องโหว่และความเสี่ยงระบบเทคโนโลยีสารสนเทศส่วนกลาง (Continuous Security Validation Platform) จำนวน ๑ รายงาน

๕. พัฒนาแพลตฟอร์มเฝ้าระวังและตอบสนองต่อภัยคุกคามไซเบอร์แบบบูรณาการ (SecOps Platform) จำนวน ๑ ระบบ โดยมีคุณลักษณะเฉพาะอย่างน้อยดังต่อไปนี้

๕.๑. ตรวจจับพฤติกรรมวิเคราะห์และบันทึกข้อมูลของระบบเครือข่ายเพื่อค้นหาพฤติกรรมที่น่าสงสัย

๕.๑.๑. สามารถตรวจจับและวิเคราะห์ Network Traffic ได้

๕.๑.๒. สามารถทำ Network Traffic Analysis ทั้งแบบ North-South และ East-West

๕.๑.๓. สามารถตรวจจับ Anomaly บน Network Traffic โดยใช้ AI/ML ได้

๕.๑.๔. สามารถตรวจจับ Protocol Abuse และ Policy Violation ได้

๕.๑.๕. สามารถวิเคราะห์ Encrypted Traffic (SSL/TLS Inspection) ได้

๕.๑.๖. สามารถทำ Network Behavior Analysis เพื่อตรวจจับ Malware Communication ได้

๕.๒. ตรวจจับพฤติกรรมที่อยู่ในข่ายน่าสงสัย โดยอาศัยเทคนิคการวางกับดักหรือเหยื่อล่อ

๕.๒.๑. สามารถจำลองบริการหลอก (Decoy Services) ที่ครอบคลุมโปรโตคอลพื้นฐาน (HTTP, FTP, SSH, SMB, etc.) ได้

๕.๒.๒. สามารถสร้าง Custom Service เพื่อจำลองระบบงานเฉพาะได้

๕.๒.๓. สามารถจัดเก็บหรือบันทึกพฤติกรรมของผู้โจมตีได้

๕.๓. จำลองรูปแบบการโจมตีเสมือนจริง (Breach and Attack Simulation)

๕.๓.๑. สามารถจำลองการโจมตีตาม MITRE ATT&CK Framework ได้

๕.๓.๒. สามารถทดสอบประสิทธิภาพของระบบป้องกันที่มีอยู่ได้

๕.๓.๓. สามารถตรวจสอบระบบ Security Control แบบอัตโนมัติได้

๕.๓.๔. สามารถจัดทำรายงานผลการทดสอบพร้อมคำแนะนำในการปรับปรุงระบบได้

๕.๓.๕. สามารถกำหนดช่วงเวลา สำหรับการทดสอบการจำลองการโจมตีได้

๕.๓.๖. มีข้อมูลรายงานสรุปผลทดสอบการจำลอง Simulation และผลข้อมูลสรุปจุดอ่อนด้านความปลอดภัย

๕.๔. คลังข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์ (Security Data Lake)

๕.๔.๑. สามารถจัดเก็บและวิเคราะห์ข้อมูลด้านความมั่นคงปลอดภัยที่รวบรวมข้อมูลจากหลายแหล่ง โดยสามารถจัดเก็บข้อมูลได้ไม่น้อยกว่า ๙๐ วัน

๕.๔.๒. สามารถรองรับการเก็บรวบรวมข้อมูล (Data Collection) จากหลายแหล่งข้อมูล เช่น Syslog, Windows Event Log, Network Flow, API, Firewall, Endpoint หรือ Log files ต่างๆ โดยสามารถรับข้อมูลได้ไม่น้อยกว่า ๕๐๐ GB/Day

๕.๔.๓. สามารถจัดการและแปลงข้อมูล (Data Parsing & Normalization) ที่รองรับการทำ Field Extraction และ Data Enrichment พร้อมความสามารถในการสร้าง Custom Parser

๕.๔.๔. สามารถวิเคราะห์ข้อมูลแบบ Real-time และ Historical Analysis พร้อมความสามารถในการสร้าง Correlation Rules และ Analytics Rules

๕.๔.๕. สามารถทำงานร่วมกับ Security Automation Engine เพื่อการวิเคราะห์และตอบสนองต่อเหตุการณ์แบบอัตโนมัติ โดยสามารถเชื่อมต่อกับ Large Language Model (LLM) ผ่าน API และมี Pre-built Playbooks สำหรับการตรวจจับภัยคุกคามและตอบสนองต่อเหตุการณ์พื้นฐาน

๕.๔.๖. สามารถสร้าง Custom Dashboard และ Visualization เพื่อแสดงผลข้อมูลในรูปแบบต่างๆ พร้อมความสามารถในการ Drill-down

๕.๔.๗. สามารถจัดทำรายงานทั้งแบบ Custom Report Template และการส่งรายงานอัตโนมัติ โดยสามารถส่งออกในรูปแบบ PDF, CSV, JSON

๕.๔.๘. สามารถเชื่อมต่อกับระบบภายนอกเพื่อทำ Automated Response ผ่าน API หรือ Integration Module

๕.๔.๙. สามารถจัดการสิทธิ์ผู้ใช้งานแบบ Role-based Access Control และ Data Access Control

๕.๕. บริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Incident Management)

๕.๕.๑. สามารถสร้างและจัดการ Service Desk สำหรับรับและจัดการคำร้องขอจากหน่วยงานในสังกัด

๕.๕.๒. สามารถกำหนดและบริหารจัดการ Service Level Agreements (SLA) ที่เหมาะสมกับงานบริการ

๕.๕.๓. สามารถจัดลำดับความสำคัญของคำร้องขอ (Prioritization) ตามระดับความเร่งด่วน

๕.๕.๔. สามารถจัดการกลุ่มเหตุการณ์ที่เกี่ยวข้องเพื่อลดการแจ้งซ้ำซ้อน

๕.๕.๕. สามารถบันทึกประวัติการแก้ ไขปัญหาเพื่อใช้อ้างอิงและการวิเคราะห์ในอนาคต

๕.๕.๖. สามารถทำงานในรูปแบบระบบ Workflow โดยกำหนดเงื่อนไขและกระบวนการอนุมัติที่เหมาะสม

๕.๕.๗. สามารถบริหารจัดการสินทรัพย์ไอที (IT Assets) และอุปกรณ์ภายในหน่วยงาน

๕.๕.๘. สามารถเชื่อมต่อกับ Active Directory (AD) เพื่อบริหารจัดการบัญชีผู้ใช้

๕.๕.๙. สามารถเชื่อมต่อกับระบบอีเมลของหน่วยงานเพื่อการแจ้งเตือนอัตโนมัติ

๕.๕.๑๐. มี API สำหรับการเชื่อมโยงและทำงานร่วมกับระบบอื่น ๆ ภายในองค์กร

๕.๕.๑๑. สามารถตั้งค่าระบบอัตโนมัติ เพื่อลดงานที่เกิดซ้ำซ้อน เช่น การกำหนดเส้นทางของคำร้องขอ

๕.๕.๑๒. มีระบบ Chatbot หรือ Virtual Agent สำหรับตอบคำถามพื้นฐานของผู้ใช้งาน

๕.๕.๑๓. มีระบบ Dashboard แสดงสถานะและสถิติของคำร้องขอแบบเรียลไทม์

๕.๕.๑๔. สามารถสร้างและปรับแต่งรายงานตามความต้องการของหน่วยงาน

๕.๕.๑๕. สามารถกำหนดสิทธิ์ผู้ใช้งานแบบ Role-based Access Control เพื่อความปลอดภัยและการควบคุมการเข้าถึงข้อมูล

๕.๖. จัดทำรายงานผลการติดตั้งและทดสอบการใช้งานแพลตฟอร์มเฝ้าระวังและตอบสนองต่อภัยคุกคามไซเบอร์แบบบูรณาการ (SecOps Platform) จำนวน ๑ รายงาน

๖. พัฒนาแพลตฟอร์มตอบสนองต่อภัยคุกคามทางไซเบอร์ และการสืบสวนสอบสวนทางนิติวิทยาศาสตร์ดิจิทัล (Digital Forensics and Incident Response Platform : DFIR) จำนวน ๑ ระบบ โดยมีคุณลักษณะเฉพาะอย่างน้อยดังต่อไปนี้

๖.๑. สามารถเฝ้าระวัง ตรวจสอบ และรวบรวมข้อมูลจากอุปกรณ์ปลายทางได้อย่างมีประสิทธิภาพ

๖.๒. สามารถติดตั้งบนระบบปฏิบัติการ Windows Server, Linux หรือระบบปฏิบัติการอื่นๆ ที่เทียบเท่า

๖.๓. มีส่วนติดต่อผู้ใช้งานแบบเว็บ (Web-based Interface) ที่ใช้งานง่ายและสามารถเข้าถึงได้ผ่านเว็บเบราว์เซอร์ทั่วไป

๖.๔. มีระบบติดตามกระบวนการ (Process Tracker) ที่สามารถติดตามโปรแกรมและโปรเซสย่อยที่ทำงานบนอุปกรณ์ปลายทางพร้อมทั้งบันทึกประวัติการทำงานไว้เพื่อการตรวจสอบย้อนหลัง

๖.๕. สามารถรวบรวมข้อมูลระบบ (System Information) จากอุปกรณ์ปลายทาง เช่น ข้อมูลฮาร์ดแวร์ ซอฟต์แวร์ที่ติดตั้ง การตั้งค่าระบบ และข้อมูลเครือข่าย

๖.๖. สามารถสร้าง ปรับแต่ง และใช้งานอาร์ติแฟคต์ (Artifacts) สำหรับการรวบรวมและวิเคราะห์ข้อมูลจากอุปกรณ์ปลายทาง

๖.๗. มีระบบไฟล์เสมือน (Virtual File System : VFS) ที่ช่วยให้สามารถเข้าถึงและดึงข้อมูลจากระบบไฟล์ของอุปกรณ์ปลายทางได้อย่างมีประสิทธิภาพ

๖.๘. สามารถสร้างสำเนาของหน่วยความจำ (Memory Dump) และฮาร์ดไดรฟ์ (Disk Image) เพื่อการวิเคราะห์ทางนิติวิทยาศาสตร์

๖.๙. มีเครื่องมือในการวิเคราะห์ข้อมูลและการทำความเข้าใจข้อมูล (Data Analytics) พร้อมทั้งแสดงผลในรูปแบบกราฟและแผนภูมิ

๖.๑๐. สามารถสร้างสมุดบันทึก (Notebooks) ที่รวมข้อความอธิบาย (Markdown) และคำสั่งสอบถามข้อมูลเพื่อการวิเคราะห์และการทำงานร่วมกัน

๖.๑๑. มีความสามารถในการส่งออกข้อมูล (Export) ในรูปแบบต่างๆ เช่น CSV หรือ JSON หรือ PDF

๖.๑๒. สามารถบูรณาการกับระบบรักษาความปลอดภัยอื่นๆ เช่น SIEM, SOAR และ Threat Intelligence Platforms

๖.๑๓. มี API ที่ครอบคลุมสำหรับการพัฒนาและบูรณาการกับระบบภายนอก

๖.๑๔. จัดทำรายงานผลการติดตั้งและทดสอบการใช้งานแพลตฟอร์มตอบสนองต่อภัยคุกคามทางไซเบอร์และการสืบสวนสอบสวนทางนิติวิทยาศาสตร์ดิจิทัล (Digital Forensics and Incident Response Platform : DFIR) จำนวน ๑ รายงาน

๗. ดำเนินงานบริการเพื่อสนับสนุนภารกิจ MOF-CSIRT ในระยะแรก (๑ ปี) จำนวน ๑ งาน โดยมี คุณลักษณะเฉพาะอย่างน้อยดังต่อไปนี้

๗.๑. จัดตั้งหน่วยปฏิบัติการ เฝ้าระวัง และตอบสนองต่อภัยคุกคามไซเบอร์ เพื่อสนับสนุนงานของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์กระทรวงการคลังให้สามารถปฏิบัติงานรับมือและตอบสนองต่อเหตุการณ์ภัยคุกคามไซเบอร์ให้แก่สำนักงานปลัดกระทรวงการคลัง หน่วยงานในสังกัด และหน่วยงานในกำกับกระทรวงการคลังได้อย่างมีประสิทธิภาพตลอด ๒๔ ชั่วโมง โดยจะต้องครอบคลุมส่วนงานดังต่อไปนี้ เป็นอย่างน้อย

๗.๑.๑. รายละเอียดส่วนงานที่รับผิดชอบ

๗.๑.๑.๑. ส่วนงานจัดการเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ (Information Security Incident Management)

๑) การรับแจ้งเหตุด้านความมั่นคงปลอดภัยไซเบอร์ (Information Security Incident Report Acceptance)

๒) การวิเคราะห์เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ (Information Security Incident Analysis)

๓) การวิเคราะห์หลักฐานทางนิติวิทยาศาสตร์ (Artifact and Forensic Evidence Analysis)

๔) การบรรเทาและสนับสนุนการกู้คืนจากเหตุการณ์ (Mitigation and Recovery)

๕) การประสานงานด้านเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ (Information Security Incident Coordination)

๖) การสนับสนุนการบริหารจัดการวิกฤติ (Crisis Management Support)

๗.๑.๑.๒. ส่วนงานจัดการช่องโหว่ (Vulnerability Management)

๑) การค้นหาและวิจัยช่องโหว่ (Vulnerability Discovery/Research)

๒) การรับแจ้งช่องโหว่ (Vulnerability Report Intake)

๓) การวิเคราะห์ช่องโหว่ (Vulnerability Analysis)

๔) การประสานงานช่องโหว่ (Vulnerability Coordination)

๕) การเปิดเผยช่องโหว่ (Vulnerability Disclosure)

๖) การตอบสนองช่องโหว่ (Vulnerability Response)

๗.๑.๑.๓. ส่วนงานติดตามและประเมินสถานการณ์ (Situational Awareness)

๑) การเก็บรวบรวมข้อมูลสถานการณ์ทางไซเบอร์ (Data Acquisition)

๒) การวิเคราะห์และสังเคราะห์ข้อมูล (Analysis and Synthesis)

๓) การสื่อสารข้อมูลและแจ้งเตือน (Communication)

๗.๑.๑.๔. ส่วนงานถ่ายทอดความรู้ (Knowledge Transfer)

๑) การสร้างความตระหนักด้านความมั่นคงปลอดภัย (Awareness Building)

๒) การฝึกอบรมและให้ความรู้ (Training and Education)

๓) การฝึกซ้อมและจำลองเหตุการณ์ (Exercises)

๔) การให้คำปรึกษาด้านเทคนิคและนโยบาย (Technical and Policy Advisory)

๗.๑.๑.๕. ส่วนงานจัดการเหตุการณ์ความมั่นคงปลอดภัยของระบบ (Information Security Event Management)

๑) การเฝ้าระวังและตรวจจับภัยคุกคาม (Monitoring and Detection)

๒) การวิเคราะห์เหตุการณ์ด้านความมั่นคงปลอดภัย (Event Analysis)

๗.๑.๒. รายงานสรุปผลการดำเนินงานของหน่วยปฏิบัติการ เฝ้าระวัง และตอบสนองต่อภัยคุกคามไซเบอร์

๗.๑.๒.๑. จัดทำรายงานสรุปการดำเนินงานประจำเดือน จำนวน ๑ รายงาน ซึ่งจะต้องครอบคลุมหัวข้อดังต่อไปนี้ เป็นอย่างน้อย

๑) รายงานผลการดำเนินงานในส่วนงานจัดการเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ (Information Security Incident Management)

๒) รายงานผลการดำเนินงานในส่วนงานจัดการช่องโหว่ (Vulnerability Management)

๓) รายงานผลการดำเนินงานในส่วนงานติดตามและประเมินสถานการณ์ (Situational Awareness)

๔) รายงานผลการดำเนินงานในส่วนงานถ่ายทอดความรู้ (Knowledge Transfer)

๕) รายงานผลการดำเนินงานในส่วนงานจัดการเหตุการณ์ความมั่นคงปลอดภัยของระบบ (Information Security Event Management)

๗.๒. บริการจากศูนย์ MOF-CSIRT เพื่อสนับสนุนและให้ความช่วยเหลือหน่วยงานในสังกัด และหน่วยงานในกำกับกระทรวงการคลัง

๗.๒.๑. ขอบเขตบริการ

๗.๒.๑.๑. บริการสนับสนุนและแลกเปลี่ยนข้อมูลข่าวกรองภัยคุกคามไซเบอร์ (Cyber Threat Intelligence Sharing)

๗.๒.๑.๒. บริการสนับสนุนการจัดการเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ (Information Security Incident Management)

๗.๒.๑.๓. บริการสนับสนุนการตรวจประเมินช่องโหว่และความเสี่ยงระบบเทคโนโลยีสารสนเทศ (Continuous Security Validation Management)

๗.๒.๑.๔. บริการสนับสนุนการแลกเปลี่ยนและถ่ายทอดความรู้ (Knowledge Transfer)

๗.๒.๒. รายงานสรุปผลการดำเนินงานที่ให้การสนับสนุนและช่วยเหลือหน่วยงานในสังกัด

๗.๒.๒.๑. จัดทำรายงานสรุปผลการดำเนินงานประจำเดือน จำนวน ๑ รายงาน

๘. ดำเนินการพัฒนาศักยภาพบุคลากรและเจ้าหน้าที่ของ MOF-CSIRT เพื่อยกระดับองค์ความรู้และทักษะความเชี่ยวชาญสำหรับการปฏิบัติภารกิจในระยะยาว ในรูปแบบการฝึกอบรมเชิงปฏิบัติการ (On the Job Training) จำนวน ๑ งาน โดยมีคุณลักษณะเฉพาะอย่างน้อยดังต่อไปนี้

๘.๑. จัดให้มีการฝึกอบรมและถ่ายทอดองค์ความรู้แก่เจ้าหน้าที่สำนักงานปลัดกระทรวงการคลังและหน่วยงานในสังกัด ในรูปแบบการฝึกอบรมเชิงปฏิบัติการ (On the Job Training) ครอบคลุมหลักสูตรสำคัญ ดังต่อไปนี้

๘.๑.๑. การวิเคราะห์และคัดกรองภัยคุกคามทางไซเบอร์ (Cyber Threat Analysis and Triage)

๘.๑.๒. การตรวจพิสูจน์หลักฐานดิจิทัลและการตอบสนองต่อเหตุการณ์ (Digital Forensics and Incident Response)

๘.๑.๓. การค้นหา ตรวจสอบ และระบุภัยคุกคามไซเบอร์เชิงรุก (Cyber Threat Hunting)

๘.๑.๔. การวิเคราะห์ข่าวกรองภัยคุกคามทางไซเบอร์ (Threat Intelligence Analysis)

๘.๑.๕. การฝึกซ้อมรับมือภัยคุกคามทางไซเบอร์ด้วยเครื่องมือโอเพนซอร์สและบุคลากร (Cyber Drill)

๘.๑.๖. การจำลองสถานการณ์การโจมตีทางไซเบอร์ (Breach and Attack Simulation)

๘.๑.๗. การตรวจประเมินและบริหารจัดการช่องโหว่ (Vulnerability Management)

๘.๑.๘. การพัฒนาแผนรับมือและตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ (Incident Response Plan)

๘.๑.๙. การพัฒนาคู่มือการปฏิบัติและขั้นตอนในการรับมือและตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ (IR Playbook)

หลักเกณฑ์การพิจารณาการคัดเลือกข้อเสนอ

การจัดจ้างครั้งนี้เป็นงานที่มีความซับซ้อนและมีข้อจำกัดด้านเทคนิค ซึ่งมีความแตกต่างกันไปตามลักษณะชนิดประเภทของงานที่ไม่อยู่บนพื้นฐานเดียวกัน ผู้ยื่นข้อเสนอต้องแสดงให้เห็นถึงความพร้อมและความเชี่ยวชาญเฉพาะด้านตามขอบเขตการดำเนินงานของสำนักงานปลัดกระทรวงการคลัง

ดังนั้นเกณฑ์การพิจารณาคัดเลือกข้อเสนอสำหรับงานจ้าง โครงการพัฒนาโครงสร้างพื้นฐานศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์กระทรวงการคลัง คณะกรรมการจะดำเนินการตรวจสอบคุณสมบัติของผู้ยื่นข้อเสนอและคุณสมบัติของระบบที่เกี่ยวข้องตามที่กำหนด เอกสารข้อเสนอที่ยื่นหากพบข้อบกพร่องไม่ถูกต้องตามหลักเกณฑ์และเงื่อนไขตามที่กำหนดคณะกรรมการจะไม่รับพิจารณา และใช้เกณฑ์การประเมินค่าประสิทธิภาพต่อราคา (Price Performance) โดยพิจารณาให้คะแนนตามปัจจัยหลักและน้ำหนักร้อยละที่กำหนด โดยกำหนดให้น้ำหนักรวมทั้งหมดเท่ากับร้อยละ ๑๐๐ รายละเอียดดังนี้

๑. พิจารณาราคาที่ยื่นเสนอ (Price) กำหนดน้ำหนักเท่ากับร้อยละ ๒๐ โดยมีเกณฑ์คะแนนตามสัดส่วน ๑๐๐ คะแนน โดยกำหนดการให้คะแนนดังนี้

๑.๑. ผู้ที่เสนอราคาต่ำสุดจะได้คะแนน ๑๐๐ คะแนน

๑.๒. ผู้ที่เสนอราคารายอื่นจะคิดจากสูตรการคำนวณ ดังนี้

$$\text{คะแนน} = ๑๐๐ - \frac{(\text{ราคาของผู้เสนอราคารายอื่น} - \text{ราคาต่ำสุด}) \times ๑๐๐}{\text{ราคาต่ำสุด}}$$

๒. พิจารณาคุณภาพหรือคุณลักษณะเฉพาะที่เป็นประโยชน์ต่อทางราชการ (ตัวแปรหลัก) กำหนดน้ำหนักเท่ากับร้อยละ ๘๐ โดยมีเกณฑ์คะแนนตามสัดส่วน ๑๐๐ คะแนน โดยกำหนดการให้คะแนนดังนี้

เกณฑ์พิจารณา		รายละเอียดการพิจารณา	คะแนนเต็ม
๒.๑	นำเสนอแนวคิดและโครงสร้างสถาปัตยกรรมของระบบได้สอดคล้องกับวัตถุประสงค์โครงการพัฒนาเทคโนโลยีสำหรับปฏิบัติการของศูนย์ MOF-CSIRT	นำเสนอแนวคิดและโครงสร้างสถาปัตยกรรมของระบบทั้ง ๔ ระบบดังนี้ ๑. แพลตฟอร์มข่าวกรองภัยคุกคามไซเบอร์ (Cyber Threat Intelligence Platform) ๒. แพลตฟอร์มตรวจประเมินช่องโหว่และความเสี่ยงระบบเทคโนโลยีสารสนเทศส่วนกลาง (Continuous Security Validation Platform) ๓. แพลตฟอร์มเฝ้าระวังและตอบสนองต่อภัยคุกคามไซเบอร์แบบบูรณาการ (SecOps Platform) ๔. แพลตฟอร์มตอบสนองต่อภัยคุกคามทางไซเบอร์และการสืบสวนสอบสวนทางนิติวิทยาศาสตร์ดิจิทัล (Digital Forensics and Incident Response Platform : DFIR)	๑๐

.....ประธาน.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการและเลขานุการ

เกณฑ์พิจารณา		รายละเอียดการพิจารณา	คะแนนเต็ม
		- นำเสนอได้ถูกต้องครบถ้วน ๔ แพลตฟอร์ม (๑๐ คะแนน) - นำเสนอได้ถูกต้องครบถ้วน ๓ แพลตฟอร์ม (๕ คะแนน) - นำเสนอได้น้อยกว่า ๓ แพลตฟอร์ม (๐ คะแนน)	
๒.๒	แสดงขีดความสามารถในการตรวจสอบหลักฐานดิจิทัลและตอบสนองเหตุการณ์ภัยคุกคามไซเบอร์ (DFIR) ที่มุ่งเป้าโจมตีระบบงานสำคัญ รวมถึงการสืบสวนทางเทคนิคเพื่อระบุสาเหตุและผลกระทบ การติดตามข้อมูลที่รั่วไหลสู่ภายนอก และการให้ข้อเสนอแนะเชิงกลยุทธ์	สาธิตการตรวจสอบหลักฐานดิจิทัลและตอบสนองเหตุการณ์ภัยคุกคามไซเบอร์ (DFIR) ที่มุ่งเป้าโจมตีระบบงานสำคัญ โดยกระทรวงฯ จะทำการจำลองสถานการณ์การถูกโจมตีระบบสารสนเทศที่สำคัญยิ่งยวด (Critical Information System) ส่งผลทำให้ระบบไม่สามารถใช้งานได้ และสันนิษฐานว่ามีข้อมูลสำคัญบางส่วนรั่วไหลออกไปสู่ภายนอก ทั้งนี้กระทรวงฯ จะจัดเตรียมระบบและสภาพแวดล้อมจำลอง พร้อมรายละเอียดโครงสร้างสถาปัตยกรรมและข้อมูลที่จำเป็นให้แก่ผู้ยื่นข้อเสนอทุกรายเหมือนกัน โดยมีระยะเวลาดำเนินการ ๓ ชั่วโมง โดยผู้ยื่นข้อเสนอจะต้องดำเนินการดังนี้ ๑) จัดส่งทีมงานผู้เชี่ยวชาญเข้าร่วมการ POC บริษัทละไม่เกิน ๓ คน ๒) จัดเตรียมเครื่องมือและซอฟต์แวร์ที่จำเป็นสำหรับการทำ DFIR (แนะนำให้ใช้เครื่องมือที่จะใช้ในการพัฒนาระบบตามข้อเสนอโครงการนี้หากเป็นผู้ได้รับการคัดเลือก) ๓) ดำเนินการตามโจทย์ที่ได้รับ และนำส่งผลลัพธ์หรือคำตอบตามช่องทางที่กำหนด (จะแจ้งให้ทราบในวัน POC) โดยจะประกอบด้วยหัวข้อดังต่อไปไปนี้ ๓.๑) แสดงกระบวนการวิเคราะห์ ๓.๑.๑) ระบุช่องทางการโจมตีแรกเริ่ม (Initial Access) ได้ (๒๕ คะแนน) - สามารถระบุช่องทางการโจมตีแรกเริ่ม (Initial Access) ได้อย่างครบถ้วนและถูกต้อง (๒๕ คะแนน) - สามารถระบุช่องทางการโจมตีแรกเริ่ม (Initial Access) ได้เพียงบางส่วน (๑๐ คะแนน) - ไม่สามารถระบุช่องทางการโจมตีแรกเริ่ม (Initial Access) ได้ (๐ คะแนน)	๙๐

.....ประธาน.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการและเลขานุการ

เกณฑ์พิจารณา		รายละเอียดการพิจารณา	คะแนนเต็ม
		๓.๑.๒) สร้างลำดับเวลาการโจมตี (Attack Timeline) ได้ (๑๐ คะแนน) - สามารถสร้างลำดับเวลาการโจมตี (Attack Timeline) ได้อย่างครบถ้วน ถูกต้องและมีหลักฐานอ้างอิง (๑๐ คะแนน) - สามารถสร้างลำดับเวลาการโจมตี (Attack Timeline) ได้เพียงบางส่วนและมีหลักฐานอ้างอิง (๕ คะแนน) - ไม่สามารถสร้างลำดับเวลาการโจมตี (Attack Timeline) ได้ (๐ คะแนน) ๓.๑.๓) สามารถระบุ Indicators of Compromise (IoCs) ที่สำคัญได้ (๑๐ คะแนน) - สามารถระบุ Indicators of Compromise (IoCs) ที่สำคัญได้ครบถ้วนและถูกต้อง (๑๐ คะแนน) - สามารถระบุ Indicators of Compromise (IoCs) ที่สำคัญได้เพียงบางส่วน (๕ คะแนน) - ไม่สามารถระบุ Indicators of Compromise (IoCs) ที่สำคัญได้ครบถ้วนและถูกต้อง (๐ คะแนน) ๓.๒) แสดงผลการสืบสวน ๓.๒.๑) สามารถระบุขอบเขตของผลกระทบ (Scope of Compromise) ได้ (๑๐ คะแนน) - สามารถระบุขอบเขตของผลกระทบ (Scope of Compromise) ได้อย่างครบถ้วนและถูกต้อง (๑๐ คะแนน) - สามารถระบุขอบเขตของผลกระทบ (Scope of Compromise) ได้เพียงบางส่วน (๕ คะแนน) - ไม่สามารถระบุขอบเขตของผลกระทบ (Scope of Compromise) ได้อย่างครบถ้วนและถูกต้อง (๐ คะแนน)	

.....ประธาน.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการและเลขานุการ

เกณฑ์พิจารณา		รายละเอียดการพิจารณา	คะแนนเต็ม
		๓.๒.๒ สามารถระบุเทคนิคการขโมยข้อมูล (Data Exfiltration) และประเมินข้อมูลที่รั่วไหลได้ (๑๐ คะแนน) - สามารถระบุเทคนิคการขโมยข้อมูล (Data Exfiltration) และประเมินข้อมูลที่รั่วไหลได้อย่างครบถ้วนและถูกต้อง (๑๐ คะแนน) - สามารถระบุเทคนิคการขโมยข้อมูล (Data Exfiltration) และประเมินข้อมูลที่รั่วไหลได้เพียงบางส่วน (๕ คะแนน) - ไม่สามารถระบุเทคนิคการขโมยข้อมูล (Data Exfiltration) และประเมินข้อมูลที่รั่วไหลได้ (๐ คะแนน) ๓.๒.๓) สามารถค้นหาและนำเสนอหลักฐานข้อมูลที่รั่วไหลบน Dark Web ได้ (๒๕ คะแนน) - สามารถค้นหาและนำเสนอหลักฐานข้อมูลที่รั่วไหลบน Dark Web ได้ครบถ้วนและถูกต้อง (๒๕ คะแนน) - สามารถค้นหาและนำเสนอหลักฐานข้อมูลที่รั่วไหลบน Dark Web ได้สำเร็จบางส่วน (๑๐ คะแนน) - ไม่สามารถค้นหาและนำเสนอหลักฐานข้อมูลที่รั่วไหลบน Dark Web ได้ (๐ คะแนน)	

.....ประธาน.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการและเลขานุการ

รายละเอียดการดำเนินงาน การติดตั้งและการทดสอบ

๑. การติดตั้งและสถานที่ติดตั้งอุปกรณ์ระบบคอมพิวเตอร์และเครือข่ายสื่อสาร

๑.๑. ผู้ชนะการประกวดราคาต้องดำเนินการส่งมอบและติดตั้งระบบที่พัฒนาทั้งหมดตามโครงการ ณ อาคาร ๑๕๐ ปี กระทรวงการคลัง หรือศูนย์คอมพิวเตอร์จังหวัดประทุมธานี หรือตามคณะกรรมการตรวจรับพัสดุกำหนด โดยระบบต้องมีความพร้อมใช้งานประกอบด้วยระบบดังต่อไปนี้

๑.๑.๑. แพลตฟอร์มข่าวกรองภัยคุกคามไซเบอร์ (Cyber Threat Intelligence Platform)

๑.๑.๒. แพลตฟอร์มตรวจประเมินช่องโหว่และความเสี่ยงระบบเทคโนโลยีสารสนเทศส่วนกลาง (Continuous Security Validation Platform)

๑.๑.๓. แพลตฟอร์มเฝ้าระวังและตอบสนองต่อภัยคุกคามไซเบอร์แบบบูรณาการ (SecOps Platform)

๑.๑.๔. แพลตฟอร์มตอบสนองต่อภัยคุกคามทางไซเบอร์ และการสืบสวนสอบสวนทางนิติวิทยาศาสตร์ดิจิทัล (Digital Forensics and Incident Response Platform : DFIR)

๑.๒. ผู้ชนะการประกวดราคาต้องดำเนินการทดสอบด้านความมั่นคงปลอดภัยก่อนการส่งมอบระบบทั้งหมดในครงการ

๒. การบริหารจัดการและเงื่อนไขในการดำเนินงาน

๒.๑. ผู้ชนะการประกวดราคาต้องเสนอโครงสร้างการบริหารโครงการและแผนการดำเนินงาน เพื่อให้คณะกรรมการตรวจรับพัสดุพิจารณาก่อนดำเนินงาน โดยแผนการดำเนินงานต้องระบุความรับผิดชอบในส่วนของผู้ชนะการประกวดราคา หรือบริษัทเจ้าของผลิตภัณฑ์ หรือส่วนของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง

๒.๒. ผู้ชนะการประกวดราคา ต้องจัดทำแผนการดำเนินงานหลัก (Master Plan) และแผนการดำเนินงานในรายละเอียด (Action Plan) และแผนการดำเนินงานอื่นๆ ที่ประกอบด้วยตารางการปฏิบัติงาน ขั้นตอนในการดำเนินการ /ขั้นตอนในการปฏิบัติงาน ผู้รับผิดชอบงานแต่ละขั้นตอน ผลงานที่จะส่งมอบ ระยะเวลาที่ใช้ในแต่ละขั้นตอนเพื่อใช้ในการบริหารและติดตามผลการดำเนินงานให้ครอบคลุมการดำเนินงานทั้งหมด

๒.๓. ผู้ชนะการประกวดราคาต้องจัดให้มีบุคลากรผู้เชี่ยวชาญที่มีประสบการณ์ในการทำงาน ประกอบด้วย

๑) ผู้บริหารโครงการ (Project Manager) จำนวน ๑ คน มีคุณวุฒิไม่ต่ำกว่าระดับปริญญาโท และมีความชำนาญหรือประสบการณ์ในการควบคุมและบริหารโครงการด้านเทคโนโลยีสารสนเทศและการสื่อสารมาแล้วไม่น้อยกว่า ๑๐ ปี

๒) บุคลากรสนับสนุน (เลขานุการ) จำนวน ๑ คน มีคุณวุฒิไม่ต่ำกว่าระดับปริญญาตรี และมีความชำนาญหรือประสบการณ์ในงานมาแล้วไม่น้อยกว่า ๓ ปี

๓) บุคลากรด้านอื่นๆ ที่เห็นว่าจำเป็นต่อการดำเนินโครงการ

๒.๔. ในกรณีที่คณะกรรมการตรวจรับพัสดุและ/หรือผู้แทนของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง เห็นว่าบุคลากรตามเสนอมา มีคุณสมบัติไม่เหมาะสมหรือทำงานไม่มีประสิทธิภาพ ผู้ชนะการประกวดราคาต้องดำเนินการปรับเปลี่ยนโดยทันทีที่ได้รับแจ้ง ทั้งนี้ ผู้ชนะการประกวดราคาจะอ้างการปรับเปลี่ยนนี้นำมาเป็นเหตุของการล่าช้าของงานไม่ได้

๒.๕. ผู้ชนะการประกวดราคาต้องเสนอรายงานความก้าวหน้าการดำเนินงานให้คณะกรรมการตรวจรับพัสดุและ/หรือผู้แทน ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลังทราบอย่างน้อยเดือนละครั้ง หรือจนกว่างานจะแล้วเสร็จ

.....ประธาน.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการและเลขานุการ

๓. การทดสอบและตรวจรับ

๓.๑. ผู้ชนะการประกวดราคาต้องส่งมอบระบบให้คณะกรรมการตรวจรับพัสดุ ณ สถานที่ตามที่กำหนด โดยส่งมอบให้สำนักงานปลัดกระทรวงการคลังตามงวดงานที่กำหนดในเอกสารขอบเขตของงาน (TOR)

๓.๒. ผู้ชนะการประกวดราคาต้องดำเนินการทดสอบด้านความมั่นคงปลอดภัยก่อนการส่งมอบระบบทั้งหมดในโครงการ

๓.๓. ผู้ชนะการประกวดราคาต้องเสนอเอกสารซึ่งประกอบด้วย รายละเอียดของระบบ System Diagram ทั้งหมด ข้อมูลวิธีการและขั้นตอนการตรวจรับของแต่ละอุปกรณ์โดยละเอียด

๓.๔. คณะกรรมการตรวจรับพัสดุและ/หรือผู้แทนของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และ/หรือผู้แทนสำนักงานปลัดกระทรวงการคลัง ที่เข้าร่วมดูแลการติดตั้งจะดำเนินการตรวจรับงานเฉพาะในเวลาทำการปกติ คือ ๐๘.๓๐ - ๑๖.๓๐ น. เว้นวันเสาร์ - อาทิตย์ และวันหยุดราชการ ในกรณีที่ผู้ชนะการประกวดราคามีความจำเป็นต้องตรวจรับงานนอกเหนือจากเวลาดังกล่าวจะต้องแจ้งให้สำนักงานปลัดกระทรวงการคลังทราบ พร้อมทั้งจะต้องรับผิดชอบค่าใช้จ่ายในการปฏิบัติงาน (ถ้ามี)

๓.๕. คณะกรรมการตรวจรับพัสดุและ/หรือผู้แทนของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และ/หรือผู้แทนสำนักงานปลัดกระทรวงการคลัง สงวนสิทธิที่จะเข้าทดสอบและตรวจสอบการทำงานของอุปกรณ์หรือระบบที่ติดตั้ง ตามสถานที่ที่กำหนด เพื่อดำเนินการตรวจรับงาน โดยผู้ชนะการประกวดราคาจะต้องอำนวยความสะดวกในการเดินทางหรือรับผิดชอบในค่าใช้จ่ายในการปฏิบัติงาน (ถ้ามี)

๓.๖. สำนักงานปลัดกระทรวงการคลัง สามารถที่จะนำอุปกรณ์ และ/หรือ งานในส่วนที่ส่งมอบแล้วไปใช้งานตามที่สำนักงานปลัดกระทรวงการคลังเห็นสมควร โดยที่ไม่กระทบกระเทือนหรือเป็นอุปสรรคในการทำงานของผู้ชนะการประกวดราคา โดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลังเพียงแต่แจ้งให้ผู้ชนะการประกวดราคาทราบ แต่หากการทดสอบอุปกรณ์/ระบบ ไม่ผ่านเงื่อนไขและเป็นเหตุให้ต้องเลิกสัญญาอันเนื่องมาจากความผิดพลาดของผู้ชนะการประกวดราคา ผู้ชนะการประกวดราคาไม่มีสิทธิเรียกร้องค่าใช้จ่ายหรือค่าเสียหายใดๆ จากสำนักงานปลัดกระทรวงการคลัง

๓.๗. หากมีข้อความใดในข้อกำหนดฉบับนี้ที่มีความขัดแย้งกัน ให้ยึดถือตามข้อกำหนดที่เป็นประโยชน์กับสำนักงานปลัดกระทรวงการคลัง

เงื่อนไขการรับประกันผลงานและความชำรุดบกพร่องและการบำรุงรักษาและซ่อมแซมแก้ไข

ผู้ชนะการประกวดราคาต้องบำรุงรักษา ซ่อมแซมแก้ไขหรือเปลี่ยนทดแทนอุปกรณ์ที่ส่งมอบในโครงการทั้งหมด เป็นระยะเวลา ๑ ปี นับตั้งแต่คณะกรรมการตรวจรับพัสดุได้ตรวจรับงานงวดสุดท้ายเสร็จสมบูรณ์ โดยต้องปฏิบัติตามเงื่อนไขดังต่อไปนี้

๑. การบำรุงรักษาแบบป้องกัน (Preventive Maintenance)

๑.๑. ผู้ชนะการประกวดราคาต้องทำการบำรุงรักษา (Preventive Maintenance) ระบบที่ส่งมอบในโครงการอย่างน้อย ๒ ครั้ง ตลอดระยะเวลารับประกัน เพื่อให้ระบบอยู่ในสภาพที่ใช้งานได้อย่างมีประสิทธิภาพตลอดเวลา โดยทำการบำรุงรักษาในช่วงระยะเวลาที่ไม่ส่งผลกระทบต่อการปฏิบัติงานของสำนักงานปลัดกระทรวงการคลัง และจะต้องแจ้งให้ทราบล่วงหน้าอย่างน้อย ๕ วันทำการ ในทุกครั้งที่เข้าดำเนินการบำรุงรักษา

๑.๒. เมื่อมีการเปลี่ยนแปลง แก้ไข ปรับปรุงเพิ่มเติม Software ของระบบที่ส่งมอบในลักษณะการ Upgrade หรือออก Version ใหม่ที่ทันสมัยขึ้น ผู้ชนะการประกวดราคาต้องแจ้งให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลังทราบ เพื่อร่วมกันพิจารณาดำเนินการ เมื่อผู้รับผิดชอบระบบจากสำนักงานปลัดกระทรวงการคลังพิจารณาแล้วเห็นควรปรับปรุงและร้องขอให้ดำเนินการ ผู้ชนะการประกวดราคาต้องรับผิดชอบดำเนินการโดยไม่คิดค่าใช้จ่ายใด ๆ

๒. การซ่อมแซมแก้ไข

๒.๑. หากอุปกรณ์หรือระบบชำรุด บกพร่อง หรือใช้งานไม่ได้ ถึงแม้ว่าจะติดตั้งอยู่ ณ สถานที่ใดตามที่กำหนดในสัญญา และความชำรุดนี้มิได้เกิดจากความผิดของสำนักงานปลัดกระทรวงการคลัง ผู้ชนะการประกวดราคาต้องเริ่มดำเนินการซ่อมแซมแก้ไขให้อยู่ในสภาพดีได้ดังเดิมโดยไม่คิดค่าใช้จ่ายใด ๆ จากสำนักงานปลัดกระทรวงการคลัง โดยเข้าดำเนินการภายใน ๔ ชั่วโมง (ในเวลาทำการ ๘.๓๐-๑๖.๓๐) นับตั้งแต่ได้รับแจ้ง

๒.๒. ในการซ่อมแซมแก้ไข หากผู้ชนะการประกวดราคาคาดว่าไม่สามารถดำเนินการได้แล้วเสร็จภายใน ๒๔ ชั่วโมง (ในเวลาทำการ ๘.๓๐-๑๖.๓๐) นับแต่เริ่มทำการซ่อมแซมแก้ไข ผู้ชนะการประกวดราคาสามารถนำเครื่องหรืออุปกรณ์สำรองที่มีประสิทธิภาพทัดเทียมกัน ที่สามารถทำให้การใช้งานเป็นปกติดังเดิม ซึ่งจะไม่ถือว่าเป็นเวลาที่เกิดเหตุขัดข้อง แต่ผู้ชนะการประกวดราคาต้องเร่งดำเนินการแก้ไขเครื่องหรืออุปกรณ์ให้สามารถใช้งานได้ตามปกติ และนำมาเปลี่ยนทดแทน โดยเร็ว

๒.๓. สำนักงานปลัดกระทรวงการคลังยอมให้อุปกรณ์หรือระบบที่ส่งมอบในโครงการมีเวลาขัดข้องได้ไม่เกินครั้งละ ๒๔ ชั่วโมง (ในเวลาทำการ ๘.๓๐-๑๖.๓๐) โดยเริ่มนับเวลาตั้งแต่ที่เริ่มซ่อมแซมแก้ไขจนถึงเวลาที่ทำการซ่อมแซมแล้วเสร็จสมบูรณ์หรือเวลาที่ทำให้ระบบสามารถกลับมาทำงานได้ตามปกติ ถ้าการขัดข้องดังกล่าว มีระยะเวลาเกินเกณฑ์ที่กำหนด ผู้ชนะการประกวดราคาต้องถูกปรับในอัตราร้อยละ ๐.๐๒๕ ของราคาตามสัญญาต่อชั่วโมง เศษของชั่วโมง ให้นับเป็น ๑ ชั่วโมง

๓. การบริการและการสนับสนุน

ผู้ชนะการประกวดราคาจะต้องดำเนินการบริการและการสนับสนุน ตลอดระยะเวลารับประกัน โดยต้องปฏิบัติดังต่อไปนี้

๓.๑. ให้ความช่วยเหลือแก่ผู้บริหารจัดการระบบ (Administrator) หรือเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ในเรื่องที่เกี่ยวข้องกับอุปกรณ์หรือระบบในโครงการ ตามที่สำนักงานปลัดกระทรวงการคลังร้องขอ (On call) โดยไม่คิดค่าใช้จ่ายใด ๆ

.....ประธาน.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการและเลขานุการ

๓.๒. ให้คำปรึกษาแนะนำความรู้ในลักษณะของการถ่ายทอดเทคนิคและวิธีการปฏิบัติงานของระบบที่มีรายละเอียดเพิ่มเติมตามความต้องการของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อให้สามารถบริหารจัดการระบบที่รับมอบต่อไปได้ภายหลังติดตั้งหรือตรวจรับหรือสิ้นสุดระยะเวลารับประกัน

๓.๓. ผู้ชนะการประกวดราคาต้องให้การสนับสนุนการดำเนินการของคณะกรรมการศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์กระทรวงการคลัง (Ministry of Finance Computer Security Incident Response Team : MOF-CSIRT) ตลอดระยะเวลาตามสัญญาและตลอดระยะเวลารับประกัน

.....ประธาน.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการและเลขานุการ

เอกสารแนบ ๓

เอกสารราคากลาง สำหรับโครงการพัฒนาโครงสร้างพื้นฐานศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์กระทรวงการคลัง

๑. การพิจารณาราคากลางตามพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. ๒๕๖๐ มาตรา ๔

๒. ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและรายละเอียดค่าใช้จ่ายการจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง (แบบ บก.๐๖)

๓. รายละเอียดการพิจารณากำหนดราคากลาง และใบเสนอราคาของผู้ประกอบการ จำนวน ๓ ราย