โครงการ

ปรับปรุงประสิทธิภาพการเฝ้าระวังภัยคุกคาม

ด้าน Cyber Security

ร่างขอบเขตของงาน

ร่างขอบเขตของงาน (Terms of Reference: TOR)
โครงการปรับปรุงประสิทธิภาพการเฝ้าระวังภัยคุกคามด้าน Cyber Security

๑. ความเป็นมา

ในปัจจุบันภัยคุกคามทางไซเบอร์มีความซับซ้อนและรุนแรงเพิ่มมากขึ้น ส่งผลต่อการรักษาความปลอดภัยทางสารสนเทศที่จำเป็นต้องปรับเปลี่ยนอย่างสม่ำเสมอ เพื่อให้ตอบสนองต่อภัยคุกคามที่มีเพิ่มมากขึ้นตลอดเวลา รวมถึงความจำเป็นของหน่วยงานภาครัฐต้องปฏิบัติตามเพื่อให้สอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และการเก็บข้อมูลจราจรทางคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ รวมถึงกฎหมายอื่นที่เกี่ยวข้อง เช่น พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ เป็นต้น ซึ่งเป็นความจำเป็นที่ กรมสรรพสามิต จะต้องดำเนินการพัฒนาขีดความสามารถในด้านความปลอดภัยไซเบอร์ให้สามารถป้องกัน (Protect) ตรวจพบ (Detect) และ ตอบสนอง (Response) ต่อภัยคุกคามที่ส่งผลกระทบต่อความปลอดภัยของระบบเทคโนโลยีสารสนเทศ และเป็นการเพิ่มประสิทธิภาพ กระบวนการทำงานเพื่อให้สามารถบริหารจัดการจัดเก็บภาษีให้มีประสิทธิภาพมากยิ่งขึ้น รวมถึงสามารถเตรียมความพร้อมเพื่อรับมือภัยคุกคามทางไซเบอร์ซึ่งอาจส่งผลกระทบต่อความปลอดภัยของข้อมูลและระบบเครือข่ายสารสนเทศของกรมสรรพสามิต

ดังนั้น กรมสรรพสามิต จำเป็นต้องเสริมสร้างความพร้อมในการรับมือภัยคุกคามยุคใหม่ที่มีความเร็วและเปลี่ยนแปลงอย่างไม่หยุดนิ่ง การพัฒนาปรับปรุงประสิทธิภาพการทำงานภายในศูนย์เฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ (Security Operation Center) เดิมให้มีขีดความสามารถและพร้อมในการตอบสนองต่อภัยคุกคามยุคใหม่โดยพัฒนาระบบและขีดความสามารถของอุปกรณ์ต่าง ๆ ให้มีความทันสมัยและเป็นระบบที่ตอบสนองกับปริมาณข้อมูลจำนวนมากในอนาคต

๒. วัตถุประสงค์

๒.๑ เพื่อปรับปรุงประสิทธิภาพการเฝ้าระวังภัยคุกคามด้าน Cyber Security ภายในศูนย์เฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ (Security Operation Center)

๒.๒ เพื่อนำเทคโนโลยี Big Data มาช่วยในการจัดเก็บข้อมูลเหตุการณ์ (Log) พร้อมทั้งประยุกต์ใช้เทคโนโลยี Machine Learning ในการตรวจหาเหตุผิดปกติ (Anomaly) รวมถึงภัยคุกคามที่อาจซ่อนเร้นหรือการละเมิดนโยบายความปลอดภัย หรือ ประเด็นด้านความปลอดภัยอื่น ๆ ที่อาจเกิดขึ้นใหม่

๒.๓ เพื่อรองรับกับการเฝ้าระวังภัยคุกคามถึงระดับ User หรือผู้ใช้งาน และแยกแยะพฤติกรรมผิดปกติของผู้ใช้งานได้ดียิ่งขึ้น

๒.๔ เพื่อเชื่อมโยงข้อมูลและเฝ้าระวังข้อมูลต่าง ๆ ของระบบงานภายในกรมสรรพสามิต ช่วยให้เพิ่มความมั่นคงปลอดภัยของระบบงาน และเป็นเพิ่มประสิทธิภาพการบริหารการจัดเก็บภาษีได้ดียิ่งขึ้น

๒.๕ เพื่อให้สอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๓. ประโยชน์ที่ได้รับ

๓.๑ กรมสรรพสามิตมีระบบ Security Incident & Event Management (SIEM) ที่มีความยืดหยุ่นและสามารถรองรับการตรวจจับภัยคุกคาม (Detect) ที่รอบด้าน

๓.๒ กรมสรรพสามิตมีศูนย์ Security Operation Center ที่มีความสามารถเพิ่มขึ้นและยกระดับในการป้องกันแก้ไขภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศของกรมสรรพสามิต

๓.๓ กรมสรรพสามิตสามารถป้องกัน (Protect) ตรวจพบ (Detect) และ ตอบสนอง (Response) ต่อภัยคุกคามที่ส่งผลกระทบแก่ความปลอดภัยของระบบเทคโนโลยีสารสนเทศ และสามารถรับมือภัยคุกคามทางไซเบอร์ซึ่งอาจส่งผลกระทบต่อความปลอดภัยของข้อมูลและระบบเครือข่ายสารสนเทศของกรมสรรพสามิต

๓.๔ กรมสรรพสามิตมีเทคโนโลยี Big Data เข้ามาช่วยในการจัดเก็บข้อมูลเหตุการณ์ (Log) ย้อนหลังพร้อมทั้งประยุกต์ใช้เทคโนโลยี Machine Learning ในการตรวจหาเหตุผิดปกติ (Anomaly) รวมถึงภัยคุกคามที่อาจซ่อนเร้น หรือการละเมิดนโยบายความปลอดภัย หรือ ประเด็นด้านความปลอดภัยอื่น ๆ ที่อาจเกิดขึ้นใหม่

๓.๕ กรมสรรพสามิตสามารถตรวจพบพฤติกรรมต้องสงสัยทั้งพฤติกรรมที่เกิดจากผู้ใช้ที่ไม่ประสงค์ดีหรือการถูกโจมตีด้วยการสวมรอยเป็นผู้ใช้ภายในจากแฮคเกอร์ภายนอก

๓.๖ กรมสรรพสามิตสามารถนำเข้าข้อมูล จาก Threat Intelligence มาใช้เพื่อเพิ่มขีดความสามารถให้สามารถตรวจพบภัยคุกคามที่ไม่รู้จักได้รวดเร็วยิ่งขึ้น

๓.๗ กรมสรรพสามิตสามารถประเมินความเสี่ยงและแยกแยะพฤติกรรมผิดปกติของผู้ใช้งาน (End-user) โดยมีระบบในการติดตามพฤติกรรมการใช้งานของผู้ใช้ตามประเภทของระบบงาน (Application) ความเสี่ยง (Risk) และ รูปแบบ (Pattern) สามารถตรวจพบพฤติกรรมต้องสงสัยทั้งพฤติกรรมที่เกิดจากผู้ใช้ที่ไม่ประสงค์ดี หรือการถูกโจมตีด้วยการสวมรอยเป็นผู้ใช้ภายในจากแฮคเกอร์ภายนอกได้

๔. คุณสมบัติของผู้เสนอราคา

๔.๑ มีความสามารถตามกฎหมาย

๔.๒ ไม่เป็นบุคคลล้มละลาย

๔.๓ ไม่อยู่ระหว่างเลิกกิจการ

๔.๔ ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

๔.๕ ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

๔.๖ มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้าง และการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

๔.๗ เป็นนิติบุคคลผู้มีอาชีพรับจ้างงานที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

๔.๘ ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่กรม ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

๔.๙ ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทยเว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

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

๔.๑๑ ผู้ยื่นข้อเสนอต้องเป็นนิติบุคคลตามกฎหมายที่จดทะเบียนในประเทศไทย ซึ่งมีวัตถุประสงค์ในการประกอบธุรกิจเป็นผู้พัฒนา หรือออกแบบติดตั้ง หรือผู้ผลิต หรือจำหน่าย หรือเช่า หรือให้เช่าซื้อทางด้านระบบคอมพิวเตอร์ หรือระบบเทคโนโลยีสารสนเทศ หรือระบบเครือข่ายคอมพิวเตอร์ โดยมีหลักฐานการจดทะเบียนซึ่งกรมพัฒนาธุรกิจการค้ากระทรวงพาณิชย์ ออกให้หรือรับรองให้ไม่เกิน ๖ เดือน นับจนถึงวันยื่นเอกสารเสนอราคา

๔.๑๒ ผู้ยื่นข้อเสนอ ผู้เสนอราคาต้องได้รับการแต่งตั้งให้เป็นตัวแทนจำหน่ายจากผู้ผลิตหรือตัวแทนจำหน่ายในประเทศไทย โดยให้ยื่นขณะเข้าเสนอราคา

๔.๑๓ ผู้ยื่นข้อเสนอต้องเคยมีผลงาน ในด้านการติดตั้งระบบรักษาความปลอดภัย (security) หรือผลงานที่มีลักษณะใกล้เคียงกัน โดยมีผลงานไม่ต่ำกว่า ๒๐,๐๐๐,๐๐๐ บาท (ยี่สิบล้านบาทถ้วน) ต่อ ๑ สัญญา และเป็นผลงานที่ได้ทำสัญญาโดยตรงกับส่วนราชการหรือรัฐวิสาหกิจ โดยต้องเสนอสำเนาเอกสารสัญญาพร้อมเอกสารแนบท้ายสัญญา หรือสำเนาหนังสือรับรองผลงานจากหน่วยงานเจ้าของงาน

๕. แบบรูปรายการ หรือคุณลักษณะเฉพาะ

รายละเอียดคุณลักษณะเฉพาะของระบบเฝ้าระวังภัยคุกคามด้าน Cyber Security

ลำดับ	รายการ	จำนวน	หน่วย
๑.	เครื่องคอมพิวเตอร์แม่ข่าย (Server)		
๑.๑	เครื่องคอมพิวเตอร์แม่ข่าย (Server) แบบที่ ๑	๑	หน่วย
๑.๒	เครื่องคอมพิวเตอร์แม่ข่าย (Server) แบบที่ ๒	๔	หน่วย
๑.๓	เครื่องคอมพิวเตอร์แม่ข่าย (Server) แบบที่ ๓	๒	หน่วย
๒.	ระบบบริหารจัดการความปลอดภัยสารสนเทศ (SIEM)	๑	ระบบ
๓.	ระบบวิเคราะห์ตัวตนและผู้ใช้ (User and Entity Behavior Analysis หรือ UEBA)	๑	ระบบ
๔.	พัฒนาและจัดทำ use case และการแจ้งเตือนการเฝ้าระวังด้านความปลอดภัย	๑	งาน

ลำดับ	รายการ	จำนวน	หน่วย
๕.	พัฒนาและจัดทำหน้าจอรายงานการแจ้งเตือนการเฝ้าระวังด้านความปลอดภัย	๑	งาน
๖.	การฝึกอบรม	๒	หลักสูตร

๖. ระยะเวลาการดำเนินโครงการ

ระยะเวลาการดำเนินงาน ๑๘๐ วัน นับถัดจากวันลงนามในสัญญา

๗. ระยะเวลาการส่งมอบงาน

ผู้ชนะการประกวดต้องส่งมอบงานตามงวดงาน ดังนี้

งวดที่ ๑ ภายใน ๓๐ วัน นับถัดจากวันลงนามในสัญญาส่งมอบเอกสารแผนการดำเนินโครงการและการออกแบบ การติดตั้งรูปแบบแผนผังเครือข่าย (Network Diagram) แบบแสดงการวางอุปกรณ์ (Rack Layout) แผนการทดสอบอุปกรณ์ทั้งหมด

งวดที่ ๒ ภายใน ๙๐ วัน นับถัดจากวันลงนามในสัญญาโดยต้องส่งมอบงานดังนี้

๑) ส่งมอบอุปกรณ์ ตามเอกสารหมายเลข ๑ ลำดับที่ ๑

๒) ส่งมอบระบบโปรแกรมและสิทธิ์การใช้งาน (license) ของอุปกรณ์รักษาความปลอดภัย ตามเอกสารหมายเลข ๑ ลำดับที่ ๒ และลำดับที่ ๓

งวดที่ ๓ ภายใน ๑๘๐ วัน นับถัดจากวันลงนามในสัญญาโดยต้องส่งมอบงานดังนี้

๑) พัฒนาและจัดทำ use case และการแจ้งเตือนการเฝ้าระวังด้านความปลอดภัย

๒) พัฒนาและจัดทำหน้าจอรายงานการแจ้งเตือนการเฝ้าระวังด้านความปลอดภัย

๓) ส่งมอบการติดตั้งและทดสอบระบบเฝ้าระวังภัยคุกคามด้าน Cyber Security

๔) จัดฝึกอบรม ตามเอกสารหมายเลข ๓

๘. ข้อกำหนดด้านการชำระเงิน

กรมสรรพสามิตจะชำระเงินตามจำนวนในสัญญาตามแต่ละงวดดังนี้

งวดที่ ๑ ชำระเงินในอัตรา ร้อยละ ๕ ของมูลค่าตามสัญญาหลังจากกรมสรรพสามิตตรวจรับงานของงวดงานที่ ๑ เรียบร้อยแล้ว

งวดที่ ๒ ชำระเงินในอัตรา ร้อยละ ๖๕ ของมูลค่าตามสัญญาหลังจากกรมสรรพสามิตตรวจรับงานของงวดงานที่ ๒ เรียบร้อยแล้ว

งวดที่ ๓ ชำระเงินในอัตรา ร้อยละ ๓๐ ของมูลค่าตามสัญญาหลังจากกรมสรรพสามิตตรวจรับงานของงวดงานที่ ๓ เรียบร้อยแล้ว

๙. การรับประกัน

ผู้รับจ้างต้องรับประกันความชำรุดบกพร่อง เป็นระยะเวลา ๑ ปี โดยมีการรับประกันในลักษณะการเข้ามาดำเนินการแก้ไขซ่อมแซมอุปกรณ์ (On-site Service) (เข้ามาตรวจสอบแก้ไข ณ กรมสรรพสามิต ในกรณีที่เกิดการขัดข้องในการใช้งาน) นับถัดจากวันที่กรมสรรพสามิตได้ตรวจรับเป็นที่เรียบร้อยแล้ว

๑๐. สถานที่ติดตั้ง

ศูนย์เทคโนโลยีสารสนเทศ กรมสรรพสามิต

๑๑. วงเงินค่าใช้จ่าย

รวมทั้งสิ้น ๔๖,๒๘๘,๘๐๐ บาท (สี่สิบหกล้านสองแสนแปดหมื่นแปดพันแปดร้อยบาทถ้วน)

๑๒. หลักเกณฑ์การพิจารณา

ในการพิจารณาผลการยื่นข้อเสนอประกวดราคาอิเล็กทรอนิกส์ครั้งนี้จะพิจารณาตัดสินโดยใช้หลักเกณฑ์ราคาพิจารณาจากราคารวม

๑๓. หน่วยงานผู้รับผิดชอบ

ศูนย์เทคโนโลยีสารสนเทศ กรมสรรพสามิต

โทร. ๐๒๒๔๑ ๕๖๐๐-๑๙ ต่อ ๖๓๕๐๑ e-mail: surasak_wo@excise.go.th