โครงการเพิ่มประสิทธิภาพการบริหารจัดการระบบป้องกัน และรักษาความมั่นคงปลอดภัยด้านข้อมูลสารสนเทศ กรมสรรพสามิต

ร่างขอบเขตของงาน (TOR)

ร่างขอบเขตของงาน (Terms of Reference : TOR)
โครงการเพิ่มประสิทธิภาพการบริหารจัดการระบบป้องกัน
และรักษาความมั่นคงปลอดภัยด้านข้อมูลสารสนเทศ กรมสรรพสามิต

.....

๑. ความเป็นมา

ในปัจจุบันภัยคุมคามทางไซเบอร์มีความซับซ้อนและรุนแรงเพิ่มมากขึ้น ส่งผลต่อการรักษาความปลอดภัยทางสารสนเทศที่จำเป็นต้องปรับเปลี่ยนอย่างสม่ำเสมอ เพื่อให้ตอบสนองต่อภัยคุกคามที่มีเพิ่มมากขึ้นตลอด รวมถึงความจำเป็นของหน่วยงานภาครัฐต้องปฏิบัติตามเพื่อให้สอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๔ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ เพื่อเตรียมความพร้อมในการรับมือภัยคุกคามทางไซเบอร์รูปแบบต่าง ๆ และเป็นการปฏิบัติตามข้อกำหนดพระราชบัญญัติทั้งสองฉบับ ซึ่งเป็นความจำเป็นที่ กรมสรรพสามิต จะต้องดำเนินการพัฒนาขีดความสามารถในด้านความปลอดภัยไซเบอร์ให้สามารถป้องกัน (Protect) ตรวจพบ (Detect) และ ตอบสนอง (Response) ต่อภัยคุกคามที่ส่งผลกระทบต่อความปลอดภัยของระบบเทคโนโลยีสารสนเทศ และเป็นการเพิ่มประสิทธิภาพ กระบวนการทำงานเพื่อให้สามารถบริหารจัดการจัดเก็บภาษีให้มีประสิทธิภาพมากยิ่งขึ้น รวมถึงสามารถเตรียมความพร้อมเพื่อรับมือภัยคุกคามทางไซเบอร์ซึ่งอาจส่งผลกระทบต่อความปลอดภัยของข้อมูล และระบบเครือข่ายสารสนเทศของ กรมสรรพสามิต

ดังนั้น กรมสรรพสามิต จำเป็นต้องเสริมสร้างความพร้อมในการรับมือภัยคุกคามยุคใหม่ที่มีความเร็ว และเปลี่ยนแปลงอย่างไม่หยุดนิ่ง การพัฒนาปรับปรุงประสิทธิภาพการทำงานภายในศูนย์เฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ (Security Operation Center) เดิมให้มีขีดความสามารถ และพร้อมในการตอบสนองต่อภัยคุกคามยุคใหม่โดยพัฒนาระบบ และขีดความสามารถของอุปกรณ์ต่าง ๆ ให้มีความทันสมัย

๒. วัตถุประสงค์

๒.๑ เพื่อสนับสนุนให้ศูนย์ปฏิบัติการความมั่นคงปลอดภัยและเฝ้าระวังความมั่นคงปลอดภัยสารสนเทศ กรมสรรพสามิต (SOC) มีความพร้อมในการเฝ้าระวังและรับมือต่อสถานการณ์ภัยคุกคามทางไซเบอร์ในรูปแบบใหม่ที่เกิดขึ้นต่อระบบสารสนเทศของกรมสรรพสามิต

๒.๒ เพื่อให้กรมสรรพสามิตมีข้อมูลภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในหน่วยงาน สำหรับใช้ในการวางแผนรับมือในอนาคต และแจ้งเตือนให้ผู้ใช้งานระบบสารสนเทศของกรมสรรพสามิตป้องกันข้อมูลที่มีความสำคัญให้ปลอดภัยได้อย่างทันท่วงที

๒.๓ เพื่อสนับสนุนให้ศูนย์ปฏิบัติการความมั่นคงปลอดภัยและเฝ้าระวังความมั่นคงปลอดภัยสารสนเทศ กรมสรรพสามิต มีอุปกรณ์ด้านความมั่นคงปลอดภัยสารสนเทศ ในการป้องกันการโจมตีในรูปแบบต่าง ๆ และมีเครื่องมือสำหรับใช้ในการตรวจหาจุดอ่อนของระบบสารสนเทศ รวมทั้งการบริการจัดการข้อมูล ช่องโหว่ของระบบสารสนเทศภายในกรมสรรพสามิต เพื่อนำมาใช้เป็นข้อมูลในการแก้ไขปัญหาและป้องกันการถูกโจมตีจากผู้ไม่ประสงค์ดีได้ในอนาคต

๒.๔ เพื่อลดความเสี่ยงจากภัยคุกคามทางไซเบอร์และเตรียมความพร้อมสำหรับยุค ๔.๐ ตามนโยบายของรัฐบาลอย่างมีประสิทธิภาพ

๓. คุณสมบัติของผู้ประสงค์เสนอราคา

๓.๑ มีความสามารถตามกฎหมาย

๓.๒ ไม่เป็นบุคคลล้มละลาย

๓.๓ ไม่อยู่ระหว่างเลิกกิจการ

๓.๔ ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลงานการปฏิบัติงานของผู้ประกอบการตามระเบียบรัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

๓.๕ ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วน ผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

๓.๖ มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

๓.๗ เป็นนิติบุคคล ผู้มีอาชีพรับจ้างงานที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

๓.๘ ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้เสนอราคารายอื่นที่เข้ายื่นเสนอราคาให้แก่กรมสรรพสามิต ณ วันที่ประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรม ในการประกวดราคาอิเล็กทรอนิกส์นี้

๓.๙ ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้เสนอราคาได้มีคำสั่งให้สละสิทธิ์ความคุ้มกันเช่นว่านั้น

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

๓.๑๑ ผู้ยื่นข้อเสนอต้องเคยมีผลงาน ในด้านการติดตั้งอุปกรณ์คอมพิวเตอร์ หรือพัฒนาระบบงานด้านเทคโนโลยีสารสนเทศ หรือระบบงานคอมพิวเตอร์โดยมีผลงานไม่ต่ำกว่า ๑๘,๐๐๐,๐๐๐ บาท (สิบแปดล้านบาทถ้วน) จำนวน ๑ สัญญา และเป็นผลงานที่ได้ทำสัญญาโดยตรงกับส่วนราชการ โดยต้องเสนอสำเนาเอกสารสัญญาพร้อมเอกสารแนบท้ายสัญญา หรือสำเนาหนังสือรับรองผลงานจากหน่วยงานเจ้าของงาน

๔. แบบรูปรายการ หรือคุณลักษณะเฉพาะ

รายละเอียดคุณลักษณะเฉพาะของระบบคอมพิวเตอร์ มีรายการ ดังนี้

ลำดับ	รายการ	จำนวน	หน่วย
๑	ระบบบริหารการจัดการภัยและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ (Security Orchestration, Automation and Response (SOAR))	๑	ระบบ
๒	ระบบตรวจจับและหยุดยั้งการโจมตีประเภท Distributed Denial of Service (DDoS)	๒	ชุด
๓	ระบบป้องกันภัยคุกคามเว็บแอพพลิเคชั่น (Web Application Firewall)	๒	ชุด
๔	ระบบตรวจจับภัยคุกคามและวิเคราะห์ความเสี่ยงภายในเครือข่ายสำหรับศูนย์ SOC (Network Threat Analysis)	๑	ระบบ
๕	ระบบตรวจสอบและบริหารจัดการช่องโหว่ด้านความมั่นคงปลอดภัยสารสนเทศ (Vulnerability Management System)	๑	ระบบ
๖	หลักสูตรฝึกอบรมจำนวน ๑ หลักสูตร		
	- หลักสูตรผู้ดูแลระบบจำนวน ๑๐ คน	๕	หลักสูตร

๕. ระยะเวลาการดำเนินการ

จำนวน ๑๒๐ วัน นับถัดจากวันที่ลงนามในสัญญา

๖. ระยะเวลาการส่งมอบงาน

ผู้ชนะการประกวดราคาต้องส่งมอบงานตามงวดงาน ดังนี้

<u>งวดที่ ๑</u> ภายใน ๓๐ วัน นับถัดจากวันลงนามในสัญญา โดยต้องส่งมอบงาน ดังนี้

(๑) ส่งมอบเอกสารแผนการดำเนินงาน (Project Plan)

(๒) ส่งมอบเอกสารแผนการติดตั้ง และแผนการทดสอบอุปกรณ์ทั้งหมด

<u>งวดที่ ๒</u> ภายใน ๙๐ วัน นับถัดจากวันลงนามในสัญญา โดยต้องส่งมอบงาน ดังนี้

(๑) ส่งมอบระบบบริหารการจัดการภัยและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ (Security Orchestration, Automation and Response (SOAR))

(๒) ส่งมอบระบบตรวจจับและหยุดยั้งการโจมตีประเภท Distributed Denial of Service (DDoS)

(๓) ส่งมอบระบบป้องกันภัยคุกคามเว็บแอพพลิเคชั่น (Web Application Firewall)

(๔) ส่งมอบระบบตรวจจับภัยคุกคามและวิเคราะห์ความเสี่ยงภายในเครือข่ายสำหรับศูนย์ SOC (Network Threat Analysis)

(๕) ส่งมอบระบบตรวจสอบและบริหารจัดการช่องโหว่ด้านความมั่นคงปลอดภัยสารสนเทศ (Vulnerability Management System)

งวดที่ ๓ ภายใน ๑๒๐ วัน นับถัดจากวันลงนามในสัญญา โดยต้องส่งมอบงาน ดังนี้

(๑) ส่งมอบการฝึกอบรม ตาม**เอกสารหมายเลข ๓**

(๒) ส่งมอบเอกสารคู่มือผู้ดูแลระบบ (Admin Manual) ฉบับภาษาไทย

(๓) ส่งมอบงานอื่น ๆ ที่ยังไม่ได้ส่งมอบการจัดจ้างตามโครงการฯ (ถ้ามี)

๗. ข้อกำหนดด้านการชำระเงิน

กรมสรรพสามิตจะชำระเงินตามจำนวนในสัญญาตามแต่ละงวดดังนี้

งวดที่ ๑ ชำระเงินในอัตราร้อยละ ๕ ของวงเงินที่จ้างตามสัญญา หลังจากกรมสรรพสามิตตรวจรับงานในงวดที่ ๑ เรียบร้อยแล้ว

งวดที่ ๒ ชำระเงินในอัตราร้อยละ ๘๕ ของวงเงินที่จ้างตามสัญญา หลังจากกรมสรรพสามิตตรวจรับงานในงวดที่ ๒ เรียบร้อยแล้ว

งวดที่ ๓ ชำระเงินในอัตราร้อยละ ๑๐ ของวงเงินที่จ้างตามสัญญา หลังจากกรมสรรพสามิตตรวจรับงานในงวดที่ ๓ เรียบร้อยแล้ว

๘. การรับประกัน

ผู้ชนะการประกวดราคาจะต้องรับประกันความชำรุดบกพร่อง หรือความขัดข้องของ“ระบบงานและอุปกรณ์” เป็นระยะเวลาไม่น้อยกว่า ๒ ปี นับจากวันที่กรมสรรพสามิตได้ตรวจรับมอบงานครบถ้วนตามสัญญาเป็นที่เรียบร้อยแล้ว

๙. สถานที่ติดตั้ง

ศูนย์เทคโนโลยีสารสนเทศ กรมสรรพสามิต

๑๐. วงเงินค่าใช้จ่าย

เงินฝากค่าใช้จ่ายเก็บภาษีท้องถิ่น ปีงบประมาณ พ.ศ. ๒๕๖๕ รวมเป็นเงินจำนวนทั้งสิ้น ๔๐,๐๐๐,๐๐๐ บาท (สี่สิบล้านบาทถ้วน) ซึ่งเป็นราคารวมภาษีมูลค่าเพิ่มแล้ว และค่าใช้จ่ายต่าง ๆ ทั้งปวงไว้ด้วยแล้ว

๑๑. หลักเกณฑ์การพิจารณา

ในการพิจารณาผลการยื่นข้อเสนอประกวดราคาอิเล็กทรอนิกส์ครั้งนี้จะพิจารณาตัดสินโดยใช้หลักเกณฑ์ราคาพิจารณาจากราคารวม

๑๒. หน่วยงานผู้รับผิดชอบ

ศูนย์เทคโนโลยีสารสนเทศ กรมสรรพสามิต

โทร ๐-๒๒๔๑-๕๖๐๐-๑๙ ต่อ ๖๓๕๐๑ e-mail: surasak_wo@excise.go.th

เอกสารหมายเลข ๑

รายละเอียดหลักเกณฑ์ และข้อกำหนด

รายละเอียดหลักเกณฑ์ และข้อกำหนด
โครงการเพิ่มประสิทธิภาพการบริหารจัดการระบบป้องกัน
และรักษาความมั่นคงปลอดภัยด้านข้อมูลสารสนเทศ ของกรมสรรพสามิต

โครงการเพิ่มประสิทธิภาพการบริหารจัดการระบบป้องกันและรักษาความมั่นคงปลอดภัยด้านข้อมูลสารสนเทศ ของกรมสรรพสามิต ซึ่งต่อไปนี้เรียกว่า "ระบบคอมพิวเตอร์" ซึ่งประกอบด้วย

ลำดับ	รายการ	จำนวน	หน่วย
๑	ระบบบริหารการจัดการภัยและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ (Security Orchestration, Automation and Response (SOAR))	๑	ระบบ
๒	ระบบตรวจจับและหยุดยั้งการโจมตีประเภท Distributed Denial of Service (DDoS)	๒	ชุด
๓	ระบบป้องกันภัยคุกคามเว็บแอพพลิเคชั่น (Web Application Firewall)	๒	ชุด
๔	ระบบตรวจจับภัยคุกคามและวิเคราะห์ความเสี่ยงภายในเครือข่ายสำหรับศูนย์ SOC (Network Threat Analysis)	๑	ระบบ
๕	ระบบตรวจสอบและบริหารจัดการช่องโหว่ด้านความมั่นคงปลอดภัยสารสนเทศ (Vulnerability Management System)	๑	ระบบ
๖	หลักสูตรฝึกอบรมจำนวน ๑ หลักสูตร		
	- หลักสูตรผู้ดูแลระบบจำนวน ๑๐ คน	๕	หลักสูตร

หมายเหตุ ผู้เสนอราคาจะต้องศึกษารายละเอียดและระบบคอมพิวเตอร์ตามเอกสารหมายเลข ๒

ผู้ยื่นข้อเสนอราคาต้องดำเนินการให้เป็นไปตามเงื่อนไขต่าง ๆ ดังต่อไปนี้

๑. ข้อกำหนดด้านเอกสารการเสนอราคา

๑.๑ ผู้ยื่นข้อเสนอจัดทำข้อเสนอด้านคุณลักษณะเฉพาะของงานตามเอกสารการประกวดราคาจ้างด้วยวิธีการทางอิเล็กทรอนิกส์ โดยให้จัดทำในรูปแบบ ดังนี้

หัวข้อ	ระบบงานตามเอกสารประกวดราคา	ข้อเสนอของบริษัท	เอกสารอ้างอิง (หน้า,ข้อ)
ระบุหัวข้อให้ตรงกับกรมสรรพสามิตกำหนด	ให้คัดลอกคุณลักษณะเฉพาะที่กรมสรรพสามิตกำหนด	ให้ระบุคุณลักษณะเฉพาะของระบบที่เสนอ	ให้ระบุหรืออ้างถึงเอกสารในข้อเสนอที่เกี่ยวข้องและขีดเส้นใต้คุณลักษณะที่เสนอในแคตตาล็อกหรือเอกสารที่เกี่ยวข้อง (ถ้ามี)

๑.๒ ผู้ยื่นข้อเสนอ ต้องจัดทำสารบัญเอกสารอ้างอิง และเอกสารอ้างอิง ตามสารบัญเอกสารอ้างอิงให้มีความครบถ้วนสมบูรณ์

๑.๓ ผู้ชนะการประกวดราคาฯ จะต้องเสนอรายละเอียดการฝึกอบรมและการสนับสนุนโดยให้มีรายละเอียดตามเอกสารหมายเลข ๓ เป็นอย่างน้อย

๑.๔ ผู้ยื่นข้อเสนอราคาจะต้องเสนอรายละเอียดข้อเสนอด้านคุณสมบัติของผู้เสนอราคา และบุคลากร **ตามเอกสารหมายเลข ๕ ดังนี้**

๑.๔.๑ ผู้จัดการโครงการ (Project Manager) จำนวน ๑ คน

- มีวุฒิการศึกษาขั้นต่ำปริญญาโท ที่เกี่ยวข้องกับด้านคอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศ
- มีประสบการณ์ที่เกี่ยวข้อง เป็นระยะเวลาอย่างน้อย ๑๑ ปี

๑.๔.๒ ผู้ช่วยผู้จัดการโครงการ (Assistant Project Manager) จำนวน ๑ คน

- มีวุฒิการศึกษาขั้นต่ำปริญญาตรี ที่เกี่ยวข้องกับด้านคอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศ
- มีประสบการณ์ที่เกี่ยวข้อง เป็นระยะเวลาอย่างน้อย ๕ ปี

๑.๔.๓ นักวิเคราะห์ระบบ (System Analyst) จำนวน ๑ คน

- มีวุฒิการศึกษาขั้นต่ำปริญญาตรี ที่เกี่ยวข้องกับด้านคอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศ
- มีประสบการณ์ที่เกี่ยวข้อง เป็นระยะเวลาอย่างน้อย ๕ ปี

๑.๔.๔ วิศวกรระบบ (System Engineer) จำนวน ๑ คน

- มีวุฒิการศึกษาขั้นต่ำปริญญาตรี ที่เกี่ยวข้องกับด้านคอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศ
- มีประสบการณ์ที่เกี่ยวข้อง เป็นระยะเวลาอย่างน้อย ๕ ปี

๑.๔.๕ วิศวกรระบบ Security (Security Engineer) จำนวน ๑ คน

- มีวุฒิการศึกษาขั้นต่ำปริญญาตรี ที่เกี่ยวข้องกับด้านคอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศ
- มีประสบการณ์ที่เกี่ยวข้อง เป็นระยะเวลาอย่างน้อย ๕ ปี

๑.๔.๖ วิศวกรเครือข่าย (Network Engineer) จำนวน ๑ คน

- มีวุฒิการศึกษาขั้นต่ำปริญญาตรี ที่เกี่ยวข้องกับด้านคอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศ
- มีประสบการณ์ที่เกี่ยวข้อง เป็นระยะเวลาอย่างน้อย ๕ ปี

๑.๔.๗ เจ้าหน้าที่ประสานงาน (Administrative office) จำนวน ๑ คน

- มีวุฒิการศึกษาขั้นต่ำปริญญาตรี ที่เกี่ยวข้องกับด้านคอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศ
- มีประสบการณ์ที่เกี่ยวข้อง เป็นระยะเวลาอย่างน้อย ๑ ปี

๑.๔.๘ เจ้าหน้าที่ตอบคำถามให้ความช่วยเหลือ และประสานงานโครงการ (Help Desk) จำนวน ๑ คน

- มีวุฒิการศึกษาขั้นต่ำปริญญาตรี ที่เกี่ยวข้องกับให้ด้านคอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศ
- มีประสบการณ์ที่เกี่ยวข้อง เป็นระยะเวลาอย่างน้อย ๑ ปี

๒. ข้อกำหนดทั่วไป ของระบบคอมพิวเตอร์ที่เสนอ

๒.๑ คุณสมบัติของระบบงาน และขอบเขตการดำเนินงานที่กำหนดไว้ **ตามเอกสารหมายเลข ๒** เป็นข้อมูลเบื้องต้นซึ่งอาจมีการปรับเปลี่ยน โดยคู่สัญญาต้องจัดส่งทีมงานตามที่เสนอมาดำเนินการรวบรวม และวิเคราะห์ความต้องการของระบบในรายละเอียดอีกครั้ง

๒.๒ อุปกรณ์ ฮาร์ดแวร์ และซอฟต์แวร์ที่เสนอใช้ในโครงการต้องเป็นรุ่น Version ล่าสุด ในวันยื่นประกวดราคาจ้างด้วยวิธีอิเล็กทรอนิกส์ในครั้งนี้ และระบบคอมพิวเตอร์ที่จะนำมาติดตั้งให้กรมสรรพสามิตจะต้องเป็นเครื่องใหม่ (New) ไม่ใช่เครื่องเก่าใช้แล้ว (Used) หรือเครื่องล้าสมัย (Obsolete) หรือเครื่องที่ใช้งานแล้วและนำมาปรับปรุงใหม่ (Reconditioned)

๒.๓ อุปกรณ์ ฮาร์ดแวร์ และซอฟต์แวร์ ที่เสนอต้องไม่เป็นผลิตภัณฑ์ของบริษัทผู้ผลิตที่อยู่ในระหว่างการคุ้มครอง การเป็นบุคคลหรือนิติบุคคลผู้ล้มละลายตามคำสั่งของศาลที่ได้สั่งการตามกฎหมายของประเทศที่บริษัทของผู้ผลิตนั้นตั้งอยู่

๒.๔ อุปกรณ์ ฮาร์ดแวร์ และซอฟต์แวร์ ที่เสนอให้รวมค่าติดตั้งและค่าอุปกรณ์อื่นเชื่อมต่อเข้ากับระบบเครือข่ายของกรมสรรพสามิต รวมถึงค่าใช้จ่ายในการดำเนินการต่าง ๆ ที่ต้องมีเพื่อให้ระบบงานสามารถทำงานร่วมกันได้อย่างมีประสิทธิภาพ โดยกรมสรรพสามิตไม่ต้องเสียค่าใช้จ่ายใด ๆ เพิ่มเติมจากที่ปรากฏในใบเสนอราคา

๒.๕ ผู้ชนะการประกวดราคาต้องเป็นผู้รับผิดชอบในการติดตั้ง “ระบบคอมพิวเตอร์” และอุปกรณ์อื่นที่กรมสรรพสามิตจัดเตรียมไว้ ให้สามารถทำงานร่วมกันได้อย่างมีประสิทธิภาพ และใช้งานได้จริง

๓. ข้อกำหนดด้านการติดตั้งและส่งมอบงาน

ผู้ชนะการประกวดราคาต้องส่งมอบงานตามงวดงาน ดังนี้

<u>งวดที่ ๑</u> ภายใน ๓๐ วัน นับถัดจากวันลงนามในสัญญา โดยต้องส่งมอบงาน ดังนี้

(๑) ส่งมอบเอกสารแผนการดำเนินงาน (Project Plan)

(๒) ส่งมอบเอกสารแผนการติดตั้ง และแผนการทดสอบอุปกรณ์ทั้งหมด

<u>งวดที่ ๒</u> ภายใน ๙๐ วัน นับถัดจากวันลงนามในสัญญา โดยต้องส่งมอบงาน ดังนี้

(๑) ส่งมอบระบบบริหารการจัดการภัยและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ (Security Orchestration, Automation and Response (SOAR))

(๒) ส่งมอบระบบตรวจจับและหยุดยั้งการโจมตีประเภท Distributed Denial of Service (DDoS)

(๓) ส่งมอบระบบป้องกันภัยคุกคามเว็บแอพพลิเคชั่น (Web Application Firewall)

(๔) ส่งมอบระบบตรวจจับภัยคุกคามและวิเคราะห์ความเสี่ยงภายในเครือข่ายสำหรับศูนย์ SOC (Network Threat Analysis)

(๕) ส่งมอบระบบตรวจสอบและบริหารจัดการช่องโหว่ด้านความมั่นคงปลอดภัยสารสนเทศ (Vulnerability Management System)

<u>งวดที่ ๓</u> ภายใน ๑๒๐ วัน นับถัดจากวันลงนามในสัญญา โดยต้องส่งมอบงาน ดังนี้

(๑) ส่งมอบการฝึกอบรม ตาม**เอกสารหมายเลข ๓**

(๒) ส่งมอบเอกสารคู่มือผู้ดูแลระบบ (Admin Manual) ฉบับภาษาไทย

(๓) ส่งมอบงานอื่น ๆ ที่ยังไม่ได้ส่งมอบการจัดจ้างตามโครงการฯ (ถ้ามี)

๔. ข้อกำหนดด้านการตรวจรับ

การส่งมอบและการตรวจรับ “ระบบคอมพิวเตอร์” ทั้งหมดตามรายละเอียดในเอกสารแนบการเสนอราคา จะถือว่าเสร็จสมบูรณ์ เมื่อมีการตรวจรับ “ระบบคอมพิวเตอร์” ตามสัญญาซื้อขายเสร็จเรียบร้อยสมบูรณ์แล้วทั้งหมดว่าสามารถใช้งานจริงได้อย่างมีประสิทธิภาพ โดยมีรายละเอียด ดังนี้

คณะกรรมการตรวจรับพัสดุ จะทดสอบและตรวจรับงาน ตามรายละเอียดการทดสอบการใช้งาน “ระบบคอมพิวเตอร์” เอกสารต่าง ๆ ตามที่กำหนด เมื่อกรมสรรพสามิตได้รับหนังสือแจ้งจากคู่สัญญาว่าได้ติดตั้งเสร็จเรียบร้อยแล้ว ตามงวดการส่งมอบงานต่าง ๆ

๕. ข้อกำหนดด้านการชำระเงิน

กรมสรรพสามิตจะชำระเงินตามจำนวนในสัญญาตามแต่ละงวดงาน ดังนี้

งวดที่ ๑ ชำระเงินในอัตราร้อยละ ๕ ของวงเงินที่จ้างตามสัญญา หลังจากกรมสรรพสามิตตรวจรับงานในงวดที่ ๑ เรียบร้อยแล้ว

งวดที่ ๒ ชำระเงินในอัตราร้อยละ ๘๕ ของวงเงินที่จ้างตามสัญญา หลังจากกรมสรรพสามิตตรวจรับงานในงวดที่ ๒ เรียบร้อยแล้ว

งวดที่ ๓ ชำระเงินในอัตราร้อยละ ๑๐ ของวงเงินที่จ้างตามสัญญา หลังจากกรมสรรพสามิตตรวจรับงานในงวดที่ ๓ เรียบร้อยแล้ว

๖. ข้อกำหนดด้านการบำรุงรักษา

๖.๑ ผู้ชนะการประกวดราคาจะต้องรับประกันความชำรุดบกพร่อง หรือความขัดข้องของ“ระบบงานและอุปกรณ์” เป็นระยะเวลาไม่น้อยกว่า ๒ ปี นับจากวันที่กรมสรรพสามิตได้ตรวจรับมอบงานครบถ้วนตามสัญญาเป็นที่เรียบร้อยแล้ว และภายในกำหนดเวลาดังกล่าวหาก “ระบบงานและอุปกรณ์” เกิดความชำรุดบกพร่อง หรือขัดข้องอันเนื่องมาจากการใช้งานตามปกติ ผู้ชนะการประกวดราคาต้องเริ่มจัดการแก้ไขภายใน ๓ วันทำการ นับแต่ได้รับแจ้งจากกรมสรรพสามิต โดยไม่ทำให้ระบบหยุดชะงักหรือเกิดความเสียหายแก่ทางราชการ หากผู้ชนะการประกวดราคาไม่เริ่มดำเนินการแก้ไขข้อขัดข้องได้ภายในเวลาดังกล่าว ผู้ชนะการประกวดราคาจ้างด้วยวิธีการทางอิเล็กทรอนิกส์ต้องชำระค่าปรับตามค่าปรับ **ตามเอกสารหมายเลข ๔**

เอกสารหมายเลข ๒

คุณลักษณะเฉพาะของระบบคอมพิวเตอร์

รายละเอียดคุณลักษณะเฉพาะของระบบคอมพิวเตอร์
โครงการเพิ่มประสิทธิภาพการบริหารจัดการระบบป้องกัน
และรักษาความมั่นคงปลอดภัยด้านข้อมูลสารสนเทศ กรมสรรพสามิต

"ระบบคอมพิวเตอร์" ที่กรมสรรพสามิต จัดซื้อในครั้งนี้ต้องเป็นของแท้ ของใหม่ ไม่เคยใช้งานมาก่อน ไม่เป็นของเก่าเก็บ ต้องอยู่ในสภาพที่จะใช้งานได้ทันที โดยคุณลักษณะเฉพาะของ **"ระบบคอมพิวเตอร์"** จะต้องเหมาะสมกับลักษณะงานของกรมสรรพสามิตตามโครงการนี้ และสามารถทำงานได้อย่างมีประสิทธิภาพ สะดวกต่อการใช้งาน โดยผู้ประสงค์จะเสนอราคาต้องเสนอ "ระบบคอมพิวเตอร์" ที่มีคุณลักษณะเฉพาะไม่ต่ำกว่าที่ระบุในเอกสารนี้

เงื่อนไขทั่วไปในการติดตั้ง "ระบบคอมพิวเตอร์"

ผู้ชนะการประกวดราคาต้องจัดหาอุปกรณ์หรือซอฟต์แวร์ที่จำเป็นสำหรับการทำงานของโครงการเพิ่มประสิทธิภาพการบริหารจัดการระบบป้องกันและรักษาความมั่นคงปลอดภัยด้านข้อมูลสารสนเทศ กรมสรรพสามิต ให้สามารถทำงานได้อย่างสมบูรณ์ โดยไม่คิดมูลค่าเพิ่มเติมจากราคาที่เสนอ โดยมีรายละเอียดคุณลักษณะเฉพาะ ดังนี้

๑. ระบบบริหารการจัดการและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ (Security Orchestration, Automation and Response (SOAR)) จำนวน ๑ ระบบ โดยมีคุณลักษณะอย่างน้อย ดังนี้

๑.๑ เป็นระบบที่ออกแบบมาเพื่อจัดการเรื่อง Security Orchestration, Automation and Response (SOAR) โดยเฉพาะ

๑.๒ เป็น Software ที่ออกแบบมาเพื่อช่วยในการบริหารการจัดการสำหรับ Security Operation Team โดยเฉพาะโดยมีเครื่องมือที่ช่วยในการทำ Accelerate Response โดยรองรับการทำงานร่วมกับระบบต่าง ๆ ดังนี้ ได้เป็นอย่างน้อย

๑.๒.๑ Security Information and Event Management (SIEM)
๑.๒.๒ Endpoint Detection and Response (EDR)
๑.๒.๓ Threats Intelligence (TI)
๑.๒.๔ Malware Analysis
๑.๒.๕ Data Loss Prevention (DLP)
๑.๒.๖ Email
๑.๒.๗ Ticketing Systems
๑.๒.๘ Users and Entity Behavior Analytic

๑.๓ มีรูปแบบการบริหารจัดการ Standardize Process และ ติดตามเหตุการณ์ที่เกิดขึ้น (incident) รวมไปถึงช่วยวิเคราะห์ (Analyst Metrics) เช่น Task-based workflows, Visual playbook editor หรือ SLA and metric tracking เป็นอย่างน้อย

๑.๔ มีหน่วยประมวลผลกลาง (CPU) ไม่น้อยกว่า ๒๔ แกนหลัก (Core) หรือดีกว่า สำหรับคอมพิวเตอร์แม่ข่าย (Server) โดยเฉพาะและมีความเร็วสัญญาณนาฬิกาพื้นฐานไม่น้อยกว่า ๒.๔ GHz จำนวน ๒ หน่วย

๑.๕ มีระบบช่วยให้ทีมผู้ดูแลระบบต่าง ๆ สามารถทำงานร่วมกัน ได้ลักษณะ Collaborate and Learn เช่น Virtual War Room หรือ มี Process Work Flow เป็นอย่างน้อย และมีระบบ Machine Learning มาช่วยในการวิเคราะห์และเชื่อมโยง เหตุการณ์ต่าง ๆ ที่เกิดขึ้นได้ หรือนำเสนอระบบอื่น ๆ เพิ่มเติมเพื่อรองรับความต้องการดังกล่าว

๑.๖ มี Play Book ที่สามารถแสดงผลในรูปแบบ Graphic User Interface (GUI) ได้

๑.๗ สามารถสร้าง Work Plan หรือ Workflow หรือ Playbook ในรูปแบบ Parallel ที่สามารถทำได้หลายงานพร้อม ๆ กัน และสามารถทำ Sub Playbook ได้ โดยมีความสามารถอย่างน้อยดังนี้

๑.๗.๑ การ Enrichment ข้อมูลร่วมกับ ข้อมูลที่ได้จาก Threat Intelligence Management หรือ Threat Intelligence Platform

๑.๗.๒ การ Enrichment ข้อมูลร่วมกับระบบงานภายนอก เช่น Active Directory

๑.๗.๓ การ Enforcement ไปยัง Protection Tools เช่น Firewall, Active Directory เป็นต้น

๑.๘ สามารถทำ Case Management เพื่อบริหารจัดการ Incident ต่าง ๆ ที่เกิดขึ้น เช่น กำหนดระยะเวลาในการตอบสนองต่อ Incident type ประเภทต่าง ๆ ได้

๑.๙ รองรับการทำงานร่วมกับ Product อื่น ๆ (Integrate) ผ่านทาง REST API, SSH/CLI ได้เป็นอย่างน้อย

๑.๑๐ สามารถบริหารแบบ GUI จัดการผ่าน Web Browser

๑.๑๑ สามารถสร้าง Workflow ในการทำงานได้ไม่น้อยกว่า ๕,๐๐๐ Workflows

๑.๑๒ มี Playbook Connector ที่สามารถทำงานร่วมกับ ระบบรักษาความปลอดภัยอื่นๆ (Security Platform) ได้ไม่น้อยกว่า ๓๐๐ ระบบ (platforms) และรองรับการปรับแต่งเพิ่มได้ในอนาคต

๑.๑๓ สามารถ สร้างกระบวนการตอบสนอง ที่มีความสลับซับซ้อนโดยสามารถกำหนดเงื่อนไขการตัดสินใจในเชิงตรรกะ และมีการกระทำแบบอัตโนมัติ (Automated actions) มากกว่า ๓,๐๐๐ actions

๑.๑๔ สามารถทำงานร่วมกับผลิตภัณฑ์ด้านความปลอดภัยเครือข่าย แบบสองทิศทาง (bidirectional) เช่น Cisco ThreatGrid และ Umbrella, IBM QRadar, Splunk, McAfee, Palo Alto, Fortinet, Arbor, Imperva ได้เป็นอย่างน้อย

๑.๑๕ สามารถสร้างกรอบกำกับข้อมูล (Module) โดยรองรับกฎระเบียบ GDPR, และ Legal เป็นอย่างน้อย

๑.๑๖ มีระบบ Case Management สำหรับบริหารจัดการ การแจ้งเตือน (Alert), เหตุการณ์ความปลอดภัย (Incident), ตัวชี้วัด (Indicators), ทรัพย์สิน (Asset) และ ภาระงาน (Tasks)

๑.๑๗ มีโปรแกรมรายงานและรูปแบบ (Templates) สำหรับประสิทธิภาพการดำเนินงาน เหตุการณ์ ภัยคุกคาม โดยเน้นบทบาทของผู้ปฏิบัติงาน เช่น นักวิเคราะห์ระดับ ๑ (Level ๑ Analyst), นักวิเคราะห์ระดับ ๒ (Level ๒ Analyst), ผู้จัดการ SOC (SOC Manager) ได้เป็นอย่างน้อย

๑.๑๘ มีคุณสมบัติ Role-Based Management เพื่อแบ่งระดับการเข้าถึงข้อมูล หรือ policies และ Dashboard หรือรายงานได้

๑.๑๙ สามารถแสดงการแจ้งเตือนที่เกี่ยวข้องกับเทคนิค MITRE ATT & CK ได้เป็นอย่างน้อย

๑.๒๐ สามารถออกรายงานในรูปแบบ PDF และ CSV ได้เป็นอย่างน้อย

๑.๒๑ สามารถทำงานร่วมกับระบบพิสูจน์ตัวตนเช่น Local, LDAP และ SAML ได้เป็น

๑.๒๒ สามารถสร้างและแก้ไข Connector ได้จากตัวช่วยสร้าง Connector ภายในตัวอุปกรณ์ได้

๑.๒๓ มีสิทธิ์ในการใช้งานอย่างน้อย ๓ ผู้ใช้งาน

๑.๒๔ มีลิขสิทธิ์การใช้งานอย่างน้อย ๒ ปี

๒. ระบบตรวจจับและหยุดยั้งการโจมตีประเภท Distributed Denial of Service (DDoS) จำนวน ๒ ชุด โดยมีคุณลักษณะอย่างน้อย ดังนี้

๒.๑ เป็นอุปกรณ์ที่ออกแบบสำหรับป้องกันภัยคุกคามบนระบบเครือข่ายแบบ Distributed Denial Of Service (DDoS) โดยมีลักษณะเป็น Hardware Appliances

๒.๒ อุปกรณ์ที่เสนอ กรณีที่เป็นแบบ Stateless ต้องทำงานไม่ขึ้นกับจำนวนการเชื่อมต่อพร้อมกัน (Simultaneous Connection) หรือ มี Legit Concurrent Sessions หรือ Maximum Concurrent Sessions หรือ Max Concurrent Connection ไม่น้อยกว่า ๑๕,๐๐๐,๐๐๐ Concurrent Sessions และ DDoS Flood Attack หรือ Inbound DDoS Traffic ไม่น้อยกว่า ๑๕,๐๐๐,๐๐๐ pps

๒.๓ สามารถเลือกการติดตั้งใช้งานได้แบบ Inline หรือ inline inactive หรือ Inline Monitoring ได้

๒.๔ มีความสามารถป้องกันภัยคุกคามหรือการโจมตีได้ทั้งการเชื่อมต่อแบบ IPv๔ และ IPv๖

๒.๕ มีความสามารถป้องกันการโจมตี แบบ Flood Attacks, Fragments หรือ Fragmentation Attacks หรือ Fragmentation Flood, TCP Stack Attacks หรือ TCP Attacks หรือ TCP Flood, Application Attacks หรือ Layer ๗-based attack, DNS Attacks หรือ DNS Query Flooding ได้เป็นอย่างน้อย

๒.๖ สามารถป้องกันการโจมตีประเภท DoS/DDoS Attack โดยใช้ Signature based และ Behavior Analysis ได้เป็นอย่างน้อย

๒.๗ สามารถป้องกันการโจมตีได้จากข้อมูล Geo Location Base หรือ Geographie และ bad IP addresses หรือ domains หรือจาก Threat Intelligent หรือเทียบเท่าได้

๒.๘ สามารถป้องกันภัยคุกคามหรือการโจมตีผ่านการเชื่อมต่อแบบ SSL หรือ TLS หรือ HTTPS ได้ไม่น้อยกว่า ๙๕,๐๐๐ Connections Per Second หรือรองรับ concurrent session ไม่น้อยกว่า ๑๕๐,๐๐๐ session

๒.๙ อุปกรณ์ (Hardware) ที่เสนอรองรับการใช้งาน Throughput โดยการขยาย Throughput license หรือมี Max Mitigation Throughput หรือ Max Throughput ได้ไม่น้อยกว่า ๔๐ Gbps หรือต้องมีความเร็วในการตรวจจับการโจมตี (Inspected Throughput) ที่สามารถใช้งานได้ไม่น้อยกว่า ๒ Gbps

๒.๑๐ มี network interface แบบ ๑๐GC (Gigabit Copper) ไม่น้อยกว่า ๘ port โดยมี bypass port ไม่น้อยกว่า ๒ pair bypass และแบบ ๑๐GF (Gigabit Fiber) ไม่น้อยกว่า ๔ port โดยมี bypass port ไม่น้อยกว่า ๒ pair bypass หรือ Inspection ports และ ๑GE จำนวนไม่น้อยกว่า ๘ พอร์ต นำเสนอพร้อมอุปกรณ์ Bypass สำหรับการทำ Bypass เมื่ออุปกรณ์ DDoS มีปัญหา โดยรองรับที่ ๔ Segment

๒.๑๑ มีหน่วยจัดเก็บข้อมูลไม่น้อยกว่า ๖๔ GB หรือดีกว่า จำนวน ๑ หน่วย บนอุปกรณ์หรือบนระบบบริหารจัดการ

๒.๑๒ สามารถบริหารจัดการแบบ Web-Based GUI บนอุปกรณ์ หรือ Centralized Management Server ได้

๒.๑๓ สามารถแจ้งเตือนผ่าน snmp, syslog, email ได้

๒.๑๔ สามารถทำงานร่วมกับอุปกรณ์จำพวก SIEM, NMS รวมถึง REST API ได้

๒.๑๕ มี Power Supply แบบ Redundant และสามารถทำ Hot Swap จำนวนอย่างน้อย ๒ หน่วย

๒.๑๖ ได้รับการรับรองจาก NSS Certification, RoHS compliance หรือ Common Criteria Certification EAL ๔

๒.๑๗ รองรับการทำ Bypass Traffic ในกรณีที่อุปกรณ์เกิดขัดข้อง

๒.๑๘ มีลิขสิทธิ์การใช้งานอย่างน้อย ๒ ปี

๓. ระบบป้องกันภัยคุกคามเว็บแอพพลิเคชั่น (Web Application Firewall) จำนวน ๒ ชุด โดยมีคุณลักษณะอย่างน้อย ดังนี้

๓.๑ อุปกรณ์ที่นำเสนอจะต้องเป็น Hardware Appliance ที่ถูกออกแบบมาสำหรับทำหน้าที่ในการป้องกันระบบงานด้าน Web Application และ Web Services (SOAP)

๓.๒ มี Port เชื่อมต่อ Network ชนิด Copper ไม่น้อยกว่า ๘ Port พร้อมคุณสมบัติ Bypass ทั้ง ๘ ports

๓.๓ มี Port เชื่อมต่อ Network ชนิด ๑G Fiber จำนวน ๔ port หรือดีกว่า

๓.๔ มี Port เชื่อมต่อ Network ชนิด ๑๐G Fiber จำนวน ๔ port พร้อม Module หรือพร้อมใช้งาน

๓.๕ สามารถใช้งาน IPv๖ ได้

๓.๖ มีหน่วยความจำขนาดไม่น้อยกว่า ๓๒ GB

๓.๗ มีหน่วยเก็บข้อมูลขนาดไม่น้อยกว่า ๒ TB หรือ ๑.๘ TB แบบ SSD

๓.๘ มีระบบ SSL Acceleration สำหรับทำงานกับ HTTPS

๓.๙ สามารถรองรับปริมาณการใช้งาน HTTP Throughput ไม่น้อยกว่า ๑๐ Gbps และ HTTPS Throughput ไม่น้อยกว่า ๕ Gbps

๓.๑๐ อุปกรณ์จะต้องเป็นแบบ Rack Mount สามารถติดตั้งในตู้เก็บอุปกรณ์มาตรฐานขนาด ๑๙ นิ้วได้

๓.๑๑ อุปกรณ์ที่นำเสนอจะต้องมีความสามารถในการทำ Web Application Firewall ได้เป็นอย่างน้อยโดยมีเครื่องหมายการค้าได้รับมาตรฐานจาก ICSA หรือ Common Criteria Certification

๓.๑๒ อุปกรณ์ที่นำเสนอจะต้องสามารถทำงานแบบ In-Line (Bridge) transparent, Reverse Proxy Mode และ Sniffer Mode ได้เป็นอย่างน้อย โดยสามารถทำ Fail Open ในการติดตั้งโหมด In-Line (Bridge) Transparent

๓.๑๓ อุปกรณ์ที่นำเสนอจะต้องสามารถป้องกันระบบ Web Application ที่พัฒนาโดย HTML ๕ Web Sockets และ Web ๒.๐ Applications ได้

๓.๑๔ อุปกรณ์ที่นำเสนอจะต้องมีระบบ Dynamic Profiling หรือ Adaptive Profiling เพื่อเรียนรู้ Parameter หรือ Method หรือ Cookie หรือ URL ของ Website ได้อัตโนมัติ

๓.๑๕ มีระบบจัดการโดยสามารถแสดง Alert หรือแจ้งเตือน ในกรณีที่เกิดเหตุการณ์ต่าง ๆ ได้ และระบบการจัดเก็บข้อมูลเพื่อใช้ในการดูรายงานย้อนหลังได้

๓.๑๖ มีระบบการตรวจสอบการ Updates Signature ทั้งในแบบ Manual และ Automatic update

๓.๑๗ สามารถบริหารจัดการอุปกรณ์โดยผ่านทาง Web Base โดยไม่ต้องติดตั้งระบบบริหารจัดการเพิ่มเติม และจะต้องสามารถกำหนดสิทธิ์ และระดับการเข้าถึงอุปกรณ์ ให้กับผู้ดูแลแต่ละคนได้

๓.๑๘ มีระบบ Monitoring ซึ่งมีความสามารถทำงานในลักษณะดังต่อไปนี้ SNMP Trap, SYSLOG และการส่ง Alert ผ่านทาง E-mail, Real-Time Dashboard

๓.๑๙ สามารถแสดงข้อมูล IP address, Port และ Service Type ได้

๓.๒๐ มีความสามารถในการตรวจจับโดยใช้เทคนิค / วิธีการดังต่อไปนี้

๒.๓.๒๐.๑ SQL Injection

๒.๓.๒๐.๒ Remote File Inclusion หรือ Malicious file upload

๒.๓.๒๐.๓ Buffer Overflow

๒.๓.๒๐.๔ Cross Site Scripting

๒.๓.๒๐.๕ Worms หรือ Virus

๒.๓.๒๐.๖ Brute Force หรือ HTTP Request Flooding

๒.๓.๒๐.๗ Data Leakage หรือ Personal Information leakage detection

๒.๓.๒๐.๘ Google Hacking หรือ Application Vulnerability

๓.๒๑ มี Pre-Define Report และสามารถ Custom Reports ในรูปแบบตารางและรูปแบบกราฟ โดยแสดงผลของรายงานเป็น MS Word และ PDF หรือ CSV ได้

๓.๒๒ สามารถ Filter Report เพื่อใช้สำหรับช่วยเจ้าหน้าที่ดูแลระบบในการค้นหา Report

๓.๒๓ สามารถบริหารจัดการผู้ใช้งานในการจัดการระบบได้

๓.๒๔ มี Power Supply แบบ Redundant และสามารถทำ Hot Swap จำนวนอย่างน้อย ๒ หน่วย

๓.๒๕ อุปกรณ์ที่นำเสนอจะต้องรองรับการทำ High Availability (HA) แบบ Active-Passive และ Active-Active ได้

๓.๒๖ สามารถถอดรหัสข้อมูลที่เข้ารหัสด้วย SSL/TLS ได้โดยไม่มีผลกระทบต่อ throughput และประสิทธิภาพการทำงานของ Web Application Firewall ในกรณีที่ไม่สามารถถอดรหัสได้จะต้องเสนออุปกรณ์เพิ่มเติม

๓.๒๗ มีความสามารถในการเฝ้าระวังการเปลี่ยนแปลงเว็บไซต์ (anti-defacement) และสามารถ restore website content จากส่วนที่ backup ไว้ ได้โดยอัตโนมัติ

๓.๒๘ สามารถทำ Administrative domains เพื่อแบ่งการบริหารจัดการนโยบาย แยกตาม host name หรือ domain ได้ไม่น้อยกว่า ๖๔ domains

๓.๒๙ สามารถตรวจสอบช่องโหว่ของเว็บแอพพลิเคชัน (Vulnerability Scan) จากตัวอุปกรณ์ได้ และรองรับการทำงานร่วมกับ ๓rd Party vulnerability scanner เช่น Acunetix, HP WebInspect, IBM AppScan, Qualys ได้เป็นอย่างน้อย

๓.๓๐ ต้องมีลิขสิทธิ์การใช้งานอย่างน้อย ๒ ปี

๔. ระบบตรวจจับภัยคุกคามและวิเคราะห์ความเสี่ยงภายในเครือข่ายสำหรับศูนย์ SOC (Network Threat Analysis) จำนวน ๑ ระบบ โดยมีคุณลักษณะอย่างน้อย ดังนี้

๔.๑ เป็นอุปกรณ์ที่ออกแบบเฉพาะ เพื่อทำหน้าที่ตรวจจับภัยคุกคามและวิเคราะห์ความเสี่ยงภายในเครือข่าย (Breach Detection System) ที่รองรับภัยคุกคามทั้ง IPv๔ และ IPv๖

๔.๒ รองรับ New Session/s ไม่น้อยกว่า ๔๐,๐๐๐ New Session/s

๔.๓ รองรับ Concurrent Session ได้สูงสุดที่ ๓,๐๐๐,๐๐๐ Concurrent Session หรือดีกว่า

๔.๔ มีพื้นที่ในการจัดเก็บข้อมูล (Storage) ไม่น้อยกว่า ๑ Terabyte

๔.๕ มีพอร์ท Gigabit Ethernet (GE) จำนวนไม่น้อยกว่า ๖ พอร์ท หรือพอร์ท ๑๐ Gigabit Ethernet (SFP+) จำนวน ไม่น้อยกว่า ๔ พอร์ท พร้อม Module

๔.๖ สามารถทำงานร่วมกัน Sysmon Endpoint Service ได้

๔.๗ มีระบบตรวจจับพฤติกรรมที่ผิดปกติ (Abnormal Behavior Detection) ที่ใช้การวิเคราะห์แบบจำลองพฤติกรรม (Behavior modeling based) เพื่อทำ Baseline จากข้อมูล Network Traffic ในระดับ Layer ๓ ถึง Layer ๗ เพื่อจับความผิดปกติ เช่น HTTP scanning, Spider, SPAM, FTP weak password ได้

๔.๘ สามารถตรวจจับการโจมตีแบบ DDoS เช่น Flood, Sock stress, zip of death, reflect, DNS query, SSL และ application DDoS ได้

๔.๙ มีระบบตรวจจับภัยคุกคามขั้นสูง (Advanced Threat Detection) ในลักษณะตรวจจับพฤติกรรม (Behavior-based) และสามารถตรวจจับ Ransomware และ cryptomining malware ได้

๔.๑๐ มีระบบวิเคราะห์ความสัมพันธ์ของภัยคุกคาม (Threat Correlation analytics) โดยวิเคราะห์ความสัมพันธ์ระหว่างภัยคุกคามที่ไม่รู้จัก (unknown threats) พฤติกรรมที่ผิดปกติ (abnormal behavior) และพฤติกรรมของแอพพลิเคชั่น (application behavior) เพื่อค้นหาภัยคุกคามหรือการโจมตีที่อาจเกิดขึ้นได้ และมีกฎความสัมพันธ์แบบหลายมิติ (Multi-dimension Correlation Rules) ที่อัพเดตแบบอัตโนมัติผ่าน Cloud ได้

๔.๑๑ มีระบบตรวจจับการบุกรุก (Intrusion Detection) ที่มี Signatures ไม่น้อยกว่า ๓๐,๐๐๐ Signatures และสามารถตรวจจับความผิดปกติของโปรโตคอล (Anomaly Detection) และ ตรวจจับแบบ Rate-based Detection ได้

๔.๑๒ สามารถตรวจจับความผิดปกติของโปรโตคอลได้ ไม่น้อยกว่า HTTP, SMTP, IMAP, POP๓, VoIP, NETBIOS และ UDP เป็นต้น

๔.๑๓ สามารถตรวจจับการโจมตีในรูปแบบ Buffer Overflow, SQL Injection และ Cross-site Scripting Attacks ได้

๔.๑๔ มีระบบแสกนไวรัส (Virus Scan) ที่มี Signature ไม่น้อยกว่า ๑๓ ล้าน Virus Signature และรองรับการสแกนไฟล์ที่ถูกบีบอัด (Compressed File Scan) ได้

๔.๑๕ มีระบบระบุแอพพลิเคชัน (Application Identification) โดยสามารถระบุได้ไม่น้อยกว่า ๓,๐๐๐ Applications เช่น IM, P๒P, Email, File Transfer, Online Games, Media Streaming เป็นต้น และสามารถแสดงสถิติข้อมูลการใช้งานแอพพลิเคชัน (Multi-dimension application statistic based) ตาม โซน (Zone), อินเตอร์เฟซ (Interface), สถานที่ (Location), ผู้ใช้งาน (User), ไอพีแอสเดรส (IP address) ได้

๔.๑๖ มีระบบในการแสดงผลแบบ Dynamic และ Real-time Dashboard

๔.๑๗ สามารถแสดงข้อมูลความเสี่ยงที่เกิดขึ้นในเครือข่าย (Internal Risk Status) Top๕ risk server/computer, Critical Asset Risk Status, Host Risk Status, Threat Severity and Type และ External Attack Geo-location เป็นต้น

๔.๑๘ สามารถการออกรายงานได้ทั้งแบบ Pre-defined Report และ User defined Report และสามารถ export ในรูปแบบ PDF ผ่านทาง Email และ FTP ได้

๔.๑๙ สามารถส่ง LOG ออกไปในรูปแบบ Syslog หรือ Email ได้

๔.๒๐ สามารถบริหารจัดการกับตัวอุปกรณ์ผ่านทาง HTTP/HTTPS, SSH, Telnet ได้

๔.๒๑ มี Power Supply จำนวน ไม่น้อยกว่า ๒ หน่วย แบบ Redundant

๔.๒๒ สามารถติดตั้งในตู้ Rack มาตรฐาน ๑๙ นิ้ว

๔.๒๓ ต้องมีลิขสิทธิ์การใช้งานอย่างน้อย ๒ ปี

๕. ระบบตรวจสอบและบริหารจัดการช่องโหว่ด้านความมั่นคงปลอดภัยสารสนเทศ (Vulnerability Management System) จำนวน ๑ ระบบ โดยมีคุณลักษณะอย่างน้อย ดังนี้

๕.๑ ระบบที่นำเสนอต้องออกแบบมาเพื่อตรวจสอบและบริการจัดการช่องโหว่โดยเฉพาะ และมีลิขสิทธิ์รองรับการตรวจสอบจำนวน IP Address สำหรับ Hardware Appliance ได้ไม่น้อยกว่า ๒๕๖ IP Addressและสามารถเลือกการตรวจสอบได้ทั้งแบบ Single IP และ IP Range เป็นระยะเวลา ๓ ปี

๕.๒ สามารถตรวจสอบ (Scan) ช่องโหว่ของระบบดังต่อไปนี้ภายใต้อุปกรณ์ที่นำเสนอ หรือสามารถที่จะเสนออุปกรณ์และซอฟต์แวร์เพิ่มเติม (Third Party) เพื่อให้ระบบสามารถทำงานได้

๕.๒.๑ ระบบฐานข้อมูล (Database) ได้แก่ Microsoft SQL Server, Oracle, MySQL, PostgreSQL, Sybase, AS/๔๐๐ และ DB๒

๕.๒.๒ ระบบปฏิบัติการ (Operating System) ได้แก่ Microsoft Windows, UNIX, AS/๔๐๐, Linux Red Hat, CentOS, Solaris และ VMware

๕.๓ รองรับการตรวจสอบ (Scan) ทั้งแบบ Non-Credential Scan และ Credential Scan

๕.๔ มีฐานข้อมูลช่องโหว่มากกว่า ๕๐,๐๐๐ ช่องโหว่

๕.๕ มีกลยุทธ์ให้คะแนนความเสี่ยง (Real risk strategy) จากการนำข้อมูลของ Exploit หรือ Malware หรือ CVSS มาประเมินและวิเคราะห์

๕.๖ ต้องสามารถตั้งค่าระดับความสำคัญหรือจัดกลุ่มของอุปกรณ์ที่ต้องการทำการตรวจสอบได้

๕.๗ สามารถกำหนดให้ตรวจสอบเฉพาะ Ports ที่ต้องการได้ และได้ทั้งTCP และ UDP ports

๕.๘ สามารถแก้ไขรูปแบบในการตรวจสอบ (Modify Scan Template) ได้

๕.๙ สามารถให้คำแนะนำหรือวิธีในการแก้ไขปัญหาของช่องโหว่ (Remediation) และแสดงแหล่งที่สามารถดาวน์โหลดซอฟต์แวร์ปรับปรุงแก้ไข (Patch/Hotfix) ต่าง ๆ ได้

๕.๑๐ สามารถอัพเดตฐานข้อมูลการตรวจสอบช่องโหว่จากผู้ผลิตได้โดยอัตโนมัติ (Automatic) หรือโดยผู้ดูแลระบบ (Manual)

๕.๑๑ สามารถตั้งค่าการตรวจสอบล่วงหน้าได้ (Schedule Scan)

๕.๑๒ สามารถทำ Vulnerability Exception ได้

๕.๑๓ สามารถสร้างรายงานได้หลากหลายรูปแบบ เช่น Audit Report, Executive Overview และ Baseline Comparison เป็นอย่างน้อย

๕.๑๔ สามารถสร้างรายงานตามรูปแบบไฟล์ PDF, HTML, XML และ CSV ได้เป็นอย่างน้อย

๕.๑๕ มีระบบ Remediation workflow หรือ Ticket system ภายในระบบเพื่อติดตามความคืบหน้าของการแก้ไข (track remediation progress) ช่องโหว่ต่าง ๆ ได้ เช่น JIRA, ServiceNow และ BMC Remedy เป็นต้น

๕.๑๖ สามารถแจ้งเตือนผลการตรวจสอบช่องโหว่และรายงานให้ผู้ดูแลระบบผ่านทาง Email, SNMP และ Syslog ได้เป็นอย่างน้อย

๕.๑๗ สามารถบริหารการจัดผ่านทาง Secure Web Browser (HTTPS) ได้

๕.๑๘ สามารถกำหนดสิทธิ์ของผู้ใช้งาน เพื่อเข้าถึงระบบด้วยสิทธิ์ที่ต่างกันได้ (Role-Based Management)

๕.๑๙ ระบบ Web Application ตามรายละเอียด ดังนี้

๕.๑๙.๑ สามารถตรวจสอบช่องโหว่ของ Web Application เช่น SQL injecti และ cross-site scripting ได้

๕.๑๙.๒ รองรับการตรวจสอบแบบ Web Spidering หรือ Crawling

๕.๑๙.๓ รองรับการทำ Credential Scan ผ่านหน้า HTTP Web Login

๕.๒๐ สามารถทำงานร่วมกับ Metasploit ได้เพื่อตรวจสอบความถูกต้องของช่องโหว่ได้

๕.๒๑ สามารถทำ Compliance เช่น PCI DSS, ISO, NERC, FISMA, HIPAA, USGCB และ CIS ได้เป็นอย่างน้อย

๕.๒๒ สามารถตั้งค่า Scan ช่องโหว่ที่เกิดขึ้นใหม่โดยไม่ต้องทำการ scan ใหม่ทั้งหมด หรือ Adaptive Security ได้เป็นอย่างน้อย

๕.๒๓ สามารถตรวจสอบช่องโหว่ของอุปกรณ์เครือข่ายโดยไม่ต้องติดตั้งโปรแกรมเพิ่มเติมในอุปกรณ์ที่ต้องการตรวจสอบ (Agentless)

๕.๒๔ ผู้เสนอราคาจะต้องได้รับการแต่งตั้งจากบริษัทเจ้าของผลิตภัณฑ์โดยตรงหรือจากตัวแทนจำหน่ายสินค้าภายในประเทศไทย โดยมีจดหมายรับรองจากเจ้าของผลิตภัณฑ์อ้างถึงโครงการอย่างชัดเจน

๕.๒๕ ต้องมีลิขสิทธิ์การใช้งานอย่างน้อย ๒ ปี

เอกสารหมายเลข ๓

รายละเอียดการฝึกอบรม

รายละเอียดการฝึกอบรม
โครงการเพิ่มประสิทธิภาพการบริหารจัดการระบบป้องกัน
และรักษาความมั่นคงปลอดภัยด้านข้อมูลสารสนเทศ กรมสรรพสามิต

ผู้ชนะการประกวดราคา ต้องเสนอรายละเอียดการฝึกอบรม โดยระบุชื่อหลักสูตรและเนื้อหา จำนวนวัน เวลา และสถานที่ฝึกอบรม โดยมีหลักสูตรอย่างน้อย ดังนี้

ลำดับ	หลักสูตร	จำนวนวัน/รุ่น (อย่างน้อย)	จำนวนคน/รุ่น (อย่างน้อย)	จำนวนรุ่น	จำนวนคนรวม
๑	หลักสูตรระบบบริหารการจัดการภัยและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ (Security Orchestration, Automation and Response (SOAR))	๑	๑๐	๑	๑๐
๒	หลักสูตรระบบตรวจจับและหยุดยั้งการโจมตีประเภท Distributed Denial of Service (DDoS)	๑	๑๐	๑	๑๐
๓	หลักสูตรระบบป้องกันภัยคุกคามเว็บแอพพลิเคชั่น (Web Application Firewall)	๑	๑๐	๑	๑๐
๔	หลักสูตรระบบตรวจจับภัยคุกคามและวิเคราะห์ความเสี่ยงภายในเครือข่ายสำหรับศูนย์ SOC (Network Threat Analysis)	๑	๑๐	๑	๑๐
๕	หลักสูตรระบบตรวจสอบและบริหารจัดการช่องโหว่ด้านความมั่นคงปลอดภัยสารสนเทศ (Vulnerability Management System)	๑	๑๐	๑	๑๐
รวมจำนวนผู้เข้าอบรมรวมทั้งหมด					**๕๐**

หมายเหตุ : จำนวนวันและจำนวนคนในการอบรมในแต่ละรุ่นอาจมีการเปลี่ยนแปลงตามที่กรมสรรพสามิตพิจารณาเห็นชอบ

๑. หลักสูตรที่จัดอบรมจะต้องสอดคล้องกับผลิตภัณฑ์ที่เสนอกรมสรรพสามิต
๒. ก่อนการฝึกอบรม ผู้ชนะการประกวดราคาต้องเสนอรายละเอียดการฝึกอบรมโดยระบุชื่อหลักสูตรวิชาและเนื้อหาจำนวนวันเวลาที่จะฝึกอบรมพร้อมประวัติผู้สอนให้กรมสรรพสามิตพิจารณาก่อนดำเนินการฝึกอบรมโดยที่หลักสูตรแต่ละหลักสูตรจะต้องผ่านการพิจารณาเห็นชอบจากกรมสรรพสามิตก่อนดำเนินการ

๓. ผู้ชนะการประกวดราคาเป็นผู้รับผิดชอบจัดหาสถานที่อุปกรณ์ (รวม LCD Projector) สื่อการเรียนการสอน ค่าวิทยากร ค่าเดินทาง ค่าเบี้ยเลี้ยง ค่าที่พัก และค่าใช้จ่ายอื่น ๆ ที่เกี่ยวข้องกับการฝึกอบรม ทั้งนี้ผู้เข้ารับการฝึกอบรมจะได้ พร้อมคู่มือในการฝึกอบรมจำนวน ๑ ชุด/คน โดยบริษัทคู่สัญญาสามารถขอใช้สถานที่ของกรมสรรพสามิตได้ตามความเหมาะสม

๔. สถานที่ฝึกอบรม ห้องอบรม อาคารศูนย์เทคโนโลยีสารสนเทศ กรมสรรพสามิต หรือสถานที่ที่กรมสรรพสามิตเห็นชอบ

เอกสารหมายเลข ๔

การบำรุงรักษาและซ่อมแซมแก้ไขฯ

การบำรุงรักษาและซ่อมแซมแก้ไข
โครงการเพิ่มประสิทธิภาพการบริหารจัดการระบบป้องกัน
และรักษาความมั่นคงปลอดภัยด้านข้อมูลสารสนเทศ กรมสรรพสามิต
ตลอดอายุการรับประกันตามสัญญา

๑. การบริการและการสนับสนุน

๑.๑ ผู้ชนะการประกวดราคาต้องจัดให้มีการสนับสนุน ด้านบุคลากร อุปกรณ์ และการฝึกอบรมบุคลากรของกรมสรรพสามิต ภายใต้เงื่อนไขและระยะเวลาที่กำหนดไว้ ตามเอกสารหมายเลข ๓

๑.๒ ผู้ชนะการประกวดราคาต้องจัดหาและให้บริการ Help Desk ในการให้บริการถาม-ตอบทางโทรศัพท์และผ่านทางช่องทางอื่น ๆ ที่มีบริการ จำนวน ๑ คน ณ กรมสรรพสามิต กรณีที่กรมสรรพสามิตไม่มีสถานที่เพียงพอ ผู้ชนะการประกวดราคามีหน้าที่รับผิดชอบในการจัดหาสถานที่ตลอดระยะเวลาการบำรุงรักษาระบบเป็นระยะเวลา ๒ ปี โดยกรมสรรพสามิตเป็นผู้จัดหาสถานที่ดำเนินการ และสายสัญญาณโทรศัพท์เพื่อใช้ในการให้บริการ กรณีที่กรมสรรพสามิตไม่มีสถานที่เพียงพอ ผู้ชนะการประกวดราคามีหน้าที่รับผิดชอบในการจัดหาสถานที่

๒. การให้บริการบำรุงรักษา

ผู้ชนะการประกวดราคาต้องรับประกันความบกพร่อง บำรุงรักษา แก้ไขระบบงานที่เกิดขึ้นทั้งหมด หรือเปลี่ยนทดแทนในทุกรายการที่เสนอ อันเนื่องจากข้อผิดพลาดของการปฏิบัติงาน ตลอดระยะเวลารับประกันเป็นเวลา ๒ ปีนับถัดจากวันที่กรมสรรพสามิตตรวจรับงานเสร็จสมบูรณ์ทั้งหมด โดยไม่คิดค่าใช้จ่ายใด ๆ ทั้งสิ้น จากกรมสรรพสามิต และในระยะเวลารับประกัน โดยต้องปฏิบัติตามเงื่อนไข ต่อไปนี้

๑. ผู้ชนะการประกวดราคาต้องทำการบำรุงรักษาระบบงานและอุปกรณ์ **ตามเอกสารหมายเลข ๒** โดยผู้ชนะการประกวดราคาต้องเริ่มจัดการปรับปรุงแก้ไขให้อยู่ในสภาพดีได้ดังเดิม โดยต้องเริ่มจัดการแก้ไขภายใน ๓ วันทำการ นับแต่ได้รับแจ้งจากกรมสรรพสามิต โดยไม่ทำให้ระบบงานหยุดชะงัก หรือเกิดความเสียหายแก่ทางราชการ

ถ้าผู้ชนะการประกวดราคาไม่สามารถแก้ไขปัญหาดังกล่าวได้ภายในระยะเวลาที่กำหนด กรมสรรพสามิตสามารถจัดจ้างผู้อื่นมาแก้ปัญหาได้ โดยคู่สัญญาจะต้องเป็นผู้ออกค่าใช้จ่ายในการจัดจ้างดังกล่าวทั้งหมด

๒. ผู้ชนะการประกวดราคาต้องทำการบำรุงรักษาและแก้ไขระบบงานให้อยู่ในสภาพใช้งานได้ดีอยู่เสมอตลอดระยะเวลาการรับประกัน หากไม่ทำการบำรุงรักษาในระยะเวลาการรับประกันดังกล่าว ผู้ชนะการประกวดราคาต้องยินยอมให้กรมสรรพสามิตคิดค่าปรับครั้งละ ๓,๐๐๐ บาท (สามพันบาทถ้วน)

๓. การเรียกเงินค่าปรับ หากผู้ชนะการประกวดราคาไม่ชำระเงินค่าปรับภายใน ๗ วัน นับแต่วันที่กรมสรรพสามิตแจ้งให้ทราบเป็นลายลักษณ์อักษร กรมสรรพสามิตมีสิทธิหักเงินค่าปรับจากเงินประกันสัญญาหรือเรียกจากธนาคารผู้ค้ำประกันได้ทันที

๔. ให้ผู้ชนะการประกวดราคา เสนอรายละเอียดการบำรุงรักษา วิธีการบำรุงรักษา เพื่อประกอบการพิจารณาทางด้านเทคนิค

๓. การบริการตลอดอายุสัญญา

ผู้ชนะการประกวดราคาจะต้องจัดให้มีบริการตลอดอายุสัญญา โดยจัดหาบุคลากรที่มีความรู้ความสามารถ เพื่อให้คำแนะนำและแก้ไขปัญหาให้แก่กรมสรรพสามิต เมื่อร้องขอทั้งในและนอกเวลาราชการในสถานที่ติดตั้ง

๔. การซ่อมแซม แก้ไขและ/หรือเปลี่ยนแทนและการปรับ

การซ่อมแซมแก้ไขคอมพิวเตอร์ ผู้ชนะการประกวดราคาต้องจัดการซ่อมแซมแก้ไขคอมพิวเตอร์ให้อยู่ในสภาพใช้งานได้ดีตามปกติตลอดระยะเวลาการรับประกันความชำรุดบกพร่องตามสัญญาหากคอมพิวเตอร์ขัดข้องจะต้องดำเนินการ ดังนี้

๔.๑ ผู้ชนะการประกวดราคามีหน้าที่บำรุงรักษา และซ่อมแซมแก้ไขคอมพิวเตอร์ ไม่ว่าจะติดตั้ง ณ สถานที่ใด ๆ ให้อยู่ในสภาพใช้งานได้ดีอยู่เสมอตลอดระยะเวลารับประกันด้วยค่าใช้จ่ายของผู้ชนะการประกวดราคา กรมสรรพสามิตยินยอมให้คอมพิวเตอร์ขัดข้อง ภายหลังที่คำนวณด้วยค่าตัวถ่วงแล้วได้ไม่เกินเดือนละ ๑๒ ชั่วโมง (ถ้าคอมพิวเตอร์ขัดข้องเกินระยะเวลา ดังกล่าวกรมสรรพสามิตจะคิดค่าปรับในส่วนที่เกินในอัตราชั่วโมงละ ๐.๐๓๕ ของราคาคอมพิวเตอร์ที่ขัดข้องนั้น ๆ) เกณฑ์การคำนวณนับชั่วโมงและค่าตัวถ่วงเป็น ดังนี้

(๑) จำนวนชั่วโมงที่ขัดข้องในขณะใดขณะหนึ่งเท่ากับค่าสูงสุดของจำนวนชั่วโมงที่ขัดข้องในขณะนั้นของอุปกรณ์แต่ละอุปกรณ์คูณด้วยค่าตัวถ่วง
จำนวนชั่วโมง = ค่าสูงสุด (ชั่วโมงที่ขัดข้อง x ค่าตัวถ่วง)
เศษของชั่วโมงนับเป็น ๑ ชั่วโมง

(๒) ค่าปรับ = ๐.๐๓๕ x (ผลรวมจำนวนชั่วโมง - ๑๒) x (ราคาคอมพิวเตอร์)

๔.๒ กำหนดค่าตัวถ่วงของระบบ ดังนี้

(๑)	ระบบบริหารการจัดการภัยและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ (Security Orchestration, Automation and Response (SOAR))	๑.๐
(๒)	ระบบตรวจจับและหยุดยั้งการโจมตีประเภท Distributed Denial of Service (DDoS)	๑.๐
(๓)	ระบบป้องกันภัยคุกคามเว็บแอพพลิเคชั่น (Web Application Firewall)	๑.๐
(๔)	ระบบตรวจจับภัยคุกคามและวิเคราะห์ความเสี่ยงภายในเครือข่ายสำหรับศูนย์ SOC (Network Threat Analysis)	๑.๐
(๕)	ระบบตรวจสอบและบริหารจัดการช่องโหว่ด้านความมั่นคงปลอดภัยสารสนเทศ (Vulnerability Management System)	๑.๐

เอกสารหมายเลข ๕

รายละเอียดข้อเสนอด้านคุณสมบัติของผู้เสนอราคา

๑. คุณสมบัติทั่วไป และประสบการณ์ของผู้เสนอราคา

(๑) บทสรุปสำหรับผู้บริหาร .....

(๒) รายละเอียดบริษัท (Company Profile).....

(๓) ประสบการณ์ของผู้เสนอราคา

ข้อมูลรายละเอียดลูกค้าที่อ้างอิง				ข้อมูลรายละเอียดโครงการที่อ้างอิง						
ชื่อลูกค้า	ที่อยู่/ประเทศ	ประเภทธุรกิจ	บุคคลที่สามารถติดต่อได้ (ชื่อ/ตำแหน่ง/โทรศัพท์/e-mail)	ชื่อโครงการ	ปีที่ดำเนินการ (ย้อนหลังไม่เกิน ๕ ปี)	ระยะเวลา		มูลค่าโครงการ	อธิบายรายละเอียดของโครงการที่ทำ	หมายเหตุ
						ตามสัญญา	ทำงานจริง			

ลงชื่อ.....

ประทับตรา (ถ้ามี) (.....)

ตำแหน่ง.....

บริษัท/.....

ผู้เสนอราคา

วันที่...../...../.....

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

๒. ตารางสรุปคุณสมบัติ ประสบการณ์ และประวัติของบุคลากรที่เสนอรายชื่อ

ลำดับที่	ชื่อ/ชื่อสกุล	ตำแหน่งในโครงการที่จัดจ้าง	วุฒิการศึกษา/สาขา	ประสบการณ์ (ปี)

ข้าพเจ้าขอรับรองว่ารายละเอียดตามรายการข้างต้นเป็นความจริงทุกประการ และยินยอมให้กรมสรรพสามิตตรวจสอบข้อมูล ตลอดจนให้ข้อมูลดังกล่าวในการใด ๆ อันเกี่ยวกับการจ้างพัฒนาระบบงานของกรมสรรพสามิต

ประทับตรา
(ถ้ามี)

ลงชื่อ.....
(.....)
ตำแหน่ง.....
บริษัท.....
ผู้เสนอราคา
วันที่...../...../.....

ประวัติ คุณสมบัติ และประสบการณ์ ของบุคลากร (ต่อ)

ชื่อ/ชื่อสกุล.....

หมายเลขประจำตัวประชาชน/หมายเลขหนังสือเดินทาง.....

อาชีพ ..... ที่อยู่.....

สัญชาติ ..... จำนวนปีที่ทำงานอยู่ในบริษัท.....

ตำแหน่งและหน้าที่ความรับผิดชอบที่ได้รับในโครงการ

ตำแหน่ง	หน้าที่ความรับผิดชอบ	ระยะเวลา

ประวัติการศึกษา

ตั้งแต่ - ถึง	ชื่อสถานศึกษา/ประเทศ	ปริญญา/ประกาศนียบัตรที่ได้รับ	คณะและภาควิชา

ประวัติการฝึกอบรม ดูงาน ฝึกงาน

ตั้งแต่ เดือน/ปี ถึง เดือน/ปี	ชื่อฝึกอบรม ดูงาน ฝึกงาน/ประเทศ	ชื่อหลักสูตร	ขอบเขต/รายละเอียด	ประโยชน์และการนำไปใช้งาน

ประวัติการทำงาน

ตั้งแต่ เดือน/ปี ถึง เดือน/ปี	ชื่อสถานที่ทำงาน/ประเทศ	ตำแหน่งและชื่อโครงการ	ขอบเขตและหน้าที่ความรับผิดชอบ	บุคคลอ้างอิง

ข้าพเจ้าขอรับรองว่ารายละเอียดตามรายการข้างต้นเป็นความจริงทุกประการ และยินยอมให้กรมสรรพสามิต ตรวจสอบข้อมูลตลอดจนใช้ข้อมูลดังกล่าวในการใด ๆ อันเกี่ยวกับการจ้างพัฒนาระบบงานของกรมสรรพสามิตได้

ลงชื่อเจ้าของประวัติ .....

(.....)

ประทับตรา
(ถ้ามี)

ลงชื่อ.....

(.....)

ตำแหน่ง.....

บริษัท .....

ผู้เสนอราคา

วันที่...../...../.....

๓. ตารางแผนงาน วิธีดำเนินการ และเครื่องมือในการพัฒนา

(๑) ตารางแผนงาน

ลำดับ	กิจกรรม	Man-Day	ระยะเวลา	เดือน													รายละเอียดทีมงาน	
				๑				๒				๓				๔	ชื่อ/ชื่อสกุล	Man-Day
				๑	๒	๓	๔	๕	๖	๗	๘	๙	...	...	...	...		

(๒) วิธีดำเนินการ และเครื่องมือในการพัฒนาและเทคนิคที่ใช้.....

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

๔. ตารางแรงงานของบุคลากร (Man-Day) ที่เสนอในการดำเนินงานโครงการ

ชื่อ/ชื่อสกุล	ตำแหน่งในโครงการ	รายละเอียดกิจกรรมที่ทำ	Man-Day	หมายเหตุ

ลงชื่อ.....

ประทับตรา (.....)

(ถ้ามี) ตำแหน่ง.....

บริษัท.....

ผู้เสนอราคา

วันที่...../...../.....

๕. ตารางบุคลากรที่ต้องใช้ในโครงการ

เมื่อเริ่มดำเนินโครงการ ผู้ชนะการประกวดราคาต้องเสนอบุคลากรตามตำแหน่งดังต่อไปนี้ เพื่อให้เพียงพอต่อการดำเนินงานตามระยะเวลาส่งมอบงาน

ลำดับที่	ตำแหน่ง	วุฒิการศึกษา	ประสบการณ์ (ปี)	จำนวน คน
๑.				
๒.				
๓.				
๔.				
๕.				
๖.				
๗.				
๘.				