(สำเนา)

ประกาศสำนักเลขาธิการคณะรัฐมนตรี

เรื่อง ประกวดราคาซื้อโครงการปรับปรุงระบบรักษาความมั่นคงปลอดภัยไซเบอร์ ด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding)

สำนักเลขาธิการคณะรัฐมนตรี มีความประสงค์จะประกวดราคาซื้อโครงการปรับปรุงระบบรักษาความมั่นคงปลอดภัยไซเบอร์ ด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding) ราคากลางของงานซื้อในการประกวดราคาครั้งนี้ เป็นเงินทั้งสิ้น ๔๗,๑๐๖,๓๐๐.๐๐ บาท (สี่สิบเจ็ดล้านหนึ่งแสนหกพันสามร้อยบาทถ้วน) ตามรายการ ดังนี้

๑. ระบบรักษาความปลอดภัยระบบเครือข่ายระดับแอปพลิเคชัน (Application Firewall) จำนวน ๒ ชุด

๒. ระบบป้องกันการโจมตีผ่านช่องโหว่ซอฟท์แวร์สำหรับเครื่องคอมพิวเตอร์ลูกข่าย จำนวน ๑ ระบบ

๓. ระบบบริหารจัดการและตอบสนองต่อภัยคุกคามไซเบอร์แบบอัตโนมัติ จำนวน ๑ ระบบ

๔. ระบบรักษาความปลอดภัยระบบเครือข่ายระดับแอปพลิเคชัน (Application Firewall) ทดแทนระบบเดิม จำนวน ๑ ระบบ

๕. แนวทางการพัฒนาศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

๖. ระบบบริหารจัดการเครือข่ายแบบรวมศูนย์ จำนวน ๑ ระบบ

๗. ระบบลงทะเบียนเข้าใช้งาน Wi-Fi ทดแทนระบบเดิม จำนวน ๑ ระบบ

๘. จัดหาและติดตั้งใบรับรอง SSL Certificate จำนวน ๑ ชุด

๙. เครื่องคอมพิวเตอร์โน้ตบุ๊ก จำนวน ๕ เครื่อง

๑๐. การฝึกอบรม

๑๑. งานเอกสารและคู่มือ

ผู้ยื่นข้อเสนอจะต้องมีคุณสมบัติ ดังต่อไปนี้

๑. มีความสามารถตามกฎหมาย

๒. ไม่เป็นบุคคลล้มละลาย

๓. ไม่อยู่ระหว่างเลิกกิจการ

๔. ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราวเนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

๕. ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

๖. มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

๗. เป็นบุคคลธรรมดาหรือนิติบุคคล ผู้มีอาชีพให้ขายพัสดุที่ประกวดราคาซื้อด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

๘. ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่สำนักเลขาธิการคณะรัฐมนตรี ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

๙. ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์ความคุ้มกันเช่นว่านั้น

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

๑๑. ผู้ยื่นข้อเสนอซึ่งได้รับคัดเลือกเป็นคู่สัญญาต้องลงทะเบียนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement : e - GP) ของกรมบัญชีกลาง ตามคณะกรรมการ ป.ป.ช. กำหนด

๑๒. ผู้ยื่นข้อเสนอต้องไม่อยู่ในฐานะเป็นผู้ไม่แสดงบัญชีรายรับรายจ่าย หรือแสดงบัญชีรายรับรายจ่ายไม่ถูกต้องครบถ้วนในสาระสำคัญ ตามที่คณะกรรมการ ป.ป.ช. กำหนด

๑๓. ผู้ยื่นข้อเสนอซึ่งได้รับคัดเลือกเป็นคู่สัญญาต้องรับและจ่ายเงินผ่านบัญชีธนาคาร เว้นแต่การจ่ายเงินแต่ละครั้งซึ่งมีมูลค่าไม่เกินสามหมื่นบาทคู่สัญญาอาจจ่ายเป็นเงินสดก็ได้ ตามที่คณะกรรมการ ป.ป.ช. กำหนด

๑๔. ผู้ยื่นข้อเสนอต้องไม่เคยถูกยกเลิกสัญญาซื้อขาย หรือสัญญาจ้างบริการบำรุงรักษาก่อนหมดอายุสัญญา โดยไม่มีเหตุผลอันควรจากหน่วยงานใด ๆ

๑๕. ผู้ยื่นข้อเสนอต้องมีผลงานเกี่ยวกับระบบคอมพิวเตอร์จากหน่วยงานของรัฐหรือหน่วยงานเอกชน โดยผลงานดังกล่าวจะต้องเป็นผลงานในการติดตั้งระบบเครือข่ายคอมพิวเตอร์และระบบรักษาความมั่นคงปลอดภัยอย่างน้อย ๒ สัญญาจ้าง และมีมูลค่าสัญญาละไม่น้อยกว่า ๒,๐๐๐,๐๐๐ บาท (สองล้านบาทถ้วน) และยังคงใช้ระบบงานดังกล่าวอยู่ในปัจจุบัน พร้อมเอกสารรายละเอียดของผลงานดังกล่าวอย่างชัดเจน โดย สลค. ขอสงวนสิทธิ์ที่จะตรวจสอบข้อเท็จจริงดังกล่าว

๑๖. ผู้ยื่นข้อเสนอต้องเสนอรายชื่อคณะทำงานทั้งหมดที่จะเข้ามาดำเนินการตามโครงการนี้ โดยที่ภายในคณะทำงานจะต้องประกอบด้วยบุคลากรที่มีความเชี่ยวชาญด้านระบบรักษาความมั่นคงปลอดภัยไซเบอร์และระบบเครือข่ายคอมพิวเตอร์ และคณะทำงานทั้งหมดต้องมายืนยันตัวตนเข้าดำเนินการโครงการต่อ สลค. ในการส่งมอบงานงวดที่ ๑ ประกอบด้วย

ลำดับ	คณะทำงาน	วุฒิการศึกษา	ประสบการณ์ด้านที่ตรงกับหน้าที่ในคณะทำงาน	จำนวน	ระยะเวลา
๑	ผู้จัดการโครงการ (Project Manager)	ปริญญาโท	ไม่น้อยกว่า ๓ ปี	๑ คน	อย่างน้อยเดือนละ ๒ ครั้ง ตลอดระยะเวลาดำเนินโครงการ

ลำดับ	คณะทำงาน	วุฒิการศึกษา	ประสบการณ์ด้านที่ตรงกับหน้าที่ในคณะทำงาน	จำนวน	ระยะเวลา
๒	ผู้เชี่ยวชาญด้านระบบรักษาความมั่นคงปลอดภัยไซเบอร์	ปริญญาตรี	ไม่น้อยกว่า ๒ ปี และเคยได้รับ Certificate ด้านระบบรักษาความมั่นคงปลอดภัย	๑ คน	ตลอดระยะเวลาดำเนินโครงการ
๓	วิศวกรเครือข่าย (Network Engineer)	ปริญญาตรี	ไม่น้อยกว่า ๒ ปี และเคยได้รับ Certificate ด้าน Network	๑ คน	ตลอดระยะเวลาดำเนินโครงการ
๔	ผู้ประสานงานโครงการ	ปริญญาตรี	ไม่น้อยกว่า ๑ ปี	๑ คน	ตลอดระยะเวลาดำเนินโครงการ

ทั้งนี้ คณะทำงานดังกล่าวจะต้องมาปฏิบัติงานที่ สลค. ตามหน้าที่ที่ตนรับผิดชอบอย่างสม่ำเสมอตลอดระยะเวลาการดำเนินงานโครงการ

๑๗. ผู้ยื่นข้อเสนอต้องเสนอเอกสารแบบรูปหรือแคตตาล็อกแสดงรายละเอียดคุณลักษณะเฉพาะหรือคุณสมบัติของผลิตภัณฑ์ที่เสนอทุกรายการ โดยยื่นมาพร้อมกับการเสนอราคา ดังนี้

หัวข้อ	ข้อกำหนดของ สลค.	ข้อเสนอของบริษัท	เอกสารอ้างอิงหน้า/ข้อ
ระบุหัวข้อให้ตรงกับที่ สลค. กำหนด	ให้คัดลอกคุณลักษณะเฉพาะที่ สลค. กำหนด	ให้ระบุคุณลักษณะเฉพาะที่เสนอ	ให้ระบุหรืออ้างอิงเอกสารในข้อเสนอที่เกี่ยวข้องและขีดเส้นใต้คุณลักษณะเฉพาะที่ สลค. กำหนดลงในแคตตาล็อกหรือเอกสารที่เกี่ยวข้อง

๑๘. การพิจารณาผลการยื่นข้อเสนอการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้ สลค. จะพิจารณาตัดสินโดยใช้เกณฑ์ราคาประกอบเกณฑ์อื่น โดยเกณฑ์อื่นเป็นการพิจารณาเกณฑ์การให้คะแนนจากผลงานที่ผ่านมา รูปแบบ และวิธีการดำเนินงาน ตลอดจนแนวทางการบริหารโครงการให้ประสบผลสำเร็จตามวัตถุประสงค์ของโครงการและข้อเสนอทางเทคนิคที่เป็นประโยชน์ต่อทางราชการเป็นสำคัญ โดยข้อเสนอต้องมีความเป็นไปได้ที่สามารถดำเนินการได้จริง และตรงกับความต้องการของ สลค. (คะแนนรวม ๑๐๐ คะแนน) และ สลค. ขอสงวนสิทธิ์ในการพิจารณาเฉพาะผู้ยื่นข้อเสนอที่ผ่านคุณสมบัติเบื้องต้นตามข้อ ๑ - ๑๗ ข้างต้นเท่านั้น ซึ่งเกณฑ์อื่นประกอบด้วยข้อพิจารณา ดังนี้

ข้อพิจารณา	คะแนน

ข้อพิจารณา	คะแนน
๑. การนำเสนอผลงานที่ผ่านมาเกี่ยวกับการติดตั้งระบบเครือข่ายคอมพิวเตอร์และระบบรักษาความมั่นคงปลอดภัย อย่างน้อย ๒ สัญญาจ้าง และมีมูลค่าสัญญาละไม่น้อยกว่า ๒,๐๐๐,๐๐๐ บาท (สองล้านบาทถ้วน) และยังคงใช้ระบบงานดังกล่าวอยู่ในปัจจุบัน พร้อมเอกสารรายละเอียดของผลงานดังกล่าวอย่างชัดเจน โดย สลค. ขอสงวนสิทธิ์ที่จะตรวจสอบข้อเท็จจริงดังกล่าว ทั้งนี้ ผลงานดังกล่าวควรแสดงให้เห็นถึงประสบการณ์และความสามารถที่เกี่ยวข้องกับโครงการอย่างน้อย ดังนี้ ๑.๑ มีระบบรักษาความปลอดภัยระบบเครือข่ายระดับแอปพลิเคชัน (Application Firewall) (คะแนนเต็ม ๑ คะแนน) ๑.๒ มีระบบป้องกันการโจมตีผ่านช่องโหว่ซอฟท์แวร์สำหรับเครื่องคอมพิวเตอร์ลูกข่าย (คะแนนเต็ม ๑ คะแนน) ๑.๓ มีระบบบริหารจัดการและตอบสนองต่อภัยคุกคามไซเบอร์แบบอัตโนมัติ (คะแนนเต็ม ๑ คะแนน) ๑.๔ มีระบบบริหารจัดการเครือข่ายแบบรวมศูนย์ (คะแนนเต็ม ๑ คะแนน) ๑.๕ มีระบบลงทะเบียนเข้าใช้งาน Wi-Fi (คะแนนเต็ม ๑ คะแนน)	**๕**
๒. การนำเสนอแนวทางการพัฒนาศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของ สลค. ตามโครงการนี้ ทั้งนี้ สลค. จะให้คะแนนโดยพิจารณาว่า ผู้ยื่นข้อเสนอได้นำเสนอแนวทางฯ ที่เป็นไปตามกฎหมายและมาตรฐานที่เกี่ยวข้อง เป็นไปตามวัตถุประสงค์ของโครงการ เป็นประโยชน์ต่อทางราชการเป็นสำคัญ และมีความเป็นไปได้ที่จะดำเนินการได้จริง ดังนี้	**๓๐**
๒.๑ การนำเสนอแนวทางการจัดทำร่างนโยบายในการรับมือเหตุการณ์ภัยคุกคามทางไซเบอร์ของ สลค. โดยอ้างอิงจากข้อกำหนดตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และแนวปฏิบัติของ NIST Cyber SecurityFramework (๑) ครบถ้วน ถูกต้อง และมีตัวอย่างนำเสนอที่ชัดเจน (๕ คะแนน) (๒) ครบถ้วน และถูกต้อง (๓ คะแนน) (๓) ครบถ้วน แต่ไม่ถูกต้อง (๑ คะแนน) (๔) ไม่เสนอ (๐ คะแนน)	(๕)

ข้อพิจารณา	คะแนน
๒.๒ การนำเสนอแนวทางการจัดทำขั้นตอนการปฏิบัติงานต่าง ๆ ดังนี้ (๑) ขั้นตอนการเฝ้าระวังเหตุการณ์ภัยคุกคามและการโจมตีทางไซเบอร์ - ครบถ้วน ถูกต้อง และมีตัวอย่างนำเสนอที่ชัดเจน (๓ คะแนน) - ครบถ้วน และถูกต้อง (๒ คะแนน) - ครบถ้วน แต่ไม่ถูกต้อง (๑ คะแนน) - ไม่นำเสนอ (๐ คะแนน) (๒) กระบวนการจัดทำ Playbook Automation รวมทั้งวิธีการเชื่อมโยง (Integrate) เข้ากับระบบความปลอดภัยเดิมที่ สลค. มีอยู่ - ครบถ้วน ถูกต้อง และมีตัวอย่างนำเสนอที่ชัดเจน (๓ คะแนน) - ครบถ้วน และถูกต้อง (๒ คะแนน) - ครบถ้วน แต่ไม่ถูกต้อง (๑ คะแนน) - ไม่นำเสนอ (๐ คะแนน) (๓) กระบวนการในการสื่อสารเมื่อเกิดเหตุการณ์ภัยคุกคามและการโจมตี - ครบถ้วน ถูกต้อง และมีตัวอย่างนำเสนอที่ชัดเจน (๒ คะแนน) - ครบถ้วน และถูกต้อง (๑ คะแนน) - ไม่นำเสนอ (๐ คะแนน) (๔) แนวทางอื่นที่เป็นประโยชน์ต่อการดำเนินโครงการ - ครบถ้วน ถูกต้อง และมีตัวอย่างนำเสนอที่ชัดเจน (๒ คะแนน) - ครบถ้วน และถูกต้อง (๑ คะแนน) - ไม่นำเสนอ (๐ คะแนน)	(๑๐)
๒.๓ การนำเสนอแนวทางการเชื่อมต่อระบบบริหารจัดการและตอบสนองต่อภัยคุกคามแบบอัตโนมัติให้สามารถทำงานร่วมกับระบบเครือข่ายและระบบรักษาความปลอดภัยเครือข่ายฯ ที่ สลค. มีอยู่เดิมได้ โดยนำเสนอวิธีการและแผนผังการเชื่อมต่อระบบฯ (๑) ครบถ้วน ถูกต้อง และมีตัวอย่างนำเสนอที่ชัดเจน (๑๐ คะแนน) (๒) ครบถ้วน และถูกต้อง (๗ คะแนน) (๓) ครบถ้วน แต่ไม่ถูกต้อง (๓ คะแนน) (๔) ไม่เสนอ (๐ คะแนน)	(๑๐)

ข้อพิจารณา	คะแนน
๒.๔ การนำเสนอตัวอย่างต้นแบบ (Template) รายงานภัยคุกคามและการโจมตีทางไซเบอร์ โดยนำเสนอตัวอย่างเอกสารและแนวทางการบริหารจัดการรายงานภัยคุกคามและการโจมตีทางไซเบอร์ (๑) ครบถ้วน ถูกต้อง และมีตัวอย่างนำเสนอที่ชัดเจน (๕ คะแนน) (๒) ครบถ้วน และถูกต้อง (๓ คะแนน) (๓) ครบถ้วน แต่ไม่ถูกต้อง (๑ คะแนน) (๔) ไม่เสนอ (๐ คะแนน)	(๕)
๓. การนำเสนอแผนการติดตั้งระบบป้องกันการโจมตีผ่านช่องโหว่ซอฟท์แวร์สำหรับเครื่องคอมพิวเตอร์ลูกข่าย ทั้งนี้ สลค. จะให้คะแนนโดยพิจารณาว่า ผู้ยื่นข้อเสนอได้นำเสนอแนวคิดฯ เป็นไปตามวัตถุประสงค์ของโครงการ เป็นประโยชน์ต่อทางราชการเป็นสำคัญ และมีความเป็นไปได้ที่จะดำเนินการได้จริง ดังนี้	๑๐
๓.๑ นำเสนอแผนการติดตั้งฯ โดยแสดงรายละเอียดการดำเนินการแต่ละกิจกรรมอย่างละเอียด (๑) ครบถ้วน ถูกต้อง และมีตัวอย่างนำเสนอที่ชัดเจน (๓ คะแนน) (๒) ครบถ้วน และถูกต้อง (๒ คะแนน) (๓) ครบถ้วน แต่ไม่ถูกต้อง (๑ คะแนน) (๔) ไม่นำเสนอ (๐ คะแนน)	(๓)
๓.๒ นำเสนอแผนรับมือกรณีเกิดเหตุสุดวิสัยที่ส่งผลให้ไม่สามารถเข้าดำเนินการติดตั้งได้ทันตามกำหนดเวลา (๑) ครบถ้วน ถูกต้อง และมีตัวอย่างนำเสนอที่ชัดเจน (๓ คะแนน) (๒) ครบถ้วน และถูกต้อง (๒ คะแนน) (๓) ครบถ้วน แต่ไม่ถูกต้อง (๑ คะแนน) (๔) ไม่นำเสนอ (๐ คะแนน)	(๓)
๓.๓ นำเสนอซอฟต์แวร์ และทีมงานที่จะช่วยให้การติดตั้งระบบฯ สามารถดำเนินการได้สะดวกและรวดเร็วยิ่งขึ้น (๑) มีเจ้าหน้าที่ช่วยดำเนินการติดตั้ง (๑ คะแนน) (๒) มีซอฟต์แวร์ช่วยในการติดตั้งระบบจากส่วนกลาง (๒ คะแนน) (๓) แนวทางอื่นเพิ่มเติม (๑ คะแนน) (๔) ไม่นำเสนอ (๐ คะแนน)	(๔)

ข้อพิจารณา	คะแนน
๔. การนำเสนอแนวคิดในการจัดหาหรือพัฒนาระบบลงทะเบียนเข้าใช้งาน Wi-Fi โดยต้อง อ้างอิงตามข้อกำหนดขอบเขตการดำเนินงานและคุณลักษณะเฉพาะการดำเนินโครงการ ทั้งนี้ สลค. จะให้คะแนนโดยพิจารณาว่า ผู้ยื่นข้อเสนอได้นำเสนอแนวคิดฯ เป็นไปตามวัตถุประสงค์ของโครงการ เป็นประโยชน์ต่อทางราชการเป็นสำคัญ และมีความเป็นไปได้ที่จะดำเนินการได้จริง ดังนี้	**๑๐**
๔.๑ การนำเสนอตัวอย่างการออกแบบระบบต้นแบบ (Prototype) พร้อมอธิบายรูปแบบการทำงาน (๑) นำเสนอระบบเสมือนจริงทั้งระบบ (๓ คะแนน) (๒) นำเสนอภาพนิ่งและระบบเสมือนจริงบางส่วน (๒ คะแนน) (๓) นำเสนอภาพนิ่ง (๑ คะแนน) (๔) ไม่นำเสนอ (๐ คะแนน)	(๓)
๔.๒ นำเสนอแผนผังอธิบายรูปแบบการติดตั้งสถาปัตยกรรมระบบคอมพิวเตอร์และเครือข่ายที่เหมาะสมและปลอดภัย (๑) ครบถ้วน และมีตัวอย่างนำเสนอที่ชัดเจน (๑ คะแนน) (๒) วิธีการเชื่อมโยงกับระบบเครือข่ายของ สลค. (๑ คะแนน) (๓) มีการอธิบายรายละเอียดที่ชัดเจน (๑ คะแนน) (๔) ไม่นำเสนอ (๐ คะแนน)	(๓)
๔.๓ ระบบมีความทันสมัย สะดวก สอดคล้องกับความต้องการใช้งาน และลดภาระค่าใช้จ่ายของ สลค. ในอนาคต (๑) มีความทันสมัย (๑ คะแนน) (๒) สะดวกในการใช้งาน (๑ คะแนน) (๓) สอดคล้องกับความต้องการใช้งาน (๑ คะแนน) (๔) ลดภาระค่าใช้จ่ายของ สลค. ในอนาคต (๑ คะแนน)	(๔)
๕. จำนวนใบอนุญาตการใช้งานระบบป้องกันการโจมตีผ่านช่องโหว่ซอฟท์แวร์สำหรับเครื่องคอมพิวเตอร์ลูกข่ายรองรับได้สูงสุด ๕.๑ จำนวนไม่น้อยกว่า ๙๐๐ สิทธิ์การใช้งาน (๑๐ คะแนน) ๕.๒ จำนวนไม่น้อยกว่า ๘๐๐ สิทธิ์การใช้งาน (๕ คะแนน)	**๑๐**
๖. จำนวนอุปกรณ์ที่ระบบลงทะเบียนเข้าใช้งาน Wi-Fi ผ่าน MAC Address สามารถรองรับได้สูงสุด ๖.๑ จำนวนไม่น้อยกว่า ๒,๐๐๐ อุปกรณ์ (๑๐ คะแนน) ๖.๒ จำนวนไม่น้อยกว่า ๑,๕๐๐ อุปกรณ์ (๕ คะแนน)	**๑๐**

ข้อพิจารณา	คะแนน
๗. การนำเสนอแผนการดำเนินงานตั้งแต่การเริ่มต้นโครงการจนสิ้นสุดโครงการ และระยะเวลารับประกันความชำรุดบกพร่อง โดยแสดงรายละเอียดกิจกรรม พร้อมกำหนดระยะเวลาแล้วเสร็จของแต่ละกิจกรรม ทั้งนี้ สลค. จะให้คะแนนโดยพิจารณาว่า ได้นำเสนอแผนการดำเนินงานฯ เป็นไปตามวัตถุประสงค์ของโครงการ เป็นประโยชน์ต่อทางราชการเป็นสำคัญ มีความเป็นไปได้ที่จะดำเนินการได้จริง ดังนี้ ๗.๑ ครบถ้วน ถูกต้อง และมีตัวอย่างนำเสนอที่ชัดเจน (๕ คะแนน) ๗.๒ ครบถ้วน และถูกต้อง (๓ คะแนน) ๗.๓ ครบถ้วน แต่ไม่ถูกต้อง (๑ คะแนน) ๗.๔ ไม่เสนอ (๐ คะแนน)	**๕**
๘ การนำเสนอค่าบำรุงรักษาในช่วงปีที่ ๑, ๒ และ ๓ ภายหลังสิ้นสุดระยะเวลาการรับประกัน ๓ ปี ซึ่งมีเกณฑ์การให้คะแนน ดังนี้ คะแนน = (๑๕% ของราคากลาง – ค่าบำรุงรักษาที่นำเสนอเฉลี่ยรายปี x ๕) / ๑๕% ของราคากลาง ทั้งนี้ หากเสนอค่าบำรุงรักษาสูงกว่าร้อยละ ๑๕ ของราคากลาง ได้ ๐ คะแนน	**๕**
๙. การนำเสนอแนวทางการดำเนินการอื่น ๆ เพิ่มเติมนอกเหนือจากข้อ ๑ – ๘ ข้างต้นอันเป็นประโยชน์ในการปรับปรุงระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของ สลค. ซึ่งเป็นข้อเสนอที่ สลค. ไม่ได้ระบุไว้ในขอบเขตการดำเนินงานและคุณลักษณะเฉพาะการดำเนินโครงการ ทั้งนี้ สลค. จะให้คะแนนโดยพิจารณาว่า ผู้ยื่นข้อเสนอได้นำเสนอแนวทางการดำเนินการอื่น ๆ เพิ่มเติมที่เป็นไปตามวัตถุประสงค์ของโครงการ เป็นประโยชน์ต่อทางราชการเป็นสำคัญ มีความเป็นไปได้ที่จะดำเนินการได้จริง ดังนี้ ๙.๑ การนำเสนอทีมงานและวิธีการในการสนับสนุนการดำเนินการโครงการนี้ตลอดระยะเวลาการรับประกัน (๐-๕ คะแนน) ๙.๒ การนำเสนอระบบหรืออุปกรณ์ เพื่อให้โครงการนี้บรรลุวัตถุประสงค์อย่างมีประสิทธิภาพ (๐-๕ คะแนน) ๙.๓ แนวทางอื่น ๆ ที่จะเป็นประโยชน์ต่อ สลค. (๐-๕ คะแนน)	**๑๕**
รวม	**๑๐๐**

๑๙. ผู้ยื่นข้อเสนอจะต้องจัดทำเอกสารประกอบการนำเสนอตามข้อ ๑๘ โดยยื่นผ่านระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement : e-GP) ของกรมบัญชีกลาง เพื่อใช้ประกอบในการนำเสนอ

๒๐. ผู้ยื่นข้อเสนอจะต้องนำเสนอให้แก่คณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์ของ สลค. รายละไม่เกิน ๒ ชั่วโมง ภายใน ๕ วันทำการ นับถัดจากวันที่ยื่นเสนอราคาผ่านระบบ ซึ่ง สลค. จะพิจารณาตามลำดับก่อนหลังตามเวลาที่ผู้ยื่นข้อเสนอได้ยื่นข้อเสนอไว้เป็นสำคัญ ทั้งนี้ สลค.

ขอสงวนสิทธิ์ในการกำหนดวันที่นำเสนองาน และไม่เชิญผู้ยื่นข้อเสนอมานำเสนอแนวคิดฯ หากปรากฏว่าผู้ยื่นข้อเสนอดังกล่าวมีคุณสมบัติไม่เป็นไปตามที่ สลค. กำหนด หรือยื่นเอกสารไม่ครบถ้วน

๒๑. สลค. จะพิจารณาตัดสินคัดเลือกเฉพาะรายที่เสนอเอกสารหลักฐานครบถ้วนถูกต้องและปฏิบัติถูกต้องตามเงื่อนไขที่ สลค. กำหนดเท่านั้น โดยการพิจารณาผลการยื่นข้อเสนอประกวดราคาอิเล็กทรอนิกส์ครั้งนี้ สลค. พิจารณาตัดสินโดยใช้หลักเกณฑ์ราคาประกอบเกณฑ์อื่น โดยพิจารณาให้คะแนนตามปัจจัยหลักและน้ำหนักที่กำหนดรายละเอียด ดังนี้

ปัจจัย	กำหนดน้ำหนักเท่ากับร้อยละ
ราคาที่ยื่นข้อเสนอ	๓๐
คุณภาพของงานที่นำเสนอและคุณสมบัติที่เป็นประโยชน์ต่อทางราชการ (รายละเอียดตามข้อ ๑๘)	๗๐
รวม	**๑๐๐**

ผู้ยื่นข้อเสนอต้องยื่นข้อเสนอและเสนอราคาทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ ในวันที่ ..... ระหว่างเวลา ..... น. ถึง ..... น.

ผู้สนใจสามารถขอซื้อเอกสารประกวดราคาอิเล็กทรอนิกส์ ในราคาชุดละ ๕๐๐.๐๐ บาท ผ่านทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์และชำระเงินผ่านทางธนาคารในระหว่างวันที่ ..... ถึงวันที่ ..... โดยดาวน์โหลดเอกสารผ่านทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ ได้ภายหลังจากชำระเงินเป็นที่เรียบร้อยแล้วจนถึงก่อนวันเสนอราคา

ผู้สนใจสามารถดูรายละเอียดได้ที่เว็บไซต์ www.soc.go.th หรือ www.gprocurement.go.th หรือสอบถามทางโทรศัพท์หมายเลข ๐-๒๒๘๐-๙๐๐๐ ต่อ ๑๑๓๓ ในวันและเวลาราชการ

ผู้สนใจต้องการทราบรายละเอียดเพิ่มเติมเกี่ยวกับรายละเอียดคุณลักษณะเฉพาะ โปรดสอบถามมายังสำนักเลขาธิการคณะรัฐมนตรี ผ่านทางอีเมล์ procurement@soc.go.th หรือช่องทางตามที่กรมบัญชีกลางกำหนด ภายในวันที่ ..... โดยสำนักเลขาธิการคณะรัฐมนตรีจะชี้แจงรายละเอียดดังกล่าวผ่านทางเว็บไซต์ www.soc.go.th และ www.gprocurement.go.th ในวันที่ .....

ประกาศ ณ วันที่ เมษายน พ.ศ. ๒๕๖๕

(นางณัฐฏ์จารี อนันตศิลป์)

เลขาธิการคณะรัฐมนตรี

หมายเหตุ ผู้ประกอบการสามารถจัดเตรียมเอกสารประกอบการเสนอราคา (เอกสารส่วนที่ ๑ และเอกสารส่วนที่ ๒) ในระบบ e-GP ได้ตั้งแต่วันที่ ซื้อเอกสารจนถึงวันเสนอราคา

สำเนาถูกต้อง

นันทิรัตน์ แก้วภราดัย

(นางนันทิรัตน์ แก้วภราดัย)

ผู้อำนวยการสำนักงานเลขาธิการ

ประกาศขึ้นเว็บวันที่ ๑๑ เมษายน ๒๕๖๕

โดย นางนันทิรัตน์ แก้วภราดัย ผู้อำนวยการสำนักงานเลขาธิการ

(สำเนา)

เอกสารประกวดราคาซื้อด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding)

เลขที่ .....

การซื้อโครงการปรับปรุงระบบรักษาความมั่นคงปลอดภัยไซเบอร์

ตามประกาศ สำนักเลขาธิการคณะรัฐมนตรี

ลงวันที่ เมษายน ๒๕๖๕

สำนักเลขาธิการคณะรัฐมนตรี ซึ่งต่อไปนี้เรียกว่า "สลค." มีความประสงค์จะประกวดราคาซื้อด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ ตามรายการ ดังนี้

๑. ระบบรักษาความปลอดภัยระบบเครือข่ายระดับแอปพลิเคชัน (Application Firewall) จำนวน ๒ ชุด

๒. ระบบป้องกันการโจมตีผ่านช่องโหว่ซอฟท์แวร์สำหรับเครื่องคอมพิวเตอร์ลูกข่าย จำนวน ๑ ระบบ

๓. ระบบบริหารจัดการและตอบสนองต่อภัยคุกคามไซเบอร์แบบอัตโนมัติ จำนวน ๑ ระบบ

๔. ระบบรักษาความปลอดภัยระบบเครือข่ายระดับแอปพลิเคชัน (Application Firewall) ทดแทนระบบเดิม จำนวน ๑ ระบบ

๕. แนวทางการพัฒนาศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

๖. ระบบบริหารจัดการเครือข่ายแบบรวมศูนย์ จำนวน ๑ ระบบ

๗. ระบบลงทะเบียนเข้าใช้งาน Wi-Fi ทดแทนระบบเดิม จำนวน ๑ ระบบ

๘. จัดหาและติดตั้งใบรับรอง SSL Certificate จำนวน ๑ ชุด

๙. เครื่องคอมพิวเตอร์โน้ตบุ๊ก จำนวน ๕ เครื่อง

๑๐. การฝึกอบรม

๑๑. งานเอกสารและคู่มือ

พัสดุที่จะซื้อนี้ต้องเป็นของแท้ ของใหม่ ไม่เคยใช้งานมาก่อน ไม่เป็นของเก่าเก็บ อยู่ในสภาพที่จะใช้งานได้ทันทีและมีคุณลักษณะเฉพาะตรงตามที่กำหนดไว้ในเอกสารประกวดราคาซื้อด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ฉบับนี้ โดยมีข้อแนะนำและข้อกำหนด ดังต่อไปนี้

๑. เอกสารแนบท้ายเอกสารประกวดราคาอิเล็กทรอนิกส์

๑.๑ รายละเอียดคุณลักษณะเฉพาะ

๑.๒ แบบใบเสนอราคาที่กำหนดไว้ในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์

๑.๓ สัญญาซื้อขายทั่วไป

๑.๔ แบบหนังสือค้ำประกัน

(๑) หลักประกันการเสนอราคา

(๒) หลักประกันสัญญา

๑.๕ บทนิยาม

(๑) ผู้ที่มีผลประโยชน์ร่วมกัน

(๒) การขัดขวางการแข่งขันอย่างเป็นธรรม

๑.๖ แบบบัญชีเอกสารที่กำหนดไว้ในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์

(๑) บัญชีเอกสารส่วนที่ ๑

(๒) บัญชีเอกสารส่วนที่ ๒

๒. คุณสมบัติของผู้ยื่นข้อเสนอ

๒.๑ มีความสามารถตามกฎหมาย

๒.๒ ไม่เป็นบุคคลล้มละลาย

๒.๓ ไม่อยู่ระหว่างเลิกกิจการ

๒.๔ ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

๒.๕ ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

๒.๖ มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

๒.๗ เป็นบุคคลธรรมดาหรือนิติบุคคลผู้มีอาชีพขายพัสดุที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

๒.๘ ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่ สลค. ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

๒.๙ ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

๒.๑๐ ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ "กิจการร่วมค้า" ต้องมีคุณสมบัติดังนี้

กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงฯจะต้องมีการกำหนดสัดส่วนหน้าที่ และความรับผิดชอบในปริมาณงาน สิ่งของ หรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลักกิจการร่วมค้านั้นต้องใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

สำหรับข้อตกลงฯ ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมค้าหลัก ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน

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

๒.๑๒ ผู้ยื่นข้อเสนอต้องไม่อยู่ในฐานะเป็นผู้ไม่แสดงบัญชีรายรับรายจ่าย หรือแสดงบัญชี

รายรับรายจ่ายไม่ถูกต้องครบถ้วนในสาระสำคัญ ตามที่คณะกรรมการ ป.ป.ช. กำหนด

๒.๑๓ ผู้ยื่นข้อเสนอซึ่งได้รับคัดเลือกเป็นคู่สัญญาต้องรับและจ่ายเงินผ่านบัญชีธนาคาร เว้นแต่การจ่ายเงินแต่ละครั้งซึ่งมีมูลค่าไม่เกินสามหมื่นบาทคู่สัญญาอาจจ่ายเป็นเงินสดก็ได้ ตามที่คณะกรรมการ ป.ป.ช. กำหนด

๒.๑๔ ผู้ยื่นข้อเสนอต้องไม่เคยถูกยกเลิกสัญญาซื้อขาย หรือสัญญาจ้างบริการบำรุงรักษาก่อนหมดอายุสัญญา โดยไม่มีเหตุผลอันควรจากหน่วยงานใด ๆ

๒.๑๕ ผู้ยื่นข้อเสนอต้องมีผลงานเกี่ยวกับระบบคอมพิวเตอร์จากหน่วยงานของรัฐหรือหน่วยงานเอกชน โดยผลงานดังกล่าวจะต้องเป็นผลงานในการติดตั้งระบบเครือข่ายคอมพิวเตอร์และระบบรักษาความมั่นคงปลอดภัย อย่างน้อย ๒ สัญญาจ้าง และมีมูลค่าสัญญาละไม่น้อยกว่า ๒,๐๐๐,๐๐๐ บาท (สองล้านบาทถ้วน) และยังคงใช้ระบบงานดังกล่าวอยู่ในปัจจุบัน พร้อมเอกสารรายละเอียดของผลงานดังกล่าวอย่างชัดเจน โดย สลค. ขอสงวนสิทธิ์ที่จะตรวจสอบข้อเท็จจริงดังกล่าว

๒.๑๖ ผู้ยื่นข้อเสนอต้องเสนอรายชื่อคณะทำงานทั้งหมดที่จะเข้ามาดำเนินการตามโครงการนี้ โดยที่ภายในคณะทำงานจะต้องประกอบด้วยบุคลากรที่มีความเชี่ยวชาญด้านระบบรักษาความมั่นคงปลอดภัยไซเบอร์และระบบเครือข่ายคอมพิวเตอร์ และคณะทำงานทั้งหมดต้องมายืนยันตัวตนเข้าดำเนินการโครงการต่อ สลค. ในการส่งมอบงานงวดที่ ๑ ประกอบด้วย

ลำดับ	**คณะทำงาน**	**วุฒิการศึกษา**	**ประสบการณ์ด้านที่ตรงกับหน้าที่ในคณะทำงาน**	**จำนวน**	**ระยะเวลา**
๑	ผู้จัดการโครงการ (Project Manager)	ปริญญาโท	ไม่น้อยกว่า ๓ ปี	๑ คน	อย่างน้อยเดือนละ ๒ ครั้ง ตลอดระยะเวลาดำเนินโครงการ
๒	ผู้เชี่ยวชาญด้านระบบรักษาความมั่นคงปลอดภัยไซเบอร์	ปริญญาตรี	ไม่น้อยกว่า ๒ ปี และเคยได้รับ Certificate ด้านระบบรักษาความมั่นคงปลอดภัย	๑ คน	ตลอดระยะเวลาดำเนินโครงการ
๓	วิศวกรเครือข่าย (Network Engineer)	ปริญญาตรี	ไม่น้อยกว่า ๒ ปี และเคยได้รับ Certificate ด้าน Network	๑ คน	ตลอดระยะเวลาดำเนินโครงการ
๔	ผู้ประสานงานโครงการ	ปริญญาตรี	ไม่น้อยกว่า ๑ ปี	๑ คน	ตลอดระยะเวลาดำเนินโครงการ

ทั้งนี้ คณะทำงานดังกล่าวจะต้องมาปฏิบัติงานที่ สลค. ตามหน้าที่ที่ตนรับผิดชอบอย่างสม่ำเสมอตลอดระยะเวลาการ

ดำเนินงานโครงการ

๒.๑๗ ผู้ยื่นข้อเสนอต้องเสนอเอกสารแบบรูปหรือแคตตาล็อกแสดงรายละเอียดคุณลักษณะเฉพาะหรือคุณสมบัติของผลิตภัณฑ์ที่เสนอทุกรายการ โดยยื่นมาพร้อมกับการเสนอราคา ดังนี้

หัวข้อ	ข้อกำหนดของ สลค.	ข้อเสนอของบริษัท	เอกสารอ้างอิงหน้า/ข้อ
ระบุหัวข้อให้ตรงกับที่ สลค. กำหนด	ให้คัดลอกคุณลักษณะเฉพาะที่ สลค. กำหนด	ให้ระบุคุณลักษณะเฉพาะที่เสนอ	ให้ระบุหรืออ้างอิงเอกสารในข้อเสนอที่เกี่ยวข้องและขีดเส้นใต้คุณลักษณะเฉพาะที่ สลค. กำหนดลงในแคตตาล็อกหรือเอกสารที่เกี่ยวข้อง

๒.๑๘ การพิจารณาผลการยื่นข้อเสนอการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้ สลค. จะพิจารณาตัดสินโดยใช้เกณฑ์ราคาประกอบเกณฑ์อื่น โดยเกณฑ์อื่นเป็นการพิจารณาเกณฑ์การให้คะแนนจากผลงานที่ผ่านมา รูปแบบ และวิธีการดำเนินงาน ตลอดจนแนวทางการบริหารโครงการให้ประสบผลสำเร็จตามวัตถุประสงค์ของโครงการและข้อเสนอทางเทคนิคที่เป็นประโยชน์ต่อทางราชการเป็นสำคัญ โดยข้อเสนอต้องมีความเป็นไปได้ที่สามารถดำเนินการได้จริง และตรงกับความต้องการของ สลค. (คะแนนรวม ๑๐๐ คะแนน) และ สลค. ขอสงวนสิทธิ์ในการพิจารณาเฉพาะผู้ยื่นข้อเสนอที่ผ่านคุณสมบัติเบื้องต้นตามข้อ ๒.๑ - ๒.๑๗ ข้างต้นเท่านั้น ซึ่งเกณฑ์อื่นประกอบด้วยข้อพิจารณา ดังนี้

ข้อพิจารณา	คะแนน
๑. การนำเสนอผลงานที่ผ่านมาเกี่ยวกับการติดตั้งระบบเครือข่ายคอมพิวเตอร์และระบบรักษาความมั่นคงปลอดภัย อย่างน้อย ๒ สัญญาจ้าง และมีมูลค่าสัญญาละไม่น้อยกว่า ๒,๐๐๐,๐๐๐ บาท (สองล้านบาทถ้วน) และยังคงใช้ระบบงานดังกล่าวอยู่ในปัจจุบัน พร้อมเอกสารรายละเอียดของผลงานดังกล่าวอย่างชัดเจน โดย สลค. ขอสงวนสิทธิ์ที่จะตรวจสอบข้อเท็จจริงดังกล่าว ทั้งนี้ ผลงานดังกล่าวควรแสดงให้เห็นถึงประสบการณ์และความสามารถที่เกี่ยวข้องกับโครงการอย่างน้อย ดังนี้ ๑.๑ มีระบบรักษาความปลอดภัยระบบเครือข่ายระดับแอปพลิเคชัน (Application Firewall) (คะแนนเต็ม ๑ คะแนน) ๑.๒ มีระบบป้องกันการโจมตีผ่านช่องโหว่ซอฟท์แวร์สำหรับเครื่องคอมพิวเตอร์ลูกข่าย (คะแนนเต็ม ๑ คะแนน) ๑.๓ มีระบบบริหารจัดการและตอบสนองต่อภัยคุกคามไซเบอร์แบบอัตโนมัติ (คะแนนเต็ม ๑ คะแนน) ๑.๔ มีระบบบริหารจัดการเครือข่ายแบบรวมศูนย์ (คะแนนเต็ม ๑ คะแนน) ๑.๕ มีระบบลงทะเบียนเข้าใช้งาน Wi-Fi (คะแนนเต็ม ๑ คะแนน)	**๕**

ข้อพิจารณา	คะแนน
๒. การนำเสนอแนวทางการพัฒนาศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของ สลค. ตามโครงการนี้ ทั้งนี้ สลค. จะให้คะแนนโดยพิจารณาว่า ผู้ยื่นข้อเสนอได้นำเสนอแนวทางฯ ที่เป็นไปตามกฎหมายและมาตรฐานที่เกี่ยวข้อง เป็นไปตามวัตถุประสงค์ของโครงการ เป็นประโยชน์ต่อทางราชการเป็นสำคัญ และมีความเป็นไปได้ที่จะดำเนินการได้จริง ดังนี้	**๓๐**
๒.๑ การนำเสนอแนวทางการจัดทำร่างนโยบายในการรับมือเหตุการณ์ภัยคุกคามทางไซเบอร์ของ สลค. โดยอ้างอิงจากข้อกำหนดตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และแนวปฏิบัติของ NIST Cyber SecurityFramework (๑) ครบถ้วน ถูกต้อง และมีตัวอย่างนำเสนอที่ชัดเจน (๕ คะแนน) (๒) ครบถ้วน และถูกต้อง (๓ คะแนน) (๓) ครบถ้วน แต่ไม่ถูกต้อง (๑ คะแนน) (๔) ไม่เสนอ (๐ คะแนน)	(๕)
๒.๒ การนำเสนอแนวทางการจัดทำขั้นตอนการปฏิบัติงานต่าง ๆ ดังนี้ (๑) ขั้นตอนการเฝ้าระวังเหตุการณ์ภัยคุกคามและการโจมตีทางไซเบอร์ - ครบถ้วน ถูกต้อง และมีตัวอย่างนำเสนอที่ชัดเจน (๓ คะแนน) - ครบถ้วน และถูกต้อง (๒ คะแนน) - ครบถ้วน แต่ไม่ถูกต้อง (๑ คะแนน) - ไม่นำเสนอ (๐ คะแนน) (๒) กระบวนการจัดทำ Playbook Automation รวมทั้งวิธีการเชื่อมโยง (Integrate) เข้ากับระบบความปลอดภัยเดิมที่ สลค. มีอยู่ - ครบถ้วน ถูกต้อง และมีตัวอย่างนำเสนอที่ชัดเจน (๓ คะแนน) - ครบถ้วน และถูกต้อง (๒ คะแนน) - ครบถ้วน แต่ไม่ถูกต้อง (๑ คะแนน) - ไม่นำเสนอ (๐ คะแนน) (๓) กระบวนการในการสื่อสารเมื่อเกิดเหตุการณ์ภัยคุกคามและการโจมตี - ครบถ้วน ถูกต้อง และมีตัวอย่างนำเสนอที่ชัดเจน (๒ คะแนน) - ครบถ้วน และถูกต้อง (๑ คะแนน) - ไม่นำเสนอ (๐ คะแนน) (๔) แนวทางอื่นที่เป็นประโยชน์ต่อการดำเนินโครงการ - ครบถ้วน ถูกต้อง และมีตัวอย่างนำเสนอที่ชัดเจน (๒ คะแนน) - ครบถ้วน และถูกต้อง (๑ คะแนน) - ไม่นำเสนอ (๐ คะแนน)	(๑๐)

ข้อพิจารณา	คะแนน
๒.๓ การนำเสนอแนวทางการเชื่อมต่อระบบบริหารจัดการและตอบสนองต่อภัยคุกคามแบบอัตโนมัติให้สามารถทำงานร่วมกับระบบเครือข่ายและระบบรักษาความปลอดภัยเครือข่ายฯ ที่ สลค. มีอยู่เดิมได้ โดยนำเสนอวิธีการและแผนผังการเชื่อมต่อระบบฯ (๑) ครบถ้วน ถูกต้อง และมีตัวอย่างนำเสนอที่ชัดเจน (๑๐ คะแนน) (๒) ครบถ้วน และถูกต้อง (๗ คะแนน) (๓) ครบถ้วน แต่ไม่ถูกต้อง (๓ คะแนน) (๔) ไม่เสนอ (๐ คะแนน)	(๑๐)
๒.๔ การนำเสนอตัวอย่างต้นแบบ (Template) รายงานภัยคุกคามและการโจมตีทางไซเบอร์ โดยนำเสนอตัวอย่างเอกสารและแนวทางการบริหารจัดการรายงานภัยคุกคามและการโจมตีทางไซเบอร์ (๑) ครบถ้วน ถูกต้อง และมีตัวอย่างนำเสนอที่ชัดเจน (๕ คะแนน) (๒) ครบถ้วน และถูกต้อง (๓ คะแนน) (๓) ครบถ้วน แต่ไม่ถูกต้อง (๑ คะแนน) (๔) ไม่เสนอ (๐ คะแนน)	(๕)
๓. การนำเสนอแผนการติดตั้งระบบป้องกันการโจมตีผ่านช่องโหว่ซอฟท์แวร์สำหรับเครื่องคอมพิวเตอร์ลูกข่าย ทั้งนี้ สลค. จะให้คะแนนโดยพิจารณาว่า ผู้ยื่นข้อเสนอได้นำเสนอแนวคิดฯ เป็นไปตามวัตถุประสงค์ของโครงการ เป็นประโยชน์ต่อทางราชการเป็นสำคัญ และมีความเป็นไปได้ที่จะดำเนินการได้จริง ดังนี้	**๑๐**
๓.๑ นำเสนอแผนการติดตั้งฯ โดยแสดงรายละเอียดการดำเนินการแต่ละกิจกรรมอย่างละเอียด (๑) ครบถ้วน ถูกต้อง และมีตัวอย่างนำเสนอที่ชัดเจน (๓ คะแนน) (๒) ครบถ้วน และถูกต้อง (๒ คะแนน) (๓) ครบถ้วน แต่ไม่ถูกต้อง (๑ คะแนน) (๔) ไม่นำเสนอ (๐ คะแนน)	(๓)
๓.๒ นำเสนอแผนรับมือกรณีเกิดเหตุสุดวิสัยที่ส่งผลให้ไม่สามารถเข้าดำเนินการติดตั้งได้ทันตามกำหนดเวลา (๑) ครบถ้วน ถูกต้อง และมีตัวอย่างนำเสนอที่ชัดเจน (๓ คะแนน) (๒) ครบถ้วน และถูกต้อง (๒ คะแนน) (๓) ครบถ้วน แต่ไม่ถูกต้อง (๑ คะแนน) (๔) ไม่นำเสนอ (๐ คะแนน)	(๓)

ข้อพิจารณา	คะแนน
๓.๓ นำเสนอซอฟต์แวร์ และทีมงานที่จะช่วยให้การติดตั้งระบบฯ สามารถดำเนินการได้สะดวกและรวดเร็วยิ่งขึ้น (๑) มีเจ้าหน้าที่ช่วยดำเนินการติดตั้ง (๑ คะแนน) (๒) มีซอฟต์แวร์ช่วยในการติดตั้งระบบจากส่วนกลาง (๒ คะแนน) (๓) แนวทางอื่นเพิ่มเติม (๑ คะแนน) (๔) ไม่นำเสนอ (๐ คะแนน)	(๔)
๔. การนำเสนอแนวคิดในการจัดหาหรือพัฒนาระบบลงทะเบียนเข้าใช้งาน Wi-Fi โดยต้อง อ้างอิงตามข้อกำหนดขอบเขตการดำเนินงานและคุณลักษณะเฉพาะการดำเนินโครงการ ทั้งนี้ สลค. จะให้คะแนนโดยพิจารณาว่า ผู้ยื่นข้อเสนอได้นำเสนอแนวคิดฯ เป็นไปตามวัตถุประสงค์ของโครงการ เป็นประโยชน์ต่อทางราชการเป็นสำคัญ และมีความเป็นไปได้ที่จะดำเนินการได้จริง ดังนี้	**๑๐**
๔.๑ การนำเสนอตัวอย่างการออกแบบระบบต้นแบบ (Prototype) พร้อมอธิบายรูปแบบการทำงาน (๑) นำเสนอระบบเสมือนจริงทั้งระบบ (๓ คะแนน) (๒) นำเสนอภาพนิ่งและระบบเสมือนจริงบางส่วน (๒ คะแนน) (๓) นำเสนอภาพนิ่ง (๑ คะแนน) (๔) ไม่นำเสนอ (๐ คะแนน)	(๓)
๔.๒ นำเสนอแผนผังอธิบายรูปแบบการติดตั้งสถาปัตยกรรมระบบคอมพิวเตอร์และเครือข่ายที่เหมาะสมและปลอดภัย (๑) ครบถ้วน และมีตัวอย่างนำเสนอที่ชัดเจน (๑ คะแนน) (๒) วิธีการเชื่อมโยงกับระบบเครือข่ายของ สลค. (๑ คะแนน) (๓) มีการอธิบายรายละเอียดที่ชัดเจน (๑ คะแนน) (๔) ไม่นำเสนอ (๐ คะแนน)	(๓)
๔.๓ ระบบมีความทันสมัย สะดวก สอดคล้องกับความต้องการใช้งาน และลดภาระค่าใช้จ่ายของ สลค. ในอนาคต (๑) มีความทันสมัย (๑ คะแนน) (๒) สะดวกในการใช้งาน (๑ คะแนน) (๓) สอดคล้องกับความต้องการใช้งาน (๑ คะแนน) (๔) ลดภาระค่าใช้จ่ายของ สลค. ในอนาคต (๑ คะแนน)	(๔)
๕. จำนวนใบอนุญาตการใช้งานระบบป้องกันการโจมตีผ่านช่องโหว่ซอฟท์แวร์สำหรับเครื่องคอมพิวเตอร์ลูกข่ายรองรับได้สูงสุด ๕.๑ จำนวนไม่น้อยกว่า ๙๐๐ สิทธิ์การใช้งาน (๑๐ คะแนน) ๕.๒ จำนวนไม่น้อยกว่า ๘๐๐ สิทธิ์การใช้งาน (๕ คะแนน)	**๑๐**

ข้อพิจารณา	คะแนน
๖. จำนวนอุปกรณ์ที่ระบบลงทะเบียนเข้าใช้งาน Wi-Fi ผ่าน MAC Address สามารถรองรับได้สูงสุด ๖.๑ จำนวนไม่น้อยกว่า ๒,๐๐๐ อุปกรณ์ (๑๐ คะแนน) ๖.๒ จำนวนไม่น้อยกว่า ๑,๕๐๐ อุปกรณ์ (๕ คะแนน)	**๑๐**
๗. การนำเสนอแผนการดำเนินงานตั้งแต่การเริ่มต้นโครงการจนสิ้นสุดโครงการ และระยะเวลารับประกันความชำรุดบกพร่อง โดยแสดงรายละเอียดกิจกรรม พร้อมกำหนดระยะเวลาแล้วเสร็จของแต่ละกิจกรรม ทั้งนี้ สลค. จะให้คะแนนโดยพิจารณาว่า ได้นำเสนอแผนการดำเนินงานฯ เป็นไปตามวัตถุประสงค์ของโครงการ เป็นประโยชน์ต่อทางราชการเป็นสำคัญ มีความเป็นไปได้ที่จะดำเนินการได้จริง ดังนี้ ๗.๑ ครบถ้วน ถูกต้อง และมีตัวอย่างนำเสนอที่ชัดเจน (๕ คะแนน) ๗.๒ ครบถ้วน และถูกต้อง (๓ คะแนน) ๗.๓ ครบถ้วน แต่ไม่ถูกต้อง (๑ คะแนน) ๗.๔ ไม่เสนอ (๐ คะแนน)	**๕**
๘ การนำเสนอค่าบำรุงรักษาในช่วงปีที่ ๑, ๒ และ ๓ ภายหลังสิ้นสุดระยะเวลาการรับประกัน ๓ ปี ซึ่งมีเกณฑ์การให้คะแนน ดังนี้ คะแนน = (๑๕% ของราคากลาง – ค่าบำรุงรักษาที่นำเสนอเฉลี่ยรายปี x ๕) / ๑๕% ของราคากลาง ทั้งนี้ หากเสนอค่าบำรุงรักษาสูงกว่าร้อยละ ๑๕ ของราคากลาง ได้ ๐ คะแนน	**๕**
๙. การนำเสนอแนวทางการดำเนินการอื่น ๆ เพิ่มเติมนอกเหนือจากข้อ ๑ – ๘ ข้างต้นอันเป็นประโยชน์ในการปรับปรุงระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของ สลค. ซึ่งเป็นข้อเสนอที่ สลค. ไม่ได้ระบุไว้ในขอบเขตการดำเนินงานและคุณลักษณะเฉพาะการดำเนินโครงการ ทั้งนี้ สลค. จะให้คะแนนโดยพิจารณาว่า ผู้ยื่นข้อเสนอได้นำเสนอแนวทางการดำเนินการอื่น ๆ เพิ่มเติมที่เป็นไปตามวัตถุประสงค์ของโครงการ เป็นประโยชน์ต่อทางราชการเป็นสำคัญ มีความเป็นไปได้ที่จะดำเนินการได้จริง ดังนี้ ๙.๑ การนำเสนอทีมงานและวิธีการในการสนับสนุนการดำเนินการโครงการนี้ตลอดระยะเวลาการรับประกัน (๐-๕ คะแนน) ๙.๒ การนำเสนอระบบหรืออุปกรณ์ เพื่อให้โครงการนี้บรรลุวัตถุประสงค์อย่างมีประสิทธิภาพ (๐-๕ คะแนน) ๙.๓ แนวทางอื่น ๆ ที่จะเป็นประโยชน์ต่อ สลค. (๐-๕ คะแนน)	**๑๕**
รวม	**๑๐๐**

๒.๑๙ ผู้ยื่นข้อเสนอจะต้องจัดทำเอกสารประกอบการนำเสนอตามข้อ ๒.๑๘ โดยยื่นผ่านระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement : e-GP)

ของกรมบัญชีกลาง เพื่อใช้ประกอบในการนำเสนอ

๒.๒๐ ผู้ยื่นข้อเสนอจะต้องนำเสนอให้แก่คณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์ของ สลค. รายละไม่เกิน ๒ ชั่วโมง ภายใน ๕ วันทำการ นับถัดจากวันที่ยื่นเสนอราคาผ่านระบบ ซึ่ง สลค. จะพิจารณาตามลำดับก่อนหลังตามเวลาที่ผู้ยื่นข้อเสนอได้ยื่นข้อเสนอไว้เป็นสำคัญ ทั้งนี้ สลค. ขอสงวนสิทธิ์ในการกำหนดวันที่นำเสนองาน และไม่เชิญผู้ยื่นข้อเสนอมานำเสนอแนวคิดฯ หากปรากฏว่าผู้ยื่นข้อเสนอดังกล่าวมีคุณสมบัติไม่เป็นไปตามที่ สลค. กำหนด หรือยื่นเอกสารไม่ครบถ้วน

๒.๒๑ สลค. จะพิจารณาตัดสินคัดเลือกเฉพาะรายที่เสนอเอกสารหลักฐานครบถ้วนถูกต้องและปฏิบัติถูกต้องตามเงื่อนไขที่ สลค. กำหนดเท่านั้น โดยการพิจารณาผลการยื่นข้อเสนอประกวดราคาอิเล็กทรอนิกส์ครั้งนี้ สลค. พิจารณาตัดสินโดยใช้หลักเกณฑ์ราคาประกอบเกณฑ์อื่น โดยพิจารณาให้คะแนนตามปัจจัยหลักและน้ำหนักที่กำหนดรายละเอียด ดังนี้

ปัจจัย	กำหนดน้ำหนักเท่ากับร้อยละ
ราคาที่ยื่นข้อเสนอ	๓๐
คุณภาพของงานที่นำเสนอและคุณสมบัติที่เป็นประโยชน์ต่อทางราชการ (รายละเอียดตามข้อ ๒.๑๘)	๗๐
รวม	**๑๐๐**

๓. หลักฐานการยื่นข้อเสนอ

ผู้ยื่นข้อเสนอจะต้องเสนอเอกสารหลักฐานยื่นมาพร้อมกับการเสนอราคาทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ โดยแยกเป็น ๒ ส่วน คือ

๓.๑ ส่วนที่ ๑ อย่างน้อยต้องมีเอกสารดังต่อไปนี้

(๑) ในกรณีผู้ยื่นข้อเสนอเป็นนิติบุคคล

(ก) ห้างหุ้นส่วนสามัญหรือห้างหุ้นส่วนจำกัด ให้ยื่นสำเนาหนังสือรับรองการจดทะเบียนนิติบุคคล บัญชีรายชื่อหุ้นส่วนผู้จัดการ ผู้มีอำนาจควบคุม (ถ้ามี) พร้อมทั้งรับรองสำเนาถูกต้อง

(ข) บริษัทจำกัดหรือบริษัทมหาชนจำกัด ให้ยื่นสำเนาหนังสือรับรองการจดทะเบียนนิติบุคคล หนังสือบริคณห์สนธิ บัญชีรายชื่อกรรมการผู้จัดการ ผู้มีอำนาจควบคุม (ถ้ามี) และบัญชีผู้ถือหุ้นรายใหญ่ (ถ้ามี) พร้อมทั้งรับรองสำเนาถูกต้อง

(๒) ในกรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดาหรือคณะบุคคลที่มิใช่นิติบุคคล ให้ยื่นสำเนาบัตรประจำตัวประชาชนของผู้นั้น สำเนาข้อตกลงที่แสดงถึงการเข้าเป็นหุ้นส่วน (ถ้ามี) สำเนาบัตรประจำตัวประชาชนของผู้เป็นหุ้นส่วน หรือสำเนาหนังสือเดินทางของผู้เป็นหุ้นส่วนที่มิได้ถือสัญชาติไทย พร้อมทั้งรับรองสำเนาถูกต้อง

(๓) ในกรณีผู้ยื่นข้อเสนอเป็นผู้ยื่นข้อเสนอร่วมกันในฐานะเป็นผู้ร่วมค้า ให้ยื่นสำเนาสัญญาของการเข้าร่วมค้า และเอกสารตามที่ระบุไว้ใน (๑) หรือ (๒) ของผู้ร่วมค้า แล้วแต่กรณี

(๔) เอกสารเพิ่มเติมอื่นๆ

(๔.๑) สำเนาใบทะเบียนพาณิชย์ (ถ้ามี)

(๔.๒) สำเนาใบทะเบียนภาษีมูลค่าเพิ่ม (ถ้ามี)

(๕) บัญชีเอกสารส่วนที่ ๑ ทั้งหมดที่ได้ยื่นพร้อมกับการเสนอราคาทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ ตามแบบในข้อ ๑.๖ (๑) โดยไม่ต้องแนบในรูปแบบ PDF File (Portable Document Format)

ทั้งนี้ เมื่อผู้ยื่นข้อเสนอดำเนินการแนบไฟล์เอกสารตามบัญชีเอกสารส่วนที่ ๑ ครบถ้วน ถูกต้องแล้ว ระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์จะสร้างบัญชีเอกสารส่วนที่ ๑ ตามแบบในข้อ ๑.๖ (๑) ให้โดยผู้ยื่นข้อเสนอไม่ต้องแนบบัญชีเอกสารส่วนที่ ๑ ดังกล่าวในรูปแบบ PDF File (Portable Document Format)

๓.๒ ส่วนที่ ๒ อย่างน้อยต้องมีเอกสารดังต่อไปนี้

(๑) ในกรณีที่ผู้ยื่นข้อเสนอมอบอำนาจให้บุคคลอื่นกระทำการแทนให้แนบหนังสือมอบอำนาจซึ่งติดอากรแสตมป์ตามกฎหมาย โดยมีหลักฐานแสดงตัวตนของผู้มอบอำนาจและผู้รับมอบอำนาจ ทั้งนี้หากผู้รับมอบอำนาจเป็นบุคคลธรรมดาต้องเป็นผู้ที่บรรลุนิติภาวะตามกฎหมายแล้วเท่านั้น

(๒) แคตตาล็อกและ/หรือแบบรูปรายการละเอียดคุณลักษณะเฉพาะ ตามข้อ ๔.๔

(๓) รายการพิจารณาที่ ๑ โครงการปรับปรุงระบบรักษาความมั่นคงปลอดภัยไซเบอร์

(๓.๑) หลักประกันการเสนอราคา ตามข้อ ๕

(๓.๒) สำเนาใบขึ้นทะเบียนผู้ประกอบการวิสาหกิจขนาดกลางและขนาดย่อม (SMEs) (ถ้ามี)

(๓.๓) สำเนาหนังสือรับรองสินค้า Made In Thailand ของสภาอุตสาหกรรมแห่งประเทศไทย (ถ้ามี)

(๔) บัญชีเอกสารส่วนที่ ๒ ทั้งหมดที่ได้ยื่นพร้อมกับการเสนอราคาทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ ตามแบบในข้อ ๑.๖ (๒) โดยไม่ต้องแนบในรูปแบบ PDF File (Portable Document Format)

ทั้งนี้ เมื่อผู้ยื่นข้อเสนอดำเนินการแนบไฟล์เอกสารตามบัญชีเอกสารส่วนที่ ๒ ครบถ้วน ถูกต้องแล้ว ระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์จะสร้างบัญชีเอกสารส่วนที่ ๒ ตามแบบในข้อ ๑.๖ (๒) ให้โดยผู้ยื่นข้อเสนอไม่ต้องแนบบัญชีเอกสารส่วนที่ ๒ ดังกล่าวในรูปแบบ PDF File (Portable Document Format)

๔. การเสนอราคา

๔.๑ ผู้ยื่นข้อเสนอต้องยื่นข้อเสนอและเสนอราคาทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ตามที่กำหนดไว้ในเอกสารประกวดราคาอิเล็กทรอนิกส์นี้ โดยไม่มีเงื่อนไขใดๆ ทั้งสิ้น และจะต้องกรอกข้อความให้ถูกต้องครบถ้วน พร้อมทั้งหลักฐานแสดงตัวตนและทำการยืนยันตัวตนของผู้ยื่นข้อเสนอโดยไม่ต้องแนบใบเสนอราคาในรูปแบบ PDF File (Portable Document Format)

๔.๒ ในการเสนอราคาให้เสนอราคาเป็นเงินบาท และเสนอราคาได้เพียงครั้งเดียวและราคาเดียวโดยเสนอราคารวม และหรือราคาต่อหน่วย และหรือต่อรายการ ตามเงื่อนไขที่ระบุไว้ท้ายใบเสนอราคาให้ถูกต้อง ทั้งนี้ ราคารวมที่เสนอจะต้องตรงกันทั้งตัวเลขและตัวหนังสือ ถ้าตัวเลขและตัวหนังสือไม่ตรงกัน ให้ถือตัวหนังสือเป็นสำคัญ โดยคิดราคารวมทั้งสิ้นซึ่งรวมค่าภาษีมูลค่าเพิ่ม ภาษีอากรอื่น ค่าขนส่ง ค่าจดทะเบียน และค่าใช้จ่ายอื่นๆ ทั้งปวงไว้แล้ว จนกระทั่งส่งมอบพัสดุให้ ณ สำนักเลขาธิการคณะรัฐมนตรี กรุงเทพฯ

ราคาที่เสนอจะต้องเสนอกำหนดยืนราคาไม่น้อยกว่า ๙๐ วัน ตั้งแต่วันเสนอราคาโดย

ภายในกำหนดยืนราคา ผู้ยื่นข้อเสนอต้องรับผิดชอบราคาที่ตนได้เสนอไว้ และจะถอนการเสนอราคามิได้

๔.๓ ผู้ยื่นข้อเสนอจะต้องเสนอกำหนดเวลาส่งมอบพัสดุไม่เกิน ๑๕๐ วัน นับถัดจากวันลงนามในสัญญาซื้อขาย หรือวันที่ได้รับหนังสือแจ้งจาก สลค. ให้ส่งมอบพัสดุ

๔.๔ ผู้ยื่นข้อเสนอจะต้องส่งแคตตาล็อก และหรือรายละเอียดคุณลักษณะเฉพาะของโครงการปรับปรุงระบบรักษาความมั่นคงปลอดภัยไซเบอร์ ไปพร้อมการเสนอราคาทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ เพื่อประกอบการพิจารณา หลักฐานดังกล่าวนี้ สลค.จะยึดไว้เป็นเอกสารของทางราชการ

สำหรับแคตตาล็อกที่แนบให้พิจารณา หากเป็นสำเนารูปถ่ายจะต้องรับรองสำเนาถูกต้องโดยผู้มีอำนาจทำนิติกรรมแทนนิติบุคคล หากคณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์มีความประสงค์จะขอดูต้นฉบับแคตตาล็อก ผู้ยื่นข้อเสนอจะต้องนำต้นฉบับมาให้คณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์ตรวจสอบภายใน ๓ วัน

๔.๕ ก่อนเสนอราคา ผู้ยื่นข้อเสนอควรตรวจดูร่างสัญญา รายละเอียดคุณลักษณะเฉพาะฯลฯ ให้ถี่ถ้วนและเข้าใจเอกสารประกวดราคาอิเล็กทรอนิกส์ทั้งหมดเสียก่อนที่จะตกลงยื่นข้อเสนอตามเงื่อนไขในเอกสารประกวดราคาซื้ออิเล็กทรอนิกส์

๔.๖ ผู้ยื่นข้อเสนอจะต้องยื่นข้อเสนอและเสนอราคาทางระบบการจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ในวันที่ ..... ระหว่างเวลา ..... น. ถึง ..... น. และเวลาในการเสนอราคาให้ถือตามเวลาของระบบการจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์เป็นเกณฑ์

เมื่อพ้นกำหนดเวลายื่นข้อเสนอและเสนอราคาแล้ว จะไม่รับเอกสารการยื่นข้อเสนอและการเสนอราคาใดๆ โดยเด็ดขาด

๔.๗ ผู้ยื่นข้อเสนอต้องจัดทำเอกสารสำหรับใช้ในการเสนอราคาในรูปแบบไฟล์เอกสารประเภท PDF File (Portable Document Format) โดยผู้ยื่นข้อเสนอต้องเป็นผู้รับผิดชอบตรวจสอบความครบถ้วนถูกต้อง และชัดเจนของเอกสาร PDF File ก่อนที่จะยืนยันการเสนอราคา แล้วจึงส่งข้อมูล (Upload) เพื่อเป็นการเสนอราคาให้แก่ สลค. ผ่านทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์

๔.๘ คณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์ จะดำเนินการตรวจสอบคุณสมบัติของผู้ยื่นข้อเสนอแต่ละรายว่า เป็นผู้ยื่นข้อเสนอที่มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่น ตามข้อ ๑.๕ (๑) หรือไม่ หากปรากฏว่าผู้ยื่นข้อเสนอรายใดเป็นผู้ยื่นข้อเสนอที่มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่น คณะกรรมการฯ จะตัดรายชื่อผู้ยื่นข้อเสนอที่มีผลประโยชน์ร่วมกันนั้นออกจากการเป็นผู้ยื่นข้อเสนอ

หากปรากฏต่อคณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์ว่า ก่อนหรือในขณะที่มีการพิจารณาข้อเสนอ มีผู้ยื่นข้อเสนอรายใดกระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมตามข้อ ๑.๕ (๒) และคณะกรรมการฯ เชื่อว่ามีการกระทำอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรม คณะกรรมการฯ จะตัดรายชื่อผู้ยื่นข้อเสนอรายนั้นออกจากการเป็นผู้ยื่นข้อเสนอ และสลค. จะพิจารณาลงโทษผู้ยื่นข้อเสนอดังกล่าวเป็นผู้ทิ้งงาน เว้นแต่ สลค. จะพิจารณาเห็นว่าผู้ยื่นข้อเสนอรายนั้นมิใช่เป็นผู้ริเริ่มให้มีการกระทำดังกล่าวและได้ให้ความร่วมมือเป็นประโยชน์ต่อการพิจารณาของ สลค.

๔.๙ ผู้ยื่นข้อเสนอจะต้องปฏิบัติ ดังนี้

(๑) ปฏิบัติตามเงื่อนไขที่ระบุไว้ในเอกสารประกวดราคาอิเล็กทรอนิกส์

(๒) ราคาที่เสนอจะต้องเป็นราคาที่รวมภาษีมูลค่าเพิ่ม และภาษีอื่นๆ (ถ้ามี) รวมค่าใช้

จ่ายทั้งปวงไว้ด้วยแล้ว

(๓) ผู้ยื่นข้อเสนอจะต้องลงทะเบียนเพื่อเข้าสู่กระบวนการเสนอราคา ตามวัน เวลา ที่กำหนด

(๔) ผู้ยื่นข้อเสนอจะถอนการเสนอราคาที่เสนอแล้วไม่ได้

(๕) ผู้ยื่นข้อเสนอต้องศึกษาและทำความเข้าใจในระบบและวิธีการเสนอราคาด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ ของกรมบัญชีกลางที่แสดงไว้ในเว็บไซต์ www.gprocurement.go.th

๕. หลักประกันการเสนอราคา

ผู้ยื่นข้อเสนอต้องวางหลักประกันการเสนอราคาพร้อมกับการเสนอราคาทางระบบการจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ โดยใช้หลักประกันอย่างหนึ่งอย่างใดดังต่อไปนี้ จำนวน ๒,๓๕๗,๘๕๐.๐๐ บาท (สองล้านสามแสนห้าหมื่นเจ็ดพันแปดร้อยห้าสิบบาทถ้วน)

๕.๑ เช็คหรือดราฟท์ที่ธนาคารเซ็นสั่งจ่าย ซึ่งเป็นเช็คหรือดราฟท์ลงวันที่ที่ใช้เช็คหรือดราฟท์นั้นชำระต่อเจ้าหน้าที่ในวันที่ยื่นข้อเสนอ หรือก่อนวันนั้นไม่เกิน ๓ วันทำการ

๕.๒ หนังสือค้ำประกันอิเล็กทรอนิกส์ของธนาคารภายในประเทศตามแบบที่คณะกรรมการนโยบายกำหนด

๕.๓ พันธบัตรรัฐบาลไทย

๕.๔ หนังสือค้ำประกันของบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยอนุโลมให้ใช้ตามตัวอย่างหนังสือค้ำประกันของธนาคารที่คณะกรรมการนโยบายกำหนด

กรณีที่ผู้ยื่นข้อเสนอนำเช็คหรือดราฟท์ที่ธนาคารสั่งจ่ายหรือพันธบัตรรัฐบาลไทยหรือหนังสือค้ำประกันของบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ มาวางเป็นหลักประกันการเสนอราคาจะต้องส่งต้นฉบับเอกสารดังกล่าวมาให้สลค.ตรวจสอบความถูกต้องในวันที่ ..... ระหว่างเวลา ..... น. ถึง ..... น.

กรณีที่ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ "กิจการร่วมค้า" ประสงค์จะใช้หนังสือค้ำประกันอิเล็กทรอนิกส์ของธนาคารในประเทศเป็นหลักประกันการเสนอราคาให้ระบุชื่อผู้เข้าร่วมค้ารายที่สัญญาร่วมค้ากำหนดให้เป็นผู้เข้ายื่นข้อเสนอกับหน่วยงานของรัฐเป็นผู้ยื่นข้อเสนอ

หลักประกันการเสนอราคาตามข้อนี้ สลค.จะคืนให้ผู้ยื่นข้อเสนอหรือผู้ค้ำประกันภายใน ๑๕ วัน นับถัดจากวันที่สลค.ได้พิจารณาเห็นชอบรายงานผลคัดเลือกผู้ชนะการประกวดราคาเรียบร้อยแล้ว เว้นแต่ผู้ยื่นข้อเสนอรายที่คัดเลือกไว้ซึ่งเสนอราคาต่ำสุดหรือได้คะแนนรวมสูงสุดไม่เกิน ๓ ราย ให้คืนได้ต่อเมื่อได้ทำสัญญาหรือข้อตกลง หรือผู้ยื่นข้อเสนอได้พ้นจากข้อผูกพันแล้ว

การคืนหลักประกันการเสนอราคา ไม่ว่าในกรณีใด ๆ จะคืนให้โดยไม่มีดอกเบี้ย

๖. หลักเกณฑ์และสิทธิ์ในการพิจารณา

๖.๑ ในการพิจารณาผลการยื่นข้อเสนอประกวดราคาอิเล็กทรอนิกส์ครั้งนี้ สลค.จะพิจารณาตัดสินโดยใช้หลักเกณฑ์ ราคาประกอบเกณฑ์อื่น

๖.๒ ในการพิจารณาผู้ชนะการยื่นข้อเสนอ ส่วนราชการจะใช้หลักเกณฑ์ราคาประกอบเกณฑ์

อื่น (Price Performance) โดยพิจารณาให้คะแนนตามปัจจัยหลักและน้ำหนักที่กำหนด ดังนี้

๖.๒.๑ รายการพิจารณา คือ โครงการปรับปรุงระบบรักษาความมั่นคงปลอดภัยไซเบอร์

(๑) ราคาที่เสนอราคา (ตัวแปรหลัก) กำหนดน้ำหนักเท่ากับร้อยละ ๓๐

(๒) ข้อเสนอด้านเทคนิคหรือข้อเสนอื่นๆ กำหนดน้ำหนักเท่ากับร้อยละ ๗๐

๖.๓ หากผู้ยื่นข้อเสนอรายใดมีคุณสมบัติไม่ถูกต้องตามข้อ ๒ หรือยื่นหลักฐานการยื่นข้อเสนอไม่ถูกต้อง หรือไม่ครบถ้วนตามข้อ ๓ หรือยื่นข้อเสนอไม่ถูกต้องตามข้อ ๔ คณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์จะไม่รับพิจารณาข้อเสนอของผู้ยื่นข้อเสนอรายนั้น เว้นแต่ ผู้ยื่นข้อเสนอรายใดเสนอเอกสารทางเทคนิคหรือรายละเอียดคุณลักษณะเฉพาะของพัสดุที่จะขายไม่ครบถ้วน หรือเสนอรายละเอียดแตกต่างไปจากเงื่อนไขที่สลค.กำหนดไว้ในประกาศและเอกสารประกวดราคาอิเล็กทรอนิกส์ ในส่วนที่มิใช่สาระสำคัญและความแตกต่างนั้นไม่มีผลทำให้เกิดการได้เปรียบเสียเปรียบต่อผู้ยื่นข้อเสนอรายอื่น หรือเป็นการผิดพลาดเล็กน้อย คณะกรรมการฯ อาจพิจารณาผ่อนปรนการตัดสิทธิผู้ยื่นข้อเสนอรายนั้น

๖.๔ สลค.สงวนสิทธิ์ไม่พิจารณาข้อเสนอของผู้ยื่นข้อเสนอโดยไม่มีการผ่อนผัน ในกรณีดังต่อไปนี้

(๑) ไม่ปรากฏชื่อผู้ยื่นข้อเสนอรายนั้นในบัญชีรายชื่อผู้รับเอกสารประกวดราคาอิเล็กทรอนิกส์ทางระบบจัดซื้อจัดจ้างด้วยอิเล็กทรอนิกส์ หรือบัญชีรายชื่อผู้ซื้อเอกสารประกวดราคาอิเล็กทรอนิกส์ทางระบบจัดซื้อจัดจ้างด้วยอิเล็กทรอนิกส์ ของสลค.

(๒) ไม่กรอกชื่อผู้ยื่นข้อเสนอในการเสนอราคาทางระบบจัดซื้อจัดจ้างด้วยอิเล็กทรอนิกส์

(๓) เสนอรายละเอียดแตกต่างไปจากเงื่อนไขที่กำหนดในเอกสารประกวดราคาอิเล็กทรอนิกส์ที่เป็นสาระสำคัญ หรือมีผลทำให้เกิดความได้เปรียบเสียเปรียบแก่ผู้ยื่นข้อเสนอรายอื่น

๖.๕ ในการตัดสินการประกวดราคาอิเล็กทรอนิกส์หรือในการทำสัญญา คณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์หรือสลค.มีสิทธิให้ผู้ยื่นข้อเสนอชี้แจงข้อเท็จจริงเพิ่มเติมได้ สลค. มีสิทธิที่จะไม่รับข้อเสนอ ไม่รับราคา หรือไม่ทำสัญญา หากข้อเท็จจริงดังกล่าวไม่เหมาะสมหรือไม่ถูกต้อง

๖.๖ สลค.ทรงไว้ซึ่งสิทธิที่จะไม่รับราคาต่ำสุด หรือราคาหนึ่งราคาใด หรือราคาที่เสนอทั้งหมดก็ได้ และอาจพิจารณาเลือกซื้อในจำนวน หรือขนาด หรือเฉพาะรายการหนึ่งรายการใด หรืออาจจะยกเลิกการประกวดราคาอิเล็กทรอนิกส์โดยไม่พิจารณาจัดซื้อเลยก็ได้ สุดแต่จะพิจารณา ทั้งนี้ เพื่อประโยชน์ของทางราชการเป็นสำคัญ และให้ถือว่าการตัดสินของ สลค.เป็นเด็ดขาด ผู้ยื่นข้อเสนอจะเรียกร้องค่าใช้จ่าย หรือค่าเสียหายใดๆ มิได้ รวมทั้งสลค. จะพิจารณายกเลิกการประกวดราคาอิเล็กทรอนิกส์และลงโทษผู้ยื่นข้อเสนอเป็นผู้ทิ้งงาน ไม่ว่าจะเป็นผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกหรือไม่ก็ตาม หากมีเหตุที่เชื่อถือได้ว่าการยื่นข้อเสนอกระทำการโดยไม่สุจริต เช่น การเสนอเอกสารอันเป็นเท็จ หรือใช้ชื่อบุคคลธรรมดา หรือนิติบุคคลอื่นมาเสนอราคาแทน เป็นต้น

ในกรณีที่ผู้ยื่นข้อเสนอรายที่เสนอราคาต่ำสุด เสนอราคาต่ำจนคาดหมายได้ว่าไม่อาจดำเนินงานตามเอกสารประกวดราคาอิเล็กทรอนิกส์ได้ คณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์หรือสลค. จะให้ผู้ยื่นข้อเสนอนั้นชี้แจงและแสดงหลักฐานที่ทำให้เชื่อได้ว่า ผู้ยื่นข้อเสนอสามารถดำเนินการตามเอกสารประกวดราคาอิเล็กทรอนิกส์ให้เสร็จสมบูรณ์ หากคำชี้แจงไม่เป็นที่รับฟังได้ สลค. มีสิทธิที่จะไม่รับข้อเสนอหรือไม่รับราคาของผู้ยื่นข้อเสนอรายนั้น ทั้งนี้ ผู้ยื่นข้อเสนอดังกล่าวไม่มีสิทธิเรียกร้องค่าใช้จ่ายหรือค่าเสียหายใดๆ จากสลค.

๖.๗ ก่อนลงนามในสัญญาสลค.อาจประกาศยกเลิกการประกวดราคาอิเล็กทรอนิกส์ หากปรากฏว่ามีการกระทำที่เข้าลักษณะผู้ยื่นข้อเสนอที่ชนะการประกวดราคาหรือที่ได้รับการคัดเลือกมีผลประโยชน์ร่วมกัน หรือมีส่วนได้เสียกับผู้ยื่นข้อเสนอรายอื่น หรือขัดขวางการแข่งขันอย่างเป็นธรรม หรือสมยอมกันกับผู้ยื่นข้อเสนอรายอื่น หรือเจ้าหน้าที่ในการเสนอราคา หรือส่อว่ากระทำการทุจริตอื่นใดในการเสนอราคา

๗. การทำสัญญาซื้อขาย

๗.๑ ในกรณีที่ผู้ชนะการประกวดราคาอิเล็กทรอนิกส์ สามารถส่งมอบสิ่งของได้ครบถ้วนภายใน ๕ วันทำการ นับแต่วันที่ทำข้อตกลงซื้อสลค.จะพิจารณาจัดทำข้อตกลงเป็นหนังสือแทนการทำสัญญาตามแบบสัญญาดังระบุ ในข้อ ๑.๓ ก็ได้

๗.๒ ในกรณีที่ผู้ชนะการประกวดราคาอิเล็กทรอนิกส์ไม่สามารถส่งมอบสิ่งของได้ครบถ้วนภายใน ๕ วันทำการ หรือสลค.เห็นว่าไม่สมควรจัดทำข้อตกลงเป็นหนังสือ ตามข้อ ๗.๑ ผู้ชนะการประกวดราคาอิเล็กทรอนิกส์จะต้องทำสัญญาซื้อขายตามแบบสัญญาดังระบุในข้อ ๑.๓ หรือทำข้อตกลงเป็นหนังสือ กับสลค.ภายใน ๗ วัน นับถัดจากวันที่ได้รับแจ้ง และจะต้องวางหลักประกันสัญญาเป็นจำนวนเงินเท่ากับร้อยละ ๕ ของราคาค่าสิ่งของที่ประกวดราคาอิเล็กทรอนิกส์ให้สลค.ยึดถือไว้ในขณะทำสัญญา โดยใช้หลักประกันอย่างหนึ่งอย่างใดดังต่อไปนี้

(๑) เงินสด

(๒) เช็คหรือดราฟท์ที่ธนาคารเซ็นสั่งจ่าย ซึ่งเป็นเช็คหรือดราฟท์ลงวันที่ที่ใช้เช็คหรือดราฟท์นั้นชำระต่อเจ้าหน้าที่ในวันทำสัญญา หรือก่อนวันนั้นไม่เกิน ๓ วันทำการ

(๓) หนังสือค้ำประกันของธนาคารภายในประเทศ ตามตัวอย่างที่คณะกรรมการนโยบายกำหนด ดังระบุในข้อ ๑.๔ (๒) หรือจะเป็นหนังสือค้ำประกันอิเล็กทรอนิกส์ตามวิธีการที่กรมบัญชีกลางกำหนด

(๔) หนังสือค้ำประกันของบริษัทเงินทุน หรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยอนุโลมให้ใช้ตามตัวอย่างหนังสือค้ำประกันของธนาคารที่คณะกรรมการนโยบายกำหนด ดังระบุในข้อ ๑.๔ (๒)

(๕) พันธบัตรรัฐบาลไทย

หลักประกันนี้จะคืนให้ โดยไม่มีดอกเบี้ยภายใน ๑๕ วัน นับถัดจากวันที่ผู้ชนะการประกวดราคาอิเล็กทรอนิกส์ (ผู้ขาย) พ้นจากข้อผูกพันตามสัญญาซื้อขายแล้ว

หลักประกันนี้จะคืนให้ โดยไม่มีดอกเบี้ย ตามอัตราส่วนของพัสดุที่ซื้อซึ่งสลค. ได้รับมอบไว้แล้ว

๘. ค่าจ้างและการจ่ายเงิน

สลค. จะจ่ายค่าสิ่งของซึ่งได้รวมภาษีมูลค่าเพิ่ม ตลอดจนภาษีอากรอื่น ๆ และค่าใช้จ่ายทั้งปวงแล้วให้แก่ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกให้เป็นผู้ขาย โดยแบ่งการชำระเป็น ๔ งวด ดังนี้

งวดที่ ๑ ร้อยละ ๕ ภายใน ๓๐ วัน นับถัดจากวันที่ลงนามในสัญญา เมื่อผู้ขายส่งมอบงานตามขอบเขตของงาน (TOR) ข้อ ๔.๑ รายงานการศึกษา วิเคราะห์ ออกแบบ และวางแผนการติดตั้งและทดสอบระบบและอุปกรณ์ตามโครงการฯ

งวดที่ ๒ ร้อยละ ๕๐ ภายใน ๙๐ วัน นับถัดจากวันที่ลงนามในสัญญา เมื่อผู้ขายส่งมอบระบบและอุปกรณ์ตามขอบเขตของงาน (TOR) ข้อ ๕.๑ - ๕.๔ และ ๕.๙ โดยยังไม่ต้องดำเนินการติดตั้ง

งวดที่ ๓ ร้อยละ ๓๕ ภายใน ๑๒๐ วัน นับถัดจากวันที่ลงนามในสัญญา เมื่อผู้ขายส่งมอบงานติด

ตั้งและทดสอบระบบและอุปกรณ์ตามขอบเขตของงาน (TOR) ข้อ ๕.๑ - ๕.๙ ครบถ้วนสมบูรณ์

งวดที่ ๔ ร้อยละ ๑๐ ภายใน ๑๕๐ วัน นับถัดจากวันที่ลงนามในสัญญา เมื่อผู้ขายดำเนินการจัดฝึกอบรมพร้อมงานเอกสารและคู่มือ และส่งมอบงานที่เหลือทั้งหมดแล้วเสร็จ

๙. อัตราค่าปรับ

ค่าปรับตามแบบสัญญาซื้อขายแนบท้ายเอกสารประกวดราคาอิเล็กทรอนิกส์นี้ หรือข้อตกลงซื้อขายเป็นหนังสือ ให้คิดในอัตราร้อยละ ๐.๒๐ ของราคาค่าสิ่งของที่ยังไม่ได้รับมอบต่อวัน

๑๐. การรับประกันความชำรุดบกพร่อง

๑๐.๑ ผู้ขายต้องรับประกันความชำรุดบกพร่องของระบบและอุปกรณ์ทั้งหมด ดังนี้

๑๐.๑.๑ ระบบ ซอฟท์แวร์ และอุปกรณ์ที่นำเสนอตามขอบเขตของงาน (TOR) ข้อ ๕.๑ - ๕.๙ ให้สามารถใช้งานได้เป็นปกติ ในระยะเวลาการรับประกัน ๓ ปี โดยไม่คิดค่าใช้จ่ายใด ๆ เพิ่มเติมทั้งสิ้น นับตั้งแต่วันที่ สลค. ตรวจรับสมบูรณ์ทั้งหมด

๑๐.๑.๒ คาบเวลาการซ่อมแซมและการบำรุงรักษาระบบ ได้แก่ วันจันทร์ - วันศุกร์ ตั้งแต่เวลา ๐๘.๓๐ - ๑๗.๓๐ น. ให้สามารถใช้งานได้ดีตลอดระยะเวลาการรับประกัน ๓ ปี โดยไม่มีค่าใช้จ่ายใด ๆ และให้มีช่างผู้ชำนาญในการให้บริการ Onsite Support ภายในระยะเวลา ๔ ชั่วโมงทำการนับตั้งแต่ได้รับแจ้งจาก สลค. และจะต้องดูแลบำรุงรักษาระบบอย่างน้อย ๓ เดือนต่อครั้ง

๑๐.๒ ผู้ขายต้องดำเนินการแก้ไข/เปลี่ยนแปลงค่าของอุปกรณ์และระบบสารสนเทศที่เสนอตามโครงการนี้ ตามคำขอแก้ไข/เปลี่ยนแปลงของ สลค. โดยไม่ชักช้าและไม่คิดค่าใช้จ่ายใด ๆ ทั้งสิ้นตลอดระยะเวลาการรับประกัน ๓ ปี

๑๑. ข้อสงวนสิทธิ์ในการยื่นข้อเสนอและอื่นๆ

๑๑.๑ เงินค่าพัสดุสำหรับการซื้อครั้งนี้ ได้มาจากเงินงบประมาณเงินงบประมาณประจำปี พ.ศ. ๒๕๖๕

การลงนามในสัญญาจะกระทำได้ ต่อเมื่อสลค.ได้รับอนุมัติเงินค่าพัสดุจากเงินงบประมาณประจำปี พ.ศ. ๒๕๖๕ แล้วเท่านั้น

๑๑.๒ เมื่อสลค.ได้คัดเลือกผู้ยื่นข้อเสนอรายใดให้เป็นผู้ขาย และได้ตกลงซื้อสิ่งของตามการประกวดราคาอิเล็กทรอนิกส์แล้ว ถ้าผู้ขายจะต้องสั่งหรือนำสิ่งของดังกล่าวเข้ามาจากต่างประเทศและของนั้นต้องนำเข้ามาโดยทางเรือในเส้นทางที่มีเรือไทยเดินอยู่ และสามารถให้บริการรับขนได้ตามที่รัฐมนตรีว่าการกระทรวงคมนาคมประกาศกำหนด ผู้ยื่นข้อเสนอซึ่งเป็นผู้ขายจะต้องปฏิบัติตามกฎหมายว่าด้วยการส่งเสริมการพาณิชยนาวี ดังนี้

(๑) แจ้งการสั่งหรือนำสิ่งของที่ซื้อขายดังกล่าวเข้ามาจากต่างประเทศต่อกรมเจ้าท่าภายใน ๗ วัน นับตั้งแต่วันที่ผู้ขายสั่ง หรือซื้อของจากต่างประเทศ เว้นแต่เป็นของที่รัฐมนตรีว่าการกระทรวงคมนาคมประกาศยกเว้นให้บรรทุกโดยเรืออื่นได้

(๒) จัดการให้สิ่งของที่ซื้อขายดังกล่าวบรรทุกโดยเรือไทย หรือเรือที่มีสิทธิเช่นเดียวกับเรือไทย จากต่างประเทศมายังประเทศไทย เว้นแต่จะได้รับอนุญาตจากกรมเจ้าท่า ให้บรรทุกสิ่งของนั้นโดยเรืออื่นที่มิใช่เรือไทย ซึ่งจะต้องได้รับอนุญาตเช่นนั้นก่อนบรรทุกของลงเรืออื่น หรือเป็นของที่รัฐมนตรีว่าการกระทรวงคมนาคมประกาศยกเว้นให้บรรทุกโดยเรืออื่น

(๓) ในกรณีที่ไม่ปฏิบัติตาม (๑) หรือ (๒) ผู้ขายจะต้องรับผิดตามกฎหมายว่าด้วยการส่งเสริมการพาณิชยนาวี

๑๑.๓ ผู้ยื่นข้อเสนอซึ่งสลค.ได้คัดเลือกแล้ว ไม่ไปทำสัญญาหรือข้อตกลงซื้อเป็นหนังสือภายในเวลาที่กำหนด ดังระบุไว้ในข้อ ๗ สลค.จะริบหลักประกันการยื่นข้อเสนอ หรือเรียกร้องจากผู้ออกหนังสือค้ำประกันการยื่นข้อเสนอทันที และอาจพิจารณาเรียกร้องให้ชดใช้ความเสียหายอื่น (ถ้ามี) รวมทั้งจะพิจารณาให้เป็นผู้ทิ้งงาน ตามระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ

๑๑.๔ สลค.สงวนสิทธิ์ที่จะแก้ไขเพิ่มเติมเงื่อนไข หรือข้อกำหนดในแบบสัญญาหรือข้อตกลงซื้อเป็นหนังสือ ให้เป็นไปตามความเห็นของสำนักงานอัยการสูงสุด (ถ้ามี)

๑๑.๕ ในกรณีที่เอกสารแนบท้ายเอกสารประกวดราคาอิเล็กทรอนิกส์นี้ มีความขัดหรือแย้งกัน ผู้ยื่นข้อเสนอจะต้องปฏิบัติตามคำวินิจฉัยของสลค. คำวินิจฉัยดังกล่าวให้ถือเป็นที่สุด และผู้ยื่นข้อเสนอไม่มีสิทธิเรียกร้องค่าใช้จ่ายใดๆ เพิ่มเติม

๑๑.๖ สลค.อาจประกาศยกเลิกการจัดซื้อในกรณีต่อไปนี้ได้ โดยที่ผู้ยื่นข้อเสนอจะเรียกร้องค่าเสียหายใดๆ จากสลค.ไม่ได้

(๑) สลค.ไม่ได้รับการจัดสรรเงินที่จะใช้ในการจัดซื้อหรือที่ได้รับจัดสรรแต่ไม่เพียงพอที่จะทำการจัดซื้อครั้งนี้ต่อไป

(๒) มีการกระทำที่เข้าลักษณะผู้ยื่นข้อเสนอที่ชนะการจัดซื้อหรือที่ได้รับการคัดเลือกมีผลประโยชน์ร่วมกัน หรือมีส่วนได้เสียกับผู้ยื่นข้อเสนอรายอื่น หรือขัดขวางการแข่งขันอย่างเป็นธรรม หรือสมยอมกันกับผู้ยื่นข้อเสนอรายอื่น หรือเจ้าหน้าที่ในการเสนอราคา หรือส่อว่ากระทำการทุจริตอื่นใดในการเสนอราคา

(๓) การทำการจัดซื้อครั้งนี้ต่อไปอาจก่อให้เกิดความเสียหายแก่สลค. หรือกระทบต่อประโยชน์สาธารณะ

(๔) กรณีอื่นในทำนองเดียวกับ (๑) (๒) หรือ (๓) ตามที่กำหนดในกฎกระทรวง ซึ่งออกตามความในกฎหมายว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ

๑๒. การปฏิบัติตามกฎหมายและระเบียบ

ในระหว่างระยะเวลาการซื้อ ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกให้เป็นผู้ขายต้องปฏิบัติตามหลักเกณฑ์ที่กฎหมายและระเบียบได้กำหนดไว้โดยเคร่งครัด

๑๓. การประเมินผลการปฏิบัติงานของผู้ประกอบการ

สลค. สามารถนำผลการปฏิบัติงานแล้วเสร็จตามสัญญาของผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกให้เป็นผู้ขายเพื่อนำมาประเมินผลการปฏิบัติงานของผู้ประกอบการ

ทั้งนี้ หากผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกไม่ผ่านเกณฑ์ที่กำหนดจะถูกระงับการยื่นข้อเสนอหรือทำสัญญากับสลค. ไว้ชั่วคราว

สำนักเลขาธิการคณะรัฐมนตรี

เมษายน ๒๕๖๕

(ร่าง)

ขอบเขตของงาน (Terms Of Reference : TOR)

โครงการปรับปรุงระบบรักษาความมั่นคงปลอดภัยไซเบอร์

---

1. หลักการและเหตุผล

สำนักเลขาธิการคณะรัฐมนตรี (สลค.) ได้นำระบบเทคโนโลยีสารสนเทศและการสื่อสารมาช่วยสนับสนุนและเพิ่มประสิทธิภาพในการปฏิบัติงานทั้งในและนอกสถานที่เพื่อสนับสนุนภารกิจหลักต่าง ๆ ของหน่วยงาน และด้วยความก้าวหน้าทางด้านเทคโนโลยีสารสนเทศและการสื่อสารทำให้มีความต้องการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารเพิ่มขึ้นอย่างมากจึงมีอุปกรณ์ด้านเทคโนโลยีสารสนเทศมาเชื่อมต่อใช้งานในระบบเครือข่ายของ สลค. เป็นจำนวนมาก ทำให้ระบบรักษาความปลอดภัยและระบบเครือข่ายของ สลค. ไม่สามารถรองรับการใช้งานได้ในบางช่วงเวลา และไม่สามารถป้องกันภัยคุกคามได้ทั้งระบบ รวมทั้งเจ้าหน้าที่ที่ดูแลงานด้านระบบรักษาความปลอดภัยของ สลค. มีจำกัดทำให้ดูแลแก้ไขปัญหาได้ล่าช้าและไม่ครอบคลุม และกรณีเกิดปัญหาการใช้งานในระบบเครือข่ายก็มักจะใช้เวลาในการตรวจสอบและแก้ไขปัญหาเป็นระยะเวลาค่อนข้างนาน หรือแก้ปัญหาไม่ตรงจุดทำให้เกิดปัญหาเดิมซ้ำ ๆ ทั้งนี้ เนื่องจาก สลค. ไม่มีเครื่องมือมาช่วยสนับสนุนการปฏิบัติงานทำให้ไม่สามารถทำการตรวจสอบวิเคราะห์สภาพปัญหาการใช้งานระบบเทคโนโลยีสารสนเทศในปัจจุบันมีความยุ่งยากซับซ้อนมากขึ้นได้ และยังพบว่าปัจจุบันได้มีการพัฒนาภัยคุกคามรูปแบบใหม่ ๆ เพิ่มขึ้นอย่างรวดเร็วโดยมีวัตถุประสงค์ในการโจมตีระบบเครือข่ายเพื่อดักจับข้อมูล หรือทำลายข้อมูลที่สำคัญให้เกิดความเสียหาย หรือวัตถุประสงค์อื่นใดที่ทำให้ สลค. ไม่สามารถปฏิบัติงานได้อย่างต่อเนื่อง และถึงแม้ว่า สลค. จะมีการติดตั้งระบบป้องกันไวรัสคอมพิวเตอร์ที่เครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ลูกข่าย (Client) แต่ระบบดังกล่าวได้สิ้นสุดการให้บริการหรืออยู่ในสถานะ End-of-Life แล้ว ซึ่งอาจจะไม่สามารถปรับปรุงระบบให้สามารถรองรับการป้องกันภัยคุกคามใหม่ ๆ ได้อย่างมีประสิทธิภาพ ประกอบกับระบบป้องกันไวรัสที่ สลค. ใช้งานอยู่ไม่สามารถติดตั้งใช้งานบนสมาร์ทโฟนและแท็บเล็ตได้ ซึ่งปัจจุบันมีการนำอุปกรณ์เหล่านี้มาเชื่อมต่อใช้งานเครือข่าย สลค. เป็นจำนวนมาก จึงนับเป็นช่องโหว่ที่มีความเสี่ยงสูงต่อการถูกโจมตีได้อย่างง่ายดาย และนอกจากสภาพปัญหาที่กล่าวมาข้างต้นแล้ว สลค. ยังพบปัญหาเกี่ยวกับการให้บริการระบบเครือข่ายไร้สาย (Wi-Fi) สำหรับบุคคลภายนอก อาทิ คณะรัฐมนตรีและคณะกรรมการต่าง ๆ ที่มาประชุม หรือเจ้าหน้าที่บริษัทและบุคคลทั่วไปที่มาปฏิบัติงานที่ สลค. ที่อาจจะยังไม่สะดวกต่อการใช้งาน และจากสภาพปัญหาที่กล่าวมาข้างต้น จึงมีความจำเป็นต้องปรับปรุงประสิทธิภาพระบบรักษาความมั่นคงปลอดภัยและระบบเครือข่ายที่เกี่ยวข้อง ได้แก่ ปรับปรุงอุปกรณ์ป้องกันเครือข่าย (Firewall) ให้ทันสมัยและสามารถป้องกันภัยคุกคามใหม่ ๆ ได้อย่างมีประสิทธิภาพ ปรับปรุงระบบป้องกันไวรัสคอมพิวเตอร์ให้สามารถบริหารจัดการไวรัสคอมพิวเตอร์ มัลแวร์ หรือภัยคุกคามรูปแบบใหม่ ๆ ในลักษณะอัตโนมัติได้ทันการณ์ และจัดหาเครื่องมือมาช่วยสนับสนุนการปฏิบัติงานในการตรวจสอบและวิเคราะห์สภาพปัญหาการใช้งานในระบบเครือข่าย สลค. เพื่อลดระยะเวลาในการค้นหาข้อผิดพลาดของระบบได้อย่างรวดเร็วและแม่นยำ รวมทั้งพัฒนาระบบลงทะเบียนเข้าใช้งาน Wi-Fi ให้ทันสมัย สะดวกและง่ายต่อการใช้งานและมีความปลอดภัยยิ่งขึ้น

ในการนี้ หาก สลค. ได้รับการปรับปรุงระบบรักษาความมั่นคงปลอดภัยไซเบอร์แล้วจะทำให้ สลค. มีระบบรักษาความมั่นคงปลอดภัยไซเบอร์แบบรวมศูนย์ที่ทันสมัยและมีศักยภาพ เพื่อทำหน้าที่เสมือนเป็นศูนย์เฝ้าระวังความปลอดภัยของระบบสารสนเทศ (Security Operations Center: SOC) ที่คอยเฝ้าดูพฤติกรรมการใช้งานในระบบเครือข่ายและทำการวิเคราะห์เพื่อตรวจจับ แจ้งเตือน และตอบสนองเหตุการณ์ภัยคุกคามได้แบบอัตโนมัติอย่างทันท่วงที นอกจากนี้ยังมีระบบบริหารจัดการเครือข่ายแบบรวมศูนย์เพื่อทำหน้าที่ควบคุมและจัดการอุปกรณ์

เครือข่าย ...

เครือข่ายทั้งระบบได้แบบอัตโนมัติ โดยจะทำหน้าที่ตรวจสอบ วิเคราะห์ และแจ้งเตือนสภาพปัญหาของการใช้งานในระบบเครือข่าย ทำให้ผู้ดูแลระบบสามารถทราบสถานะและประสิทธิภาพการทำงานของอุปกรณ์เครือข่ายได้ตลอดเวลา และกรณีเกิดปัญหาการใช้งานในระบบเครือข่ายก็สามารถตรวจสอบและวิเคราะห์หาสาเหตุของปัญหาได้รวดเร็วแม่นยำและตรงจุด ซึ่งจะช่วยลดระยะเวลาในการค้นหาความผิดพลาดที่เกิดขึ้นในระบบและเป็นการป้องกันไม่ให้เกิดความล้มเหลวแบบจุดเดียว (Single Point of Failure) อันจะนำมาซึ่งการล่มของเครือข่ายทั้งระบบ อีกทั้งยังมีความยืดหยุ่นและเอื้อต่อการวางแผนขยายโครงข่ายของ สลค. ในอนาคตให้สอดคล้องและเหมาะสมกับสภาวการณ์ได้อย่างมีประสิทธิภาพและมีเสถียรภาพมากยิ่งขึ้น

2. วัตถุประสงค์ของโครงการ

2.1 เพื่อให้ สลค. มีระบบรักษาความปลอดภัยเครือข่ายระดับแอปพลิเคชัน (Application Firewall) ระบบป้องกันการโจมตีผ่านช่องโหว่ซอฟท์แวร์สำหรับเครื่องคอมพิวเตอร์ลูกข่าย และระบบบริหารจัดการภัยและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ (Automation) ที่ทันสมัยและสามารถป้องกันภัยคุกคามหรือการโจมตีรูปแบบใหม่ ๆ ในปัจจุบันได้ทันการณ์และมีประสิทธิภาพ รวมทั้งสามารถรองรับจำนวนผู้ใช้งานผ่านระบบเครือข่ายทั้งในและนอกสถานที่ที่มีจำนวนผู้ใช้งานมากขึ้นได้อย่างปลอดภัยและมีประสิทธิภาพ

2.2 เพื่อให้ สลค. มีระบบบริหารจัดการเครือข่ายแบบรวมศูนย์สำหรับใช้ค้นหาและจัดการอุปกรณ์เครือข่ายและตรวจสอบอายุการใช้งานอุปกรณ์ทั้งระบบแบบอัตโนมัติ รวมทั้งสามารถตรวจสอบวิเคราะห์สภาพปัญหาการใช้งานในระบบเครือข่ายของ สลค. ได้อย่างรวดเร็วแม่นยำ เพื่อให้สามารถแก้ปัญหาได้ตรงจุด

2.3 เพื่อให้ สลค. มีระบบลงทะเบียนเข้าใช้งาน Wi-Fi ที่ทันสมัย สะดวกและง่ายต่อการใช้งาน โดยยังคงมีระบบรักษาความมั่นคงปลอดภัยที่รัดกุม

3. คุณสมบัติของผู้ที่จะยื่นข้อเสนอ

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราวเนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วน ผู้จัดการ กรรมการ ผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้าง และการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 เป็นบุคคลธรรมดาหรือนิติบุคคลผู้มีอาชีพรับจ้างงานที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่ สลค. ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

3.10 ผู้ยื่นข้อเสนอ ...

3.10 ผู้ยื่นข้อเสนอต้องลงทะเบียนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement : e – GP) ของกรมบัญชีกลาง

3.11 ผู้ยื่นข้อเสนอซึ่งได้รับการคัดเลือกเป็นคู่สัญญาต้องลงทะเบียนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement : e – GP) ของกรมบัญชีกลางตามที่คณะกรรมการ ป.ป.ช. กำหนด

3.12 ผู้ยื่นข้อเสนอต้องไม่อยู่ในฐานะเป็นผู้ไม่แสดงบัญชีรายรับรายจ่าย หรือแสดงบัญชีรายรับรายจ่ายไม่ถูกต้องครบถ้วนในสาระสำคัญ ตามที่คณะกรรมการ ป.ป.ช. กำหนด

3.13 ผู้ยื่นข้อเสนอซึ่งได้รับคัดเลือกเป็นคู่สัญญาต้องรับและจ่ายเงินผ่านบัญชีธนาคาร เว้นแต่การจ่ายเงินแต่ละครั้งซึ่งมีมูลค่าไม่เกินสามหมื่นบาท คู่สัญญาอาจจ่ายเป็นเงินสดก็ได้ตามที่คณะกรรมการ ป.ป.ช. กำหนด

3.14 ผู้ยื่นข้อเสนอต้องไม่เคยถูกยกเลิกสัญญาซื้อขาย หรือสัญญาจ้างบริการบำรุงรักษาก่อนหมดอายุสัญญาโดยไม่มีเหตุผลอันควรจากหน่วยงานใด ๆ

3.15 ผู้ยื่นข้อเสนอต้องมีผลงานเกี่ยวกับระบบคอมพิวเตอร์จากหน่วยงานของรัฐหรือหน่วยงานเอกชน โดยผลงานดังกล่าวจะต้องเป็นผลงานในการติดตั้งระบบเครือข่ายคอมพิวเตอร์และระบบรักษาความมั่นคงปลอดภัย อย่างน้อย 2 สัญญาจ้าง และมีมูลค่าสัญญาละไม่น้อยกว่า 2,000,000 บาท (สองล้านบาทถ้วน) และยังคงใช้ระบบงานดังกล่าวอยู่ในปัจจุบัน พร้อมเอกสารรายละเอียดของผลงานดังกล่าวอย่างชัดเจน โดย สลค. ขอสงวนสิทธิ์ที่จะตรวจสอบข้อเท็จจริงดังกล่าว

3.16 ผู้ยื่นข้อเสนอต้องเสนอรายชื่อคณะทำงานทั้งหมดที่จะเข้ามาดำเนินการตามโครงการนี้ โดยที่ภายในคณะทำงานจะต้องประกอบด้วยบุคลากรที่มีความเชี่ยวชาญด้านระบบรักษาความมั่นคงปลอดภัยไซเบอร์และระบบเครือข่ายคอมพิวเตอร์ และคณะทำงานทั้งหมดต้องมายืนยันตัวตนเข้าดำเนินการโครงการต่อ สลค. ในการส่งมอบงานงวดที่ 1 ประกอบด้วย

ลำดับ	คณะทำงาน	วุฒิการศึกษา	ประสบการณ์ด้านที่ตรงกับหน้าที่ในคณะทำงาน	จำนวน	ระยะเวลา
1	ผู้จัดการโครงการ (Project Manager)	ปริญญาโท	ไม่น้อยกว่า 3 ปี	1 คน	อย่างน้อยเดือนละ 2 ครั้ง ตลอดระยะเวลาดำเนินโครงการ
2	ผู้เชี่ยวชาญด้านระบบรักษาความมั่นคงปลอดภัยไซเบอร์	ปริญญาตรี	ไม่น้อยกว่า 2 ปี และเคยได้รับ Certificate ด้านระบบรักษาความมั่นคงปลอดภัย	1 คน	ตลอดระยะเวลาดำเนินโครงการ
3	วิศวกรเครือข่าย (Network Engineer)	ปริญญาตรี	ไม่น้อยกว่า 2 ปี และเคยได้รับ Certificate ด้าน Network	1 คน	ตลอดระยะเวลาดำเนินโครงการ
4	ผู้ประสานงานโครงการ	ปริญญาตรี	ไม่น้อยกว่า 1 ปี	1 คน	ตลอดระยะเวลาดำเนินโครงการ

ทั้งนี้ ...

ทั้งนี้ คณะทำงานดังกล่าวจะต้องมาปฏิบัติงานที่ สลค. ตามหน้าที่ที่ตนรับผิดชอบอย่างสม่ำเสมอตลอดระยะเวลาการดำเนินงานโครงการ

3.17 ผู้ยื่นข้อเสนอต้องเสนอเอกสารแบบรูปหรือแคตตาล็อคแสดงรายละเอียดคุณลักษณะเฉพาะหรือคุณสมบัติของผลิตภัณฑ์ที่เสนอทุกรายการ โดยยื่นมาพร้อมกับการเสนอราคา ดังนี้

หัวข้อ	ข้อกำหนดของ สลค.	ข้อเสนอของบริษัท	เอกสารอ้างอิงหน้า/ข้อ
ระบุหัวข้อให้ตรงกับที่ สลค. กำหนด	ให้คัดลอกคุณลักษณะเฉพาะ ที่ สลค. กำหนด	ให้ระบุคุณลักษณะเฉพาะที่เสนอ	ให้ระบุหรืออ้างอิงเอกสารในข้อเสนอที่เกี่ยวข้องและขีดเส้นใต้คุณลักษณะเฉพาะที่ สลค. กำหนดลงในแคตตาล็อคหรือเอกสารที่เกี่ยวข้อง

3.18 การพิจารณาผลการยื่นข้อเสนอการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้ สลค. จะพิจารณาตัดสินโดยใช้เกณฑ์ราคาประกอบเกณฑ์อื่น โดยเกณฑ์อื่นเป็นการพิจารณาเกณฑ์การให้คะแนนจากผลงานที่ผ่านมารูปแบบ และวิธีการดำเนินงาน ตลอดจนแนวทางการบริหารโครงการให้ประสบผลสำเร็จตามวัตถุประสงค์ของโครงการและข้อเสนอทางเทคนิคที่เป็นประโยชน์ต่อทางราชการเป็นสำคัญ โดยข้อเสนอต้องมีความเป็นไปได้ที่สามารถดำเนินการได้จริง และตรงกับความต้องการของ สลค. (คะแนนรวม 100 คะแนน) และ สลค. ขอสงวนสิทธิ์ในการพิจารณาเฉพาะผู้ยื่นข้อเสนอที่ผ่านคุณสมบัติเบื้องต้นตามข้อ 3.1 – 3.17 ข้างต้นเท่านั้น ซึ่งเกณฑ์อื่นประกอบด้วยข้อพิจารณา ดังนี้

ข้อพิจารณา	คะแนน
1. การนำเสนอผลงานที่ผ่านมาเกี่ยวกับการติดตั้งระบบเครือข่ายคอมพิวเตอร์และระบบรักษาความมั่นคงปลอดภัย อย่างน้อย 2 สัญญาจ้าง และมีมูลค่าสัญญาละไม่น้อยกว่า 2,000,000 บาท (สองล้านบาทถ้วน) และยังคงใช้ระบบงานดังกล่าวอยู่ในปัจจุบัน พร้อมเอกสารรายละเอียดของผลงานดังกล่าวอย่างชัดเจน โดย สลค. ขอสงวนสิทธิ์ที่จะตรวจสอบข้อเท็จจริงดังกล่าว ทั้งนี้ ผลงานดังกล่าวควรแสดงให้เห็นถึงประสบการณ์และความสามารถที่เกี่ยวข้องกับโครงการอย่างน้อย ดังนี้ 1.1 มีระบบรักษาความปลอดภัยระบบเครือข่ายระดับแอปพลิเคชัน (Application Firewall) (คะแนนเต็ม 1 คะแนน) 1.2 มีระบบป้องกันการโจมตีผ่านช่องโหว่ซอฟท์แวร์สำหรับเครื่องคอมพิวเตอร์ลูกข่าย (คะแนนเต็ม 1 คะแนน) 1.3 มีระบบบริหารจัดการและตอบสนองต่อภัยคุกคามไซเบอร์แบบอัตโนมัติ (คะแนนเต็ม 1 คะแนน) 1.4 มีระบบบริหารจัดการเครือข่ายแบบรวมศูนย์ (คะแนนเต็ม 1 คะแนน) 1.5 มีระบบลงทะเบียนเข้าใช้งาน Wi-Fi (คะแนนเต็ม 1 คะแนน)	5

2. การนำเสนอ ...

ข้อพิจารณา	คะแนน
2. การนำเสนอแนวทางการพัฒนาศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของ สลค. ตามโครงการนี้ ทั้งนี้ สลค. จะให้คะแนนโดยพิจารณาว่า ผู้ยื่นข้อเสนอได้นำเสนอแนวทางฯ ที่เป็นไปตามกฎหมายและมาตรฐานที่เกี่ยวข้อง เป็นไปตามวัตถุประสงค์ของโครงการ เป็นประโยชน์ต่อทางราชการเป็นสำคัญ และมีความเป็นไปได้ที่จะดำเนินการได้จริง ดังนี้	30
2.1 การนำเสนอแนวทางการจัดทำร่างนโยบายในการรับมือเหตุการณ์ภัยคุกคามทางไซเบอร์ของ สลค. โดยอ้างอิงจากข้อกำหนดตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และแนวปฏิบัติของ NIST Cyber Security Framework (1) ครบถ้วน ถูกต้อง และมีตัวอย่างนำเสนอที่ชัดเจน (5 คะแนน) (2) ครบถ้วน และถูกต้อง (3 คะแนน) (3) ครบถ้วน แต่ไม่ถูกต้อง (1 คะแนน) (4) ไม่เสนอ (0 คะแนน)	(5)
2.2 การนำเสนอแนวทางการจัดทำขั้นตอนการปฏิบัติงานต่าง ๆ ดังนี้ (1) ขั้นตอนการเฝ้าระวังเหตุการณ์ภัยคุกคามและการโจมตีทางไซเบอร์ - ครบถ้วน ถูกต้อง และมีตัวอย่างนำเสนอที่ชัดเจน (3 คะแนน) - ครบถ้วน และถูกต้อง (2 คะแนน) - ครบถ้วน แต่ไม่ถูกต้อง (1 คะแนน) - ไม่นำเสนอ (0 คะแนน) (2) กระบวนการจัดทำ Playbook Automation รวมทั้งวิธีการเชื่อมโยง (Integrate) เข้ากับระบบความปลอดภัยเดิมที่ สลค. มีอยู่ - ครบถ้วน ถูกต้อง และมีตัวอย่างนำเสนอที่ชัดเจน (3 คะแนน) - ครบถ้วน และถูกต้อง (2 คะแนน) - ครบถ้วน แต่ไม่ถูกต้อง (1 คะแนน) - ไม่นำเสนอ (0 คะแนน) (3) กระบวนการในการสื่อสารเมื่อเกิดเหตุการณ์ภัยคุกคามและการโจมตี - ครบถ้วน ถูกต้อง และมีตัวอย่างนำเสนอที่ชัดเจน (2 คะแนน) - ครบถ้วน และถูกต้อง (1 คะแนน) - ไม่นำเสนอ (0 คะแนน) (4) แนวทางอื่นที่เป็นประโยชน์ต่อการดำเนินโครงการ - ครบถ้วน ถูกต้อง และมีตัวอย่างนำเสนอที่ชัดเจน (2 คะแนน) - ครบถ้วน และถูกต้อง (1 คะแนน) - ไม่นำเสนอ (0 คะแนน)	(10)
2.3 การนำเสนอแนวทางการเชื่อมต่อระบบบริหารจัดการและตอบสนองต่อภัยคุกคามแบบอัตโนมัติให้สามารถทำงานร่วมกับระบบเครือข่ายและระบบรักษาความปลอดภัยเครือข่ายฯ ที่ สลค. มีอยู่เดิมได้ โดยนำเสนอวิธีการและแผนผังการเชื่อมต่อระบบฯ (1) ครบถ้วน ถูกต้อง และมีตัวอย่างนำเสนอที่ชัดเจน (10 คะแนน) (2) ครบถ้วน และถูกต้อง (7 คะแนน) (3) ครบถ้วน แต่ไม่ถูกต้อง (3 คะแนน) (4) ไม่เสนอ (0 คะแนน)	(10)

2.4 การนำเสนอ ...

ข้อพิจารณา	คะแนน
2.4 การนำเสนอตัวอย่างต้นแบบ (Template) รายงานภัยคุกคามและการโจมตีทางไซเบอร์ โดยนำเสนอตัวอย่างเอกสารและแนวทางการบริหารจัดการรายงานภัยคุกคามและการโจมตีทางไซเบอร์ (1) ครบถ้วน ถูกต้อง และมีตัวอย่างนำเสนอที่ชัดเจน (5 คะแนน) (2) ครบถ้วน และถูกต้อง (3 คะแนน) (3) ครบถ้วน แต่ไม่ถูกต้อง (1 คะแนน) (4) ไม่เสนอ (0 คะแนน)	(5)
3. การนำเสนอแผนการติดตั้งระบบป้องกันการโจมตีผ่านช่องโหว่ซอฟท์แวร์สำหรับเครื่องคอมพิวเตอร์ลูกข่าย ทั้งนี้ สลค. จะให้คะแนนโดยพิจารณาว่า ผู้ยื่นข้อเสนอได้นำเสนอแนวคิดฯ เป็นไปตามวัตถุประสงค์ของโครงการ เป็นประโยชน์ต่อทางราชการเป็นสำคัญ และมีความเป็นไปได้ที่จะดำเนินการได้จริง ดังนี้	**10**
3.1 นำเสนอแผนการติดตั้งฯ โดยแสดงรายละเอียดการดำเนินการแต่ละกิจกรรมอย่างละเอียด (1) ครบถ้วน ถูกต้อง และมีตัวอย่างนำเสนอที่ชัดเจน (3 คะแนน) (2) ครบถ้วน และถูกต้อง (2 คะแนน) (3) ครบถ้วน แต่ไม่ถูกต้อง (1 คะแนน) (4) ไม่นำเสนอ (0 คะแนน)	(3)
3.2 นำเสนอแผนรับมือกรณีเกิดเหตุสุดวิสัยที่ส่งผลให้ไม่สามารถเข้าดำเนินการติดตั้งได้ทันตามกำหนดเวลา (1) ครบถ้วน ถูกต้อง และมีตัวอย่างนำเสนอที่ชัดเจน (3 คะแนน) (2) ครบถ้วน และถูกต้อง (2 คะแนน) (3) ครบถ้วน แต่ไม่ถูกต้อง (1 คะแนน) (4) ไม่นำเสนอ (0 คะแนน)	(3)
3.3 นำเสนอซอฟต์แวร์ และทีมงานที่จะช่วยให้การติดตั้งระบบฯ สามารถดำเนินการได้สะดวกและรวดเร็วยิ่งขึ้น (1) มีเจ้าหน้าที่ช่วยดำเนินการติดตั้ง (1 คะแนน) (2) มีซอฟต์แวร์ช่วยในการติดตั้งระบบจากส่วนกลาง (2 คะแนน) (3) แนวทางอื่นเพิ่มเติม (1 คะแนน) (4) ไม่นำเสนอ (0 คะแนน)	(4)
4. การนำเสนอแนวคิดในการจัดหาหรือพัฒนาระบบลงทะเบียนเข้าใช้งาน Wi-Fi โดยต้อง อ้างอิงตามข้อกำหนดขอบเขตการดำเนินงานและคุณลักษณะเฉพาะการดำเนินโครงการ ทั้งนี้ สลค. จะให้คะแนนโดยพิจารณาว่า ผู้ยื่นข้อเสนอได้นำเสนอแนวคิดฯ เป็นไปตามวัตถุประสงค์ของโครงการ เป็นประโยชน์ต่อทางราชการเป็นสำคัญ และมีความเป็นไปได้ที่จะดำเนินการได้จริง ดังนี้	**10**
4.1 การนำเสนอตัวอย่างการออกแบบระบบต้นแบบ (Prototype) พร้อมอธิบายรูปแบบการทำงาน (1) นำเสนอระบบเสมือนจริงทั้งระบบ (3 คะแนน) (2) นำเสนอภาพนิ่งและระบบเสมือนจริงบางส่วน (2 คะแนน) (3) นำเสนอภาพนิ่ง (1 คะแนน) (4) ไม่นำเสนอ (0 คะแนน)	(3)

4.2 นำเสนอ ...

ข้อพิจารณา	คะแนน
4.2 นำเสนอแผนผังอธิบายรูปแบบการติดตั้งสถาปัตยกรรมระบบคอมพิวเตอร์และเครือข่ายที่เหมาะสมและปลอดภัย (1) ครบถ้วน และมีตัวอย่างนำเสนอที่ชัดเจน (1 คะแนน) (2) วิธีการเชื่อมโยงกับระบบเครือข่ายของ สลค. (1 คะแนน) (3) มีการอธิบายรายละเอียดที่ชัดเจน (1 คะแนน) (4) ไม่นำเสนอ (0 คะแนน)	(3)
4.3 ระบบมีความทันสมัย สะดวก สอดคล้องกับความต้องการใช้งาน และลดภาระค่าใช้จ่ายของ สลค. ในอนาคต (1) มีความทันสมัย (1 คะแนน) (2) สะดวกในการใช้งาน (1 คะแนน) (3) สอดคล้องกับความต้องการใช้งาน (1 คะแนน) (4) ลดภาระค่าใช้จ่ายของ สลค. ในอนาคต (1 คะแนน)	(4)
5. จำนวนใบอนุญาตการใช้งานระบบป้องกันการโจมตีผ่านช่องโหว่ซอฟท์แวร์สำหรับเครื่องคอมพิวเตอร์ลูกข่ายรองรับได้สูงสุด 5.1 จำนวนไม่น้อยกว่า 900 สิทธิ์การใช้งาน (10 คะแนน) 5.2 จำนวนไม่น้อยกว่า 800 สิทธิ์การใช้งาน (5 คะแนน)	10
6. จำนวนอุปกรณ์ที่ระบบลงทะเบียนเข้าใช้งาน Wi-Fi ผ่าน MAC Address สามารถรองรับได้สูงสุด 6.1 จำนวนไม่น้อยกว่า 2,000 อุปกรณ์ (10 คะแนน) 6.2 จำนวนไม่น้อยกว่า 1,500 อุปกรณ์ (5 คะแนน)	10
7. การนำเสนอแผนการดำเนินงานตั้งแต่การเริ่มต้นโครงการจนสิ้นสุดโครงการ และระยะเวลารับประกันความชำรุดบกพร่อง โดยแสดงรายละเอียดกิจกรรม พร้อมกำหนดระยะเวลาแล้วเสร็จของแต่ละกิจกรรม ทั้งนี้ สลค. จะให้คะแนนโดยพิจารณาว่า ได้นำเสนอแผนการดำเนินงานฯ เป็นไปตามวัตถุประสงค์ของโครงการ เป็นประโยชน์ต่อทางราชการเป็นสำคัญ มีความเป็นไปได้ที่จะดำเนินการได้จริง ดังนี้ 7.1 ครบถ้วน ถูกต้อง และมีตัวอย่างนำเสนอที่ชัดเจน (5 คะแนน) 7.2 ครบถ้วน และถูกต้อง (3 คะแนน) 7.3 ครบถ้วน แต่ไม่ถูกต้อง (1 คะแนน) 7.4 ไม่เสนอ (0 คะแนน)	5
8. การนำเสนอค่าบำรุงรักษาในช่วงปีที่ 1, 2 และ 3 ภายหลังสิ้นสุดระยะเวลาการรับประกัน 3 ปี ซึ่งมีเกณฑ์การให้คะแนน ดังนี้ $\text{คะแนน} = \frac{15\% \text{ ของราคากลาง} - \text{ค่าบำรุงรักษาที่นำเสนอเฉลี่ยรายปี}}{15\% \text{ ของราคากลาง}} \times 5$ ทั้งนี้ หากเสนอค่าบำรุงรักษาสูงกว่าร้อยละ 15 ของราคากลาง ได้ 0 คะแนน	5

9. การนำเสนอ ...

ข้อพิจารณา	คะแนน
9. การนำเสนอแนวทางการดำเนินการอื่น ๆ เพิ่มเติมนอกเหนือจากข้อ 1.–8. ข้างต้น อันเป็นประโยชน์ในการปรับปรุงระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของ สลค. ซึ่งเป็นข้อเสนอที่ สลค. ไม่ได้ระบุไว้ในขอบเขตการดำเนินงานและคุณลักษณะเฉพาะการดำเนินโครงการ ทั้งนี้ สลค. จะให้คะแนนโดยพิจารณาว่าผู้ยื่นข้อเสนอได้นำเสนอแนวทางการดำเนินการอื่น ๆ เพิ่มเติมที่เป็นไปตามวัตถุประสงค์ของโครงการ เป็นประโยชน์ต่อทางราชการเป็นสำคัญ มีความเป็นไปได้ที่จะดำเนินการได้จริง ดังนี้ 9.1 การนำเสนอทีมงานและวิธีการในการสนับสนุนการดำเนินการโครงการนี้ตลอดระยะเวลาการรับประกัน (0-5 คะแนน) 9.2 การนำเสนอระบบหรืออุปกรณ์ เพื่อให้โครงการนี้บรรลุวัตถุประสงค์อย่างมีประสิทธิภาพ (0-5 คะแนน) 9.3 แนวทางอื่น ๆ ที่จะเป็นประโยชน์ต่อ สลค. (0-5 คะแนน)	15
รวม	100

3.19 ผู้ยื่นข้อเสนอจะต้องจัดทำเอกสารประกอบการนำเสนอตามข้อ 3.18 โดยยื่นผ่านระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement : e-GP) ของกรมบัญชีกลาง เพื่อใช้ประกอบในการนำเสนอ

3.20 ผู้ยื่นข้อเสนอจะต้องนำเสนอให้แก่คณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์ของ สลค. รายละไม่เกิน 2 ชั่วโมง ภายใน 5 วันทำการ นับถัดจากวันที่ยื่นเสนอราคาผ่านระบบ ซึ่ง สลค. จะพิจารณาตามลำดับก่อนหลังตามเวลาที่ผู้ยื่นข้อเสนอได้ยื่นข้อเสนอไว้เป็นสำคัญ ทั้งนี้ สลค. ขอสงวนสิทธิ์ในการกำหนดวันที่นำเสนองาน และไม่เชิญผู้ยื่นข้อเสนอมานำเสนอแนวคิดฯ หากปรากฏว่าผู้ยื่นข้อเสนอดังกล่าวมีคุณสมบัติไม่เป็นไปตามที่ สลค. กำหนด หรือยื่นเอกสารไม่ครบถ้วน

3.21 สลค. จะพิจารณาตัดสินคัดเลือกเฉพาะรายที่เสนอเอกสารหลักฐานครบถ้วนถูกต้อง และปฏิบัติถูกต้องตามเงื่อนไขที่ สลค. กำหนดเท่านั้น โดยการพิจารณาผลการยื่นข้อเสนอประกวดราคาอิเล็กทรอนิกส์ครั้งนี้ สลค. พิจารณาตัดสินโดยใช้หลักเกณฑ์ราคาประกอบเกณฑ์อื่น โดยพิจารณาให้คะแนนตามปัจจัยหลักและน้ำหนักที่กำหนดรายละเอียด ดังนี้

ปัจจัย	กำหนดน้ำหนักเท่ากับร้อยละ
ราคาที่ยื่นข้อเสนอ	30
คุณภาพของงานที่นำเสนอและคุณสมบัติที่เป็นประโยชน์ต่อทางราชการ (รายละเอียดตามข้อ 3.18)	70
รวม	100

4. ขอบเขต ...

4. ขอบเขตการดำเนินงาน

4.1 การศึกษา วิเคราะห์ ออกแบบ และวางแผนการติดตั้งและทดสอบระบบและอุปกรณ์ตามโครงการนี้

4.2 จัดหาและติดตั้งระบบรักษาความปลอดภัยระบบเครือข่ายระดับแอปพลิเคชัน (Application Firewall) ทดแทนระบบเดิม จำนวน 2 ชุด โดยจะต้องตั้งค่านโยบาย (Policy) การรักษาความมั่นคงปลอดภัยต่าง ๆ บนอุปกรณ์ที่จัดหาตามโครงการนี้ให้ได้เทียบเท่าหรือดีกว่าระบบเดิม และสามารถทำงานได้อย่างมีประสิทธิภาพ

4.3 จัดหาระบบป้องกันการโจมตีผ่านช่องโหว่ซอฟท์แวร์สำหรับเครื่องคอมพิวเตอร์ลูกข่าย จำนวน 1 ระบบ ที่รองรับการใช้งานได้ไม่น้อยกว่า 700 สิทธิ์การใช้งาน พร้อมทั้งติดตั้งทดแทนระบบป้องกันไวรัสคอมพิวเตอร์ที่ติดตั้งใช้งานอยู่บนเครื่องคอมพิวเตอร์ลูกข่ายของ สลค. รวมจำนวนไม่น้อยกว่า 500 เครื่อง ให้สามารถทำงานได้อย่างมีประสิทธิภาพ

4.4 จัดหาและติดตั้งระบบบริหารจัดการและตอบสนองต่อภัยคุกคามไซเบอร์แบบอัตโนมัติ จำนวน 1 ระบบ ให้สามารถนำเทคโนโลยี Artificial Intelligence และ Machine Learning รวมถึงเครื่องมือที่มีความทันสมัยต่าง ๆ มาช่วยในการป้องกัน เฝ้าระวัง และตรวจจับภัยคุกคามไซเบอร์แบบอัจฉริยะได้อย่างรวดเร็วและมีประสิทธิภาพสูงสุด โดยสามารถทำงานร่วมกับระบบรักษาความปลอดภัยระบบเครือข่ายระดับแอปพลิเคชัน (Application Firewall) และระบบป้องกันการโจมตีผ่านช่องโหว่ซอฟท์แวร์สำหรับเครื่องคอมพิวเตอร์ลูกข่ายได้อย่างมีประสิทธิภาพ

4.5 จัดหาและติดตั้งระบบรักษาความปลอดภัยระบบเครือข่ายระดับแอปพลิเคชัน (Application Firewall) ทดแทนระบบเดิม จำนวน 1 ระบบ ที่รองรับการทำงานร่วมกับระบบ Multi Factor Authentication ในการยืนยันตัวตนเพื่อตรวจสอบการใช้งานร่วมกับระบบ Azure AD ที่ สลค. มีอยู่ เพื่อใช้งาน VPN ตามโครงการนี้ และ VPN ของระบบรักษาความปลอดภัยระบบเครือข่ายระดับแอปพลิเคชัน (Application Firewall) ที่มีอยู่เดิมได้อย่างมีประสิทธิภาพ

4.6 จัดทำตามแนวทางการพัฒนาศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศที่เสนอต่อ สลค. ตามโครงการนี้

4.7 จัดหาและติดตั้งระบบบริหารจัดการเครือข่ายแบบรวมศูนย์ จำนวน 1 ระบบ ให้สามารถควบคุมอุปกรณ์กระจายสัญญาณเครือข่าย (Switch) และอุปกรณ์กระจายสัญญาณเครือข่ายไร้สาย (Wireless) รวมจำนวนไม่น้อยกว่า 59 ชุด ที่ สลค. ใช้งานอยู่ได้อย่างมีประสิทธิภาพ

4.8 จัดหาและติดตั้งระบบลงทะเบียนเข้าใช้งาน Wi-Fi ทดแทนระบบเดิม จำนวน 1 ระบบ

4.8.1 สามารถลงทะเบียนเข้าใช้งาน Wi-Fi ด้วยตนเอง (Self Service) โดยการยืนยันตัวตนผู้ลงทะเบียนด้วยการส่งรหัสผ่านแบบใช้งานครั้งเดียว (One Time Password: OTP) ไปยังเบอร์โทรศัพท์ของผู้ลงทะเบียนผ่านการเชื่อมต่อกับผู้ให้บริการ SMS Gateway โดยผู้ขายต้องจัดหาใบอนุญาต (Licenses) ที่รองรับการใช้งานได้ไม่น้อยกว่า 50,000 ข้อความ ตลอดระยะเวลาการรับประกันความชำรุดบกพร่อง

4.8.2 สามารถกำหนดบัญชีผู้ใช้ (Account) ให้กับผู้ใช้งานแต่ละรายได้

4.8.3 สามารถลงทะเบียนเข้าใช้งานด้วย MAC Address ของเครื่องคอมพิวเตอร์ สมาร์ทโฟน และแท็บเล็ต ได้ไม่น้อยกว่า 1,000 อุปกรณ์

4.9 จัดหา ...

4.9 จัดหาและติดตั้งใบรับรอง SSL Certificate จำนวน 1 ชุด สำหรับใช้ในการยืนยันตัวตนผู้ใช้งานเพื่อเข้าระบบ Wi-Fi ด้วยมาตรฐาน IEEE 802.1X บนเครื่องคอมพิวเตอร์ สมาร์ทโฟน และแท็บเล็ต

4.10 จัดหาเครื่องคอมพิวเตอร์โน้ตบุ๊ก สำหรับบริหารจัดการระบบและอุปกรณ์ตามโครงการนี้ จำนวน 5 เครื่อง

4.11 จัดฝึกอบรมการใช้งานระบบและอุปกรณ์ให้กับบุคลากรของ สลค. พร้อมทั้งจัดทำเอกสารและคู่มือการใช้งานต่าง ๆ

4.12 ต้องรับประกันความชำรุดบกพร่องของระบบและอุปกรณ์ตามโครงการนี้ เป็นระยะเวลาไม่น้อยกว่า 3 ปี หลังจากส่งมอบงานทั้งหมดและคณะกรรมการได้ดำเนินการตรวจรับเรียบร้อยแล้ว

ทั้งนี้ หากมีความจำเป็นต้องจัดหาอุปกรณ์อื่นใดเพิ่มเติมเพื่อให้ระบบดังกล่าวข้างต้นมีประสิทธิภาพ ผู้ขายจะต้องดำเนินการจัดหาอุปกรณ์เพิ่มเติมโดยไม่คิดค่าใช้จ่ายใด ๆ จาก สลค.

5. คุณลักษณะเฉพาะการดำเนินโครงการ

5.1 **ระบบรักษาความปลอดภัยระบบเครือข่ายระดับแอปพลิเคชัน (Application Firewall) จำนวน 2 ชุด** ที่มีคุณลักษณะเฉพาะอย่างน้อย ดังนี้

5.1.1 เป็นอุปกรณ์ Appliance-Based Firewall ที่สร้างขึ้นเพื่อทำหน้าที่ตรวจจับและควบคุม Application, User, Content โดยเฉพาะ (Application Firewall) โดยแยก Hardware ประมวลผลสำหรับบริหารจัดการ Management/Control Plane และหน่วยประมวลผลสำหรับข้อมูล (Data Plane) ออกจากกัน เพื่อไม่กระทบกับการทำงานโดยรวมในกรณีที่ส่วนใดส่วนหนึ่งเกิดปัญหา

5.1.2 มี Network Interface อย่างน้อย ดังนี้

(1) ช่องเชื่อมต่อแบบ 10/100/1000 Gigabit หรือดีกว่า ไม่น้อยกว่า 12 ช่อง

(2) ช่องเชื่อมต่อแบบ 1/10 Gigabit SFP/SFP+ หรือดีกว่า ไม่น้อยกว่า 8 ช่อง

5.1.3 มีช่องเชื่อมต่อ HA แบบ 10/100/1000 หรือดีกว่า ไม่น้อยกว่า 2 ช่อง, 10 Gigabit SFP+ หรือดีกว่า ไม่น้อยกว่า 1 ช่อง และมีช่องเชื่อมต่อสำหรับบริหารจัดการโดยเฉพาะ (Out of Band Management) ไม่น้อยกว่า 1 ช่อง โดยทั้งหมดไม่นับรวมกับ interface จากข้อ 5.1.2 และต้องเสนอสายหรืออุปกรณ์มาพร้อมสำหรับการทำ HA

5.1.4 มี Next Generation Firewall Throughput ในแบบ Appmix หรือ Enterprise testing condition หรือ Enterprise traffic mix ไม่น้อยกว่า 5.5 Gbps และ Threat prevention Throughput ในแบบ Appmix หรือ Enterprise testing condition หรือ Enterprise traffic mix ไม่น้อยกว่า 2.5 Gbps และรองรับจำนวน Max Sessions ได้ไม่น้อยกว่า 1,000,000 sessions และ New Sessions ไม่น้อยกว่า 60,000 new sessions ต่อวินาที

5.1.5 มี storage สำหรับ system ชนิด SSD ขนาดไม่ต่ำกว่า 240 GB

5.1.6 สามารถติดตั้งในรูปแบบ Transparent Inline, Non-Inline Monitoring (Tap), L2 และ L3 ได้

5.1.7 สามารถสร้าง VLAN ตามมาตรฐาน 802.1Q VLAN tags ได้ไม่น้อยกว่า 4,094 VLANs ต่ออุปกรณ์

5.1.8 สามารถ ...

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

5.1.9 สามารถทำการตรวจสอบข้อมูลจราจรที่เข้ารหัส SSL ด้วยการทำ SSL decryption (ทั้งแบบ Inbound และ Outbound) และการถอดรหัส SSL ให้อุปกรณ์อื่นในระบบ พร้อมทั้งทำการเข้ารหัส (Re-Encryption) ก่อนส่ง Traffic ออกจากระบบ (SSL Decryption Broker) ได้ หรือนำเสนออุปกรณ์อื่น ๆ เพิ่มเติม โดยอุปกรณ์ที่นำเสนอต้องมี Throughput ไม่น้อยกว่า Next Generation Firewall Throughput

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

5.1.11 สามารถควบคุมประเภทของไฟล์ที่อนุญาตให้ download และ upload บนแต่ละ Application ได้ รวมทั้งสามารถป้องกันการรั่วไหลของข้อมูล (Data Filtering) ออกจากระบบเครือข่าย เช่น หมายเลขบัตรเครดิต และสามารถสร้างรูปแบบการตรวจสอบได้ตามความต้องการ

5.1.12 สามารถป้องกันภัยคุกคามประเภท Vulnerability, Virus และ Spyware ได้โดยสามารถทำการอัพเดท Signature ใหม่แบบอัตโนมัติ

5.1.13 มีระบบตรวจจับ Advanced Malware แบบ Cloud-Based โดยใช้เทคโนโลยีแบบ Sandbox เพื่อใช้ระบุ Malware ประเภทใหม่ (Zero-day Malware) ซึ่งไม่มีใน Signature มาก่อน และสามารถสร้าง Signature ขึ้นมาเพื่อใช้ป้องกันระบบเครือข่ายได้โดยอัตโนมัติ

5.1.14 สามารถกำหนดนโยบายการเข้าถึงเว็บไซต์ (URL Filtering) สามารถติดตามและควบคุมการเข้าถึงเว็บไซต์ได้ตาม Category, Block list, Allow list ที่กำหนดได้ โดยต้องมีการจัด category ให้กับแต่ละเว็บไซต์ไม่น้อยกว่า 2 category โดยอัตโนมัติ รวมถึงมี Machine Learning เพื่อวิเคราะห์และป้องกัน Malicious URLs ที่ไม่เคยพบมาก่อน (Never-before-seen threats) และป้องกันเว็บไซต์ที่ใช้เทคนิคการหลบเลี่ยงการตรวจจับ เช่น Cloaking และ Fake CAPTCHAs ได้ หรือเสนออุปกรณ์เพิ่มเติมเพื่อให้ทำได้ตามข้อกำหนด โดยอุปกรณ์ที่นำเสนอต้องมี throughput ไม่น้อยกว่า Next Generation Firewall Throughput

5.1.15 สามารถตรวจจับและป้องกันการเข้าถึง Malicious Domain จากในองค์กรได้ โดยต้องมีความสามารถอย่างน้อย ดังนี้

(1) มีระบบ Machine Learning ในการตรวจหาเทคนิคอัลกอริทึม Domain Generation Algorithms (DGA) เพื่อวิเคราะห์คาดการณ์ ป้องกัน Malicious Domain ที่ไม่เคยพบมาก่อนได้

(2) สามารถตรวจจับและป้องกัน DNS Tunneling ได้ทั้งในรูปแบบ Known และ unknown เพื่อป้องกันการขโมยข้อมูลในองค์กรผ่านช่องทาง DNS

(3) ทำงานแบบ Real time และสามารถรองรับปริมาณ Malicious Domain ที่เพิ่มขึ้นในอนาคต โดยตรวจจับผ่านทาง DNS และต้องไม่ส่งผลกระทบกับ Performance ของระบบ

5.1.16 สามารถรับ Syslog จากระบบที่มีอยู่ได้ เพื่อใช้ในการยืนยันตัวตนของ User ที่ใช้งาน โดยรองรับทั้ง User Log-in และ User Log-out ได้ หรือเสนอระบบเพิ่มเติมเพื่อให้ทำได้ตามข้อกำหนด โดยมีลิขสิทธิ์ครอบคลุมการใช้งานของ สลค.

5.1.17 สามารถส่ง Syslog ไปยังระบบภายนอกโดยมีการเข้ารหัสแบบ SSL ได้เพื่อความปลอดภัยของระบบ

5.1.18 สามารถ ...

5.1.18 สามารถเรียกดูสรุปข้อมูลของ Data ในรูปแบบของกราฟฟิก และสามารถทำรายงานต่าง ๆ ได้อย่างน้อย ดังนี้

(1) Top Application, Application Category

(2) Top Source, User, Destination

(3) User activity report

5.1.19 สามารถทำรายงานรวมถึงปรับแต่งรายงานตามความต้องการในรูปแบบ PDF ได้เป็นอย่างน้อย พร้อมทั้งตั้งเวลาส่งรายงานผ่านทาง E-mail แบบอัตโนมัติได้

5.1.20 สามารถจัดเก็บบันทึกข้อมูลโดยส่ง Syslog, Netflow และ SNMP ไปยังระบบจัดการเครือข่ายที่รองรับคุณสมบัติดังกล่าวได้

5.1.21 สามารถบริหารจัดการผ่านทาง Web User Interface และ Command Line Interface ได้

5.1.22 มีเครื่องมือในการทำ Optimization Firewall โดยสามารถทำการวิเคราะห์ Log โดยใช้ Machine Learning และสามารถสร้าง Security Policy based on Traffic logs ที่เรียนรู้จากในองค์กร และสามารถประเมิน, Optimize Firewall ได้อย่างน้อย ดังนี้

(1) Architecture review

(2) System Health Check

(3) Configuration audit

(4) Optional product tuning และ configuration change implementation

5.1.23 มีเครื่องมือที่สามารถวิเคราะห์ตรวจจับภัยคุกคามบนระบบเครือข่ายโดยใช้ Technology Machine Learning และ AI ในการวิเคราะห์พฤติกรรมที่เกิดขึ้นโดยการหาความสัมพันธ์ของข้อมูลที่ได้มาจาก log ของระบบรักษาความปลอดภัยระบบเครือข่ายระดับแอปพลิเคชัน (Application Firewall) และระบบป้องกันการโจมตีผ่านช่องโหว่ซอฟท์แวร์สำหรับเครื่องคอมพิวเตอร์ลูกข่ายที่เสนอตามโครงการนี้ โดยมีความสามารถอย่างน้อย ดังนี้

(1) Network traffic analysis (NTA)

(2) User behavior analytics (UBA)

(3) Root cause analysis of alerts

(4) Timeline analysis of alerts

(5) Threat hunting

(6) Post-incident impact analysis

(7) Dashboards and reporting

(8) Incident response and recovery

5.1.24 สามารถทำงานร่วมกับระบบบริหารจัดการอุปกรณ์รักษาความปลอดภัยระบบเครือข่ายระดับแอปพลิเคชันแบบรวมศูนย์ (Application Firewall Management) ที่มีอยู่เดิมของ สลค. ได้เพื่อประสิทธิภาพในการบริหารจัดการในภาพรวม

5.1.25 รองรับการติดตั้งเพื่อทำ High Availability แบบ Active-Active และ Active-Passive ได้

5.1.26 มีแหล่งจ่ายไฟฟ้า (Power Supply) แบบ redundant และมีพัดลมระบายอากาศแบบ Hotswap แยกต่างหากจาก Power Supply

5.1.27 ต้อง ...

5.1.27 ต้องได้รับการรับรองมาตรฐาน FCC และ VCCI ได้เป็นอย่างน้อย

5.1.28 ต้องได้รับการจัดอันดับให้อยู่ในกลุ่ม Leader ของ Gartner Magic Quadrant ในกลุ่มผลิตภัณฑ์ Enterprise Network Firewalls ปี 2020 หรือปีล่าสุด

5.2 **ระบบป้องกันการโจมตีผ่านช่องโหว่ซอฟท์แวร์สำหรับเครื่องคอมพิวเตอร์ลูกข่าย จำนวน 1 ระบบ** ที่มีคุณลักษณะเฉพาะอย่างน้อย ดังนี้

5.2.1 เป็นซอฟต์แวร์ป้องกันการโจมตีผ่านช่องโหว่และแอดวานซ์มัลแวร์ ที่บริหารจัดการความปลอดภัยบนเครื่องคอมพิวเตอร์สำหรับองค์กร (endpoint) ที่ประกอบไปด้วยเทคโนโลยีทางด้าน Exploit Prevention, Malware Prevention, Vulnerability Management เป็นอย่างน้อย และทำงานได้ใน Agent เดียว

5.2.2 สามารถบริหารจัดการจากศูนย์กลาง (centralize management) ผ่าน Web Browser ได้

5.2.3 มีใบอนุญาต (Licenses) ที่รองรับการใช้งานได้จำนวนไม่น้อยกว่า 700 สิทธิ์การใช้งาน

5.2.4 สามารถติดตั้งบนระบบปฏิบัติการต่าง ๆ ได้อย่างน้อย ดังนี้

(1) Windows 10

(2) Windows Server

(3) macOS

(4) Red Hat Enterprise Linux

(5) Ubuntu

(6) Android

5.2.5 การเชื่อมต่อระหว่าง Agent และ Management Console ต้องเป็นแบบ SSL เพื่อความปลอดภัย

5.2.6 สามารถกำหนด Password สำหรับถอนการติดตั้ง Agent จาก Management Console เพื่อป้องกันไม่ให้ User ถอนการติดตั้ง Agent software ได้

5.2.7 สามารถป้องกันการโจมตีช่องโหว่ด้วยรูปแบบการป้องกันได้อย่างน้อย ดังนี้

(1) Anti-Ransomware

(2) CPL Protection

(3) Data execution prevention (DEP)

(4) DLL Security

(5) DLL-Hijacking Protection

5.2.8 Agent software ต้องสามารถป้องกัน Exploit และ Malware ได้ทันทีหลังติดตั้งสำเร็จ โดยไม่ต้องทำการ update ฐานข้อมูล (Signature)

5.2.9 Agent software ต้องสามารถป้องกัน Exploit และ Malware ได้โดยไม่ต้องทำการ scan ไฟล์ในเครื่องผู้ใช้งาน

5.2.10 Agent software ต้องสามารถตรวจวิเคราะห์ (Local Analysis) และป้องกัน Malware ด้วยตัวเองในกรณีที่เป็น Malware ที่ไม่เคยตรวจพบมาก่อน

5.2.11 Agent software ต้องสามารถป้องกัน Exploit และ Malware ในกรณีที่ไม่สามารถติดต่อกับ Management Console ได้

5.2.12 Agent software สามารถทำการ quarantine malware ที่ตรวจพบได้

5.2.13 สามารถ ...

5.2.13 สามารถติดต่อกับ Cloud Sandboxing เดียวกับระบบรักษาความปลอดภัยระบบเครือข่ายระดับแอปพลิเคชัน (Application Firewall) ที่นำเสนอตามโครงการนี้ เพื่อตรวจสอบ Malware ที่ยังไม่เคยตรวจสอบมาก่อนเพื่อรับข้อมูลกลับมาใช้ในการป้องกัน Malware ได้

5.2.14 สามารถกำหนด policy ในการ exception จากค่าต่าง ๆ เช่น HASH ได้

5.2.15 สามารถทำการ Isolate เครื่อง endpoints ได้

5.2.16 สามารถแสดงรายการเครื่องคอมพิวเตอร์ลูกข่ายที่ใช้ระบบปฏิบัติการ Windows ที่มีการเข้ารหัส Disk (Disk Encryption) โดยใช้ Microsoft BitLocker ได้ หรือนำเสนอระบบอื่น ๆ เพิ่มเติม เพื่อให้สามารถทำตามความต้องการดังกล่าว

5.2.17 สามารถตรวจสอบช่องโหว่ของระบบปฏิบัติการ (Vulnerability) บนระบบปฏิบัติการ Windows และ Linux โดยอ้างอิงช่องโหว่ตาม Common Vulnerabilities and Exposures (CVE) หรือนำเสนอระบบอื่น ๆ เพิ่มเติม เพื่อให้สามารถทำตามความต้องการดังกล่าว โดยต้องมีลิขสิทธิ์ครอบคลุมการใช้งานของ สลค.

5.3 **ระบบบริหารจัดการและตอบสนองต่อภัยคุกคามไซเบอร์แบบอัตโนมัติ จำนวน 1 ระบบ** ที่มีคุณลักษณะเฉพาะอย่างน้อย ดังนี้

5.3.1 เป็นระบบที่ออกแบบมาเพื่อจัดการเรื่อง Security Orchestration, Automation and Response (SOAR) โดยเฉพาะ และมีระบบ Threat Intelligence Management (TIM) อยู่ภายในระบบเดียวกันแบบพร้อมใช้งานภายในระบบดังกล่าว หรือนำเสนอ Threat Intelligence Platform เพิ่มเติม โดยระบบที่นำเสนอจะต้องเป็น Commercial Product และมีสำนักงานในประเทศไทย เพื่อให้มีประสิทธิภาพในการทำงานสูงสุด

5.3.2 เป็น Software ที่ออกแบบมาเพื่อช่วยในการบริหารการจัดการสำหรับ Security Operation Team โดยเฉพาะ โดยมีเครื่องมือที่ช่วยในการทำ Accelerate Response และรองรับการทำงานร่วมกับระบบต่าง ๆ ได้อย่างน้อย ดังนี้

(1) Security Information and Event Management (SIEM)
(2) Endpoint Detection and Response (EDR)
(3) Threats Intelligence (TI)
(4) Malware Analysis
(5) Data Loss Prevention (DLP)
(6) Email
(7) Ticketing Systems
(8) Users and Entity Behavior Analytic

5.3.3 มีรูปแบบการบริหารจัดการ Standardize Process และติดตามเหตุการณ์ที่เกิดขึ้น (incident) รวมไปถึงช่วยวิเคราะห์ (Analyst Metrics) เช่น Task-based workflows, Visual playbook editor, SLA and metric tracking ได้เป็นอย่างน้อย

5.3.4 ระบบบริหารการจัดการภัยและตอบสนองต่อภัยคุกคามแบบอัตโนมัติที่นำเสนอจะต้องรองรับการทำงานร่วมกับระบบจัดเก็บและวิเคราะห์ข้อมูลจราจรคอมพิวเตอร์ (Security Information and Event Management, SIEM) ได้

5.3.5 มีระบบ ...

5.3.5 มีระบบช่วยให้ทีมผู้ดูแลระบบต่าง ๆ สามารถทำงานร่วมกันได้ลักษณะ Collaborate and Learn เช่น Virtual War Room ได้เป็นอย่างน้อย หรือนำเสนอระบบอื่น ๆ เพิ่มเติมเพื่อรองรับความต้องการดังกล่าว โดยระบบ Collaborate and Learn ที่นำเสนอเพิ่มเติมจะต้องสามารถเชื่อมโยงข้อมูลการสนทนาที่เกี่ยวข้องกับ Incident นั้น ๆ จากระบบ SOAR ไปยังระบบ Collaborate and Learn ได้

5.3.6 สามารถสร้าง Work Plan หรือ WorkFlow หรือ Playbook ในรูปแบบ Parallel ที่สามารถทำได้หลายงานพร้อม ๆ กัน และสามารถทำ Sub Playbook ได้

5.3.7 สามารถทำ Case Management เพื่อบริหารจัดการ Incident ต่าง ๆ ที่เกิดขึ้น เช่น กำหนดระยะเวลาในการตอบสนองต่อ Incident type ประเภทต่าง ๆ ได้ รวมถึงแสดงผลการทำงานในภาพรวม ลักษณะ SLA Dashboard ได้ หรือนำเสนอระบบอื่น ๆ เพิ่มเติมเพื่อรองรับการทำงานลักษณะดังกล่าว

5.3.8 สามารถบริหารจัดการความรับผิดชอบงาน (Shift Management) ของผู้ดูแลระบบความปลอดภัย และสามารถส่ง Incident ให้กับผู้ดูแลระบบความปลอดภัยตามความรับผิดชอบงานหรือภาระงาน (load) ได้เป็นอย่างน้อย

5.3.9 สามารถทำงานร่วมกับระบบรักษาความปลอดภัยระบบเครือข่ายระดับแอปพลิเคชัน (Application Firewall) ที่นำเสนอตามโครงการนี้ เช่น ทำการสั่ง Block IP Address, URL แบบอัตโนมัติได้

5.3.10 สามารถทำงานร่วมกับระบบรักษาความปลอดภัยระบบเครือข่ายระดับแอปพลิเคชัน (Application Firewall) ที่นำเสนอตามโครงการนี้ หรือระบบบริหารจัดการอุปกรณ์รักษาความปลอดภัยระบบเครือข่ายระดับแอปพลิเคชันแบบรวมศูนย์ (Application Firewall Management) ที่มีอยู่เดิมของ สลค. เพื่อ Query Firewall Log ต่าง ๆ เช่น Traffic, Threat เข้ามาในระบบได้

5.3.11 สามารถทำงานร่วมกับระบบรักษาความปลอดภัยระบบเครือข่ายระดับแอปพลิเคชัน (Application Firewall) ที่นำเสนอตามโครงการนี้ หรือระบบบริหารจัดการอุปกรณ์รักษาความปลอดภัยระบบเครือข่ายระดับแอปพลิเคชันแบบรวมศูนย์ (Application Firewall Management) ที่มีอยู่เดิมของ สลค. เพื่อทำ Best Practice assessment ในรูปแบบ Playbook

5.3.12 สามารถทำงานร่วมกับ API ของระบบป้องกันการโจมตีผ่านช่องโหว่ซอฟท์แวร์สำหรับเครื่องคอมพิวเตอร์ลูกข่ายที่นำเสนอตามโครงการนี้ เพื่อบริหารจัดการ Incident ร่วมกันได้อย่างมีประสิทธิภาพ เสมือนเป็นระบบเดียวกัน เช่น สามารถดึงข้อมูล incident จากระบบป้องกันการโจมตีผ่านช่องโหว่ซอฟท์แวร์สำหรับเครื่องคอมพิวเตอร์ลูกข่ายที่นำเสนอตามโครงการนี้ขึ้นมาเพื่อบริหารจัดการผ่านระบบบริหารการจัดการภัยและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ (Security Orchestration, Automation and Response (SOAR)) ได้ เป็นต้น

5.3.13 สามารถทำงานร่วมกับระบบป้องกันและวิเคราะห์ภัยคุกคามขั้นสูง (Unknown Threat) ของระบบรักษาความปลอดภัยระบบเครือข่ายระดับแอปพลิเคชัน (Application Firewall) ที่นำเสนอตามโครงการนี้ เพื่อส่งไฟล์ และ URL ไปตรวจสอบ รวมถึงสามารถดึงตัวอย่างไฟล์จากระบบดังกล่าวได้โดยอัตโนมัติในรูปแบบ Playbook

5.3.14 รองรับการทำงานร่วมกับระบบอื่น ๆ (Integrate) ผ่านทาง REST API, SSH/CLI ได้เป็นอย่างน้อย

5.3.15 สามารถ ...

5.3.15 สามารถบริหารจัดการแบบ GUI ผ่าน Web Browser และมี Application เพื่อช่วยในการบริหารจัดการผ่าน Mobile Device โดยต้องสามารถแสดง Personal Dashboard และ Task list ของผู้ดูแลระบบรักษาความปลอดภัยได้เป็นอย่างน้อย

5.3.16 มี Built-in Report และ Dashboard และสามารถปรับเปลี่ยนการแสดงผลในรูปแบบ Bar, Column, Line, Pie และ Number ดังต่อไปนี้

(1) Incident Report, Mean Time to Detection (MTTD), Mean Time to Remediation (MTTR) และ SLA

(2) Indicator Report

5.3.17 สามารถ Custom Report และ Dashboard ได้ และมีความสามารถอื่น ๆ ได้อย่างน้อยดังนี้

(1) ระบบสามารถ Export รายงานออกมาได้ในรูปแบบ PDF และ DOC

(2) สามารถตั้งเวลา (schedule) ในการทำรายงานและส่งอีเมล์ไปยังผู้รับได้อัตโนมัติ

5.3.18 มีใบอนุญาต (Licenses) การใช้งานที่สามารถรองรับผู้ใช้งานระดับ Security Analyst ได้ไม่น้อยกว่า 2 ผู้ใช้งาน โดยระบบต้องสามารถสร้าง Workflow ในการทำงานได้ไม่น้อยกว่า 5,000 Workflows และไม่มีค่าใช้จ่ายเพิ่มเติมในส่วนของใบอนุญาตการใช้งาน

5.3.19 มี Playbook Marketplace ที่สามารถนำ Playbook จาก Marketplace หรือจากการพัฒนาเพิ่มเติม มาติดตั้งและใช้งานได้ไม่น้อยกว่า 500 Playbook

5.4 **ระบบรักษาความปลอดภัยระบบเครือข่ายระดับแอปพลิเคชัน (Application Firewall) ทดแทนระบบเดิม จำนวน 1 ระบบ** โดยมีคุณลักษณะเฉพาะอย่างน้อย ดังนี้

5.4.1 เป็นอุปกรณ์หรือซอฟต์แวร์ Virtual Appliance Firewall ที่สร้างขึ้นเพื่อทำหน้าที่ตรวจจับและควบคุม Application, User และ Content โดยเฉพาะ (Application Firewall) และใช้โครงสร้างสถาปัตยกรรมแบบ Single Pass Software

5.4.2 มี Application Firewall หรือ Next Generation Firewall Throughput ไม่น้อยกว่า 4 Gbps, Threat Prevention Throughput ไม่น้อยกว่า 2 Gbps สำหรับ SR-IOV และมีจำนวนเซสชันสูงสุด (Max Sessions) ไม่น้อยกว่า 700,000 sessions และรองรับการสร้างเซสชันใหม่ได้ไม่น้อยกว่า 15,000 sessions ต่อวินาทีสำหรับ SR-IOV

5.4.3 สามารถทำ Remote VPN เพื่อเพิ่มความปลอดภัยให้กับ Mobile User ที่รองรับจำนวน Users ไม่น้อยกว่า 200 Users โดยรองรับการใช้งานทั้ง Laptops, Smartphones, Tablets บนระบบปฏิบัติการต่าง ๆ อย่างน้อย ดังนี้

(1) Apple iOS

(2) Apple macOS

(3) Google Android

(4) Linux CentOS

(5) Red Hat Enterprise Linux

(6) Ubuntu

(7) Windows

5.4.4 สามารถ ...

5.4.4 สามารถตรวจสอบและกำหนดนโยบายเครื่องที่ทำการ VPN เข้ามาในระบบโดยตรวจสอบจาก Operating System, Antivirus version, Host firewall version และ registry เป็นอย่างน้อยสามารถทำงานร่วมกับระบบการพิสูจน์ตัวตน (Authentication) ได้แก่ SAML, LDAP, Client certificates, Kerberos, RADIUS, Two-factor authentication

5.4.5 รองรับการทำงานร่วมกับระบบ Multi Factor Authentication ในการยืนยันตัวตนเพื่อตรวจสอบการใช้งานร่วมกับระบบ Azure AD ที่ สลค. มีอยู่ โดยทำงานร่วมกับ VPN ของระบบรักษาความปลอดภัยระบบเครือข่ายระดับแอปพลิเคชัน (Application Firewall) ที่มีอยู่เดิม โดยลิขสิทธิ์ของระบบต้องครอบคลุมผู้ใช้งานได้ไม่น้อยกว่า 200 ผู้ใช้งาน

5.4.6 สามารถควบคุมประเภทของไฟล์ที่อนุญาตให้ดาวน์โหลดและอัพโหลดบนแต่ละ Applications ได้ รวมทั้งสามารถป้องกันการรั่วไหลของข้อมูล (Data Filtering) ออกจากระบบเครือข่าย เช่น หมายเลขบัตรเครดิต และสามารถสร้างรูปแบบได้ตามความต้องการ

5.4.7 สามารถป้องกันภัยคุกคามประเภท Vulnerability, Virus และ Spyware และสามารถอัพเดท Signature ใหม่แบบอัตโนมัติได้

5.4.8 มีระบบตรวจจับ Advanced Malware แบบ Cloud-Based โดยใช้เทคโนโลยีแบบ Sandbox เพื่อใช้ระบุ Malware ประเภทใหม่ (Zero-day Malware) ซึ่งไม่มีใน Signature มาก่อน และสามารถสร้าง Signature ขึ้นมาเพื่อใช้ป้องกันระบบเครือข่ายได้โดยอัตโนมัติ

5.4.9 สามารถกำหนดนโยบายการเข้าถึงเว็บไซต์ (URL Filtering) สามารถติดตามและควบคุมการเข้าถึงเว็บไซต์ได้ตาม Category, Block list, Allow list ที่กำหนดได้ และต้องมีการจัด category ให้กับแต่ละเว็บไซต์ไม่น้อยกว่า 2 category โดยอัตโนมัติ หรือเสนออุปกรณ์เพิ่มเติมเพื่อให้ทำได้ตามข้อกำหนด โดยอุปกรณ์ที่นำเสนอต้องมี throughput ไม่น้อยกว่า Next Generation Firewall Throughput

5.4.10 สามารถตรวจจับและป้องกันการเข้าถึง Malicious Domain จากในองค์กรได้ โดยต้องมีความสามารถอย่างน้อย ดังนี้

(1) มีระบบ Machine Learning ในการตรวจหาเทคนิคอัลกอริทึม Domain Generation Algorithms (DGA) เพื่อวิเคราะห์คาดการณ์ ป้องกัน Malicious Domain ที่ไม่เคยพบมาก่อนได้

(2) สามารถตรวจจับและป้องกัน DNS Tunneling ได้ทั้งในรูปแบบ Known และ unknown เพื่อป้องกันการขโมยข้อมูลในองค์กร ผ่านช่องทาง DNS

(3) ทำงานแบบ Real time และรองรับปริมาณ Malicious Domain ที่เพิ่มขึ้นในอนาคต โดยตรวจจับผ่านทาง DNS และไม่ส่งผลกระทบกับ Performance ของระบบ

5.4.11 สามารถรับ Syslog จากระบบที่มีอยู่ได้ เพื่อใช้ในการยืนยันตัวตน ของ User ที่ใช้งาน โดยรองรับทั้ง User Log-in และ User Log-out ได้ หรือเสนอระบบเพิ่มเติมเพื่อให้ทำได้ตามข้อกำหนด โดยมีลิขสิทธิ์ครอบคลุมการใช้งานของ สลค.

5.4.12 สามารถทำงานร่วมกับระบบบริหารจัดการอุปกรณ์รักษาความปลอดภัยระบบเครือข่ายระดับแอปพลิเคชันแบบรวมศูนย์ (Application Firewall Management) ที่มีอยู่เดิมของ สลค. ได้เพื่อประสิทธิภาพในการบริหารจัดการในภาพรวม

5.5 **ผู้ขาย** ...

5.5 ผู้ขายจะต้องดำเนินการจัดทำแนวทางการพัฒนาศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศอย่างน้อย ดังนี้

5.5.1 จัดทำร่างนโยบายในการรับมือเหตุการณ์ภัยคุกคามทางไซเบอร์ของ สลค. โดยอ้างอิงจากข้อกำหนดตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และแนวปฏิบัติของ NIST Cyber Security Framework

5.5.2 จัดทำขั้นตอนการปฏิบัติงานต่าง ๆ โดยกระบวนการที่นำเสนอจะต้องคำนึงถึงเครื่องมือด้านเทคนิคที่ สลค. มีการใช้งานอยู่ในปัจจุบัน ดังนี้

(1) จัดทำขั้นตอนการปฏิบัติงานเฝ้าระวังเหตุการณ์ภัยคุกคามและการโจมตีทางไซเบอร์ในศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Detection Workflow/Process)

(2) กำหนดเงื่อนไขและกระบวนการในการเพิ่มระดับและสื่อสารเมื่อเกิดเหตุการณ์ภัยคุกคามและการโจมตีทางไซเบอร์ (Cyber Incident Escalation and Communication Workflow/Process)

(3) จัดทำคู่มือการตอบสนองภัยคุกคามและการโจมตีทางไซเบอร์ (Cyber Security Playbook) พร้อมจัดทำระบบบริหารจัดการและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ (Security Orchestration, Automation and Response: SOAR) จำนวนอย่างน้อย 5 Playbook โดยวิเคราะห์ และประเมินภัยคุกคามและการโจมตีทางไซเบอร์ที่สำคัญ และอาจเกิดขึ้นกับระบบคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์

(4) จัดทำระบบบริหารจัดการและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ (Security Orchestration, Automation and Response: SOAR) ในรูปแบบของ Playbook Automation เพิ่มเติม ให้แก่ สลค. จำนวนอย่างน้อย 5 Playbook ต่อปี รวมทั้งเชื่อมโยงการทำงาน (Integrate) เข้ากับระบบความปลอดภัยเดิมที่ สลค. มีอยู่ ตามที่ สลค. ร้องขอ

(5) จัดทำขั้นตอนอื่น ๆ ที่เกี่ยวข้องหลังจากเกิดเหตุการณ์ภัยคุกคามด้านไซเบอร์ เช่น ขั้นตอนในการจัดเก็บองค์ความรู้เกี่ยวกับการรับมือเหตุการณ์ภัยคุกคามด้านไซเบอร์ที่เคยเกิดขึ้นในอดีตเป็นอย่างน้อย

5.5.3 ติดตั้งอุปกรณ์ที่เสนอพร้อม Configuration ให้เรียบร้อยพร้อมเชื่อมโยง (Integrate) อุปกรณ์และระบบที่จัดหาตามโครงการนี้ให้สามารถทำงานร่วมกันในรูปแบบ WorkFlow/Playbook Automation ได้อย่างมีประสิทธิภาพ

5.5.4 ทำการเชื่อมต่อระบบบริหารจัดการภัยและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ (Security Orchestration, Automation and Response: SOAR) ให้สามารถทำงานร่วมกับระบบรักษาความปลอดภัยเครือข่ายระดับแอปพลิเคชัน (Application Firewall) ที่มีอยู่เดิมของ สลค. ได้ เช่น ทำการ Block IP Address และทำการ Block URL ได้โดยอัตโนมัติ

5.5.5 ทำการเชื่อมต่อระบบบริหารจัดการภัยและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ (Security Orchestration, Automation and Response: SOAR) ให้สามารถทำงานร่วมกับระบบป้องกันการโจมตีผ่านช่องโหว่ซอฟท์แวร์สำหรับเครื่องคอมพิวเตอร์ลูกข่าย โดยมีความสามารถอย่างน้อย ดังนี้

(1) ดึงข้อมูล Incident จากระบบป้องกันการโจมตีผ่านช่องโหว่ซอฟท์แวร์สำหรับเครื่องคอมพิวเตอร์ลูกข่าย (Fetch Incidents from XDR)

(2) Update Incident ในระบบป้องกันการโจมตีผ่านช่องโหว่ซอฟท์แวร์สำหรับเครื่องคอมพิวเตอร์ลูกข่าย (Update Incident in XDR)

(3) สั่งงาน ...

(3) สั่งงานให้ Isolate และยกเลิกการ Isolate เครื่อง Endpoint (Isolate/Unisolate Endpoints)

(4) ดึงข้อมูล (Query) Audit Report จาก Agent ที่ติดตั้งอยู่บนเครื่องแม่ข่าย (Query for Agent Audit Reports)

(5) สามารถทำ Incident Mirroring โดยเมื่อมีการเปลี่ยนแปลง Incident ที่ระบบบริหารการจัดการภัยและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ (Security Orchestration, Automation and Response: SOAR) ระบบจะต้องทำการเปลี่ยนแปลงที่ระบบป้องกันการโจมตีผ่านช่องโหว่ซอฟท์แวร์สำหรับเครื่องคอมพิวเตอร์ลูกข่ายด้วย และในกรณีที่มีการเปลี่ยนแปลง incident ที่ให้สามารถทำงานร่วมกับระบบป้องกันการโจมตีผ่านช่องโหว่ซอฟท์แวร์สำหรับเครื่องคอมพิวเตอร์ลูกข่าย จะต้องเปลี่ยนแปลงกลับมาที่ระบบบริหารการจัดการภัยและตอบสนองต่อภัยคุกคามแบบอัตโนมัติด้วย (Security Orchestration, Automation and Response: SOAR) (XDR Incident Mirroring)

5.5.6 จัดทำต้นแบบ (Template) รายงานภัยคุกคามและการโจมตีทางไซเบอร์ ซึ่งจะต้องประกอบไปด้วยรายงานต่าง ๆ อย่างน้อย ดังนี้

(1) รายงานประจำวัน โดยมีรายละเอียดเกี่ยวกับการสรุปเหตุการณ์ภัยคุกคามที่เกิดขึ้นในระยะเวลา 1 วัน อย่างครบถ้วน

(2) รายงานประจำเดือน ซึ่งจะต้องประกอบไปด้วย บทสรุปผู้บริหาร (Executive Summary) เพื่อรายงานผลการเฝ้าระวังและตรวจจับภัยคุกคามทางไซเบอร์รายเดือน

5.6 **ระบบบริหารจัดการเครือข่ายแบบรวมศูนย์ จำนวน 1 ระบบ** ที่มีคุณลักษณะเฉพาะอย่างน้อย ดังนี้

5.6.1 เป็นอุปกรณ์ Hardware Controller ที่มีคุณสมบัติอย่างน้อย ดังนี้

(1) เป็น Appliance หรือ Server ที่มีขนาดไม่เกิน 4U

(2) มีหน่วยประมวลผลกลาง (CPU) ที่มีความเร็วสัญญาณนาฬิกาพื้นฐานไม่น้อยกว่า 2.1 GHz หรือดีกว่า จำนวนไม่น้อยกว่า 2 หน่วย

(3) มีหน่วยความจำหลัก (RAM) ชนิด DDR4 หรือดีกว่า ขนาดไม่น้อยกว่า 256 GB

(4) สนับสนุนการทำงาน RAID ไม่น้อยกว่า RAID 1, 10

(5) มีหน่วยจัดเก็บข้อมูล (Hard Disk) ชนิด SATA SSD หรือดีกว่า ที่มีขนาดความจุไม่น้อยกว่า 1.9 TB จำนวนไม่น้อยกว่า 6 หน่วย และขนาดความจุไม่น้อยกว่า 480 GB จำนวนไม่น้อยกว่า 2 หน่วย

(6) มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10 Gigabit Ethernet (SFP+) จำนวนไม่น้อยกว่า 2 ช่อง พร้อมเสนอโมดูล Transceiver ยี่ห้อเดียวกับอุปกรณ์ที่เสนอ แบบ 10GBASE-SR จำนวนไม่น้อยกว่า 2 โมดูล

(7) มี Power Supply แบบ Redundant หรือ Hot Swap จำนวน 2 หน่วย

(8) สามารถทำงานกับระบบไฟฟ้าในประเทศไทยแบบ 220 VAC, 50Hz ได้

(9) ผ่านการรับรองตามมาตรฐานความปลอดภัย IEC, FCC หรือ 47CFR Part 15 (CFR 47) Class A และ UL

(10) สามารถติดตั้งบนตู้ Rack ขนาดมาตรฐาน 19" ได้

5.6.2 สามารถ ...

5.6.2 สามารถควบคุมอุปกรณ์กระจายสัญญาณเครือข่าย (Switch) และอุปกรณ์กระจายสัญญาณเครือข่ายไร้สาย (Wireless) ที่ สลค. ใช้งานอยู่ได้อย่างมีประสิทธิภาพ โดยต้องรองรับการควบคุมอุปกรณ์ในอนาคตได้รวมจำนวนไม่น้อยกว่า 500 ชุด

5.6.3 สามารถตรวจพบ (discovery) อุปกรณ์เครือข่ายที่เชื่อมโยงในระบบเครือข่ายของ สลค. ได้

5.6.4 สามารถจัดเก็บรายละเอียดของอุปกรณ์ (Inventory) ในรูปแบบ Network Information Database โดยเก็บข้อมูลได้แก่ serial number, IP address, MAC address, OS/Firmware version, Up time, Memory size, Status up/down, Interface name, MAC address of the interface และ Configuration ได้เป็นอย่างน้อย

5.6.5 สามารถสร้างแผนผังการเชื่อมต่ออุปกรณ์เครือข่าย (physical topology map) และแสดงรายละเอียดของอุปกรณ์ได้

5.6.6 รองรับการสั่งงานเพื่อกำหนดค่าคุณภาพของการให้บริการรับส่งข้อมูลในระบบเครือข่าย (Quality of Service) ที่เสนอได้

5.6.7 รองรับการทำ Zero Touch Deployment (ZTD) หรือ Network Plug and Play (PnP) ให้กับอุปกรณ์เครือข่ายของ สลค. ได้

5.6.8 อุปกรณ์ Software Defined Network Controller สามารถส่งซอฟต์แวร์ (image) และชุดคำสั่งที่กำหนดไว้ล่วงหน้า (pre-define configuration) ไปให้อุปกรณ์เครือข่าย โดยอ้างอิงจาก Device Identifier อาทิ Serial Number ได้

5.6.9 สามารถสร้างแผนผังการเชื่อมต่ออุปกรณ์เครือข่ายให้สัมพันธ์กับแผนผังอาคาร (Floor Plan) ได้

5.6.10 รองรับการตรวจสอบหาเส้นทางการรับส่งข้อมูลของแต่ละ application ในระบบเครือข่ายได้

5.6.11 รองรับการแสดงข้อมูลสถิติการใช้งานต่าง ๆ อาทิ Interface, QoS, Device Information และ Performance Monitor ของเส้นทางรับส่งข้อมูลได้

5.6.12 รองรับการแสดงข้อมูล Routing protocol และ Layer 3 Interface ของเส้นทางรับส่งข้อมูลได้

5.6.13 รองรับการวิเคราะห์ผลกระทบที่เกิดจากการทำ Access Control List (ACL) ในเส้นทางรับส่งข้อมูลได้

5.6.14 กรณีเกิดปัญหากับอุปกรณ์เครือข่ายที่เชื่อมต่อกับระบบบริหารจัดการเครือข่ายแบบรวมศูนย์ ระบบสามารถแจ้งเตือนไปยังอีเมลของผู้ดูแลระบบที่กำหนดไว้ได้

5.6.15 รองรับการทำ High Availability เพื่อสร้างระบบสำรองและเพิ่มประสิทธิภาพของ Software Defined Network Controller ที่เสนอได้

5.6.16 สามารถเก็บ audit log ของผู้ใช้งานเพื่อมาตรวจสอบย้อนหลังได้

5.6.17 หากอุปกรณ์ Controller ขัดข้องจะต้องไม่ส่งผลกระทบต่อการทำงานของระบบเครือข่ายของ สลค. ไม่ว่าส่วนใดส่วนหนึ่ง

5.7 **ระบบ** ...

5.7 **ระบบลงทะเบียนเข้าใช้งาน Wi-Fi ทดแทนระบบเดิม จำนวน 1 ระบบ** ที่มีคุณลักษณะเฉพาะอย่างน้อย ดังนี้

5.7.1 **ผู้ใช้งานลงทะเบียนเข้าใช้งาน Wi-Fi ด้วยตนเอง (Self Service)**

(1) สามารถลงทะเบียนเข้าใช้งาน Wi-Fi ผ่านเว็บไซต์ ด้วยเครื่องคอมพิวเตอร์โน้ตบุ๊ก สมาร์ทโฟน และแท็บเล็ต ที่ใช้ระบบปฏิบัติการ Windows, Mac OS, iOS และ Android ได้

(2) สามารถยืนยันตัวตนผู้ลงทะเบียนด้วยการส่ง OTP ไปยังเบอร์โทรศัพท์ของผู้ลงทะเบียนผ่านการเชื่อมต่อกับผู้ให้บริการ SMS Gateway ได้ โดยผู้ขายต้องจัดหา SMS Gateway พร้อมใบอนุญาต (Licenses) ที่รองรับการใช้งานได้ไม่น้อยกว่า 50,000 ข้อความ

(3) สามารถกำหนดช่วงระยะเวลาที่อนุญาตให้ใช้งานได้ เช่น จำนวนวัน และจำนวนชั่วโมง เป็นต้น

(4) เมื่อผู้ใช้งานล็อกอินเข้าใช้งานสำเร็จ ระบบสามารถแสดงรายละเอียดวัน เวลา และระยะเวลาคงเหลือที่ใช้งานได้ผ่านทางหน้าจอของผู้ใช้งาน หรือสามารถส่งข้อมูลแสดงช่วงระยะเวลาที่สามารถใช้งานได้ (Valid Date) ไปยังผู้ใช้งานได้

5.7.2 **ผู้ดูแลระบบกำหนดบัญชีผู้ใช้ (Account) ให้กับผู้ใช้งาน**

กรณีที่ผู้ใช้งานไม่สามารถลงทะเบียนใช้งาน Wi-Fi ด้วยตนเองได้ ผู้ดูแลระบบจะสามารถกำหนดบัญชีผู้ใช้ (Account) ให้กับผู้ใช้งานแต่ละรายได้ ดังนี้

(1) สามารถกำหนดบัญชีผู้ใช้ให้กับผู้ใช้งาน 1 คน หรือหลายคนได้ในคราวเดียวกัน

(2) สามารถกำหนดช่วงระยะเวลาที่อนุญาตให้ผู้ใช้งานแต่ละรายใช้งานได้

(3) สามารถสั่งพิมพ์บัญชีผู้ใช้ออกทางเครื่องพิมพ์ได้ หรือสามารถนำบัญชีผู้ใช้ที่สร้างไว้ส่งออกจากระบบในรูปแบบ CSV หรือ Excel หรือ PDF เพื่อสั่งพิมพ์ออกทางเครื่องพิมพ์ได้

(4) เมื่อผู้ใช้งานล็อกอินเข้าใช้งานสำเร็จ ระบบสามารถแสดงรายละเอียดวัน เวลา และระยะเวลาคงเหลือที่ใช้งานได้ผ่านทางหน้าจอของผู้ใช้งาน

5.7.3 **ผู้ดูแลระบบกำหนดสิทธิ์การใช้งานด้วย MAC Address ของอุปกรณ์ Mobile Device**

(1) สามารถนำ MAC address จากเครื่องคอมพิวเตอร์โน้ตบุ๊ก สมาร์ทโฟน และแท็บเล็ต มาลงทะเบียนเพื่อใช้งาน Wi-Fi ได้

(2) สามารถกำหนดช่วงระยะเวลาที่อนุญาตให้ผู้ใช้แต่ละรายใช้งานได้

(3) รองรับการลงทะเบียนด้วย MAC Address ได้ไม่น้อยกว่า 1,000 อุปกรณ์

5.7.4 **คุณลักษณะเฉพาะอื่น ๆ**

(1) สามารถจัดเก็บข้อมูลผู้ใช้งานบน Software Radius Server และ Database หรือจัดเก็บในรูปแบบ Local Database ได้

(2) สามารถจัดทำรายงานสถิติการใช้งานอินเทอร์เน็ตของผู้ใช้งานแต่ละรายได้ โดยสามารถค้นหาข้อมูลผู้ใช้งาน พร้อมออกรายงาน และพิมพ์รายงานได้ตามรูปแบบที่ สลค. กำหนด

(3) สามารถจัดเก็บข้อมูลจราจร (Log) เพื่อให้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 พร้อมทั้งสามารถสร้างรายงานในรูปแบบไฟล์ CSV หรือ Excel หรือ PDF ได้เป็นอย่างน้อย

5.7.5 ติดตั้งระบบลงทะเบียนเข้าใช้งาน Wi-Fi ที่จัดหาตามโครงการนี้ ให้สามารถทำงานทดแทนระบบลงทะเบียนเข้าใช้งาน Wi-Fi ระบบเดิมได้อย่างมีประสิทธิภาพ

5.8 **จัดหา ...**

5.8 **จัดหาและติดตั้งใบรับรอง SSL Certificate จำนวน 1 ชุด** ที่มีคุณลักษณะเฉพาะอย่างน้อย ดังนี้

5.8.1 เป็นใบรับรอง SSL Certificate ที่ออกโดยหน่วยงานรับรองความปลอดภัยทางอิเล็กทรอนิกส์ของผู้ให้บริการ Certificate Authority (CA)

5.8.2 ผู้ใช้งานที่มีบัญชีผู้ใช้ (Account) ของ สลค. สามารถเข้าใช้งาน Wi-Fi โดยการยืนยันตัวตนผู้ใช้งานด้วยมาตรฐาน IEEE 802.1X บนเครื่องคอมพิวเตอร์ สมาร์ทโฟน และแท็บเล็ตได้

5.9 **เครื่องคอมพิวเตอร์โน้ตบุ๊ก จำนวน 5 เครื่อง** ที่มีคุณลักษณะเฉพาะอย่างน้อย ดังนี้

5.9.1 มีหน่วยประมวลผลกลาง (CPU) ไม่น้อยกว่า 4 แกนหลัก (4 core) และ 8 แกนเสมือน (8 Thread) และมีเทคโนโลยีเพิ่มสัญญาณนาฬิกาได้ในกรณีที่ต้องใช้ความสามารถในการประมวลผลสูง (Turbo Boost หรือ Max Boost) โดยมีความเร็วสัญญาณนาฬิกาสูงสุด ไม่น้อยกว่า 4.10 GHz จำนวน 1 หน่วย

5.9.2 หน่วยประมวลผลกลาง (CPU) มีหน่วยความจำแบบ Cache Memory รวมในระดับ (Level) เดียวกัน ขนาดไม่น้อยกว่า 6 MB

5.9.3 มีหน่วยความจำหลัก (RAM) ชนิด DDR4 หรือดีกว่า ขนาดรวมไม่น้อยกว่า 16 GB

5.9.4 มีหน่วยจัดเก็บข้อมูล Solid State Drive ขนาดความจุไม่น้อยกว่า 500 GB จำนวน 1 หน่วย

5.9.5 มีจอภาพที่รองรับความละเอียดไม่น้อยกว่า 1,920 x 1,080 Pixel และมีขนาดจอภาพระหว่าง 13 - 13.9 นิ้ว

5.9.6 มีช่องเชื่อมต่อ (Interface) แบบ USB 3.0 หรือดีกว่า ไม่น้อยกว่า 2 ช่อง

5.9.7 มีช่องเชื่อมต่อแบบ HDMI จำนวนไม่น้อยกว่า 1 ช่อง

5.9.8 มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10/100/1000 Base-T หรือดีกว่า แบบติดตั้งภายใน (Internal) หรือภายนอก (External) จำนวนไม่น้อยกว่า 1 ช่อง

5.9.9 สามารถใช้งาน Wi-Fi (IEEE 802.11ax) และ Bluetooth ได้เป็นอย่างน้อย

5.9.10 ติดตั้งซอฟต์แวร์ทั้งหมดที่ใช้ในการบริหารจัดการอุปกรณ์ทั้งหมดตามโครงการนี้

6. การฝึกอบรม

ผู้ขายจะต้องจัดการฝึกอบรมให้กับบุคลากรของ สลค. ตามรายละเอียดอย่างน้อย ดังนี้

ลำดับ	รายละเอียดหลักสูตร	จำนวนคน	จำนวนวัน
1	การติดตั้งและการใช้งานระบบรักษาความปลอดภัยระบบเครือข่ายระดับแอปพลิเคชัน (Application Firewall)	3	1
2	การติดตั้งและการใช้งานระบบบริหารจัดการและตอบสนองต่อภัยคุกคามไซเบอร์แบบอัตโนมัติ และระบบป้องกันการโจมตีผ่านช่องโหว่ซอฟท์แวร์สำหรับเครื่องคอมพิวเตอร์ลูกข่าย	3	2
3	การติดตั้งและการใช้งานระบบ VPN	5	1
4	การปฏิบัติตามแนวทางการพัฒนาศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ	3	1
5	การติดตั้งและการใช้งานระบบบริหารจัดการเครือข่ายแบบรวมศูนย์	3	1
6	การติดตั้งและการใช้งานระบบลงทะเบียนเข้าใช้งาน Wi-Fi	5	1

ทั้งนี้ ผู้ขายเป็นผู้รับผิดชอบค่าอาหาร ค่าจัดทำเอกสารคู่มือ ค่าวิทยากร และค่าใช้จ่ายในการฝึกอบรมทั้งหมด

7. งานเอกสาร ...

7. งานเอกสารและคู่มือ

ผู้ขายต้องส่งมอบงานเอกสารและคู่มือต่าง ๆ อย่างน้อย ดังนี้

7.1 เอกสาร System Document ของระบบและอุปกรณ์ตามโครงการทั้งหมด พร้อมอธิบายโดยละเอียดทุกขั้นตอน โดยใช้ภาษาไทยเป็นหลัก ยกเว้นคำศัพท์เฉพาะ

7.2 คู่มือสำหรับผู้ดูแลระบบ โดยจะต้องมีรายละเอียดเกี่ยวกับหัวข้อต่อไปนี้เป็นอย่างน้อย

7.2.1 เอกสารแนวทางการพัฒนาศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

7.2.2 คู่มือการติดตั้งและใช้งานระบบรักษาความมั่นคงปลอดภัย ดังนี้

(1) ระบบรักษาความปลอดภัยระบบเครือข่ายระดับแอปพลิเคชัน (Application Firewall)

(2) ระบบป้องกันการโจมตีผ่านช่องโหว่ซอฟท์แวร์สำหรับเครื่องคอมพิวเตอร์ลูกข่าย

(3) ระบบบริหารจัดการและตอบสนองต่อภัยคุกคามไซเบอร์แบบอัตโนมัติ

(4) ระบบ Multi Factor Authentication ในการยืนยันตัวตนร่วมกับระบบ Azure AD ที่ สลค. มีอยู่ เพื่อการทำ Remote VPN

7.2.3 คู่มือการติดตั้งและใช้งานระบบบริหารจัดการเครือข่ายแบบรวมศูนย์

7.2.4 คู่มือการติดตั้งและใช้งานระบบลงทะเบียนเข้าใช้งาน Wi-Fi

7.2.5 คู่มือการติดตั้งและการกำหนดค่าใบรับรอง SSL Certificate สำหรับใช้งาน Wi-Fi

7.3 คู่มือสำหรับผู้ใช้งาน (Users) โดยจะต้องมีรายละเอียดเกี่ยวกับหัวข้อต่อไปนี้เป็นอย่างน้อย

7.3.1 คู่มือการการยืนยันตัวตนร่วมกับระบบ Azure AD เพื่อการทำ Remote VPN

7.3.2 คู่มือการใช้งานระบบลงทะเบียนเข้าใช้งาน Wi-Fi ดังนี้

(1) คู่มือลงทะเบียนเข้าใช้งาน Wi-Fi ด้วยตนเอง (Self Service) โดยการยืนยันตัวตนผ่าน OTP

(2) คู่มือลงทะเบียนเข้าใช้งาน Wi-Fi ด้วยบัญชีผู้ใช้ (Account) ที่ออกให้โดยผู้ดูแลระบบ

7.3.3 คู่มือการยืนยันตัวตนผู้ใช้งาน Wi-Fi ด้วยมาตรฐาน IEEE 802.1X

8. วิธีการดำเนินงาน

จัดซื้อจัดจ้างโดยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-Bidding)

9. ระยะเวลาดำเนินการ

ผู้ขายจะต้องส่งมอบงานทั้งหมดภายใน 150 วัน นับถัดจากวันที่ลงนามในสัญญา โดยต้องแจ้งกำหนดเวลาส่งมอบงานให้ สลค. ทราบเป็นลายลักษณ์อักษรล่วงหน้าอย่างน้อย 5 วันทำการ ก่อนถึงกำหนดวันส่งมอบงานของแต่ละงวดงาน

10. วงเงินในการจัดหา

วงเงินงบประมาณประจำปี พ.ศ. 2565 จำนวน 47,157,000 บาท (สี่สิบเจ็ดล้านหนึ่งแสนห้าหมื่นเจ็ดพันบาทถ้วน)

ราคากลาง จำนวน 47,106,300 บาท (สี่สิบเจ็ดล้านหนึ่งแสนหกพันสามร้อยบาทถ้วน)

11. การส่งมอบ ...

11. การส่งมอบและการชำระเงิน

สลค. ตกลงจะชำระเงินโดยแบ่งการชำระเป็น 4 งวด ดังนี้

งวดที่ 1 ร้อยละ 5 ภายใน 30 วัน นับถัดจากวันที่ลงนามในสัญญา เมื่อผู้ขายส่งมอบงานตามขอบเขตการดำเนินงาน ข้อ 4.1 รายงานการศึกษา วิเคราะห์ ออกแบบ และวางแผนการติดตั้งและทดสอบระบบและอุปกรณ์ตามโครงการฯ

งวดที่ 2 ร้อยละ 50 ภายใน 90 วัน นับถัดจากวันที่ลงนามในสัญญา เมื่อผู้ขายส่งมอบระบบและอุปกรณ์ตามข้อ 5.1 – 5.4 และ 5.9 โดยยังไม่ต้องดำเนินการติดตั้ง

งวดที่ 3 ร้อยละ 35 ภายใน 120 วัน นับถัดจากวันที่ลงนามในสัญญา เมื่อผู้ขายส่งมอบงานติดตั้งและทดสอบระบบและอุปกรณ์ตามข้อ 5.1 - 5.9 ครบถ้วนสมบูรณ์

งวดที่ 4 ร้อยละ 10 ภายใน 150 วัน นับถัดจากวันที่ลงนามในสัญญา เมื่อผู้ขายดำเนินการจัดฝึกอบรมพร้อมงานเอกสารและคู่มือ และส่งมอบงานที่เหลือทั้งหมดแล้วเสร็จ

12. การรับประกันความชำรุดบกพร่อง

12.1 ผู้ขายต้องรับประกันความชำรุดบกพร่องของระบบและอุปกรณ์ทั้งหมด ดังนี้

12.1.1 ระบบ ซอฟท์แวร์ และอุปกรณ์ที่นำเสนอตามข้อ 5.1 – 5.9 ให้สามารถใช้งานได้เป็นปกติในระยะเวลาการรับประกัน 3 ปี โดยไม่คิดค่าใช้จ่ายใด ๆ เพิ่มเติมทั้งสิ้น นับตั้งแต่วันที่ สลค. ตรวจรับสมบูรณ์ทั้งหมด

12.1.2 คาบเวลาการซ่อมแซมและการบำรุงรักษาระบบ ได้แก่ วันจันทร์ – วันศุกร์ ตั้งแต่เวลา 08.30 – 17.30 น. ให้สามารถใช้งานได้ดีตลอดระยะเวลาการรับประกัน 3 ปี โดยไม่มีค่าใช้จ่ายใด ๆ และให้มีช่างผู้ชำนาญในการให้บริการ Onsite Support ภายในระยะเวลา 4 ชั่วโมงทำการนับตั้งแต่ได้รับแจ้งจาก สลค. และจะต้องดูแลบำรุงรักษาระบบอย่างน้อย 3 เดือนต่อครั้ง

12.2 ผู้ขายต้องดำเนินการแก้ไข/เปลี่ยนแปลงค่าของอุปกรณ์และระบบสารสนเทศที่เสนอตามโครงการนี้ตามคำขอแก้ไข/เปลี่ยนแปลงของ สลค. โดยไม่ชักช้าและไม่คิดค่าใช้จ่ายใด ๆ ทั้งสิ้นตลอดระยะเวลาการรับประกัน 3 ปี

13. เงื่อนไขอื่น ๆ

13.1 ในกรณีที่มีปัญหาหรือข้อสงสัยใด ๆ ในการปฏิบัติตามขอบเขตของงาน (TOR) และเอกสารประกวดราคาอิเล็กทรอนิกส์ (e-Bidding) โครงการปรับปรุงระบบรักษาความมั่นคงปลอดภัยไซเบอร์ ตามประกาศ สลค. ลงวันที่..... ให้ สลค. เป็นผู้วินิจฉัย และคำวินิจฉัยของ สลค. ให้ถือเป็นที่สุด

13.2 ผู้ขายจะต้องทำการศึกษา วิเคราะห์ และออกแบบ รวมถึงพัฒนาระบบให้เป็นไปตามขอบเขตของงานที่กำหนดไว้ แต่หาก สลค. เห็นว่ามีความจำเป็นต้องเพิ่มเติมหรือปรับเปลี่ยนไปจากขอบเขตของงานที่กำหนดไว้เพื่อให้เกิดความเหมาะสมกับการใช้งาน ผู้ขายต้องดำเนินการและไม่คิดค่าใช้จ่ายใด ๆ เพิ่มเติม

13.3 การติดตั้งและการส่งมอบระบบแต่ละงวดงานจะถือว่าเสร็จสมบูรณ์ เมื่อมีการติดตั้งระบบและอุปกรณ์ การฝึกอบรม งานเอกสารและคู่มือ รวมทั้งการทดสอบใช้งานของระบบทั้งหมดแล้วว่า สามารถใช้งานได้เป็นอย่างดีและมีประสิทธิภาพ ทั้งนี้ หากตรวจพบว่าไม่สามารถใช้งานได้ตามความต้องการของ สลค. ผู้ขายจะต้องจัดหาระบบหรืออุปกรณ์ชุดใหม่ หรือจัดหาระบบหรืออุปกรณ์เพิ่มเติม หรือปรับปรุงระบบหรืออุปกรณ์ที่ส่งมอบตามโครงการนี้ ให้สามารถใช้งานได้เป็นอย่างดีและมีประสิทธิภาพ โดยจะไม่คิดค่าใช้จ่ายใด ๆ เพิ่มเติมจาก สลค.

และหาก ...

และหาก สลค. ได้ดำเนินการตรวจรับงานโครงการเป็นที่เรียบร้อยแล้วและพบในภายหลังว่า ระบบหรืออุปกรณ์ที่ส่งมอบตามโครงการนี้มีการทำงานที่ผิดพลาด ผู้ขายจะต้องจัดหาระบบหรืออุปกรณ์ชุดใหม่ให้ สลค. ภายในระยะเวลาไม่เกิน 3 วันทำการและไม่คิดค่าใช้จ่ายใด ๆ ทั้งสิ้น

2.2 ผลิตภัณฑ์ที่เสนอต้องเป็นรุ่นที่ยังอยู่ในสายการผลิต เป็นอุปกรณ์ใหม่ที่ยังไม่เคยติดตั้งใช้งานมาก่อนและไม่เป็นอุปกรณ์ที่ถูกนำมาปรับปรุงสภาพใหม่
