กรมสอบสวนคดีพิเศษ

ร่างขอบเขตของงาน (Terms of Reference : TOR)

โครงการจัดหาอุปกรณ์รักษาความปลอดภัยระบบเครือข่าย กรมสอบสวนคดีพิเศษ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร จำนวน ๑ โครงการ ปีงบประมาณ พ.ศ. ๒๕๖๙

---

๑. ความเป็นมา

ด้วยสภาวะการณ์ปัจจุบันที่ภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ทวีความรุนแรง แผ่ขยายเป็นวงกว้างมากขึ้นและส่งผลกระทบต่อความสงบเรียบร้อยทางสังคมและความมั่นคงทางเศรษฐกิจของประเทศ โดยเฉพาะหน่วยงานที่มีความสำคัญต่อความมั่นคงและการอำนวยความยุติธรรมให้แก่ประชาชน จึงมีความเสี่ยงต่อภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์อย่างมาก ดังนั้นการเตรียมความพร้อมในการับมืออาชญากรรมไซเบอร์ จึงมีความสำคัญยิ่งสำหรับหน่วยงานและองค์กรภายใต้กระทรวงยุติธรรม รวมทั้งหน่วยงานรัฐ โดยเฉพาะอย่างยิ่งหน่วยงานโครงสร้างพื้นฐานสำคัญทางด้านความมั่นคงของรัฐ ซึ่งหากเกิดการโจมตีไซเบอร์ขึ้น อาจส่งผลกระทบต่อการอำนวยความยุติธรรมให้แก่ประชาชน หรือสร้างความเสียหายต่อความสงบเรียบร้อยของประเทศได้

ทั้งนี้กรมสอบสวนคดีพิเศษเป็นหน่วยงานภายใต้สังกัดกระทรวงยุติธรรม มีภารกิจในการอำนวยความยุติธรรมให้แก่ประชาชนและเป็นหน่วยงานด้านความมั่นคงของรัฐ จึงมีความจำเป็นต้องเฝ้าระวัง ป้องกัน ตรวจจับ และตอบโต้ต่อภัยคุกคามที่อาจจะเกิดขึ้นกับระบบสารสนเทศของกรมฯ รวมถึงการจัดการช่องโหว่ ตรวจสอบ และประมวลผลหลังเกิดเหตุ เพื่อเป็นแนวทางสำหรับการป้องกันระบบสารสนเทศ จึงได้จัดหาอุปกรณ์รักษาความปลอดภัยและป้องกันการบุกรุกทางไซเบอร์ของกรมสอบสวนคดีพิเศษ เพื่อให้สามารถติดตาม เฝ้าระวัง ตรวจสอบ วิเคราะห์สถานการณ์ด้านภัยคุกคามทางไซเบอร์ที่อาจจะเกิดขึ้น เพื่อไม่ให้เกิดผลกระทบต่อการให้บริการประชาชน

๒. วัตถุประสงค์

๒.๑ เพื่อจัดหาอุปกรณ์รักษาความปลอดภัยและป้องกันการบุกรุกทางไซเบอร์ที่ทันสมัยและมีประสิทธิภาพ สำหรับการป้องกันภัยคุกคามไซเบอร์ต่อระบบสารสนเทศของกรมสอบสวนคดีพิเศษ

๒.๒ เพื่อให้ระบบสารสนเทศสามารถพัฒนาและให้บริการประชาชนได้อย่างต่อเนื่องและมีประสิทธิภาพ

๓. คุณสมบัติของผู้ยื่นข้อเสนอ

๓.๑ มีความสามารถตามกฎหมาย

๓.๒ ไม่เป็นบุคคลล้มละลาย

๓.๓ ไม่อยู่ระหว่างเลิกกิจการ

๓.๔ ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

๓.๕ ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในภารกิจของนิติบุคคลนั้นด้วย

๓.๖ มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

๓.๗...

๓.๗ เป็นบุคคลธรรมดา หรือนิติบุคคลผู้มีอาชีพขาย หรือรับจ้างทำพัสดุที่ส่วนราชการจะซื้อหรือจ้างครั้งนี้

๓.๘ ไม่เป็นผู้ได้รับเอกสิทธิ์ หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทยเว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละสิทธิ์ และความคุ้มกันเช่นว่านั้น

๓.๙ ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่กรมสอบสวนคดีพิเศษ ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรม ในการเสนอราคาครั้งนี้

๓.๑๐ ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ "กิจการร่วมค้า" ต้องมีคุณสมบัติดังนี้
กิจการร่วมค้าที่ยื่นข้อเสนอ ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ ในเอกสารเชิญชวน เว้นแต่ในกรณีกิจการร่วมค้าที่มีข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใด รายหนึ่งเป็นผู้เข้าร่วมค้าหลัก กิจการร่วมค้านั้นสามารถใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นก่อสร้าง ของกิจการร่วมค้าที่ยื่นข้อเสนอ

กรณีมีข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงดังกล่าวจะต้องมีการกำหนดสัดส่วนหน้าที่ และความรับผิดชอบในปริมาณงาน สิ่งของหรือมูลค่าตามสัญญา มากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

๓.๑๑ ผู้ยื่นข้อเสนอต้องลงทะเบียนที่มีข้อมูลถูกต้องครบถ้วนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement : e-GP) ของกรมบัญชีกลาง

๓.๑๒ ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ ดังนี้

(๑) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยซึ่งได้จดทะเบียนเกินกว่า ๑ ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก ๑ ปีสุดท้ายก่อนวันยื่นข้อเสนอ

(๒) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ให้พิจารณาการกำหนดมูลค่าของทุนจดทะเบียน โดยผู้ยื่นข้อเสนอจะต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอ ดังนี้

(๒.๑) มูลค่าการจัดซื้อจัดจ้างไม่เกิน ๑ ล้านบาท ไม่ต้องกำหนดทุนจดทะเบียน

(๒.๒) มูลค่าการจัดซื้อจัดจ้างเกิน ๑ ล้านบาท แต่ไม่เกิน ๕ ล้านบาท ต้องระบุต้องมีทุนจดทะเบียนไม่ต่ำกว่า ๑ ล้านบาท

(๒.๓) มูลค่าการจัดซื้อจัดจ้างเกิน ๕ ล้านบาท แต่ไม่เกิน ๑๐ ล้านบาท ต้องระบุต้องมีทุนจดทะเบียนไม่ต่ำกว่า ๒ ล้านบาท

(๒.๔) มูลค่าการจัดซื้อจัดจ้างเกิน ๑๐ ล้านบาท แต่ไม่เกิน ๒๐ ล้านบาท ต้องระบุต้องมีทุนจดทะเบียนไม่ต่ำกว่า ๓ ล้านบาท

(๒.๕) มูลค่าการจัดซื้อจัดจ้างเกิน ๒๐ ล้านบาท แต่ไม่เกิน ๖๐ ล้านบาท ต้องระบุต้องมีทุนจดทะเบียนไม่ต่ำกว่า ๘ ล้านบาท

(๒.๖) มูลค่าการจัดซื้อจัดจ้างเกิน ๖๐ ล้านบาท แต่ไม่เกิน ๑๕๐ ล้านบาทต้องระบุต้องมีทุนจดทะเบียนไม่ต่ำกว่า ๒๐ ล้านบาท

(๒.๗) มูลค่าการจัดซื้อจัดจ้างเกิน ๑๕๐ ล้านบาท แต่ไม่เกิน ๓๐๐ ล้านบาท ต้องระบุต้องมีทุนจดทะเบียนไม่ต่ำกว่า ๖๐ ล้านบาท

(๒.๘)...

(๒.๘) มูลค่าการจัดซื้อจัดจ้างเกิน ๓๐๐ ล้านบาท แต่ไม่เกิน ๕๐๐ ล้านบาท ต้องระบุต้องมีทุนจดทะเบียนไม่ต่ำกว่า ๑๐๐ ล้านบาท

(๒.๙) มูลค่าการจัดซื้อจัดจ้างเกิน ๕๐๐ ล้านบาทขึ้นไป ต้องระบุ ต้องมีทุนจดทะเบียนไม่ต่ำกว่า ๒๐๐ ล้านบาท

(๓) สำหรับการจัดซื้อจัดจ้างครั้งหนึ่งที่มีวงเงินเกิน ๕๐๐,๐๐๐ บาทขึ้นไป กรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดา โดยพิจารณาจากบัญชีเงินฝากธนาคาร ณ วันยื่นข้อเสนอ โดยต้องมีเงินฝากคงเหลือในบัญชีธนาคารเป็นมูลค่า ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง และหากเป็นผู้ชนะการจัดซื้อจัดจ้างหรือเป็นผู้ได้รับการคัดเลือกจะต้องแสดงหนังสือรับรองบัญชีเงินฝากที่มีมูลค่าดังกล่าวอีกครั้งหนึ่ง ในวันลงนามในสัญญา

(๔) กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอที่จะเข้า ยื่นข้อเสนอ ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ ๑ ใน ๔ ของมูลค่างบประมาณ ของโครงการหรือรายการที่ยื่นข้อเสนอในครั้งนั้น (สินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์ และประกอบธุรกิจค้าประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยจะพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรองหรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ (นับถึงวันยื่นข้อเสนอไม่เกิน ๙๐ วัน)

(๕) กรณีตาม (๑) - (๔) ยกเว้นสำหรับกรณีดังต่อไปนี้

(๕.๑) กรณีผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐ

(๕.๒) นิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการตามพระราชบัญญัติล้มละลาย (ฉบับที่ ๑๐) พ.ศ. ๒๕๖๑

๓.๑๓ ผู้ยื่นข้อเสนอต้องได้รับการแต่งตั้งให้เป็นตัวแทนจำหน่ายจากผู้ผลิตหรือตัวแทนจำหน่ายในประเทศไทย โดยให้ยื่นขณะเข้าเสนอราคา

๓.๑๔ ผู้ยื่นข้อเสนอจะต้องมีผลงานเกี่ยวกับงานระบบรักษาความปลอดภัยเครือข่าย หรือระบบเครือข่ายคอมพิวเตอร์ หรือระบบเครือข่ายสารสนเทศ หรืองานติดตั้งระบบรักษาความปลอดภัยเครือข่าย หรืองานติดตั้งระบบเครือข่ายสารสนเทศ หรืองานติดตั้งเครือข่ายคอมพิวเตอร์ ในวงเงินไม่น้อยกว่า ๑๕,๐๐๐,๐๐๐ บาท และเป็นสัญญาที่ดำเนินการแล้วเสร็จ ตามสัญญา จำนวนอย่างน้อย ๑ สัญญา พร้อมร่างขอบเขตของงาน (TOR) ซึ่งได้มีการส่งมอบงานและตรวจรับงวดสุดท้ายเรียบร้อยแล้ว โดยเป็นผลงานของผู้ยื่นข้อเสนอโดยตรงที่ทำสัญญากับส่วนราชการ หรือรัฐวิสาหกิจ หรือองค์กรภาครัฐ หรือเอกชนภายในประเทศที่ตรวจสอบได้ โดยผู้ยื่นข้อเสนอต้องแสดงหนังสือรับรองผลงาน โดยให้ยื่นขณะเข้าเสนอราคา

๓.๑๕ ผู้ยื่นข้อเสนอต้องจัดทำเอกสารตารางเปรียบเทียบร่างขอบเขตของงาน **<u>รายละเอียดตามข้อกำหนดทุกข้อ</u>** ที่กรมสอบสวนคดีพิเศษ กำหนด กับรายละเอียดที่ผู้เสนอราคา เสนอตามตัวอย่างข้างล่าง โดยระบุเอกสารอ้างอิง แค็ตตาล็อก ให้ถูกต้องถ้ามีรายละเอียดใดที่แตกต่างจากข้อกำหนดจะต้องอธิบายพร้อมทั้งเปรียบเทียบข้อดีข้อเสีย ให้เข้าใจชัดเจน โดยให้ยื่นขณะเข้าเสนอราคา

ตัวอย่าง...

ตัวอย่างตารางเปรียบเทียบ

ร่างขอบเขตของงานที่ กรมสอบสวนคดีพิเศษกำหนด	ร่างขอบเขตของงาน ที่ผู้ยื่นข้อเสนอ เสนอ	การเปรียบเทียบ (สูงกว่า/เทียบเท่า)	เอกสารอ้างอิง (แค็ตตาล็อก/อื่นๆ)
๑. ..... ๒.			

๔. รายการและจำนวนพัสดุตามโครงการประกอบด้วย

๔.๑ อุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall) จำนวนไม่น้อยกว่า ๒ ชุด

๔.๒ ระบบบันทึกและตรวจสอบสิทธิการเข้าถึงระบบสารสนเทศและอุปกรณ์เครือข่าย (Privileged Access Management) จำนวนไม่น้อยกว่า ๑ ระบบ

๔.๓ ซอฟต์แวร์ความปลอดภัยของอุปกรณ์ปลายทาง และการเข้าถึงเครือข่าย แบบ Zero Trust จำนวนไม่น้อยกว่า ๑ ระบบ

๔.๔ ระบบวิเคราะห์และป้องกันภัยไซเบอร์แบบ XDR Security Platform จำนวนไม่น้อยกว่า ๑ ระบบ

๕. รายละเอียดคุณลักษณะเฉพาะของพัสดุ

ตามรายละเอียดคุณลักษณะเฉพาะ ภาคผนวก ๑

๖. กำหนดเวลาส่งมอบพัสดุ

ผู้ยื่นข้อเสนอต้องส่งมอบพัสดุตามสัญญาฯ จำนวน ๒ งวด (ภายใน ๑๘๐ วัน) รายละเอียด ดังนี้

๖.๑ งวดที่ ๑ เข้ามาดำเนินการสำรวจพื้นที่, ส่งมอบแผนการปฏิบัติงาน, แผนผังการติดตั้งอุปกรณ์และระบบทั้งหมด และส่งมอบอุปกรณ์พร้อมติดตั้งอุปกรณ์หรือระบบทั้งหมดตามสัญญา ภายใน ๑๕๐ วันนับถัดจากวันที่ลงนามในสัญญา

๖.๒ งวดที่ ๒ ทดสอบระบบการทำงาน และจัดฝึกอบรมการใช้งาน ภายใน ๑๘๐ วันนับถัดจากวันที่ลงนามในสัญญา

๗. หลักเกณฑ์การพิจารณาข้อเสนอ

ในการพิจารณาผลการยื่นข้อเสนอครั้งนี้ กรมสอบสวนคดีพิเศษจะพิจารณาตัดสินโดยใช้หลักเกณฑ์ราคา โดยหน่วยงานจะพิจารณาคัดเลือกผู้ยื่นข้อเสนอที่มีคุณสมบัติถูกต้อง ครบถ้วน และเป็นประโยชน์ต่อหน่วยงาน

๘. วงเงินงบประมาณ/วงเงินที่ได้รับจัดสรร

เป็นเงินทั้งสิ้น ๔๔,๕๐๐,๐๐๐.๐๐ บาท ราคารวมภาษีมูลค่าเพิ่มและค่าใช้จ่ายทั้งปวงแล้ว

๙. งวดงานและการจ่ายเงิน

กรมสอบสวนคดีพิเศษ จะจ่ายเงินเป็นรายงวด ดังนี้

งวดที่ ๑ ส่งมอบภายใน ๑๕๐ วัน นับถัดจากวันลงนามในสัญญา ชำระเงินร้อยละ ๔๐ เมื่อผู้ชนะการประกวดราคาฯ ดำเนินการตามข้อ ๖.๑ และคณะกรรมการตรวจรับฯ พิจารณาเห็นชอบให้รับไว้ใช้ในราชการ

งวดที่ ๒ ส่งมอบภายใน ๑๘๐ วัน นับถัดจากวันลงนามในสัญญา ชำระเงินร้อยละ ๖๐ เมื่อผู้ชนะการประกวดราคาฯ ดำเนินการตามข้อ ๖.๒ และจัดฝึกอบรมการใช้งานพร้อมจัดส่งคู่มือการปฏิบัติงาน จำนวนไม่น้อยกว่า ๕ ชุด ในรูปแบบรูปเล่มเอกสารและรูปแบบไฟล์ PDF รวมทั้งเอกสารอื่น ๆ ที่เกี่ยวข้อง เสนอให้

คณะ...

คณะกรรมการตรวจรับฯ พิจารณาเห็นชอบให้รับไว้ใช้ในราชการ และต้องดำเนินการให้แล้วเสร็จภายในวันสุดท้ายของงวดงานนั้น หากวันสุดท้ายของงวดงานตรงกับวันหยุดราชการให้สามารถส่งมอบงานในวันทำการถัดไปได้ให้คณะกรรมการตรวจรับฯ พิจารณาเห็นชอบให้รับไว้ใช้ในราชการ พร้อมติดตั้งอุปกรณ์ทั้งหมดและทดสอบการทำงาน

๑๐. อัตราค่าปรับ

ในกรณีที่ผู้ขายไม่สามารถส่งมอบพัสดุภายในกำหนดระยะเวลา ผู้ขายจะต้องชำระค่าปรับให้ผู้ซื้อเป็นรายวันในอัตราร้อยละ ๐.๒๐ ของราคาสิ่งของที่ยังไม่ได้รับมอบ นับถัดจากวันครบกำหนดตามสัญญาจนถึงวันที่ผู้ขายได้นำสิ่งของมาส่งมอบให้แก่ผู้ซื้อจนถูกต้องครบถ้วนตามสัญญา

๑๑. การกำหนดระยะเวลารับประกันความชำรุดบกพร่อง

ผู้เสนอราคาต้องรับประกันความชำรุดบกพร่องหรือขัดข้องของอุปกรณ์รักษาความปลอดภัยระบบเครือข่าย และการติดตั้ง ซึ่งรวมค่าอะไหล่และค่าแรงแบบ (On-site Service) และ Remote Support โดยอะไหล่ต้องเป็นของใหม่ที่ไม่เคยใช้งานมาก่อน เป็นเวลา ๓ ปี หรือตามข้อกำหนดในสัญญา นับถัดจากวันที่กรมสอบสวนคดีพิเศษได้รับมอบอุปกรณ์รักษาความปลอดภัยระบบเครือข่ายทั้งหมด โดยถูกต้องครบถ้วนตามสัญญาและคณะกรรมการตรวจรับ ได้ตรวจรับพัสดุไว้ใช้ในราชการแล้ว ถ้าภายในระยะเวลาดังกล่าวอุปกรณ์รักษาความปลอดภัยระบบเครือข่าย ชำรุดบกพร่องหรือขัดข้อง หรือใช้งานไม่ได้ทั้งหมดหรือแต่บางส่วน หรือเกิดความชำรุดบกพร่องหรือขัดข้องจากการติดตั้ง เว้นแต่ความชำรุดบกพร่องหรือขัดข้องดังกล่าวเกิดขึ้นจากความผิดของกรมสอบสวนคดีพิเศษ ซึ่งไม่ได้เกิดขึ้นจากการใช้งานตามปกติ ผู้เสนอราคาจะต้องจัดการซ่อมแซมแก้ไขให้อยู่ในสภาพใช้การได้ดีดังเดิม โดยต้องเริ่มจัดการซ่อมแซมภายใน ๗ วัน นับจากวันที่ได้รับแจ้งปัญหา โดยไม่คิดค่าใช้จ่ายใด ๆ ทั้งสิ้น หากไม่สามารถแก้ปัญหาให้เสร็จได้ทันตามกำหนดผู้เสนอราคาต้องจัดหาอุปกรณ์ที่มีคุณลักษณะเดียวกันหรือดีกว่ามาสำรองใช้งานไปพลางก่อน จนกว่าจะแก้ไขแล้วเสร็จ ทั้งนี้หากอุปกรณ์ที่ชำรุด ไม่สามารถซ่อมแซมแก้ไขได้ ผู้เสนอราคาต้องจัดหาอุปกรณ์ใหม่ที่มีคุณลักษณะเทียบเท่าหรือดีกว่า และไม่เคยผ่านการใช้งานมาก่อนส่งมอบให้กรมสอบสวนคดีพิเศษแทน หากผู้ขายไม่จัดการซ่อมแซมหรือแก้ไขภายในกำหนดเวลาดังกล่าว ผู้ซื้อมีสิทธิที่จะทำการนั้นเองหรือจ้างผู้อื่นให้ทำการแทนผู้ขาย โดยผู้ขายต้องเป็นผู้ออกค่าใช้จ่ายเองทั้งสิ้น

ผู้เสนอราคาต้องแก้ไขปัญหาเมื่อเกิดปัญหาความปลอดภัยระบบเครือข่าย โดยต้องจัดหาเจ้าหน้าที่ ที่มีความรู้ความสามารถ เข้ามาทำการตรวจสอบ วิเคราะห์ และแก้ไขปัญหา โดยเข้ามา ณ สถานที่ของกรมสอบสวนคดีพิเศษ ภายใน ๔ ชั่วโมง ตลอดระยะเวลาการรับประกัน และดำเนินการแก้ไขให้ระบบเครือข่ายของกรมสอบสวนคดีพิเศษ กลับมาใช้งานได้เบื้องต้น (สามารถใช้งานระบบเครือข่ายภายในและเครือข่ายอินเทอร์เน็ต) ได้ ภายใน ๒๔ ชั่วโมง และประสานงานร่วมกับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เพื่อดำเนินการจัดทำรายงานสรุปสาเหตุของปัญหาที่เกิดขึ้นและข้อเสนอแนะ ภายใน ๗ วัน

ผู้เสนอราคามีหน้าที่บำรุงรักษาและซ่อมแซมแก้ไขอุปกรณ์รักษาความปลอดภัยระบบเครือข่ายให้อยู่ในสภาพใช้งานได้ดีอยู่เสมอตลอดระยะเวลาดังกล่าวในวรรคหนึ่ง ด้วยค่าใช้จ่ายของผู้เสนอราคา

๑๒. หลักเกณฑ์การพิจารณาอื่น ๆ

(๑) หากผู้ยื่นข้อเสนอซึ่งเป็นผู้ประกอบการ SMEs เสนอราคาสูงกว่าราคาต่ำสุดของผู้ยื่นข้อเสนอรายอื่นไม่เกินร้อยละ ๑๐ กรมจะจัดซื้อจากผู้ประกอบการ SMEs ดังกล่าว โดยจัดเรียงลำดับผู้ยื่นข้อเสนอซึ่งเป็นผู้ประกอบการ SMEs ซึ่งเสนอราคาสูงกว่าราคาต่ำสุดของผู้ยื่นข้อเสนอรายอื่นไม่เกินร้อยละ ๑๐ ที่จะเรียกมาทำสัญญาไม่เกิน ๓ ราย

ผู้...

ผู้ยื่นข้อเสนอที่เป็นกิจการร่วมค้าที่จะได้สิทธิตามวรรคหนึ่ง ผู้เข้าร่วมค้าทุกรายจะต้องเป็นผู้ประกอบการ SMEs

ทั้งนี้ ผู้ประกอบการ SMEs ที่จะได้แต้มต่อด้านราคาตามวรรคหนึ่ง จะต้องมีวงเงินสัญญาสะสมตามปีปฏิทินรวมกับราคาที่เสนอในครั้งนี้แล้ว มีมูลค่ารวมกันไม่เกินมูลค่าของรายได้ตามขนาดที่ขึ้นทะเบียนไว้กับสำนักงานส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม (สสว.)

(๒) หากผู้ยื่นข้อเสนอได้เสนอพัสดุที่ได้รับการรับรองและออกเครื่องหมายสินค้าที่ผลิตภายในประเทศ (Made in Thailand) จากสภาอุตสาหกรรมแห่งประเทศไทย เสนอราคาสูงกว่าราคาต่ำสุดของผู้ยื่นข้อเสนอรายอื่นไม่เกินร้อยละ ๕ กรมจะพิจารณาจัดซื้อจัดจ้างจากผู้ยื่นข้อเสนอที่เสนอพัสดุที่เป็นพัสดุที่ผลิตภายในประเทศที่ได้รับการรับรองและออกเครื่องหมายสินค้าที่ผลิตภายในประเทศไทย (Made in Thailand) จากสภาอุตสาหกรรมแห่งประเทศไทย

สำหรับการประกวดราคาอิเล็กทรอนิกส์ ที่มีการเสนอราคาหลายรายการและกำหนดเงื่อนไขเป็นกรณีการพิจารณาราคารวม หากผู้ยื่นข้อเสนอได้เสนอพัสดุที่เป็นพัสดุที่ผลิตภายในประเทศ ที่ได้รับการรับรองและออกเครื่องหมายสินค้าที่ผลิตภายในประเทศไทยฯ มีสัดส่วนมูลค่าตั้งแต่ร้อยละ ๖๐ ขึ้นไปให้ได้แต้มต่อในการเสนอราคาตามวรรคหนึ่ง

อนึ่ง หากในการเสนอราคาครั้งนั้น ผู้ยื่นข้อเสนอรายใดมีคุณสมบัติทั้ง (๑) และ (๒) ให้ผู้ยื่นข้อเสนอรายนั้นได้แต้มต่อในการเสนอราคาสูงกว่าผู้ประกอบการรายอื่นไม่เกินร้อยละ ๑๕

(๓) หากผู้ยื่นข้อเสนอซึ่งมิใช่ผู้ประกอบการ SMEs แต่เป็นบุคคลธรรมดาที่ถือสัญชาติไทยหรือนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยเสนอราคาสูงกว่าราคาต่ำสุดของผู้ยื่นข้อเสนอซึ่งเป็นบุคคลธรรมดาที่มิได้ถือสัญชาติไทยหรือนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายของต่างประเทศไม่เกินร้อยละ ๓ ให้จัดซื้อหรือจัดจ้างจากผู้ยื่นข้อเสนอซึ่งเป็นบุคคลธรรมที่ถือสัญชาติหรือนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย

(๔) คู่สัญญาต้องจัดทำแผนการทำงานมาให้ภายใน ๖๐ วัน นับถัดจากวันลงนามในสัญญา เว้นแต่เป็นกรณีการเช่า หรือกรณีสัญญามีอายุไม่เกิน ๙๐ วัน หรือกรณีการซื้อซึ่งสัญญากำหนดส่งงานงวดเดียว หรือกรณีการซื้อ การเช่า การจ้าง และการจ้างก่อสร้างซึ่งสัญญาหรือบันทึกข้อตกลงเป็นหนังสือมีวงเงินไม่เกิน ๕๐๐,๐๐๐ บาท

ทั้งนี้ แผนการทำงานดังกล่าวให้ถือเป็นเอกสารส่วนหนึ่งของสัญญา

๑๓. ข้อกำหนดอื่น ๆ

๑๓.๑ ผู้เสนอราคาจะต้องเข้ามาดำเนินการสำรวจพื้นที่ และส่งมอบแผนการปฏิบัติงาน และแผนผังการติดตั้งอุปกรณ์และระบบทั้งหมดภายใน ๖๐ วันนับจากวันลงนามในสัญญา และจะต้องได้รับความเห็นชอบจากคณะกรรมการตรวจรับฯ ก่อนเริ่มดำเนินการติดตั้ง

๑๓.๒ ผู้เสนอราคาต้องติดตั้ง และกำหนดค่าการใช้งานต่าง ๆ (Configuration) ที่จัดซื้อในโครงการทั้งหมด ตามแบบการติดตั้ง หรือตามที่กรมสอบสวนคดีพิเศษกำหนด หรือตามความเหมาะสมของสถานที่ให้ระบบสามารถทำงานร่วมกันได้อย่างมีประสิทธิภาพ

๑๓.๓ ผู้เสนอราคาจะต้องจัดทำหรือติดตั้งระบบเฝ้าระวังและตอบสนองต่อภัยคุกคามทางไซเบอร์ (Extended Detection and Response) เพื่อรวบรวมและแสดงเหตุการณ์ ความเสี่ยง แสดงในรูปแบบ Dashboard สำหรับป้องกันและตรวจจับภัยคุกคามในระดับเครื่องผู้ใช้งาน (Client) และเครื่องแม่ข่าย (Server) ในโครงการให้อยู่ในระบบเดียวกัน (Single Console) ได้

๑๓.๔...

๑๓.๔ ผู้เสนอราคาจะต้องจัดทำหรือติดตั้งระบบซอฟต์แวร์ความปลอดภัยของอุปกรณ์ปลายทางและการเข้าถึงเครือข่าย แบบ Zero Trust สำหรับเครื่องลูกข่าย, เครื่องแม่ข่าย และเว็บแอปพลิเคชัน เพื่อรวบรวมและใช้งานในลักษณะการเชื่อมต่อระยะไกล (VPN) แสดงในรูปแบบ Dashboard สำหรับการเข้าถึงและใช้งานอุปกรณ์ต่าง ๆ ในระดับเครื่องผู้ใช้งาน (Client) หรือเครื่องแม่ข่าย (Server) โดยระบบดังกล่าวในโครงการให้อยู่ในระบบเดียวกัน (Single Console) ได้

๑๓.๕ ในกรณีที่ผลิตภัณฑ์ที่เสนอ ต้องใช้อุปกรณ์หรือระบบหรือซอฟต์แวร์อื่น ๆ เพิ่มเติมเพื่อให้สามารถทำงานได้ตามคุณลักษณะเฉพาะที่กำหนด ผู้เสนอราคาต้องเป็นผู้จัดหาและรับผิดชอบค่าใช้จ่ายที่เกิดขึ้นทั้งหมด

๑๓.๖ ผู้เสนอราคาต้องปรับปรุงและติดตั้งอุปกรณ์และระบบและสายสัญญาณต่าง ๆ หรืออื่น ๆ (ถ้ามี) ให้เป็นระเบียบเรียบร้อย

๑๓.๗ ต้นทางและปลายสายสัญญาณระบบทุกเส้นจะต้องติดเครื่องหมาย หรือสัญลักษณ์ สำหรับการตรวจสอบทุกจุด (ถ้ามี)

๑๓.๘ ผู้เสนอราคาต้องทำให้อุปกรณ์และระบบที่จัดซื้อในโครงการนี้สามารถใช้งานได้

๑๓.๙ ผู้เสนอราคาต้องแจ้งรายชื่อเจ้าหน้าที่ที่เป็นผู้รับผิดชอบและประสานงานโครงการให้ชัดเจนตลอดอายุสัญญาจนสิ้นระยะเวลาการรับประกัน ทั้งนี้หากมีการเปลี่ยนแปลงผู้รับผิดชอบและประสานงานต้องแจ้งให้กรมสอบสวนคดีพิเศษทราบภายใน ๗ วัน

๑๓.๑๐ การกระทำใด ๆ อันจะก่อให้เกิดความเสียหายต่อระบบของกรมสอบสวนคดีพิเศษ จะต้องแจ้งและได้รับอนุญาตจากเจ้าหน้าที่ผู้รับผิดชอบของกรมสอบสวนคดีพิเศษก่อน

๑๓.๑๑ ผลเสียหายที่เกิดขึ้นจากการกระทำใด ๆ ของผู้เสนอราคา ผู้เสนอราคาต้องรับผิดชอบการกระทำนั้น ๆ ทั้งหมด

๑๓.๑๒ ผู้เสนอราคาจะต้องจัดทำป้ายสติ๊กเกอร์ที่มีความคงทน ไม่หลุดลอกง่าย ติดบนอุปกรณ์ในโครงการทุกเครื่อง โดยจะต้องมีข้อมูลดังต่อไปนี้เป็นอย่างน้อย ได้แก่ หมายเลขประจำเครื่อง (Serial No.) ชื่อบริษัทผู้ชนะการเสนอราคา เลขที่สัญญา ระยะเวลาสิ้นสุดการรับประกันตามสัญญาโดยประมาณ หมายเลขโทรศัพท์ติดต่อกรณีเครื่องชำรุด เป็นอย่างน้อย โดยแนบมาพร้อมวันส่งมอบ

๑๓.๑๓ ผู้เสนอราคาจะต้องส่งมอบรายละเอียดรายการอุปกรณ์ทั้งหมด โดยจะต้องมีข้อมูลดังต่อไปนี้เป็นอย่างน้อย ได้แก่ ๑.ลำดับ ๒.ยี่ห้อ ๓.รุ่น ๔.บริษัทผู้ผลิต ๕.หมายเลขประจำเครื่อง (Serial No.) ฯลฯ (ข้อมูลตามที่มีจริง) โดยส่งมอบเป็น ไฟล์ Excel และไฟล์ PDF และเอกสาร ในวันส่งมอบ

๑๔. การฝึกอบรมและคู่มือการใช้งาน

๑๔.๑ ผู้เสนอราคาต้องจัดฝึกอบรมให้เจ้าหน้าที่ผู้ดูแลระบบของกรมสอบสวนคดีพิเศษ จำนวนไม่น้อยกว่า ๓ คน เป็นระยะเวลาไม่น้อยกว่า ๘ ชั่วโมง โดยมีเนื้อหาครอบคลุมถึงการบริหารจัดการและการใช้งานอุปกรณ์และระบบทั้งหมดที่ส่งมอบให้กับกรมสอบสวนคดีพิเศษ รวมทั้งการดูแลบำรุงรักษาอุปกรณ์และระบบได้อย่างมีประสิทธิภาพ และรับผิดชอบค่าใช้จ่ายในการฝึกอบรมทั้งหมด

๑๔.๒ ผู้เสนอราคาต้องส่งมอบคู่มือการใช้งานอุปกรณ์และระบบที่เสนอทั้งหมด จำนวนไม่น้อยกว่า ๕ ชุด ในรูปแบบรูปเล่มเอกสาร และรูปแบบไฟล์ PDF ให้กับกรมสอบสวนคดีพิเศษในวันที่ส่งมอบ

๑๕. ลิขสิทธิ์โปรแกรม

๑๕.๑ ผู้เสนอราคาต้องส่งมอบลิขสิทธิ์การใช้งานโปรแกรมหรือซอฟต์แวร์หรือระบบที่จัดซื้อในโครงการนี้ทั้งหมด ให้เป็นลิขสิทธิ์การใช้งานของกรมสอบสวนคดีพิเศษ

๑๕.๒...

๑๕.๒ ในกรณีที่บุคคลภายนอกกล่าวอ้าง หรือใช้สิทธิเรียกร้องใด ๆ ว่ามีการละเมิดลิขสิทธิ์ หรือสิทธิบัตรเกี่ยวกับอุปกรณ์รักษาความปลอดภัยระบบเครือข่าย ตามสัญญานี้ โดยผู้ซื้อไม่ได้แก้ไขดัดแปลงไปจากเดิม ผู้ขายจะต้องดำเนินการทั้งปวง เพื่อให้การกล่าวอ้าง หรือเรียกร้องดังกล่าวระงับสิ้นไปโดยเร็ว หากผู้ขายมิอาจกระทำได้และผู้ซื้อต้องรับผิด ชดใช้ค่าเสียหายต่อบุคคลภายนอกเนื่องจากผลแห่งการละเมิดลิขสิทธิ์หรือสิทธิบัตรดังกล่าว ผู้ขายต้องชำระค่าเสียหายและค่าใช้จ่าย รวมทั้งค่าฤชาธรรมเนียม และค่าทนายความแทนผู้ซื้อ ทั้งนี้ผู้ซื้อจะแจ้งผู้ขายให้ทราบเป็นลายลักษณ์อักษรในการกล่าวอ้างหรือเรียกร้องดังกล่าว

๑๖. การรักษาความลับว่าด้วยกฎหมายคุ้มครองข้อมูลส่วนบุคคล

ผู้รับจ้างจะไม่นำออกไปซึ่งข้อมูลหรือข้อความอื่นใด ๆ ที่เกี่ยวเนื่องกับขอบเขตงานตามสัญญา ไม่ว่าจะอยู่ในรูปแบบใด ซึ่งผู้รับจ้างได้รับจากการดำเนินการตามสัญญานี้ทั้งหมดหรือบางส่วน และจะต้องไม่เปิดเผยให้ผู้อื่นทราบถึงข้อมูลหรือเทคนิคที่ใช้ในการดำเนินการเกี่ยวกับขอบเขตงานตามสัญญานี้ เว้นแต่จะได้รับความยินยอมเป็นหนังสือจากกรมสอบสวนคดีพิเศษ ในกรณีที่สัญญาสิ้นสุดหรือมีการบอกเลิกสัญญา ผู้รับจ้างต้องทำลายข้อมูลต่าง ๆ ซึ่งผู้รับจ้างได้รับจากกรมสอบสวนคดีพิเศษในการดำเนินการตามสัญญานี้ โดยสิ้นเชิงภายใน ๗ (เจ็ด) วัน นับแต่วันที่สัญญาสิ้นสุดหรือบอกเลิกสัญญา

คณะกรรมการกำหนดร่างขอบเขตของงาน ตามคำสั่งกรมสอบสวนคดีพิเศษ ที่ ๔๘/๒๕๖๙ ลงวันที่ ๒๐ มกราคม พ.ศ. ๒๕๖๙

(นายนิติภัทร แสงพัฒน์)
พนักงานสอบสวนคดีพิเศษชำนาญการพิเศษ
ประธานคณะกรรมการกำหนดร่างขอบเขตของงานและกำหนดราคากลาง

(นายพงศ์บัณฑิต ชัยชาญ)
เจ้าหน้าที่คดีพิเศษชำนาญการ
กรรมการ

(นางสาวกานทิพย์ โพธิ์อ่อน)
เจ้าหน้าที่คดีพิเศษชำนาญการ
กรรมการ

(นายธัมมจิต รุจนวงศ์)
เจ้าหน้าที่คดีพิเศษชำนาญการ
กรรมการ

(นายนฤนาท เจริญมาก)
นักจัดการงานทั่วไป
กรรมการ

กรมสอบสวนคดีพิเศษ

ภาคผนวก 1

รายละเอียดคุณลักษณะเฉพาะ

1. อุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall) จำนวนไม่น้อยกว่า 2 ชุด มีคุณลักษณะอย่างน้อยดังนี้

1.1 เป็นอุปกรณ์ทำหน้าที่ในการป้องกันด้าน Web Application หรือ Web Service โดยเฉพาะ

1.2 สามารถส่งข้อมูล Log ไปยังระบบจัดเก็บและวิเคราะห์ข้อมูลความปลอดภัยของระบบเครือข่ายกรมสอบสวนคดีพิเศษ ในรูปแบบ Syslog ได้เป็นอย่างน้อย

1.3 มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10/100/1000 Base-T (RJ45) หรือดีกว่า จำนวนไม่น้อยกว่า 8 ช่อง และรองรับการทำงานแบบ Bypass ได้

1.4 มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 1G (SFP) หรือดีกว่า จำนวนไม่น้อยกว่า 4 ช่อง

1.5 มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10G (SFP+) หรือดีกว่า จำนวนไม่น้อยกว่า 2 ช่อง

1.6 มีความเร็วในการส่งผ่านข้อมูล (Throughput) ไม่น้อยกว่า 2 Gbps

1.7 มี HTTPS Trans/Sec ไม่น้อยกว่า 40,000 Trans/Sec

1.8 สามารถรับการเชื่อมต่อ HTTP พร้อมกันได้ไม่น้อยกว่า 1,300,000 Concurrent Connections

1.9 สามารถรับการเชื่อมต่อ HTTPS ได้ไม่น้อยกว่า 800,000 Concurrent Connections

1.10 สามารถทำงานลักษณะ High Availability (HA) แบบ Active-Active ได้

1.11 มีหน่วยจัดเก็บข้อมูลชนิด SSD หรือดีกว่า ขนาดความจุไม่น้อยกว่า 480 GB จำนวนไม่น้อยกว่า 2 หน่วย

1.12 สามารถบริหารจัดการอุปกรณ์ผ่านทางโปรแกรม Web Browser หรือ CLI ได้เป็นอย่างน้อย

1.13 สามารถตรวจจับพฤติกรรมการใช้งาน Web Application ของผู้ที่เข้ามาใช้บริการ Web Application บนเครื่องคอมพิวเตอร์แม่ข่ายต่าง ๆ ได้

1.14 อุปกรณ์ที่นำเสนอจะต้องสามารถทำงานแบบ Reverse Proxy, In-Line (Bridge) หรือ Transparent และ Span-Mode (หรือ Monitor หรือ Sniffing Mode หรือ Offline Sniffing) สำหรับตรวจสอบพฤติกรรมได้เป็นอย่างน้อย

1.15 มีความสามารถในการทำงานและปกป้อง Web Application ต่าง ๆ ได้ โดยรองรับ HTTPS ได้เป็นอย่างน้อย

1.16 มีความสามารถตรวจสอบและป้องกันไวรัสคอมพิวเตอร์ในไฟล์ซึ่งถูก Upload จากเครื่องผู้ใช้งานมายัง Web Server ได้ หรือ Filter File ที่จะ Upload ได้ หรือเทียบเท่าได้

1.17 สามารถทำงานเป็น Load Balancer สำหรับ Web Server ได้ โดยมีวิธีการกระจายข้อมูลดังต่อไปนี้ ได้เป็นอย่างน้อย

1.17.1 Round Robin

1.17.2 Weighted Round Robin

1.17.3 Least Connection

1.17.4...

1.17.4 Source IP Hash

1.17.5 Host Hash

1.18 ป้องกันเว็บไซต์จากการโจมตีด้วยวิธีการ Denial Of Service (DoS) หรือ DDoS ได้

1.19 มีความสามารถตรวจสอบหาช่องโหว่ (Vulnerability Scan) บน Web Server ด้วยโปรโตคอล HTTP และ HTTPS ได้

1.20 สามารถเก็บและส่งรายละเอียดและตรวจสอบการใช้งาน (Logging/Monitoring) ในรูปแบบ Syslog ได้

1.21 รองรับการป้องกันการถูกโจมตีด้วยวิธีต่าง ๆ ดังนี้ ได้เป็นอย่างน้อย

1.21.1 Cross-site Scripting

1.21.2 Cookie Poisoning

1.21.3 Buffer Overflow

1.21.4 SQL Injection

1.22 สามารถใช้งานตามมาตรฐาน IPv6 ได้

1.23 สามารถบริหารจัดการอุปกรณ์ผ่านทางโปรแกรม Web Browser หรือ CLI ได้เป็นอย่างน้อย

1.24 ตัวอุปกรณ์ หรือระบบปฏิบัติการ หรือระบบที่เสนอมีเครื่องหมายการค้า ที่เข้าร่วมประเมิน หรือทดสอบโดยมีผลการประเมินอยู่ในกลุ่มผู้นำ (Leader) จาก SecurelQLab ด้าน CyberRisk Validation Comparative Report Cloud Web Application และ API Protection (WAAP) หรือ GigaOM ด้าน Application and API Security หรือ KuppinggerCole – Leadership Compass ด้าน Web Application Firewalls ตั้งแต่ปี 2022 ขึ้นไป

1.25 สามารถ Update ข้อมูลรูปแบบภัยคุกคามใหม่จากบริษัทผู้ผลิตได้อัตโนมัติ หรือ Update Version ได้ไม่น้อยกว่า 3 ปี โดยไม่เสียค่าใช้จ่ายเพิ่มเติม

1.26 ผู้เสนอราคาจะต้องให้การสนับสนุน ช่วยเหลือทางเทคนิค และการบริการหลังการขายจากผู้ผลิตหรือตัวแทนผู้ผลิตในประเทศไทย สำหรับผลิตภัณฑ์ที่เสนอในโครงการนี้ เพื่อให้การใช้งานเป็นไปอย่างมีประสิทธิภาพ ผลิตภัณฑ์ที่เสนอต้องเป็นผลิตภัณฑ์ใหม่ ไม่เคยใช้งานมาก่อนยังอยู่ในสายการผลิต สนับสนุนการประกัน (Warranty)

2. ระบบบันทึกและตรวจสอบสิทธิการเข้าถึงระบบสารสนเทศและอุปกรณ์เครือข่าย (Privileged Access Management) จำนวนไม่น้อยกว่า 1 ระบบ โดยมีคุณลักษณะอย่างน้อยดังนี้

2.1 ระบบที่เสนอต้องเป็นแบบ Virtual Appliance ที่มีการ Hardening มาแล้วจากผู้ผลิต ที่สามารถทำหน้าที่ในการบันทึกกิจกรรมการทำงานของผู้ใช้งานอุปกรณ์ปลายทาง ได้แก่ เครื่องแม่ข่ายและอุปกรณ์เครือข่าย ในรูปแบบภาพเคลื่อนไหว

2.2 สามารถส่งข้อมูล Log ไปยังระบบจัดเก็บและวิเคราะห์ข้อมูลความปลอดภัยของระบบเครือข่ายกรมสอบสวนคดีพิเศษ ในรูปแบบ Syslog ได้เป็นอย่างน้อย

2.3 มีลิขสิทธิ์ใช้งานอย่างน้อย 100 Device

2.4 สามารถทำงานได้โดยไม่ต้องติดตั้ง Software บนอุปกรณ์ปลายทางที่ต้องการเก็บบันทึกกิจกรรมการทำงาน (Agentless)

2.5...

2.5 สามารถทำงานในรูปแบบ Single Sign-On (SSO) โดยที่ไม่ต้องเปิดเผยรหัสผ่านของอุปกรณ์ปลายทางให้ผู้ใช้งานรับทราบ

2.6 สามารถรองรับการเข้าถึงอุปกรณ์ปลายทางด้วยโปรโตคอลดังนี้ SSH, RDP (Remote Desktop Protocol), VNC, SFTP, Telnet, Rlogin และ Raw TCP/IP

2.7 สามารถควบคุมสิทธิของผู้ใช้งานในการเข้าถึงอุปกรณ์ปลายทางโดยสามารถกำหนดนโยบายได้อย่างน้อยดังนี้

2.7.1 สามารถควบคุมให้ผู้ใช้งานสามารถเข้าถึงเฉพาะอุปกรณ์ปลายทางที่ได้รับอนุญาตเท่านั้น

2.7.2 สามารถควบคุมให้ผู้ใช้งานเข้าถึงอุปกรณ์ปลายทางด้วย User Account ตามที่กำหนด

2.7.3 สามารถควบคุมช่วงเวลาที่อนุญาตให้เข้าถึงอุปกรณ์ปลายทาง

2.7.4 สามารถควบคุมโปรโตคอลที่อนุญาตให้ใช้สำหรับการเข้าถึงอุปกรณ์ปลายทาง

2.8 สามารถใช้งานผ่าน Client Software เช่น PuTTY, FileZilla, WinSCP และ Terminal Server Client (Remote Desktop Connection) ได้

2.9 สามารถเลือกกำหนดให้อุปกรณ์บันทึกกิจกรรมการทำงานของผู้ใช้งานในรูปแบบภาพเคลื่อนไหวเฉพาะบางอุปกรณ์ปลายทางที่ต้องการเท่านั้น

2.10 มี Optical Character Recognition (OCR) Engine ที่สามารถวิเคราะห์การใช้งานผ่าน RDP และ VNC แบบ Real-Time และสามารถแจ้งเตือนเมื่อตรวจพบพฤติกรรมของผู้ใช้งานที่ไม่เหมาะสม

2.11 สามารถแสดงรายการภาพวิดีโอตัวอย่าง (Screenshot list) ของแต่ละช่วงเวลาตั้งแต่เริ่มต้นจนถึงสิ้นสุดการใช้งาน เพื่อให้เจ้าหน้าที่สามารถเรียกดูกิจกรรมการทำงานในรูปแบบภาพเคลื่อนไหวในช่วงเวลาดังกล่าวได้

2.12 สามารถเรียกดูเซสชั่น (Session) ที่ผู้ใช้งานกำลังปฏิบัติงานอยู่ ณ ขณะนั้นแบบ Real-Time และสามารถตัดสิทธิ (Terminate) การใช้งานของผู้ใช้งาน ที่กำลังใช้งานอยู่ ณ ขณะนั้นได้

2.13 สามารถตัดสิทธิ (Terminate) การใช้งานเมื่อมีการเรียกใช้คำสั่ง (Command) ที่ไม่อนุญาตบนอุปกรณ์ปลายทางที่ใช้งานด้วยโปรโตคอล SSH ได้

2.14 สามารถทำ Session Sharing และ Remote Control บน RDP Session ขณะที่ผู้ใช้งานกำลังใช้งานอยู่ได้

2.15 มีการใช้ Session Probe ในการเก็บข้อมูล Metadata บน RDP Session เพื่อเก็บ Activity ของผู้ใช้งานได้

2.16 สามารถควบคุมการใช้งาน RDP Session เช่น ห้ามใช้งาน Process และ Program ที่กำหนดได้ โดยไม่ต้องติดตั้งซอฟต์แวร์บนอุปกรณ์ปลายทาง

2.17 สามารถเชื่อมต่อกับอุปกรณ์จัดเก็บข้อมูลภายนอกผ่านทาง NFS และ SMB/CIFS เพื่อใช้ในการเก็บบันทึกไฟล์บันทึกกิจกรรมการทำงานของผู้ใช้งาน (Video Recording)

2.18 สามารถ Update ข้อมูลรูปแบบภัยคุกคามใหม่จากบริษัทผู้ผลิตได้อัตโนมัติ หรือ Update Version ได้ไม่น้อยกว่า 3 ปี โดยไม่เสียค่าใช้จ่ายเพิ่มเติม

2.19...

2.19 ผู้เสนอราคาจะต้องให้การสนับสนุน ช่วยเหลือทางเทคนิค และการบริการหลังการขายจากผู้ผลิตหรือตัวแทนผู้ผลิตในประเทศไทย สำหรับผลิตภัณฑ์ที่เสนอในโครงการนี้ เพื่อให้การใช้งานเป็นไปอย่างมีประสิทธิภาพ ผลิตภัณฑ์ที่เสนอต้องเป็นผลิตภัณฑ์ใหม่ ไม่เคยใช้งานมาก่อนยังอยู่ในสายการผลิต สนับสนุนการประกัน (Warranty)

3. ซอฟต์แวร์ความปลอดภัยของอุปกรณ์ปลายทาง และการเข้าถึงเครือข่าย แบบ Zero Trust จำนวนไม่น้อยกว่า 1 ระบบ โดยมีคุณลักษณะอย่างน้อยดังนี้

3.1 สามารถเข้าใช้งานพร้อมกัน (Concurrent User) ได้ไม่น้อยกว่า 150 ผู้ใช้งาน

3.2 สามารถสร้างการเชื่อมต่อจากเครือข่ายภายนอกองค์กร ไปยังแอปพลิเคชันหรือระบบงานภายในองค์กรได้โดยไม่ต้องใช้อุปกรณ์ VPN

3.3 สามารถตรวจสอบการเข้าถึงแอปพลิเคชันหรือระบบงานภายในองค์กรที่สามารถประเมินความเสี่ยงของอุปกรณ์เชื่อมต่อและผู้ใช้งานก่อนอนุญาตหรือไม่อนุญาตให้เข้าถึงระบบงานภายในได้

3.4 สามารถกำหนดเวลาในการเข้าถึง (Time Control), แอปพลิเคชัน (Application), ตำแหน่งทางภูมิศาสตร์ (Geolocation), ผู้ใช้งาน (User/Group) และคะแนนความเสี่ยง (Risk Score) ในการเข้าถึงแอปพลิเคชันหรือระบบงานขององค์กรได้เป็นอย่างน้อย

3.5 สามารถทำ Device Posture เพื่อตรวจสอบ OS Version, Company/Client Certificate, Firewall Status, File Present, Vulnerability Detection, Antivirus Software, EDR Software, Device Joined Domain, Screen Lock Status และ Disk Encryption status ก่อนอนุญาตให้อุปกรณ์เข้าถึงแอปพลิเคชันหรือระบบงานขององค์กร ได้เป็นอย่างน้อย

3.6 รองรับการทำงานบนระบบปฏิบัติการ Windows, MacOS, Android, iOS/iPadOS ได้เป็นอย่างน้อย

3.7 จุดเชื่อมต่อเครือข่ายภายใน (Connector) สามารถตั้งค่าโดยใช้ Private IP โดยไม่จำเป็นต้องเปิด Port เพื่อรองรับการเชื่อมต่อจากภายนอก

3.8 สามารถส่งข้อมูล Log ไปยังระบบจัดเก็บและวิเคราะห์ข้อมูลความปลอดภัยของระบบเครือข่ายกรมสอบสวนคดีพิเศษ ในรูปแบบ Syslog ได้เป็นอย่างน้อย

3.9 สามารถ Update ข้อมูลรูปแบบภัยคุกคามใหม่จากบริษัทผู้ผลิตได้อัตโนมัติ หรือ Update Version ได้ไม่น้อยกว่า 3 ปี โดยไม่เสียค่าใช้จ่ายเพิ่มเติม

3.10 ผู้เสนอราคาจะต้องให้การสนับสนุน ช่วยเหลือทางเทคนิค และการบริการหลังการขายจากผู้ผลิตหรือตัวแทนผู้ผลิตในประเทศไทย สำหรับอุปกรณ์ที่เสนอในโครงการนี้ เพื่อให้การใช้งานเป็นไปอย่างมีประสิทธิภาพ อุปกรณ์ที่เสนอต้องเป็นอุปกรณ์ใหม่ ไม่เคยใช้งานมาก่อนยังอยู่ในสายการผลิต สนับสนุนการประกัน (Warranty)

4. ระบบวิเคราะห์และป้องกันภัยไซเบอร์แบบ XDR Security Platform จำนวนไม่น้อยกว่า 1 ระบบ โดยมีคุณลักษณะอย่างน้อยดังนี้

4.1 ซอฟต์แวร์ป้องกันภัยคุกคามทางไซเบอร์ สำหรับเครื่องคอมพิวเตอร์แม่ข่าย จำนวนอย่างน้อย 100 License โดยมีคุณลักษณะอย่างน้อยดังนี้

4.1.1 เป็นระบบรักษาความปลอดภัยที่สามารถทำงานบนระบบปฏิบัติการ Microsoft Windows Server รวมถึงรองรับระบบปฏิบัติการอื่นๆ อาทิ เช่น Debian Linux, Red Hat Enterprise Linux, Ubuntu, SUSE Linux Enterprise ได้เป็นอย่างน้อย

4.1.2 สามารถส่งข้อมูล Log ไปยังระบบจัดเก็บและวิเคราะห์ข้อมูลความปลอดภัยของระบบเครือข่ายกรมสอบสวนคดีพิเศษ ในรูปแบบ Syslog ได้เป็นอย่างน้อย

4.1.3 สามารถเชื่อมต่อกับ VMware vCenter, AWS และ Microsoft Azure เพื่อค้นหา (Discover) Workload ที่ทำงานอยู่ได้

4.1.4 สามารถทำ Agent Self-Protection เพื่อป้องกัน Local User จากการ Tampering Agent เช่น Uninstall และแก้ไขตัว Agent ได้

4.1.5 สามารถตรวจสอบ Malware ด้วยเทคโนโลยี Machine Learning และ Behavior Monitor เพื่อป้องกัน Malware ที่เกิดใหม่ได้

4.1.6 สามารถกู้คืนไฟล์เอกสารที่ถูกโจมตีด้วย Ransomware บนแพลตฟอร์ม Windows ได้โดยอัตโนมัติ

4.1.7 สามารถตรวจหา Malware ในไฟล์ที่ถูกเขียนผ่าน Docker Container บนแพลตฟอร์ม Linux ได้

4.1.8 สามารถป้องกัน Malware และ ภัยคุกคามทางเว็บไซต์ต่าง ๆ ด้วยเทคโนโลยี Reputation กับระบบ Cloud ของเจ้าของผลิตภัณฑ์ได้ เพื่อเพิ่มประสิทธิภาพในการป้องกัน และตรวจจับ

4.1.9 สามารถทำ Stateful Firewall ในลักษณะของ Host-Based Firewall ที่สามารถตั้งนโยบายความปลอดภัยให้กับระบบปฏิบัติการแต่ละเครื่องได้โดยใช้นโยบายที่แตกต่างกัน

4.1.10 สามารถป้องกันช่องโหว่ของระบบปฏิบัติการทางเครือข่ายได้ โดยที่ไม่จำเป็นต้องทำการติดตั้ง Patches หรือซอฟต์แวร์ใด ๆ บนระบบปฏิบัติการเหล่านั้นจริง เพื่อป้องกันปัญหาที่อาจเกิดขึ้นจากการ Patches โดยที่ยังไม่ได้ทำการทดสอบกับการใช้งานจริง

4.1.11 สามารถสแกนเครื่องคอมพิวเตอร์เพื่อหา Vulnerable Software แล้วจัดหาการตั้งค่า Recommended Security ที่เหมาะสมให้ หรือนำเสนอ Vulnerability Assessment Tool ที่มีลิขสิทธิ์การทำงานถูกต้องเพื่อตรวจหา Vulnerable Software บนเครื่องคอมพิวเตอร์ปลายทางโดยต้องมีการอัปเดตฐานข้อมูลให้มีความทันสมัยตลอดอายุการใช้งานได้

4.1.12...

4.1.12 สามารถป้องกันการโจมตีในระดับ Application-Layer อาทิเช่น SQL Injection และ Cross-Site Script หรือสามารถเสนอ Web Application Firewall ที่มี Throughput ไม่ต่ำกว่า 4 Gbps ได้

4.1.13 สามารถถอดรหัส Traffic ประเภท SSL/TLS บนระบบปฏิบัติการ Windows และ Linux ได้เพื่อป้องกันการโจมตีผ่านช่องโหว่ หรือนำเสนออุปกรณ์ SSL Decryption ที่มี Throughput ไม่น้อยกว่า 4 Gbps ได้

4.1.14 สามารถตรวจจับและป้องกันช่องโหว่ประเภท Zero-Day Vulnerabilities ได้ โดยรวมถึง Exploits ประเภทต่าง ๆ ด้วย

4.1.15 สามารถวิเคราะห์ Log File ของระบบปฏิบัติการณ์และแอปพลิเคชันต่าง ๆ หรือ User Activity และ Process Monitoring และแจ้งเตือนถึงเหตุการณ์น่าสงสัย (Suspicious Activity) หรือเหตุการณ์เกี่ยวกับความปลอดภัยของระบบที่ใช้งานได้

4.1.16 สามารถทำ Device Control เพื่อควบคุมการใช้งาน External Storage Device บนแพลตฟอร์ม Windows ได้เป็นอย่างน้อย

4.1.17 สามารถทำ Application Control เพื่อควบคุมการทำงานแอปพลิเคชันแปลกปลอม บนระบบปฏิบัติการ Windows และ Linux ได้ หรือเสนอระบบอื่น ๆ เพิ่มเติม

4.1.18 สามารถตรวจจับและโต้ตอบต่อภัยคุกคามข้ามเลเยอร์ เพื่อการค้นหาและวิเคราะห์ภัยคุกคามที่มาจากหลายทิศทางแบบเชิงลึก (Extended Detection and Response: XDR)

4.1.19 สามารถทำการเก็บข้อมูลหลักฐานต่าง ๆ ของเครื่องคอมพิวเตอร์ (Forensic Analysis) เพื่อตรวจสอบเหตุการณ์การทำงานของมัลแวร์ได้ย้อนหลังไม่น้อยกว่า 30 วัน โดยมีการเก็บข้อมูลไว้บนบริการที่ได้รับมาตรฐาน ISO 27001:2013 หรือ ISO 27017:2015 ได้เป็นอย่างน้อย

4.1.20 สามารถตรวจสอบสิ่งที่เกิดขึ้น เช่น File, Process, Registry, User Account Activity และ Network Communication ได้

4.1.21 สามารถวิเคราะห์ Flow การทำงานของมัลแวร์โดยสร้างเป็นแผนภาพที่แสดง Root Cause Analysis หรือ Execution Profile ได้

4.1.22 สามารถ Update ข้อมูลรูปแบบภัยคุกคามใหม่จากบริษัทผู้ผลิตได้อัตโนมัติ หรือ Update Version ได้ไม่น้อยกว่า 3 ปี โดยไม่เสียค่าใช้จ่ายเพิ่มเติม

4.1.23 ผู้เสนอราคาจะต้องให้การสนับสนุน ช่วยเหลือทางเทคนิค และการบริการหลังการขายจากผู้ผลิตหรือตัวแทนผู้ผลิตในประเทศไทย สำหรับผลิตภัณฑ์ที่เสนอในโครงการนี้ เพื่อให้การใช้งานเป็นไปอย่างมีประสิทธิภาพ ผลิตภัณฑ์ที่เสนอต้องเป็นผลิตภัณฑ์ใหม่ ไม่เคยใช้งานมาก่อนยังอยู่ในสายการผลิต สนับสนุนการประกัน (Warranty)

4.2...

4.2 **ซอฟต์แวร์ป้องกันภัยคุกคามทางไซเบอร์ สำหรับเครื่องคอมพิวเตอร์ลูกข่าย จำนวนไม่น้อยกว่า 1500 License โดยมีคุณลักษณะอย่างน้อยดังนี้**

4.2.1 สามารถป้องกัน Malware, Spyware, Rootkit และ Virus บนระบบปฏิบัติการ Windows 10, Windows 11, MacOS ได้เป็นอย่างน้อย

4.2.2 สามารถติดตั้งระบบบริหารจัดการได้แบบ Software as a Service หรือ Cloud Delivered หรือ Cloud Based ที่มี Web-Based Management เพื่อใช้ในการบริหารจัดการเครื่องคอมพิวเตอร์ลูกข่าย

4.2.3 สามารถตรวจสอบ Malware แบบอ้างอิงจากฐานข้อมูล (Signature) และแบบวิเคราะห์พฤติกรรม (Heuristic Technology) อย่างน้อยดังนี้

4.2.3.1 Virtual Patching หรือ Intrusion Prevention (HIPS) หรือ Attack Surface Reduction หรือ Exploit Preventions

4.2.3.2 Behavior Monitoring

4.2.3.3 Machine Learning

4.2.4 สามารถป้องกันช่องโหว่ทางเครือข่ายของระบบปฏิบัติการ โดยที่ไม่จำเป็นต้องทำการติดตั้ง Patches บนระบบปฏิบัติการเหล่านั้นจริงได้ เพื่อป้องกันปัญหาที่อาจเกิดขึ้นจากการ Patches โดยที่ยังไม่ได้ทำการทดสอบกับการใช้งานจริงได้

4.2.5 สามารถป้องกัน Ransomware ด้วยพฤติกรรม และสามารถกู้คืนไฟล์เอกสารที่ถูกโจมตีด้วย Ransomware ได้โดยอัตโนมัติ

4.2.6 สามารถทำการป้องกันอันตรายที่มาจากทางเว็บไซต์ต่าง ๆ (Web Threats) ได้ในแบบ Web Reputation ได้เป็นอย่างน้อย

4.2.7 สามารถกำหนดสิทธิ์การใช้งาน เช่น Full Access, Read, Read and Execute, Modify หรือ List Content ให้กับอุปกรณ์ USB Storage Devices ได้และสามารถอนุญาตให้ใช้งาน USB Storage ได้เป็นรายยี่ห้อ (Vendor ID) และ Serial Number ที่มีการลงทะเบียนในระบบเท่านั้น

4.2.8 มีความสามารถในการป้องกันข้อมูลสำคัญขององค์กรไม่ให้รั่วไหลออกไปภายนอกองค์กร (Data Loss Prevention) ผ่านทาง FTP, HTTP, Web Mail, Printer, Windows Clipboard, และ Removable Storage ได้ โดยใช้เงื่อนไขอย่างน้อยดังนี้ File Attributes, Keywords และ Regular Expressions หรือเสนอระบบเพิ่มเติมเพื่อให้สามารถทำคุณลักษณะดังกล่าวได้

4.2.9 สามารถทำการป้องกันโปรแกรมประยุกต์ที่ไม่ได้รับอนุญาต (Lockdown, Block และ Allow) และไม่ต้องการให้ติดตั้งบนเครื่องคอมพิวเตอร์ลูกข่ายได้ (Application Control) และสามารถกำหนด Rule โดยใช้เงื่อนไขต่าง ๆ ได้ หรือเสนอระบบอื่นเพิ่มเติมเพื่อให้สามารถทำ Application Control ได้

4.2.10 สามารถ Update ข้อมูลรูปแบบภัยคุกคามใหม่จากบริษัทผู้ผลิตได้อัตโนมัติ หรือ Update Version ได้ไม่น้อยกว่า 3 ปี โดยไม่เสียค่าใช้จ่ายเพิ่มเติม

4.2.11...

4.2.11 ผลิตภัณฑ์ที่นำเสนอ ต้องได้รับการจัดอันดับ Forrester Wave Endpoint Security (อยู่ในกลุ่ม Leaders) และ Gartner Magic Quadrant for Endpoint Protection Platforms (อยู่ในกลุ่ม Leader) ตั้งแต่ปี 2022 ขึ้นไป

4.2.12 ผู้เสนอราคาจะต้องให้การสนับสนุน ช่วยเหลือทางเทคนิค และการบริการหลังการขายจากผู้ผลิตหรือตัวแทนผู้ผลิตในประเทศไทย สำหรับผลิตภัณฑ์ที่เสนอในโครงการนี้ เพื่อให้การใช้งานเป็นไปอย่างมีประสิทธิภาพ ผลิตภัณฑ์ที่เสนอต้องเป็นผลิตภัณฑ์ใหม่ไม่เคยใช้งานมาก่อน ยังอยู่ในสายการผลิต สนับสนุนการประกัน (Warranty)

4.3 **ระบบตรวจสอบและวิเคราะห์ภัยคุกคามเครื่องคอมพิวเตอร์แบบ Extended Detection And Response – XDR จำนวน 1 ระบบ โดยมีคุณลักษณะอย่างน้อยดังนี้**

4.3.1 สามารถบันทึกหลักฐานต่าง ๆ ของเครื่องคอมพิวเตอร์ (Telemetry หรือ Forensic Analysis) เพื่อตรวจสอบเหตุการณ์การทำงานของมัลแวร์ได้ย้อนหลังไม่น้อยกว่า 30 วัน และสามารถดูการแจ้งเตือนเหตุการณ์ย้อนหลังได้ไม่น้อยกว่า 180 วัน

4.3.2 สามารถบันทึกและตรวจสอบสิ่งที่เกิดขึ้น เช่น File หรือ Process หรือ Network Communication หรือ Network Events ได้

4.3.3 สามารถทำงาน Response เช่น Isolate Endpoint ได้

4.3.4 สามารถทำงานค้นหาร่องรอยการโจมตี (Sweeping / Hunting) จากข้อมูลที่บันทึกโดยมี Threat Intelligence จากเจ้าของผลิตภัณฑ์เองและสามารถเพิ่มแหล่งข้อมูลจาก STIX File, TAXII Feeds ได้

4.3.5 สามารถทำ Security Playbook เพื่อจัดการความเสี่ยงที่เกิดขึ้นได้โดยอัตโนมัติ

4.3.6 สามารถ Update ข้อมูลรูปแบบภัยคุกคามใหม่จากบริษัทผู้ผลิตได้อัตโนมัติ หรือ Update Version ได้ไม่น้อยกว่า 3 ปี โดยไม่เสียค่าใช้จ่ายเพิ่มเติม

4.3.7 ผลิตภัณฑ์ที่นำเสนอ ต้องได้รับการจัดอันดับ Forrester Wave Extended Detection And Response Platforms (อยู่ในกลุ่ม Leaders หรือ Strong Performers) ตั้งแต่ปี 2022 ขึ้นไป

4.3.8 ผู้เสนอราคาจะต้องให้การสนับสนุน ช่วยเหลือทางเทคนิค และการบริการหลังการขายจากผู้ผลิตหรือตัวแทนผู้ผลิตในประเทศไทย สำหรับผลิตภัณฑ์ที่เสนอในโครงการนี้ เพื่อให้การใช้งานเป็นไปอย่างมีประสิทธิภาพ ผลิตภัณฑ์ที่เสนอต้องเป็นผลิตภัณฑ์ใหม่ ไม่เคยใช้งานมาก่อน ยังอยู่ในสายการผลิต สนับสนุนการประกัน (Warranty)

****