



ประกาศสำนักเลขาธิการนายกรัฐมนตรี
เรื่อง ประกวดราคาจ้างบริหารจัดการระบบรักษาความปลอดภัยไซเบอร์ของสำนักเลขาธิการ
นายกรัฐมนตรี
ด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding)

สำนักเลขาธิการนายกรัฐมนตรี มีความประสงค์จะประกวดราคาจ้างบริหารจัดการระบบรักษาความปลอดภัยไซเบอร์ของสำนักเลขาธิการนายกรัฐมนตรี ด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding) ราคาของงานจ้าง ในการประกวดราคาครั้งนี้ เป็นเงินทั้งสิ้น ๓๗,๕๐๐,๐๐๐.๐๐ บาท (สามสิบล้านห้าแสนบาทถ้วน)

ผู้ยื่นข้อเสนอต้องยื่นข้อเสนอโดยแสดงหลักฐานถึงขีดความสามารถและความพร้อมที่มีอยู่ในวันยื่นข้อเสนอ โดยมีรายละเอียดดังนี้

๑. ผู้ยื่นข้อเสนอจะต้องมีคุณสมบัติให้เป็นไปตามเอกสารประกวดราคาอิเล็กทรอนิกส์กำหนด
๒. ผู้ยื่นข้อเสนอต้องเสนอราคาทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์

ในวันที่ ๒๔ สิงหาคม ๒๕๖๙ ระหว่างเวลา ๐๙.๐๐ น. ถึง ๑๒.๐๐ น. ซึ่งสามารถจัดเตรียมเอกสารข้อเสนอได้ตั้งแต่วันที่ประกาศจนถึงวันเสนอราคา

๓. ผู้สนใจสามารถดูรายละเอียดและดาวน์โหลดเอกสารประกวดราคาอิเล็กทรอนิกส์เลขที่ E ๑๙/๒๕๖๙ ลงวันที่ ๑๓ สิงหาคม พ.ศ. ๒๕๖๙ ผ่านทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ ได้ตั้งแต่วันที่ประกาศจนถึงวันเสนอราคา ได้ที่เว็บไซต์ <https://spm.thaigov.go.th> หรือ www.gprocurement.go.th

ประกาศ ณ วันที่ ๑๓ สิงหาคม พ.ศ. ๒๕๖๙

ณิชา เกษมสุข

(นางชนิดา เกษมสุข)

รองเลขาธิการนายกรัฐมนตรีฝ่ายบริหาร
ปฏิบัติราชการแทน เลขาธิการนายกรัฐมนตรี

เอกสารประกวดราคาจ้างด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding)

เลขที่ E ๑๙/๒๕๖๙

การจ้างบริหารจัดการระบบรักษาความปลอดภัยไซเบอร์ของสำนักเลขาธิการนายกรัฐมนตรี

ตามประกาศสำนักเลขาธิการนายกรัฐมนตรี

ลงวันที่ ๑๓ สิงหาคม ๒๕๖๙

สำนักเลขาธิการนายกรัฐมนตรี ซึ่งต่อไปนี้จะเรียกว่า "กรม" มีความประสงค์จะประกวดราคาจ้างบริหารจัดการระบบรักษาความปลอดภัยไซเบอร์ของสำนักเลขาธิการนายกรัฐมนตรี ด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding) ตามรายการ ดังนี้

จ้างบริหารจัดการระบบรักษาความปลอดภัยไซเบอร์ของสำนักเลขาธิการนายกรัฐมนตรี	จำนวน	๑	งาน
--	-------	---	-----

โดยมีข้อแนะนำและข้อกำหนดดังต่อไปนี้

๑. เอกสารแนบท้ายเอกสารประกวดราคาอิเล็กทรอนิกส์

๑.๑ ขอบเขตของงาน

๑.๒ แบบใบเสนอราคาที่กำหนดไว้ในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์

๑.๓ แบบสัญญาจ้างทำของ

๑.๔ แบบหนังสือคำประกัน

(๑) หลักประกันการเสนอราคา

(๒) หลักประกันสัญญา

๑.๕ บทนิยาม

(๑) ผู้ที่มีผลประโยชน์ร่วมกัน

(๒) การขัดขวางการแข่งขันอย่างเป็นธรรม

๑.๖ แบบบัญชีเอกสารที่กำหนดไว้ในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์

(๑) บัญชีเอกสารส่วนที่ ๑

(๒) บัญชีเอกสารส่วนที่ ๒

๑.๗ แผนการทำงาน

๑.๘ แผนการใช้พัสดุที่ผลิตภายในประเทศ

๑.๙ ใบแจ้งการชำระเงิน สำหรับชำระเงินหลักประกันการเสนอราคา

๒. คุณสมบัติของผู้ยื่นขอเสนอ

๒.๑ มีความสามารถตามกฎหมาย

๒.๒ ไม่เป็นบุคคลล้มละลาย

๒.๓ ไม่อยู่ระหว่างเลิกกิจการ

๒.๔ ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

๒.๕ ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทำงานและได้แจ้งเวียนชื่อให้เป็นผู้ทำงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทำงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

๒.๖ มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

๒.๗ เป็นนิติบุคคลผู้มีอาชีพรับจ้างงานที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

๒.๘ ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่กรม ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

๒.๙ ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาล ของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นนั้น

๒.๑๐ ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ "กิจการร่วมค้า" ต้องมีคุณสมบัติดังนี้

(๑) การกำหนดสัดส่วนในการเข้าร่วมค้าของคู่สัญญา

กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงฯ จะต้องมีการกำหนดสัดส่วนหน้าที่ และความรับผิดชอบในปริมาณงาน สิ่งของ หรือมูลค่า ตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

(๒) กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก กิจการร่วมค่านั้นต้องใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

สำหรับข้อตกลงฯ ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมค้าหลัก ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน

(๓) การยื่นข้อเสนอของกิจการร่วมค้า

(๓.๑) กรณีที่ข้อตกลงฯ กำหนดให้มีการมอบหมายผู้เข้าร่วมค้า รายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า การยื่นข้อเสนอดังกล่าวต้องมีหนังสือมอบอำนาจ

สำหรับข้อตกลงฯ ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้ยื่น ข้อเสนอ ผู้เข้าร่วมค้าทุกรายจะต้องลงลายมือชื่อในหนังสือมอบอำนาจให้ผู้เข้าร่วมค้ารายใดรายหนึ่ง เป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า

(๓.๒) การยื่นข้อเสนอด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e - bidding) ให้ผู้เข้าร่วมคำที่ได้รับมอบหมายหรือมอบอำนาจตามข้อ (๓.๑) ดำเนินการซื้อเอกสารประกวดราคาอิเล็กทรอนิกส์ กรณีที่มีการจำหน่ายเอกสารซื้อหรือจ้าง

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

๒.๑๒ ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ ดังนี้

๑. กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยหรือต่างประเทศ ซึ่งได้จดทะเบียนเกินกว่า ๑ ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิ ที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก ๑ ปีสุดท้ายก่อนวันยื่นข้อเสนอ งบแสดงฐานะการเงิน ๑ ปีสุดท้ายก่อนวันยื่นข้อเสนอ หมายถึง งบแสดงฐานะการเงินย้อนไปก่อนวันที่หน่วยงานของรัฐกำหนดให้เป็นวันยื่นข้อเสนอ ๑ ปีปฏิทิน เว้นแต่กรณีนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย หากวันยื่นข้อเสนอเป็นช่วงระยะเวลาที่กรมพัฒนาธุรกิจการค้ากำหนดให้นิติบุคคลยื่นงบแสดงฐานะการเงิน กับกรมพัฒนาธุรกิจการค้า ซึ่งจะอยู่ในช่วงเดือนมกราคม - เดือนพฤษภาคม ของทุกปี โดยนิติบุคคลที่เป็นผู้ยื่นข้อเสนอที่ยังอยู่ในช่วงของการยื่นงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า คือ ช่วงเดือนมกราคม - เดือนพฤษภาคม กรณีนี้ให้สามารถยื่นงบแสดงฐานะการเงินย้อนไปอีก ๑ ปี ได้

๒. กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มี การรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า หรือกรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้น ตามกฎหมายต่างประเทศซึ่งยังไม่มี การรายงานงบแสดงฐานะการเงิน ให้พิจารณาการกำหนดมูลค่าของ ทุนจดทะเบียน โดยผู้ยื่นข้อเสนอจะต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอ ดังนี้

(๑) มูลค่าการจัดซื้อจัดจ้างไม่เกิน ๑ ล้านบาท ไม่ต้องกำหนดทุนจดทะเบียน

(๒) มูลค่าการจัดซื้อจัดจ้างเกิน ๑ ล้านบาท แต่ไม่เกิน ๕ ล้านบาท
ต้องมีทุนจดทะเบียนไม่ต่ำกว่า ๑ ล้านบาท

(๓) มูลค่าการจัดซื้อจัดจ้างเกิน ๕ ล้านบาท แต่ไม่เกิน ๑๐ ล้านบาท
ต้องมีทุนจดทะเบียนไม่ต่ำกว่า ๒ ล้านบาท

(๔) มูลค่าการจัดซื้อจัดจ้างเกิน ๑๐ ล้านบาท แต่ไม่เกิน ๒๐ ล้านบาท
ต้องมีทุนจดทะเบียนไม่ต่ำกว่า ๓ ล้านบาท

(๕) มูลค่าการจัดซื้อจัดจ้างเกิน ๒๐ ล้านบาท แต่ไม่เกิน ๖๐ ล้านบาท
ต้องมีทุนจดทะเบียนไม่ต่ำกว่า ๘ ล้านบาท

(๖) มูลค่าการจัดซื้อจัดจ้างเกิน ๖๐ ล้านบาท แต่ไม่เกิน ๑๕๐ ล้านบาท
ต้องมีทุนจดทะเบียนไม่ต่ำกว่า ๒๐ ล้านบาท

(๗) มูลค่าการจัดซื้อจัดจ้างเกิน ๑๕๐ ล้านบาท แต่ไม่เกิน ๓๐๐ ล้านบาท ต้องมีทุนจดทะเบียนไม่ต่ำกว่า ๖๐ ล้านบาท

(๘) มูลค่าการจัดซื้อจัดจ้างเกิน ๓๐๐ ล้านบาท แต่ไม่เกิน ๕๐๐ ล้านบาท ต้องมีทุนจดทะเบียนไม่ต่ำกว่า ๑๐๐ ล้านบาท

(๙) มูลค่าการจัดซื้อจัดจ้างเกิน ๕๐๐ ล้านบาทขึ้นไป ต้องมีทุนจดทะเบียนไม่ต่ำกว่า ๒๐๐ ล้านบาท

๓. สำหรับการจัดซื้อจัดจ้างครั้งหนึ่งที่มีวงเงินเกิน ๕๐๐,๐๐๐ บาทขึ้นไป กรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดา ให้พิจารณาจากหนังสือรับรองบัญชีเงินฝากไม่เกิน ๙๐ วัน ก่อนวันยื่นข้อเสนอ โดยต้องมีเงินฝากคงเหลือในบัญชีธนาคารเป็นมูลค่า ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง และหากเป็นผู้ชนะการจัดซื้อจัดจ้างหรือเป็นผู้ได้รับการคัดเลือกจะต้องแสดงหนังสือรับรองบัญชีเงินฝากที่มีมูลค่าดังกล่าวอีกครั้งหนึ่งในวันลงนามในสัญญา

๔. กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ สามารถดำเนินการได้ดังนี้

(๑) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย หรือบุคคลธรรมดาที่ถือสัญชาติไทย ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง จะเป็นสินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์ และประกอบธุรกิจค้าประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรอง หรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอไม่เกิน ๙๐ วัน

(๒) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศ หรือบุคคลธรรมดาที่มีได้ถือสัญชาติไทย ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง จะเป็นสินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์ และประกอบธุรกิจค้าประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ หรือเป็นสินเชื่อที่ธนาคารต่างประเทศหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้าประกันตามประกาศของธนาคารกลางต่างประเทศนั้น ตามรายชื่อบริษัทที่ธนาคารกลางต่างประเทศนั้นแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรอง หรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอไม่เกิน ๙๐ วัน

๕. กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศ หรือ บุคคลธรรมดาที่มีได้ถือสัญชาติไทยตามข้อ ๒ ข้อ ๓ และข้อ ๔ (๒) มูลค่าจะต้องเป็นไปตามอัตราแลกเปลี่ยนเงินตราตามประกาศที่ธนาคารแห่งประเทศไทยกำหนด ในช่วงระหว่างวันที่เผยแพร่ประกาศและเอกสารประกวดราคาในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (e - GP) จนถึงวันเสนอราคา

ทั้งนี้ ผู้ยื่นข้อเสนอจะต้องยื่นเอกสารที่แสดงให้เห็นถึงข้อมูลเกี่ยวกับมูลค่าสุทธิของกิจการแล้วแต่กรณี ประกอบกับเอกสารดังกล่าวจะต้องผ่านการรับรองตามระเบียบกระทรวงการต่างประเทศว่าด้วยการรับรองเอกสาร พ.ศ. ๒๕๓๙ และที่แก้ไขเพิ่มเติม กำหนด โดยจะต้องยื่นเอกสารดังกล่าวในวันยื่นข้อเสนอ หากผู้ยื่นข้อเสนอได้มีการยื่นเอกสารดังกล่าวมาพร้อมกับการยื่นข้อเสนอให้ถือว่าผู้ยื่นข้อเสนอรายนั้นยื่นเอกสารไม่ครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารประกวดราคา

๖. กรณีตาม ข้อ ๑ - ข้อ ๕ ไม่ใช่บังคับกรณีดังต่อไปนี้

(๖.๑) กรณีที่ผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐภายในประเทศ

(๖.๒) นิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการตามพระราชบัญญัติล้มละลาย พ.ศ. ๒๕๔๓ และที่แก้ไขเพิ่มเติม

(๖.๓) งานจ้างก่อสร้างที่กรมบัญชีกลางได้ขึ้นทะเบียนผู้ประกอบการงานก่อสร้างแล้ว และงานจ้างก่อสร้างที่หน่วยงานของรัฐที่ได้มีการจัดทำบัญชีผู้ประกอบการงานก่อสร้างที่มีคุณสมบัติเบื้องต้นไว้แล้วก่อนวันที่พระราชบัญญัติการจัดซื้อจัดจ้างฯ มีผลใช้บังคับ

(๖.๔) การจัดซื้อจัดจ้างตามมาตรา ๕๖ วรรคหนึ่ง (๒) (ข) และ (ค) แห่งพระราชบัญญัติการจัดซื้อจัดจ้างฯ

(๖.๕) การซื้อสังหาริมทรัพย์และการเช่าสังหาริมทรัพย์

(๖.๖) กรณีงานจ้างบริการหรืองานจ้างเหมาบริการกับบุคคลธรรมดา เช่น จ้างพนักงานขับรถ ครูชาวต่างชาติ พนักงานเก็บขยะ พนักงานบันทึกข้อมูล เป็นต้น

๒.๑๓ ผู้ยื่นข้อเสนอต้องได้รับการรับรองมาตรฐานสากลด้านความมั่นคงปลอดภัยสารสนเทศ ISO 27001 (Information Security Management System หรือ ISMS) โดยให้ยื่นใบรับรองมาตรฐานที่ยังไม่หมดอายุขณะเข้าเสนอราคา

๓. หลักฐานการยื่นข้อเสนอ

ผู้ยื่นข้อเสนอจะต้องเสนอเอกสารหลักฐานยื่นมาพร้อมกับการเสนอราคาทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ โดยแยกเป็น ๒ ส่วน คือ

๓.๑ ส่วนที่ ๑ อย่างน้อยต้องมีเอกสารดังต่อไปนี้

(๑) ในกรณีผู้ยื่นข้อเสนอเป็นนิติบุคคล

(ก) ห้างหุ้นส่วนสามัญหรือห้างหุ้นส่วนจำกัด ให้ยื่นสำเนาหนังสือรับรองการจดทะเบียนนิติบุคคล บัญชีรายชื่อหุ้นส่วนผู้จัดการ

(ข) บริษัทจำกัดหรือบริษัทมหาชนจำกัด ยื่นสำเนาหนังสือรับรองการจดทะเบียนนิติบุคคล หนังสือบริคณห์สนธิ บัญชีรายชื่อกรรมการผู้จัดการ และบัญชีผู้ถือหุ้นรายใหญ่ (ถ้ามี)

(๒) ในกรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดาหรือคณะบุคคลที่มีใช้นิติบุคคลให้ยื่นสำเนาบัตรประจำตัวประชาชนของผู้ยื่น ข้อเสนอข้อตกลงที่แสดงถึงการเข้าเป็นหุ้นส่วน (ถ้ามี) สำเนาบัตรประจำตัวประชาชนของผู้เป็นหุ้นส่วน หรือสำเนาหนังสือเดินทางของผู้เป็นหุ้นส่วนที่มีได้ถือสัญชาติไทย

(๓) ในกรณีผู้ยื่นข้อเสนอเป็นผู้ยื่นข้อเสนอร่วมกันในฐานะเป็นผู้ร่วมค้าให้ยื่นสำเนาสัญญาของการเข้าร่วมค้า และเอกสารตามที่ระบุไว้ใน (๑) หรือ (๒) ของผู้ร่วมค้า แล้วแต่กรณี

(๔) ผู้ยื่นข้อเสนอต้องแสดงหลักฐานเกี่ยวกับมูลค่าสุทธิของกิจการ ดังนี้

๑. กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยหรือต่างประเทศ ซึ่งได้จดทะเบียนเกินกว่า ๑ ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก ๑ ปีสุดท้ายก่อนวันยื่นข้อเสนอ งบแสดงฐานะการเงิน ๑ ปีสุดท้ายก่อนวันยื่นข้อเสนอ หมายถึง งบแสดงฐานะการเงินย้อนไปก่อนวันที่หน่วยงานของรัฐกำหนดให้เป็นวันยื่นข้อเสนอ ๑ ปีปฏิทิน เว้นแต่กรณีนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย หากวันยื่นข้อเสนอเป็นช่วงระยะเวลาที่กรมพัฒนาธุรกิจการค้ากำหนดให้นิติบุคคล ยื่นงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ซึ่งจะอยู่ในช่วงเดือนมกราคม - เดือนพฤษภาคม ของทุกปี โดยนิติบุคคลที่เป็นผู้ยื่นข้อเสนออยู่นั้นยังอยู่ในช่วงของการยื่นงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า คือ ช่วงเดือนมกราคม - เดือนพฤษภาคม กรณีนี้ให้สามารถยื่นงบแสดงฐานะการเงินย้อนไปอีก ๑ ปี ได้

๒. กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยซึ่งยังไม่มี การรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า หรือกรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศซึ่งยังไม่มี การรายงานงบแสดงฐานะการเงิน ให้พิจารณาการกำหนดมูลค่าของทุนจดทะเบียน โดยผู้ยื่นข้อเสนอจะต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอ ดังนี้

(๑) มูลค่าการจัดซื้อจัดจ้างไม่เกิน ๑ ล้านบาท ไม่ต้องกำหนด

ทุนจดทะเบียน

(๒) มูลค่าการจัดซื้อจัดจ้างเกิน ๑ ล้านบาท แต่ไม่เกิน ๕ ล้านบาท
ต้องมีทุนจดทะเบียนไม่ต่ำกว่า ๑ ล้านบาท

(๓) มูลค่าการจัดซื้อจัดจ้างเกิน ๕ ล้านบาท แต่ไม่เกิน ๑๐ ล้านบาท
ต้องมีทุนจดทะเบียนไม่ต่ำกว่า ๒ ล้านบาท

(๔) มูลค่าการจัดซื้อจัดจ้างเกิน ๑๐ ล้านบาท แต่ไม่เกิน ๒๐ ล้านบาท
ต้องมีทุนจดทะเบียนไม่ต่ำกว่า ๓ ล้านบาท

(๕) มูลค่าการจัดซื้อจัดจ้างเกิน ๒๐ ล้านบาท แต่ไม่เกิน ๖๐ ล้านบาท ต้องมีทุนจดทะเบียนไม่ต่ำกว่า ๘ ล้านบาท

(๖) มูลค่าการจัดซื้อจัดจ้างเกิน ๖๐ ล้านบาท แต่ไม่เกิน ๑๕๐ ล้านบาท ต้องมีทุนจดทะเบียนไม่ต่ำกว่า ๒๐ ล้านบาท

(๗) มูลค่าการจัดซื้อจัดจ้างเกิน ๑๕๐ ล้านบาท แต่ไม่เกิน ๓๐๐ ล้านบาท ต้องมีทุนจดทะเบียนไม่ต่ำกว่า ๖๐ ล้านบาท

(๘) มูลค่าการจัดซื้อจัดจ้างเกิน ๓๐๐ ล้านบาท แต่ไม่เกิน ๕๐๐ ล้านบาท ต้องมีทุนจดทะเบียนไม่ต่ำกว่า ๑๐๐ ล้านบาท

(๙) มูลค่าการจัดซื้อจัดจ้างเกิน ๕๐๐ ล้านบาทขึ้นไป ต้องมีทุนจดทะเบียนไม่ต่ำกว่า ๒๐๐ ล้านบาท

๓. สำหรับการจัดซื้อจัดจ้างครั้งหนึ่งที่มีวงเงินเกิน ๕๐๐,๐๐๐ บาทขึ้นไป กรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดา ให้พิจารณาจากหนังสือรับรองบัญชีเงินฝากไม่เกิน ๙๐ วัน ก่อนวันยื่นข้อเสนอ โดยต้องมีเงินฝากคงเหลือในบัญชีธนาคารเป็นมูลค่า ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง และหากเป็นผู้ชนะการจัดซื้อจัดจ้างหรือเป็นผู้ได้รับการคัดเลือกจะต้องแสดงหนังสือรับรองบัญชีเงินฝากที่มีมูลค่าดังกล่าวอีกครั้งหนึ่งในวันลงนามในสัญญา

๔. กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ สามารถดำเนินการได้ดังนี้

(๑) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย หรือบุคคลธรรมดาที่ถือสัญชาติไทย ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง จะเป็นสินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้าประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรอง หรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอไม่เกิน ๙๐ วัน

(๒) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศ หรือบุคคลธรรมดาที่มีถิ่นสัญชาติไทย ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง จะเป็นสินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์ และประกอบธุรกิจค้าประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อ

บริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ หรือเป็นสินเชื่อที่ธนาคารต่างประเทศหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้าประกัน ตามประกาศของธนาคารกลางต่างประเทศนั้น ตามรายชื่อบริษัทที่ธนาคารกลางต่างประเทศนั้นแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรอง หรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอไม่เกิน ๙๐ วัน

๕. กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศ หรือบุคคลธรรมดาที่มีได้ถือสัญชาติไทยตามข้อ ๒ ข้อ ๓ และข้อ ๔ (๒) มูลค่าจะต้องเป็นไปตามอัตราแลกเปลี่ยนเงินตราตามประกาศที่ธนาคารแห่งประเทศไทยกำหนด ในช่วงระหว่างวันที่เผยแพร่ประกาศ และเอกสารประกวดราคาในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (e - GP) จนถึงวันเสนอราคา

ทั้งนี้ ผู้ยื่นข้อเสนอจะต้องยื่นเอกสารที่แสดงให้เห็นถึงข้อมูลเกี่ยวกับมูลค่าสุทธิของกิจการแล้วแต่กรณี ประกอบกับเอกสารดังกล่าวจะต้องผ่านการรับรองตามระเบียบกระทรวงการต่างประเทศว่าด้วยการรับรองเอกสาร พ.ศ. ๒๕๓๙ และที่แก้ไขเพิ่มเติม กำหนด โดยจะต้องยื่นเอกสารดังกล่าวในวันยื่นข้อเสนอ หากผู้ยื่นข้อเสนอได้มีการยื่นเอกสารดังกล่าวมาพร้อมกับการยื่นข้อเสนอให้ถือว่าผู้ยื่นข้อเสนอรายนั้นยื่นเอกสารไม่ครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารประกวดราคา

(๕) สำเนาใบทะเบียนพาณิชย์ สำเนาใบสำคัญแสดงการจดทะเบียนทางหุ้นส่วนบริษัท สำเนาใบสำคัญแสดงการจดทะเบียนทางหุ้นส่วนจำกัด สำเนาใบทะเบียนภาษีมูลค่าเพิ่ม (ถ้ามี)

(๖) 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) หลักประกันการเสนอราคา ตามข้อ ๕
- (๒) สำเนาใบขึ้นทะเบียนผู้ประกอบการวิสาหกิจขนาดกลางและขนาดย่อม (SMEs) (ถ้ามี)
- (๓) ใบรับการรับรองมาตรฐานสากลด้านความมั่นคงปลอดภัยสารสนเทศ ISO 27001 (Information Security Management System หรือ ISMS) ที่ยังไม่หมดอายุ

(๔) แคลคูลัส เอกสาร หรือหนังสือคู่มือที่แสดงให้เห็นรูปแบบและรายละเอียดคุณสมบัติของอุปกรณ์ที่ยื่นเสนอราคาให้ครบถ้วนเพียงพอที่คณะกรรมการจะพิจารณาได้

(๕) ตารางเปรียบเทียบขอบเขตของงานตามรายการที่ปรากฏในขอบเขตของงานข้อที่ ๔ ให้ครบถ้วนทุกรายการ “พร้อมทำเครื่องหมายขีดเส้นใต้ หรือเครื่องหมายเน้นข้อความ และเขียนหมายเลขข้อกำกับในเอกสารอ้างอิงที่แสดงถึงข้อเสนอให้ถูกต้อง ตรงตามข้อเสนอทุกรายการ ทั้งนี้ขอบเขตของงานที่ผู้เสนอราคาเสนอในตารางเปรียบเทียบจะต้องตรงตามเอกสารอ้างอิงทุกรายการ เพื่อประกอบการพิจารณาของคณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์ และถือเป็นสาระสำคัญในการพิจารณา หากไม่ยื่นรายละเอียดดังกล่าวหรือยื่นแต่ไม่ถูกต้องครบถ้วนจะไม่ได้รับการพิจารณา” ตามตัวอย่างตารางในขอบเขตของงาน ข้อ ๑๑.๓

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

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

๔. การเสนอราคา

๔.๑ ผู้ยื่นข้อเสนอต้องยื่นข้อเสนอและเสนอราคาทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ตามที่กำหนดไว้ในเอกสารประกวดราคาอิเล็กทรอนิกส์นี้ โดยไม่มีเงื่อนไขใด ๆ ทั้งสิ้น และจะต้องกรอกข้อความให้ถูกต้องครบถ้วน พร้อมทั้งหลักฐานแสดงตัวตนและทำการยืนยันตัวตนของผู้ยื่นข้อเสนอโดยไม่ต้องแนบบใบเสนอราคาในรูปแบบ PDF File (Portable Document Format)

๔.๒ ในการเสนอราคาให้เสนอราคาเป็นเงินบาทและเสนอราคาได้เพียงครั้งเดียว และราคาเดียวโดยเสนอราคารวม ตามเงื่อนไขที่ระบุไว้ตามข้อ ๖.๒ ให้ถูกต้อง ทั้งนี้ ราคารวมที่เสนอจะต้องตรงกันทั้งตัวเลขและตัวหนังสือ ถ้าตัวเลขและตัวหนังสือไม่ตรงกัน ให้ถือตัวหนังสือเป็นสำคัญ โดยคิดราคารวมทั้งสิ้นซึ่งรวมค่าภาษีมูลค่าเพิ่ม ภาษีอากรอื่น ค่าขนส่ง ค่าจดทะเบียนและค่าใช้จ่ายอื่น ๆ ทั้งปวงไว้แล้ว

ราคาที่เสนอจะต้องเสนอกำหนดยื่นราคาไม่น้อยกว่า ๑๒๐ วัน นับถัดจากวันเสนอราคา โดยภายในกำหนดยื่นราคา ผู้ยื่นข้อเสนอต้องรับผิดชอบราคาที่ตนได้เสนอไว้และจะถอนการเสนอราคามีได้

๔.๓ ผู้ยื่นข้อเสนอต้องส่งแคตตาล็อก เอกสาร หรือหนังสือคู่มือที่แสดงให้เห็นรูปแบบและรายละเอียดคุณสมบัติของอุปกรณ์ที่ยื่นเสนอราคาให้ครบถ้วนเพียงพอที่คณะกรรมการจะพิจารณาได้ โดยให้ยื่นขณะเข้าเสนอราคา

๔.๔ ผู้ยื่นข้อเสนอต้องจัดทำตารางเปรียบเทียบขอบเขตของงานตามรายการที่ปรากฏในขอบเขตของงานข้อที่ ๔ ให้ครบถ้วนทุกรายการ “พร้อมทำเครื่องหมายขีดเส้นใต้ หรือเครื่องหมายเน้นข้อความ และเขียนหมายเลขข้อกำกับในเอกสารอ้างอิงที่แสดงถึงข้อเสนอให้ถูกต้องตรงตามข้อเสนอทุกรายการ ทั้งนี้ขอบเขตของงานที่ผู้เสนอราคาเสนอในตารางเปรียบเทียบจะต้องตรงตามเอกสารอ้างอิงทุกรายการ เพื่อประกอบการพิจารณาของคณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์ และถือเป็นสาระสำคัญในการพิจารณา หากไม่ยื่นรายละเอียดดังกล่าวหรือยื่นแต่ไม่ถูกต้องครบถ้วนจะไม่ได้รับการพิจารณา” โดยยื่นข้อเสนอขณะเข้าเสนอราคา ตามตัวอย่างตารางในขอบเขตของงาน
ข้อ ๑๑.๓

๔.๕ ผู้ยื่นข้อเสนอจะต้องเสนอกำหนดเวลาดำเนินการแล้วเสร็จไม่เกิน ๑,๑๐๑ วัน นับถัดจากวันที่ลงนามในสัญญา

๔.๖ ก่อนเสนอราคา ผู้ยื่นข้อเสนอควรตรวจสอบร่างสัญญา รายละเอียดขอบเขตของงาน ฯลฯ ให้ถี่ถ้วนและเข้าใจเอกสารประกวดราคาอิเล็กทรอนิกส์ทั้งหมดเสียก่อนที่จะตกลงยื่นข้อเสนอตามเงื่อนไข ในเอกสารประกวดราคาอิเล็กทรอนิกส์

๔.๗ ผู้ยื่นข้อเสนอจะต้องยื่นข้อเสนอและเสนอราคาทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ในวันที่ ๒๔ สิงหาคม ๒๕๖๙ ระหว่างเวลา ๐๙.๐๐ น. ถึง ๑๒.๐๐ น. และเวลาในการเสนอราคาให้ถือตามเวลาของระบบการจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์เป็นเกณฑ์ เมื่อพ้นกำหนดเวลายื่นข้อเสนอและเสนอราคาแล้ว จะไม่รับเอกสารการยื่นข้อเสนอ และการเสนอราคาใด ๆ โดยเด็ดขาด

๔.๘ ผู้ยื่นข้อเสนอต้องจัดทำเอกสารสำหรับใช้ในการเสนอราคาในรูปแบบไฟล์เอกสารประเภท PDF File (Portable Document Format) โดยผู้ยื่นข้อเสนอต้องเป็นผู้รับผิดชอบตรวจสอบความครบถ้วน ถูกต้อง และชัดเจนของเอกสาร PDF File ก่อนที่จะยืนยันการเสนอราคา แล้วจึงส่งข้อมูล (Upload) เพื่อเป็นการเสนอราคาให้แก่กรมผ่านทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์

๔.๙ คณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์จะดำเนินการตรวจสอบคุณสมบัติของผู้ยื่นข้อเสนอแต่ละรายว่า เป็นผู้ยื่นข้อเสนอที่มีผลประโยชน์ร่วมกันกับผู้ยื่นเสนอรายอื่นตามข้อ ๑.๕ (๑) หรือไม่ หากปรากฏว่าผู้ยื่นเสนอรายใดเป็นผู้ยื่นข้อเสนอที่มีผลประโยชน์ร่วมกันกับผู้ยื่นเสนอรายอื่น คณะกรรมการพิจารณาผลฯ จะตัดรายชื่อผู้ยื่นข้อเสนอที่มีผลประโยชน์ร่วมกันนั้น ออกจากการเป็นผู้ยื่นข้อเสนอ

หากปรากฏต่อคณะกรรมการพิจารณาผลฯ ว่า ก่อนหรือ ในขณะที่มีการพิจารณาข้อเสนอ มีผู้ยื่นข้อเสนอรายใดกระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมตามข้อ ๑.๕ (๒) และคณะกรรมการพิจารณาผลฯ เชื่อว่ามีการกระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรม คณะกรรมการพิจารณาผลฯ จะตัดรายชื่อผู้ยื่นข้อเสนอรายนั้นออกจากการเป็นผู้ยื่นข้อเสนอ และกรม จะพิจารณาลงโทษผู้ยื่นข้อเสนอดังกล่าวเป็นผู้ทำงาน เว้นแต่กรมจะพิจารณาเห็นว่าผู้ยื่นข้อเสนอรายนั้นมิใช่เป็นผู้ริเริ่มให้มีการกระทำได้ดังกล่าวและได้ให้ความร่วมมือเป็นประโยชน์ต่อการพิจารณาของกรม

๔.๑๐ ผู้ยื่นข้อเสนอจะต้องปฏิบัติ ดังนี้

- (๑) ปฏิบัติตามเงื่อนไขที่ระบุไว้ในเอกสารประกวดราคาอิเล็กทรอนิกส์
- (๒) ราคาที่เสนอจะต้องเป็นราคาที่รวมภาษีมูลค่าเพิ่ม และภาษีอื่น ๆ (ถ้ามี) รวมค่าใช้จ่ายที่ส่งไปเรียบร้อยแล้ว
- (๓) ผู้ยื่นข้อเสนอจะต้องลงทะเบียนเพื่อเข้าสู่กระบวนการเสนอราคาตามวัน เวลา ที่กำหนด
- (๔) ผู้ยื่นข้อเสนอจะถอนการเสนอราคาที่เสนอแล้วไม่ได้
- (๕) ผู้ยื่นข้อเสนอต้องศึกษาและทำความเข้าใจในระบบและวิธีการเสนอราคา

ด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ของกรมบัญชีกลางที่แสดงไว้ในเว็บไซต์ www.gprocurement.go.th

๔.๑๑ ผู้ยื่นข้อเสนอที่เป็นผู้ชนะการเสนอราคาต้องจัดทำแผนการใช้พัสดุที่ผลิตภายในประเทศ โดยยื่นให้หน่วยงานของรัฐภายใน ๖๐ วัน นับถัดจากวันลงนามในสัญญา เว้นแต่กรณีที่ยังระยะเวลาดำเนินการตามสัญญาไม่เกิน ๖๐ วัน

๔.๑๒ คู่สัญญาต้องจัดทำแผนการทำงานมาให้ภายใน ๓๐ วัน นับถัดจากวันลงนามในสัญญา เว้นแต่เป็นกรณีสัญญาที่มีอายุไม่เกิน ๙๐ วัน หรือกรณีการจ้างซึ่งสัญญาหรือบันทึกข้อตกลงเป็นหนังสือที่มีวงเงินไม่เกิน ๕๐๐,๐๐๐ บาท ทั้งนี้ แผนการทำงานดังกล่าวให้ถือเป็นเอกสารส่วนหนึ่งของสัญญา

๕. หลักประกันการเสนอราคา

ผู้ยื่นข้อเสนอต้องวางหลักประกันการเสนอราคาพร้อมกับการเสนอราคาทางระบบการจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ โดยใช้หลักประกันอย่างหนึ่งอย่างใดดังต่อไปนี้จำนวน ๑,๘๙๔,๖๘๐.๐๐ บาท (หนึ่งล้านแปดแสนเก้าหมื่นสี่พันหกร้อยแปดสิบบาทถ้วน)

๕.๑ เงินสด

๕.๒ หนังสือค้ำประกันอิเล็กทรอนิกส์ของธนาคารภายในประเทศตามแบบที่คณะกรรมการนโยบายกำหนด

๕.๓ พันธบัตรรัฐบาลไทย

๕.๔ หนังสือคำประกันของบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้าประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยอนุโลมให้ใช้ตามตัวอย่างหนังสือคำประกันของธนาคารที่คณะกรรมการนโยบายกำหนด

กรณีที่ผู้ยื่นข้อเสนอ นำพันธบัตรรัฐบาลไทยหรือหนังสือคำประกันของบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ มาวางเป็นหลักประกันการเสนอราคาจะต้องส่งต้นฉบับเอกสารดังกล่าวมาให้กรมตรวจสอบความถูกต้องในวันที่ ๓๑ สิงหาคม ๒๕๖๔ ระหว่างเวลา ๐๘.๓๐ น. ถึง ๑๖.๓๐ น.

กรณีที่ผู้ยื่นข้อเสนอประสงค์จะวางหลักประกันการเสนอราคาเป็นเงินสด ให้ผู้ยื่นข้อเสนอ ดำเนินการชำระเงินผ่านช่องทางการชำระเงิน ดังนี้

ผ่านบริการรับชำระเงิน (Bill Payment) ผ่านระบบ KTB Corporate Online ตามใบแจ้งการชำระเงิน ที่แนบมาพร้อมกับเอกสารเชิญชวนนี้

และส่งหลักฐานการชำระเงินกับธนาคาร พร้อมทั้งแบบแจ้งความประสงค์ชำระเงิน ค่าหลักประกันการเสนอราคา (เฉพาะกรณีที่มิใช่หลักประกันการเสนอราคาหลายรายการพิจารณา) มาให้กรมตรวจสอบความถูกต้อง โดยยื่นมาพร้อมกับการยื่นข้อเสนอผ่านระบบ e-GP โดยการชำระเงิน และส่งหลักฐานการชำระเงินให้ดำเนินการในวันและเวลาที่หน่วยงานของรัฐกำหนดให้เป็นวันและเวลาเสนอราคาเท่านั้น

กรณีที่ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ "กิจการร่วมค้า" ประสงค์จะใช้หนังสือคำประกันอิเล็กทรอนิกส์ของธนาคารในประเทศเป็นหลักประกันการเสนอราคาให้ระบุชื่อผู้เข้าร่วมค้ารายที่สัญญาร่วมค้ากำหนดให้เป็นผู้เข้ายื่นข้อเสนอกับหน่วยงานของรัฐเป็นผู้ยื่นข้อเสนอ

หลักประกันการเสนอราคาตามข้อนี้ กรมจะคืนให้ผู้ยื่นข้อเสนอหรือผู้ค้าประกันภายใน ๑๕ วัน นับถัดจากวันที่กรมได้พิจารณาเห็นชอบรายงานผลคัดเลือกผู้ชนะการประกวดราคาเรียบร้อยแล้ว เว้นแต่ผู้ยื่นเสนอรายที่คัดเลือกไว้ซึ่งเสนอราคาต่ำสุดหรือได้คะแนนรวมสูงสุดไม่เกิน ๓ ราย ให้คืนได้ต่อเมื่อได้ทำสัญญาหรือข้อตกลง หรือผู้ยื่นข้อเสนอได้พ้นจากข้อผูกพันแล้ว

การคืนหลักประกันการเสนอราคา ไม่ว่าในกรณีใด ๆ จะคืนให้โดยไม่มีดอกเบี้ย

๖. หลักเกณฑ์และสิทธิในการพิจารณา

๖.๑ ในการพิจารณาผลการยื่นข้อเสนอประกวดราคาอิเล็กทรอนิกส์ครั้งนี้ กรมจะพิจารณาตัดสินโดยใช้หลักเกณฑ์ราคา

๖.๒ การพิจารณาผู้ชนะการยื่นข้อเสนอ

กรณีใช้หลักเกณฑ์ราคาในการพิจารณาผู้ชนะการยื่นข้อเสนอ กรมจะพิจารณาจากราคารวม

๖.๓ หากผู้ยื่นข้อเสนอรายใดมีคุณสมบัติไม่ถูกต้องตามข้อ ๒ หรือยื่นหลักฐานการยื่นข้อเสนอไม่ถูกต้อง หรือไม่ครบถ้วนตามข้อ ๓ หรือยื่นข้อเสนอไม่ถูกต้องตามข้อ ๔ คณะกรรมการพิจารณาผลฯ จะไม่รับพิจารณาข้อเสนอของผู้ยื่นข้อเสนอรายนั้น เว้นแต่ ผู้ยื่นข้อเสนอรายใดเสนอเอกสารทางเทคนิคหรือขอบเขตงานที่จะจ้างไม่ครบถ้วน หรือเสนอรายละเอียดแตกต่างไปจากเงื่อนไขที่กรมกำหนดไว้ในประกาศและเอกสารประกวดราคาอิเล็กทรอนิกส์ ในส่วนที่มีสาระสำคัญและความแตกต่างนั้นไม่มีผลทำให้เกิดการได้เปรียบเสียเปรียบต่อผู้ยื่นข้อเสนอรายอื่น หรือเป็นการผิดพลาดเล็กน้อย คณะกรรมการพิจารณาผลฯ อาจพิจารณาผ่อนปรนการตัดสิทธิ ผู้ยื่นข้อเสนอรายนั้น

๖.๔ กรมสงวนสิทธิไม่พิจารณาข้อเสนอของผู้ยื่นข้อเสนอโดยไม่มีการผ่อนผันในกรณีดังต่อไปนี้

(๑) ไม่กรอกชื่อผู้ยื่นข้อเสนอในการเสนอราคาทางระบบจัดซื้อจัดจ้างด้วยอิเล็กทรอนิกส์

(๒) เสนอรายละเอียดแตกต่างไปจากเงื่อนไขที่กำหนดในเอกสารประกวดราคาอิเล็กทรอนิกส์ที่เป็นสาระสำคัญ หรือมีผลทำให้เกิดความได้เปรียบเสียเปรียบแก่ผู้ยื่นข้อเสนอรายอื่น

๖.๕ ในการตัดสินใจการประกวดราคาอิเล็กทรอนิกส์หรือในการทำสัญญา คณะกรรมการพิจารณาผลฯ หรือกรม มีสิทธิให้ผู้ยื่นข้อเสนอชี้แจงข้อเท็จจริงเพิ่มเติมได้ กรมมีสิทธิที่จะไม่รับข้อเสนอ ไม่รับราคา หรือไม่ทำสัญญา หากข้อเท็จจริงดังกล่าวไม่เหมาะสมหรือไม่ถูกต้อง

๖.๖ กรมทรงไว้ซึ่งสิทธิที่จะไม่รับราคาต่ำสุด หรือราคาหนึ่งราคาใด หรือราคาที่เสนอทั้งหมดก็ได้ และอาจพิจารณาเลือกจ้างในจำนวน หรือขนาด หรือเฉพาะรายการหนึ่งรายการใด หรืออาจยกเลิกการประกวดราคาอิเล็กทรอนิกส์โดยไม่พิจารณาจัดจ้างเลยก็ได้ สุดแต่จะพิจารณา ทั้งนี้ เพื่อประโยชน์ของทางราชการเป็นสำคัญ และให้ถือว่า การตัดสินใจของกรมเป็นเด็ดขาด ผู้ยื่นข้อเสนอจะเรียกร้องค่าใช้จ่าย หรือค่าเสียหายใด ๆ มิได้ รวมทั้งกรมจะพิจารณายกเลิกการประกวดราคาอิเล็กทรอนิกส์และลงโทษผู้ยื่นข้อเสนอเป็นผู้ทำงาน ไม่ว่าจะเป็นผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกหรือไม่ก็ตาม หากมีเหตุที่เชื่อได้ว่า การยื่นข้อเสนอกระทำการโดยไม่สุจริต เช่น การเสนอเอกสารอันเป็นเท็จ หรือใช้ข้อมูลคลลธรรมดา หรือนิติบุคคลอื่นมายื่นข้อเสนอแทน เป็นต้น

ในกรณีที่ผู้ยื่นข้อเสนอรายใดเสนอราคาต่ำสุด เสนอราคาต่ำจนคาดหมายได้ว่า ไม่อาจดำเนินงานตามเอกสารประกวดราคาอิเล็กทรอนิกส์ได้ คณะกรรมการพิจารณาผลฯ หรือกรมจะให้ผู้ยื่นข้อเสนอชี้แจงและแสดงหลักฐานที่ทำให้เชื่อได้ว่า ผู้ยื่นข้อเสนอสามารถดำเนินการตามเอกสารประกวดราคาอิเล็กทรอนิกส์ให้เสร็จสมบูรณ์ หากคำชี้แจงไม่เป็นที่รับฟังได้ กรมมีสิทธิที่จะไม่รับข้อเสนอ หรือไม่รับราคาของผู้ยื่นข้อเสนอรายนั้น ทั้งนี้ ผู้ยื่นข้อเสนอดังกล่าวไม่มีสิทธิเรียกร้องค่าใช้จ่ายหรือค่าเสียหายใด ๆ จากกรม

๖.๗ ก่อนลงนามในสัญญา กรมอาจประกาศยกเลิกการประกวดราคาอิเล็กทรอนิกส์ หากปรากฏว่ามีการกระทำที่เข้าลักษณะผู้ยื่นข้อเสนอที่ชนะการประกวดราคาหรือที่ได้รับการคัดเลือก มีผลประโยชน์ร่วมกัน หรือมีส่วนได้เสียกับผู้ยื่นข้อเสนอรายอื่น หรือขัดขวางการแข่งขันอย่างเป็นธรรม หรือสมยอมกันกับผู้ยื่นข้อเสนอรายอื่น หรือเจ้าหน้าที่ในการเสนอราคา หรือสื่อว่ากระทำการทุจริตอื่นใด ในการเสนอราคา

๖.๘ หากผู้ยื่นข้อเสนอซึ่งเป็นผู้ประกอบการ SMEs เสนอราคาสูงกว่าราคาต่ำสุดของผู้ยื่นข้อเสนอรายอื่นที่ไม่เกินร้อยละ ๑๐ ให้จัดซื้อจัดจ้างกับผู้ประกอบการ SMEs ดังกล่าว โดยจัดเรียงลำดับผู้ยื่นข้อเสนอซึ่งเป็นผู้ประกอบการ SMEs ซึ่งเสนอราคาสูงกว่าราคาต่ำสุดของผู้ยื่นข้อเสนอรายอื่นไม่เกินร้อยละ ๑๐ ที่จะเรียกมาทำสัญญาไม่เกิน ๓ ราย

ผู้ยื่นข้อเสนอที่เป็นกิจการร่วมค้าที่จะได้สิทธิตามวรรคหนึ่ง ผู้เข้าร่วมค้าทุกราย จะต้องเป็นผู้ประกอบการ SMEs

ทั้งนี้ ผู้ประกอบการ SMEs ที่จะได้แต้มต่อด้านราคาตามวรรคหนึ่ง จะต้อง มีวงเงินสัญญาสะสมตามปีปฏิทินรวมกับราคาที่เสนอในครั้งแล้ว มีมูลค่ารวมกันไม่เกินมูลค่าของรายได้ตามขนาดที่ขึ้นทะเบียนไว้กับ สสว.

๖.๙ หากผู้ยื่นข้อเสนอซึ่งมิใช่ผู้ประกอบการ SMEs แต่เป็นบุคคลธรรมดาที่ถือสัญชาติไทยหรือนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยเสนอราคาสูงกว่าราคาต่ำสุดของผู้ยื่นข้อเสนอซึ่งเป็นผู้ประกอบการ SMEs ที่มีได้ถือสัญชาติไทยหรือนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายของต่างประเทศไม่เกินร้อยละ ๓ ให้จัดซื้อจัดจ้างกับบุคคลธรรมดาที่ถือสัญชาติไทยหรือนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยดังกล่าว

ผู้ยื่นข้อเสนอที่เป็นกิจการร่วมค้าที่จะได้สิทธิตามวรรคหนึ่ง ผู้เข้าร่วมค้าทุกราย จะต้องเป็นบุคคลธรรมดาที่ถือสัญชาติไทยหรือนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย

๗. การทำสัญญาจ้าง

ผู้ชนะการประกวดราคาอิเล็กทรอนิกส์จะต้องทำสัญญาจ้างตามแบบสัญญา ดังระบุในข้อ ๑.๓ หรือทำข้อตกลงเป็นหนังสือกับกรม ภายใน ๑๐ วัน นับถัดจากวันที่ได้รับแจ้ง และ จะต้องวางหลักประกันสัญญาเป็นจำนวนเงินเท่ากับร้อยละ ๕ ของราคาค่าจ้างที่ประกวดราคาอิเล็กทรอนิกส์ได้ ให้กรมยึดถือไว้ในขณะทำสัญญา โดยใช้หลักประกันอย่างหนึ่งอย่างใดดังต่อไปนี้

๗.๑ เงินสด

๗.๒ เช็คหรือตราฟัที่ธนาคารสั่งจ่ายให้แก่กรม ซึ่งเป็นเช็คหรือตราฟัลงวันที่ที่ใช้เช็คหรือตราฟันั้นชำระต่อเจ้าหน้าที่ในวันทำสัญญา หรือก่อนวันนั้น ไม่เกิน ๓ วันทำการ

๗.๓ หนังสือค้ำประกันของธนาคารภายในประเทศ ตามตัวอย่างที่คณะกรรมการนโยบายกำหนด ดังระบุในข้อ ๑.๔ (๒) หรือจะเป็นหนังสือค้ำประกันอิเล็กทรอนิกส์ตามวิธีการที่กรมบัญชีกลาง กำหนด

๗.๔ หนังสือค้ำประกันของบริษัทเงินทุน หรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้ำประกัน ตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยอนุโลมให้ใช้ตามตัวอย่างหนังสือค้ำประกันของธนาคารที่คณะกรรมการนโยบายกำหนด ดังระบุในข้อ ๑.๔ (๒)

๗.๕ พันธบัตรรัฐบาลไทย

หลักประกันนี้จะคืนให้ โดยไม่มีดอกเบี้ยภายใน ๑๕ วันนับถัดจากวันที่ผู้ชนะการประกวดราคาอิเล็กทรอนิกส์ (ผู้รับจ้าง) พ้นจากข้อผูกพันตามสัญญาจ้างแล้ว
หลักประกันนี้จะคืนให้ โดยไม่มีดอกเบี้ย ตามอัตราส่วนของงานจ้างซึ่งกรมได้รับมอบไว้แล้ว

๘. ค่าจ้างและการจ่ายเงิน

กรมจะจ่ายค่าจ้างซึ่งได้รวมภาษีมูลค่าเพิ่มตลอดจนภาษีอากรอื่น ๆ และค่าใช้จ่ายทั้งปวงด้วยแล้วให้แก่ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกให้เป็นผู้รับจ้าง โดยแบ่งออกเป็น ๑๓ งวด ดังนี้

งวดที่ ๑ เป็นจำนวนเงินในอัตราร้อยละ ๑๕ ของค่าจ้างทั้งหมดตามสัญญา เมื่อผู้รับจ้างได้ปฏิบัติงานและส่งมอบงาน งวดที่ ๑ ตามขอบเขตของงาน ข้อ ๘ ให้แล้วเสร็จภายใน ๖๑ วัน และกรมได้ตรวจรับงานจ้างเรียบร้อยแล้ว

งวดที่ ๒ เป็นจำนวนเงินในอัตราร้อยละ ๕ ของค่าจ้างทั้งหมดตามสัญญา เมื่อผู้รับจ้างได้ปฏิบัติงานและส่งมอบงาน งวดที่ ๒ ตามขอบเขตของงาน ข้อ ๘ ให้แล้วเสร็จภายใน ๙๖ วัน และกรมได้ตรวจรับงานจ้างเรียบร้อยแล้ว

งวดที่ ๓ เป็นจำนวนเงินในอัตราร้อยละ ๓ ของค่าจ้างทั้งหมดตามสัญญา เมื่อผู้รับจ้างได้ปฏิบัติงานและส่งมอบงาน งวดที่ ๓ ตามขอบเขตของงาน ข้อ ๘ ให้แล้วเสร็จภายใน ๑๘๖ วัน และกรมได้ตรวจรับงานจ้างเรียบร้อยแล้ว

งวดที่ ๔ เป็นจำนวนเงินในอัตราร้อยละ ๒ ของค่าจ้างทั้งหมดตามสัญญา เมื่อผู้รับจ้างได้ปฏิบัติงานและส่งมอบงาน งวดที่ ๔ ตามขอบเขตของงาน ข้อ ๘ ให้แล้วเสร็จภายใน ๒๗๘ วัน และกรมได้ตรวจรับงานจ้างเรียบร้อยแล้ว

งวดที่ ๕ เป็นจำนวนเงินในอัตราร้อยละ ๑๕ ของค่าจ้างทั้งหมดตามสัญญา เมื่อผู้รับจ้างได้ปฏิบัติงานและส่งมอบงาน งวดที่ ๕ ตามขอบเขตของงาน ข้อ ๘ ให้แล้วเสร็จภายใน ๓๗๐ วัน และกรมได้ตรวจรับงานจ้างเรียบร้อยแล้ว

งวดที่ ๖ เป็นจำนวนเงินในอัตราร้อยละ ๕ ของค่าจ้างทั้งหมดตามสัญญา เมื่อผู้รับจ้างได้ปฏิบัติงานและส่งมอบงาน งวดที่ ๖ ตามขอบเขตของงาน ข้อ ๘ ให้แล้วเสร็จภายใน ๔๖๑ วัน และกรมได้ตรวจรับงานจ้างเรียบร้อยแล้ว

งวดที่ ๗ เป็นจำนวนเงินในอัตราร้อยละ ๕ ของค่าจ้างทั้งหมดตามสัญญา เมื่อผู้รับจ้างได้ปฏิบัติงานและส่งมอบงาน งวดที่ ๗ ตามขอบเขตของงาน ข้อ ๘ ให้แล้วเสร็จภายใน ๕๕๒ วัน และกรมได้ตรวจรับงานจ้างเรียบร้อยแล้ว

งวดที่ ๘ เป็นจำนวนเงินในอัตราร้อยละ ๕ ของค่าจ้างทั้งหมดตามสัญญา เมื่อผู้รับจ้างได้ปฏิบัติงานและส่งมอบงาน งวดที่ ๘ ตามขอบเขตของงาน ข้อ ๘ ให้แล้วเสร็จภายใน ๖๔๔ วัน และกรมได้ตรวจรับงานจ้างเรียบร้อยแล้ว

งวดที่ ๙ เป็นจำนวนเงินในอัตราร้อยละ ๑๕ ของค่าจ้างทั้งหมดตามสัญญา เมื่อผู้รับจ้างได้ปฏิบัติงานและส่งมอบงาน งวดที่ ๙ ตามขอบเขตของงาน ข้อ ๘ ให้แล้วเสร็จภายใน ๗๓๖ วัน และกรมได้ตรวจรับงานจ้างเรียบร้อยแล้ว

งวดที่ ๑๐ เป็นจำนวนเงินในอัตราร้อยละ ๕ ของค่าจ้างทั้งหมดตามสัญญา เมื่อผู้รับจ้างได้ปฏิบัติงานและส่งมอบงาน งวดที่ ๑๐ ตามขอบเขตของงาน ข้อ ๘ ให้แล้วเสร็จภายใน ๘๒๗ วัน และกรมได้ตรวจรับงานจ้างเรียบร้อยแล้ว

งวดที่ ๑๑ เป็นจำนวนเงินในอัตราร้อยละ ๕ ของค่าจ้างทั้งหมดตามสัญญา เมื่อผู้รับจ้างได้ปฏิบัติงานและส่งมอบงาน งวดที่ ๑๑ ตามขอบเขตของงาน ข้อ ๘ ให้แล้วเสร็จภายใน ๙๑๗ วัน และกรมได้ตรวจรับงานจ้างเรียบร้อยแล้ว

งวดที่ ๑๒ เป็นจำนวนเงินในอัตราร้อยละ ๕ ของค่าจ้างทั้งหมดตามสัญญา เมื่อผู้รับจ้างได้ปฏิบัติงานและส่งมอบงาน งวดที่ ๑๒ ตามขอบเขตของงาน ข้อ ๘ ให้แล้วเสร็จภายใน ๑,๐๐๙ วัน และกรมได้ตรวจรับงานจ้างเรียบร้อยแล้ว

งวดที่ ๑๓ (งวดสุดท้าย) เป็นจำนวนเงินในอัตราร้อยละ ๑๕ ของค่าจ้างทั้งหมดตามสัญญา เมื่อผู้รับจ้างได้ปฏิบัติงานและส่งมอบงาน งวดที่ ๑๓ (งวดสุดท้าย) ตามขอบเขตของงาน ข้อ ๘ และงานทั้งหมดให้แล้วเสร็จเรียบร้อยแล้วตามสัญญาภายใน ๑,๑๐๑ วัน และกรมได้ตรวจรับมอบงานจ้างเรียบร้อยแล้ว

๙. อัตราค่าปรับ

ค่าปรับตามแบบสัญญาจ้างแนบท้ายเอกสารประกวดราคาอิเล็กทรอนิกส์นี้ หรือข้อตกลงจ้างเป็นหนังสือจะกำหนด ดังนี้

๙.๑ กรณีที่ผู้รับจ้างนำงานที่รับจ้างไปจ้างช่วงให้ผู้อื่นทำอีกทอดหนึ่งโดยไม่ได้รับอนุญาตจากกรม จะกำหนดค่าปรับสำหรับการฝ่าฝืนดังกล่าวเป็นจำนวนร้อยละ ๑๐ (สิบ) ของวงเงินของงานจ้างช่วงนั้น

๙.๒ กรณีที่ผู้รับจ้างปฏิบัติผิดสัญญาจ้างนอกเหนือจากข้อ ๙.๑ และข้อ ๙.๓ จะกำหนดค่าปรับเป็นรายวัน ในอัตราร้อยละ ๐.๑๐ (ศูนย์จุดหนึ่งศูนย์) ของราคาค่าจ้างทั้งหมดในแต่ละงวด โดยกำหนดค่าปรับเป็นรายงวด

๙.๓ กรณีการให้บริการระบบและอุปกรณ์ในโครงการ หากเกิดความเสียหาย ชำรุดบกพร่อง หรือไม่สามารถใช้งานทั้งหมดหรือเพียงบางส่วน ผู้รับจ้างต้องจัดการซ่อมแก้ไขให้แล้วเสร็จภายในระยะเวลาที่กำหนดไว้ในขอบเขตของงานข้อ ๑๒.๓ รวมถึงหากไม่สามารถให้บริการได้ตามระดับการให้บริการ (Service Level Agreement) ที่กำหนดในขอบเขตของงานข้อ ๑๒.๖ และข้อ ๑๒.๗ ผู้รับจ้างจะต้องชำระค่าปรับให้แก่สำนักเลขาธิการนายกรัฐมนตรี เป็นรายวันในอัตราร้อยละ ๐.๑๐ ของราคางานจ้างทั้งหมดตามสัญญา ยกเว้นในขอบเขตของงานข้อ ๑๒.๓.๑ คิดอัตราค่าปรับชั่วโมงละ ๕๐๐ บาท เศษของชั่วโมงคิดเป็น ๑ ชั่วโมง

๑๐. การรับประกันความชำรุดบกพร่อง

ผู้ชนะการประกวดราคาอิเล็กทรอนิกส์ซึ่งได้ทำสัญญาจ้างตามแบบดังระบุในข้อ ๑.๓ หรือทำข้อตกลงจ้างเป็นหนังสือ แล้วแต่กรณี จะต้องรับประกันความชำรุดบกพร่องของงานจ้างที่เกิดขึ้นภายในระยะเวลาไม่น้อยกว่า ๓ ปี นับถัดจากวันที่กรมได้รับมอบงาน โดยต้องรับผิดชอบซ่อมแซมแก้ไขให้ใช้งานได้ดังเดิมภายใน ๖ วัน นับถัดจากวันที่ได้รับแจ้งความชำรุดบกพร่อง รายละเอียดตามขอบเขตของงานข้อ ๑๒

๑๑. ข้อสงวนสิทธิ์ในการยื่นข้อเสนอและอื่น ๆ

๑๑.๑ เงินค่าจ้างสำหรับงานจ้างครั้งนี้ ได้มาจากเงินงบประมาณประจำปี พ.ศ. ๒๕๖๙ - ๒๕๗๒ ผูกพันงบประมาณ ๔ ปี

๑๑.๒ เมื่อกรมได้คัดเลือกผู้ยื่นข้อเสนอรายใดให้เป็นผู้รับจ้าง และได้ตกลงจ้างตามการประกวดราคาอิเล็กทรอนิกส์แล้ว ถ้าผู้รับจ้างจะต้องสั่งหรือนำสิ่งของมาเพื่องานจ้างดังกล่าวเข้ามาจากต่างประเทศ และของนั้นต้องนำเข้ามาโดยทางเรือในเส้นทางที่มีเรือไทยเดินอยู่ และสามารถให้บริการรับขนได้ตามที่รัฐมนตรีว่าการกระทรวงคมนาคมประกาศกำหนด ผู้ยื่นข้อเสนอซึ่งเป็นผู้รับจ้างจะต้องปฏิบัติตามกฎหมายว่าด้วยการส่งเสริมการพาณิชย์ ดังนี้

(๑) แจ้งการสั่งหรือนำสิ่งของดังกล่าวเข้ามาจากต่างประเทศ ต่อกรมเจ้าท่าภายใน ๗ วัน นับตั้งแต่วันที่ผู้รับจ้างสั่งหรือซื้อของจากต่างประเทศ เว้นแต่เป็นของที่รัฐมนตรีว่าการกระทรวงคมนาคมประกาศยกเว้นให้บรรทุกโดยเรืออื่นได้

(๒) จัดการให้สิ่งของดังกล่าวบรรทุกโดยเรือไทย หรือเรือที่มีสิทธิเช่นเดียวกับเรือไทย จากต่างประเทศมายังประเทศไทย เว้นแต่จะได้รับอนุญาตจากกรมเจ้าท่า ให้บรรทุกสิ่งของนั้นโดยเรืออื่นที่มีใช้เรือไทย ซึ่งจะต้องได้รับอนุญาตเช่นนั้นก่อนบรรทุกของลงเรืออื่น หรือเป็นของที่รัฐมนตรีว่าการกระทรวงคมนาคมประกาศยกเว้นให้บรรทุกโดยเรืออื่น

(๓) ในกรณีที่ไม่ปฏิบัติตาม (๑) หรือ (๒) ผู้รับจ้างจะต้องรับผิดชอบตามกฎหมายว่าด้วยการส่งเสริมการพาณิชย์

๑๑.๓ ผู้ยื่นข้อเสนอซึ่งกรมได้คัดเลือกแล้ว ไม่ไปทำสัญญา หรือข้อตกลงจ้างเป็นหนังสือ ภายในเวลาที่กำหนดดังระบุไว้ในข้อ ๗ กรมจะริบหลักประกันการยื่นข้อเสนอ หรือเรียกร่องจากผู้ออกหนังสือ คำประกันการยื่นข้อเสนอทันที และอาจพิจารณาเรียกร่องให้ชดใช้ความเสียหายอื่น (ถ้ามี) รวมทั้งจะพิจารณา ให้เป็นผู้ทำงานตามระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ

๑๑.๔ กรมสงวนสิทธิ์ที่จะแก้ไขเพิ่มเติมเงื่อนไข หรือข้อกำหนดในแบบสัญญาหรือ ข้อตกลงจ้างเป็นหนังสือให้เป็นไปตามความเห็นของสำนักงานอัยการสูงสุด (ถ้ามี)

๑๑.๕ ในกรณีที่เอกสารแนบท้ายเอกสารประกวดราคาอิเล็กทรอนิกส์นี้ มีความขัด หรือแย้งกัน ผู้ยื่นข้อเสนอจะต้องปฏิบัติตามคำวินิจฉัยของกรม คำวินิจฉัยดังกล่าวให้ถือเป็นที่สุด และ ผู้ยื่นข้อเสนอไม่มีสิทธิเรียกร่องค่าใช้จ่ายใด ๆ เพิ่มเติม

๑๑.๖ กรมอาจประกาศยกเลิกการจัดจ้างในกรณีต่อไปนี้ได้ โดยที่ผู้ยื่นข้อเสนอ จะเรียกร่องค่าเสียหายใด ๆ จากกรมไม่ได้

(๑) กรมไม่ได้รับการจัดสรรเงินที่จะใช้ในการจัดจ้างหรือได้รับจัดสรร แต่ไม่เพียงพอที่จะทำการจัดจ้างครั้งนี้ต่อไป

(๒) มีการกระทำที่เข้าลักษณะผู้ยื่นข้อเสนอที่ชนะการจัดจ้างหรือที่ได้รับการ คัดเลือก มีผลประโยชน์ร่วมกัน หรือมีส่วนได้เสียกับผู้ยื่นข้อเสนอรายอื่น หรือขัดขวางการแข่งขัน อย่างเป็นธรรม หรือสมยอมกันกับผู้ยื่นข้อเสนอรายอื่น หรือเจ้าหน้าที่ในการเสนอราคา หรือถือว่ากระทำการ ทุจริตอื่นใด ในการเสนอราคา

(๓) การทำการจัดจ้างครั้งนี้ต่อไปอาจก่อให้เกิดความเสียหายแก่กรม หรือกระทบต่อประโยชน์สาธารณะ

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

๑๑.๗ ผู้ยื่นข้อเสนอจะต้องเลือกช่องทางการอุทธรณ์และช่องทางการรับหนังสือ แจ้งตอบผลการพิจารณาอุทธรณ์ไว้ตั้งแต่ขั้นตอนการยื่นข้อเสนอ และหากผู้ยื่นข้อเสนอมีความประสงค์ ที่จะอุทธรณ์ผลการประกาศผู้ชนะการจัดซื้อจัดจ้าง จะต้องยื่นอุทธรณ์และรับหนังสือแจ้งตอบการพิจารณา อุทธรณ์ผ่านช่องทางที่ได้เลือกไว้เท่านั้น

๑๒. การปฏิบัติตามกฎหมายและระเบียบ

ในระหว่างระยะเวลาการจ้าง ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกให้เป็นผู้รับจ้างต้องปฏิบัติ ตามหลักเกณฑ์ที่กฎหมายและระเบียบได้กำหนดไว้โดยเคร่งครัด

๑๓. การประเมินผลการปฏิบัติงานของผู้ประกอบการ

กรม สามารถนำผลการปฏิบัติงานแล้วเสร็จตามสัญญาของผู้ยื่นข้อเสนอ
ที่ได้รับการคัดเลือกให้เป็นผู้รับจ้างเพื่อนำมาประเมินผลการปฏิบัติงานของผู้ประกอบการ
ทั้งนี้ หากผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกไม่ผ่านเกณฑ์ที่กำหนดจะถูกระงับ
การยื่นข้อเสนอหรือทำสัญญากับกรม ไว้ชั่วคราว



ขอบเขตของงาน (Terms of Reference: TOR)

จ้างบริหารจัดการระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักเลขาธิการนายกรัฐมนตรี

1. ความเป็นมา

ในปีงบประมาณ พ.ศ. 2563 ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.) ได้ดำเนินโครงการปรับปรุงประสิทธิภาพของระบบเครือข่ายคอมพิวเตอร์ไร้สายของสำนักเลขาธิการนายกรัฐมนตรี ซึ่งเป็นการดำเนินการตามแผนปฏิบัติการดิจิทัลระยะ 4 ปี (พ.ศ. 2562 - 2565) ของสำนักเลขาธิการนายกรัฐมนตรี ในยุทธศาสตร์ที่ 1 เรื่อง “การยกระดับโครงสร้างพื้นฐาน” เพื่อพัฒนาโครงสร้างพื้นฐานเทคโนโลยีดิจิทัลที่ทันสมัย และเพิ่มประสิทธิภาพการรักษาความมั่นคงปลอดภัยของเทคโนโลยีดิจิทัล โดยโครงการดังกล่าวมีอุปกรณ์ และระบบรักษาความปลอดภัยระบบเครือข่ายที่สำคัญ ใช้สำหรับป้องกันการบุกรุกเข้ามาในระบบ โดยผู้ไม่หวังดี และบุคคลภายนอกที่ไม่ได้รับอนุญาต ประกอบด้วย 1) ระบบรักษาความปลอดภัยระบบเครือข่ายระดับแอปพลิเคชัน (Application Firewall) จำนวน 2 ระบบ ทำหน้าที่ป้องกันการบุกรุกและภัยคุกคามที่เกิดขึ้นบนระบบเครือข่าย รวมถึงการบริหารจัดการสิทธิ์ผู้ใช้งานเพื่อควบคุมการเข้าถึง และการเข้าใช้งานระบบเครือข่ายของบุคลากร เจ้าหน้าที่ และผู้มาติดต่อราชการ ภายในสำนักเลขาธิการนายกรัฐมนตรี 2) ระบบวิเคราะห์ตรวจจับภัยคุกคามทางด้านไซเบอร์อัตโนมัติ และรักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์แบบรวมศูนย์ จำนวน 1 ระบบ ทำหน้าที่จัดเก็บ และรวบรวมข้อมูล เพื่อวิเคราะห์เหตุการณ์การโจมตีที่เกิดขึ้นแบบรวมศูนย์ และ 3) ระบบป้องกันการโจมตีผ่านช่องโหว่ซอฟต์แวร์สำหรับเครื่องคอมพิวเตอร์ลูกข่าย จำนวน 1 ระบบ ทำหน้าที่ป้องกันการโจมตีและเผื่อระวังพฤติกรรมที่ผิดปกติ หรือต้องสงสัยของผู้ใช้งานภายในระบบเครือข่าย ซึ่งระบบรักษาความปลอดภัยดังกล่าวนี้ครอบคลุมการใช้งานของระบบเครือข่ายภายใต้สำนักเลขาธิการนายกรัฐมนตรี และมีหน้าที่หลักในการช่วยป้องกันภัยคุกคามที่มาจากบุคคลภายนอกองค์กร รวมทั้งเก็บรวบรวมข้อมูลที่เกิดขึ้นบนเครื่องคอมพิวเตอร์ลูกข่ายที่ได้มีการติดตั้งซอฟต์แวร์ป้องกันการโจมตี มีระยะเวลาในการรับประกันความสามารถดังกล่าวเป็นระยะเวลา 3 ปี โดยปัจจุบันได้พ้นกำหนดระยะเวลาดังกล่าวแล้ว สำนักเลขาธิการนายกรัฐมนตรีได้สูญเสียความสามารถในการป้องกันตนเองจากการโจมตีที่เกิดขึ้นจากบุคคลภายนอก อีกทั้งยังไม่สามารถปรับปรุงฐานข้อมูลให้มีความทันสมัยเพื่อต่อสู้กับภัยคุกคามต่าง ๆ ได้ส่งผลให้สำนักเลขาธิการนายกรัฐมนตรีมีความเสี่ยงในการถูกโจมตีไซเบอร์มากยิ่งขึ้น

ปัจจุบันเหตุการณ์ภัยคุกคามทางไซเบอร์นั้นทวีความรุนแรง และมีปริมาณเพิ่มมากขึ้นเกิดการโจมตีได้ตลอดเวลา รวมถึงปัญหาการขาดแคลนบุคลากรที่มีความรู้ และความเชี่ยวชาญเฉพาะด้าน ส่งผลให้เกิดความล่าช้าในการตรวจสอบ และแก้ไขปัญหาที่เกิดขึ้น ด้วยภารกิจดังกล่าว สำนักเลขาธิการนายกรัฐมนตรีจึงมีความจำเป็นในการดำเนินการจ้างบริหารจัดการระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักเลขาธิการนายกรัฐมนตรี เพื่อให้สามารถป้องกัน และรักษาความมั่นคงปลอดภัยบนระบบเครือข่ายของสำนักเลขาธิการนายกรัฐมนตรี รวมทั้งจัดหาทีมงานผู้เชี่ยวชาญด้านภัยคุกคามทางไซเบอร์มาช่วยในการดำเนินการแก้ไขปัญหาต่าง ๆ ที่เกิดขึ้น ให้สามารถดำเนินการได้อย่างรวดเร็ว และมีประสิทธิภาพมากยิ่งขึ้น อีกทั้งเป็นการปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ที่มีหน้าที่ในการป้องกันภัยคุกคาม

คณะกรรมการจัดทำขอบเขตของงานฯ วันที่ 9 กรกฎาคม 2569

						
นายจักรกฤษ พรพิทักษ์ ประธานกรรมการ	น.ส.ณัชชา ขยารัตนาวัตร กรรมการ	น.ส.วรรณ นุ่มนวล กรรมการ	นายสุกฤษฎี สรหงษ์ กรรมการ	น.ส.จุฑามาศ อนรรชกุล กรรมการ	น.ส.ธนณัฐ หงษ์ทอง กรรมการ	นายชาญณิธิ ตีลี กรรมการ

3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอดำเนินการให้สละเอกสิทธิ์และความคุ้มกันเช่นนั้น

3.10 ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ “กิจการร่วมค้า” ต้องมีคุณสมบัติ ดังนี้

(1) การกำหนดสัดส่วนในการเข้าร่วมค้าของกลุ่มสัญญา

กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงฯ จะต้องมีการกำหนดสัดส่วนหน้าที่ และความรับผิดชอบในปริมาณงาน สิ่งของ หรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

(2) กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก
กิจการร่วมค้านั้นต้องใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

สำหรับข้อตกลงฯ ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค่ายใดเป็นผู้เข้าร่วมค่าหลักผู้เข้าร่วมค่าย
ทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน

(3) การยื่นข้อเสนองานของกิจการร่วมค้า

(3.1) กรณีที่ข้อตกลงฯ กำหนดให้มีการมอบหมายผู้เข้าร่วมค้ารายใดรายหนึ่ง เป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า การยื่นข้อเสนอดังกล่าวไม่ต้องมีหนังสือมอบอำนาจ

สำหรับข้อตกลงฯ ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้ยื่นข้อเสนอ ผู้เข้าร่วมค้าทุกรายจะต้องลงลายมือชื่อในหนังสือมอบอำนาจให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอ ในนามกิจการร่วมค้า

(3.2) การยื่นข้อเสนอด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e - bidding) ให้ผู้เข้าร่วมคำ
ที่ได้รับมอบหมายหรือมอบอำนาจตามข้อ (3.1) ดำเนินการซื้อเอกสารประกวดราคาอิเล็กทรอนิกส์
กรณีที่มีการจำหน่ายเอกสารซื้อหรือจ้าง

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

3.12 ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ ดังนี้

1. กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยหรือต่างประเทศ ซึ่งได้จดทะเบียนเกินกว่า 1 ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิ ที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก 1 ปีสุดท้ายก่อนวันยื่น ข้อเสนอ งบแสดงฐานะการเงิน 1 ปีสุดท้ายก่อนวันยื่นข้อเสนอ หมายถึง งบแสดงฐานะการเงินย้อนไปก่อนวันที่ หน่วยงานของรัฐกำหนดให้เป็นวันยื่นข้อเสนอ 1 ปีปฏิทิน เว้นแต่กรณีนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย หากวันยื่นข้อเสนอเป็นช่วงระยะเวลาที่กรมพัฒนาธุรกิจการค้ากำหนดให้นิติบุคคลยื่นงบแสดงฐานะการเงิน กับกรมพัฒนาธุรกิจการค้า ซึ่งจะอยู่ในช่วงเดือนมกราคม - เดือนพฤษภาคม ของทุกปีโดยนิติบุคคลที่เป็นผู้ยื่น ข้อเสนอ นั้นยังอยู่ในช่วงของการยื่นงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้าคือ ช่วงเดือนมกราคม - เดือนพฤษภาคม กรณีนี้ให้สามารถยื่นงบแสดงฐานะการเงินย้อนไปอีก 1 ปี ได้

คณะกรรมการจัดทำขอบเขตของงานฯ วันที่ 9 กรกฎาคม 2569

						
นายจักรกร กุศลพิทักษ์ ประธานกรรมการ	น.ส.ณัฏฐา ขยิทธิวัฒน์ กรรมการ	น.ส.รณิณี นุ่มนวล กรรมการ	นายสุกฤษฎ์ สรหงษ์ กรรมการ	น.ส.จุฬามาศ อนรรฆกุล กรรมการ	น.ส.ธนฉัตร หงษ์ทอง กรรมการ	นายชาญนิธิ ตีลี กรรมการ

2. กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า หรือกรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศซึ่งยังไม่มีรายงานงบแสดงฐานะการเงิน ให้พิจารณาการกำหนดมูลค่าของทุนจดทะเบียนโดยผู้ยื่นข้อเสนอจะต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอ ดังนี้

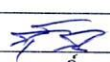
- (1) มูลค่าการจัดซื้อจัดจ้างไม่เกิน 1 ล้านบาท ไม่ต้องกำหนดทุนจดทะเบียน
- (2) มูลค่าการจัดซื้อจัดจ้างเกิน 1 ล้านบาท แต่ไม่เกิน 5 ล้านบาท ต้องมีทุนจดทะเบียนไม่ต่ำกว่า 1 ล้านบาท
- (3) มูลค่าการจัดซื้อจัดจ้างเกิน 5 ล้านบาท แต่ไม่เกิน 10 ล้านบาท ต้องมีทุนจดทะเบียนไม่ต่ำกว่า 2 ล้านบาท
- (4) มูลค่าการจัดซื้อจัดจ้างเกิน 10 ล้านบาท แต่ไม่เกิน 20 ล้านบาท ต้องมีทุนจดทะเบียนไม่ต่ำกว่า 3 ล้านบาท
- (5) มูลค่าการจัดซื้อจัดจ้างเกิน 20 ล้านบาท แต่ไม่เกิน 60 ล้านบาท ต้องมีทุนจดทะเบียนไม่ต่ำกว่า 8 ล้านบาท
- (6) มูลค่าการจัดซื้อจัดจ้างเกิน 60 ล้านบาท แต่ไม่เกิน 150 ล้านบาท ต้องมีทุนจดทะเบียนไม่ต่ำกว่า 20 ล้านบาท
- (7) มูลค่าการจัดซื้อจัดจ้างเกิน 150 ล้านบาท แต่ไม่เกิน 300 ล้านบาท ต้องมีทุนจดทะเบียนไม่ต่ำกว่า 60 ล้านบาท
- (8) มูลค่าการจัดซื้อจัดจ้างเกิน 300 ล้านบาท แต่ไม่เกิน 500 ล้านบาท ต้องมีทุนจดทะเบียนไม่ต่ำกว่า 100 ล้านบาท
- (9) มูลค่าการจัดซื้อจัดจ้างเกิน 500 ล้านบาทขึ้นไป ต้องมีทุนจดทะเบียนไม่ต่ำกว่า 200 ล้านบาท

3. สำหรับการจัดซื้อจัดจ้างครั้งหนึ่งที่มีวงเงินเกิน 500,000 บาทขึ้นไป กรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดาให้พิจารณาจากหนังสือรับรองบัญชีเงินฝากไม่เกิน 90 วัน ก่อนวันยื่นข้อเสนอ โดยต้องมีเงินฝากคงเหลือในบัญชีธนาคารเป็นมูลค่า 1 ใน 4 ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง และหากเป็นผู้ชนะการจัดซื้อจัดจ้างหรือเป็นผู้ได้รับการคัดเลือกจะต้องแสดงหนังสือรับรองบัญชีเงินฝากที่มีมูลค่าดังกล่าวอีกครั้งหนึ่งในวันลงนามในสัญญา

4. กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ สามารถดำเนินการได้ดังนี้

(1) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย หรือบุคคลธรรมดาที่ถือสัญชาติไทย ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ 1 ใน 4 ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง จะเป็นสินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุน หรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจ

คณะกรรมการจัดทำขอบเขตของงานฯ วันที่ 9 กรกฎาคม 2569

						
นายจักรกฤษ พรพิทักษ์ ประธานกรรมการ	น.ส.ณิชา ขยารัตนาวัตร กรรมการ	น.ส.วรรณ นุ่มนวล กรรมการ	นายสุกฤษฏ์ สรหงษ์ กรรมการ	น.ส.จุฑามาศ อนรรฆกุล กรรมการ	น.ส.ธนัญญ์ หงษ์ทอง กรรมการ	นายชาญนิจ์ ดีสี กรรมการ

คำประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทย
แจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรอง หรือที่สำนักงานสาขา
รับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอไม่เกิน 90 วัน

(2) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศ หรือบุคคล
ธรรมดาที่มีได้ถือสัญชาติไทย ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ 1 ใน 4 ของมูลค่า
งบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง จะเป็นสินเชื่อที่ธนาคารภายในประเทศหรือ
บริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์ และ
ประกอบธุรกิจค้าประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคาร
แห่งประเทศไทยแจ้งเวียนให้ทราบ หรือเป็นสินเชื่อที่ธนาคารต่างประเทศหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับ
อนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้าประกันตามประกาศของธนาคารกลาง
ต่างประเทศนั้น ตามรายชื่อบริษัทที่ธนาคารกลางต่างประเทศนั้นแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงิน
รวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรอง หรือที่สำนักงานสาขารับรอง (กรณีที่ได้รับมอบอำนาจจาก
สำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอไม่เกิน 90 วัน

5. กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศ หรือบุคคลธรรมดา
ที่มีได้ถือสัญชาติไทยตามข้อ 2 ข้อ 3 และ ข้อ 4 (2) มูลค่าจะต้องเป็นไปตามอัตราแลกเปลี่ยนเงินตรา
ตามประกาศที่ธนาคารแห่งประเทศไทยกำหนด ในช่วงระหว่างวันที่เผยแพร่ประกาศและเอกสารประกวดราคา
ในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (e - GP) จนถึงวันเสนอราคา

ทั้งนี้ ผู้ยื่นข้อเสนอจะต้องยื่นเอกสารที่แสดงให้เห็นถึงข้อมูลเกี่ยวกับมูลค่าสุทธิ
ของกิจการแล้วแต่กรณี ประกอบกับเอกสารดังกล่าวจะต้องผ่านการรับรองตามระเบียบกระทรวง
การต่างประเทศว่าด้วยการรับรองเอกสาร พ.ศ. 2539 และที่แก้ไขเพิ่มเติม กำหนด โดยจะต้องยื่นเอกสาร
ดังกล่าวในวันยื่นข้อเสนอ หากผู้ยื่นข้อเสนอไม่ได้มีการยื่นเอกสารดังกล่าวมาพร้อมกับการยื่นข้อเสนอให้ถือว่า
ผู้ยื่นเสนอรายนั้นยื่นเอกสารไม่ครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารประกวดราคา

6. กรณีตามข้อ 1 - ข้อ 5 ไม่ใช่บังคับกับกรณีดังต่อไปนี้

(6.1) กรณีที่ผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐภายในประเทศ

(6.2) นิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการตาม
พระราชบัญญัติล้มละลาย พ.ศ. 2483 และที่แก้ไขเพิ่มเติม

(6.3) งานจ้างก่อสร้างที่กรมบัญชีกลางได้ขึ้นทะเบียนผู้ประกอบการงานก่อสร้างแล้ว
และงานจ้างก่อสร้างที่หน่วยงานของรัฐที่ได้มีการจัดทำบัญชีผู้ประกอบการงานก่อสร้างที่มีคุณสมบัติเบื้องต้นไว้
แล้วก่อนวันที่พระราชบัญญัติการจัดซื้อจัดจ้างฯ มีผลใช้บังคับ

(6.4) การจัดซื้อจัดจ้างตามมาตรา 56 วรรคหนึ่ง (2) (ข) และ (ค) แห่งพระราชบัญญัติ
การจัดซื้อจัดจ้างฯ

(6.5) การซื้ออสังหาริมทรัพย์และการเช่าอสังหาริมทรัพย์

คณะกรรมการจัดทำขอบเขตของงานฯ วันที่ 9 กรกฎาคม 2569

						
นายจักรกฤษ พรพิทักษ์ ประธานกรรมการ	น.ส.ณัชชา ขยารัตนาวัตร กรรมการ	น.ส.วรรณ นุ่มนวล กรรมการ	นายสุกฤษ ศรีทอง กรรมการ	น.ส.จุฑามาศ อนรรฆกุล กรรมการ	น.ส.ธนัญญา หงษ์ทอง กรรมการ	นายชาญนิต ติลี กรรมการ

(6.6) กรณีงานจ้างบริการหรืองานจ้างเหมาบริการกับบุคคลธรรมดา เช่น จ้างพนักงาน ขับรถ ครูชาวต่างชาติ พนักงานเก็บขยะ พนักงานบันทึกข้อมูล เป็นต้น

3.13 ผู้ยื่นข้อเสนอต้องได้รับการรับรองมาตรฐานสากลด้านความมั่นคงปลอดภัยสารสนเทศ ISO 27001 (Information Security Management System หรือ ISMS) โดยให้ยื่นใบรับรองมาตรฐาน ที่ยังไม่หมดอายุขณะเข้าเสนอราคา

4. ขอบเขตของงาน

จ้างบริหารจัดการระบบรักษาความมั่นคงปลอดภัยไซเบอร์ ของสำนักเลขาธิการนายกรัฐมนตรี มีขอบเขตของงานดังนี้

4.1 บริการศูนย์เฝ้าระวังตรวจสอบการโจมตีทางไซเบอร์ (Cyber Security Operations Center: CSOC Managed Service) จำนวน 1 ระบบ

4.2 บริการตรวจจับและตอบสนองต่อภัยคุกคามทางไซเบอร์ในระดับ Endpoint (Managed Detection and Response: MDR) จำนวน 1 ระบบ

4.3 บริการบุคลากรผู้มีความรู้ความเชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security)

4.4 บริการตรวจสอบและเตรียมความพร้อมด้านความปลอดภัยไซเบอร์ (Cybersecurity Assessment and Readiness Services)

4.5 จัดหาอุปกรณ์ป้องกันเครือข่าย (Firewall) จำนวน 1 ระบบ

4.6 จัดหาระบบป้องกันเว็บแอปพลิเคชันและ API จำนวน 1 ระบบ

4.7 จัดหาระบบยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) จำนวน 1 ระบบ

โดยมีขอบเขตของงานตาม ภาคผนวก

5. กำหนดเวลาส่งมอบงาน

5.1 กำหนดการให้บริการ จำนวน 13 งวด (ตั้งแต่วันที่ 1 กันยายน 2569 – 31 สิงหาคม 2572)

5.2 กำหนดให้ผู้รับจ้างต้องส่งมอบงานให้แล้วเสร็จภายในวันที่ 5 กันยายน 2572 โดยแบ่งเป็น 13 งวด ดังนี้

5.2.1 งวดที่ 1 ผู้รับจ้างต้องส่งมอบงานให้แล้วเสร็จภายในวันที่ 31 ตุลาคม 2569

5.2.2 งวดที่ 2 ผู้รับจ้างต้องส่งมอบงานให้แล้วเสร็จภายในวันที่ 5 ธันวาคม 2569

5.2.3 งวดที่ 3 ผู้รับจ้างต้องส่งมอบงานให้แล้วเสร็จภายในวันที่ 5 มีนาคม 2570

5.2.4 งวดที่ 4 ผู้รับจ้างต้องส่งมอบงานให้แล้วเสร็จภายในวันที่ 5 มิถุนายน 2570

5.2.5 งวดที่ 5 ผู้รับจ้างต้องส่งมอบงานให้แล้วเสร็จภายในวันที่ 5 กันยายน 2570

5.2.6 งวดที่ 6 ผู้รับจ้างต้องส่งมอบงานให้แล้วเสร็จภายในวันที่ 5 ธันวาคม 2570

5.2.7 งวดที่ 7 ผู้รับจ้างต้องส่งมอบงานให้แล้วเสร็จภายในวันที่ 5 มีนาคม 2571

คณะกรรมการจัดทำขอบเขตของงานฯ วันที่ 9 กรกฎาคม 2569

						
นายจักรกฤษ พรพิทักษ์ ประธานกรรมการ	น.ส.ณัชชา ขยาดาวัตร์ กรรมการ	น.ส.วรรณ นุ่มนวล กรรมการ	นายสุกฤษฎี สรหงษ์ กรรมการ	น.ส.จุฑามาศ อนรรฆกุล กรรมการ	น.ส.ธนัญญ์ หงษ์ทอง กรรมการ	นายชาญนิธิ ดีลี กรรมการ

- | | | | | | | |
|---|---|---|---|---|--|---|
|  |  |  |  |  |  |  |
| นายจักรกฤษ พงษ์ทิพย์
ประธานกรรมการ | น.ส.ณัฏฐา ขยริติตัวรัตน์
กรรมการ | น.ส.วรรณ นุ่มนวล
กรรมการ | นายสุกฤษฎี สรพงษ์
กรรมการ | น.ส.จุฑามาศ อนรรฆกุล
กรรมการ | น.ส.ธนภัฏฐ์ หงษ์ทอง
กรรมการ | นายชาญนิตี ดีลี
กรรมการ |

งวดที่ 2 คิดเป็นจำนวนเงินร้อยละ 5 ของราคาค่าจ้างทั้งหมดตามสัญญา เมื่อผู้รับจ้างได้ปฏิบัติงานและส่งมอบงานให้แล้วเสร็จภายในวันที่ 5 ธันวาคม 2569 ดังนี้

รายงานสรุปผลการให้บริการตั้งแต่วันที่ 1 พฤศจิกายน 2569 – 30 พฤศจิกายน 2569 จำนวน 2 ชุด พร้อมไฟล์อิเล็กทรอนิกส์ในรูปแบบ Word และ PDF ดังนี้

รายเดือน: สรุปเหตุการณ์ตามประเภทและระดับความรุนแรง (Incident Report) ได้แก่ สรุป 10 อันดับสูงสุดของการโจมตี สรุป 10 อันดับสูงสุดของเป้าหมายที่โดนโจมตี สรุป 10 อันดับสูงสุดของผู้โจมตี สรุป 10 อันดับสูงสุดของช่องทางที่ถูกใช้โจมตี บทวิเคราะห์แนวโน้มของภัยคุกคามต่าง ๆ ที่เกิดขึ้นในแต่ละเดือนที่ผ่านมา และสรุปคำแนะนำ

งวดที่ 3 คิดเป็นเงินร้อยละ 3 ของราคาค่าจ้างทั้งหมดตามสัญญา เมื่อผู้รับจ้างได้ปฏิบัติงานและส่งมอบงานให้แล้วเสร็จภายในวันที่ 5 มีนาคม 2570 ดังนี้

1) รายงานผลการดำเนินงาน จำนวน 2 ชุด พร้อมไฟล์อิเล็กทรอนิกส์ในรูปแบบ Word และ PDF ดังนี้

(1) รายงานสรุปผลการให้บริการตั้งแต่วันที่ 1 ธันวาคม 2569 – 28 กุมภาพันธ์ 2570 ดังนี้

(1.1) รายเดือน: สรุปเหตุการณ์ตามประเภทและระดับความรุนแรง (Incident Report) ได้แก่ สรุป 10 อันดับสูงสุดของการโจมตี สรุป 10 อันดับสูงสุดของเป้าหมายที่โดนโจมตี สรุป 10 อันดับสูงสุดของผู้โจมตี สรุป 10 อันดับสูงสุดของช่องทางที่ถูกใช้โจมตี บทวิเคราะห์แนวโน้มของภัยคุกคามต่าง ๆ ที่เกิดขึ้นในแต่ละเดือนที่ผ่านมา และสรุปคำแนะนำ

(1.2) รายไตรมาส: รายงานระดับคะแนนความปลอดภัยทางไซเบอร์ขององค์กรภาพรวม (Cybersecurity Rating Report), บทวิเคราะห์ความเสี่ยง คำแนะนำและแนวทางการปรับปรุงระดับคะแนน และการเปรียบเทียบค่าระดับคะแนนจากไตรมาสที่ผ่านมา

(2) รายงานผลการประเมินหาช่องโหว่ประจำปี รอบที่ 1

(3) รายงานผลการทดสอบเจาะระบบภายนอกและระบบที่เปิดให้เข้าถึงจากภายนอกประจำปี (Annual External Network and Public-Facing Penetration Test - Black-box) รอบที่ 1

(4) รายงานผลทดสอบความพร้อมของบุคลากรผ่านการจำลองสถานการณ์ประจำปี (Cyber Drill Testing: Phishing Mail) รอบที่ 1

2) ผูกอบรมการใช้งานระบบงาน และอุปกรณ์ทั้งหมดในโครงการตามข้อ 16 ให้กับเจ้าหน้าที่ผู้ปฏิบัติงาน

งวดที่ 4 คิดเป็นเงินร้อยละ 2 ของราคาค่าจ้างทั้งหมดตามสัญญา เมื่อผู้รับจ้างได้ปฏิบัติงานและส่งมอบรายงานผลการดำเนินงาน จำนวน 2 ชุด พร้อมไฟล์อิเล็กทรอนิกส์ในรูปแบบ Word และ PDF ให้แล้วเสร็จภายในวันที่ 5 มิถุนายน 2570 ดังนี้

คณะกรรมการจัดทำขอบเขตของงานฯ วันที่ 9 กรกฎาคม 2569

						
นายจักรกฤษ พรพิทักษ์ ประธานกรรมการ	น.ส.ณัชนา ขยารัตนาวัตร กรรมการ	น.ส.วรรณิ นุ่มนวล กรรมการ	นายสุกฤษฎี สรหงษ์ กรรมการ	น.ส.จุฑามาศ อนุธรรมกุล กรรมการ	น.ส.ธนัญญ์ หงษ์ทอง กรรมการ	นายชาญนิจิ ตีลี กรรมการ

1) รายงานสรุปผลการให้บริการตั้งแต่วันที่ 1 มีนาคม 2570 – 31 พฤษภาคม 2570 ดังนี้

(1) รายเดือน: สรุปเหตุการณ์ตามประเภทและระดับความรุนแรง (Incident Report) ได้แก่ สรุป 10 อันดับสูงสุดของการโจมตี สรุป 10 อันดับสูงสุดของเป้าหมายที่โดนโจมตี สรุป 10 อันดับสูงสุดของผู้โจมตี สรุป 10 อันดับสูงสุดของช่องทางที่ถูกใช้โจมตี บทวิเคราะห์แนวโน้มของภัยคุกคามต่าง ๆ ที่เกิดขึ้นในแต่ละเดือนที่ผ่านมา และสรุปคำแนะนำ

(2) รายไตรมาส: รายงานระดับคะแนนความปลอดภัยทางไซเบอร์ขององค์กรภาพรวม (Cybersecurity Rating Report) บทวิเคราะห์ความเสี่ยง คำแนะนำและแนวทางการปรับปรุงระดับคะแนน การเปรียบเทียบค่าระดับคะแนนจากไตรมาสที่ผ่านมา

2) รายงานผลการประเมินหาช่องโหว่ประจำปี รอบที่ 2

3) รายงานผลการทดสอบเจาะระบบภายนอกและระบบที่เปิดให้เข้าถึงจากภายนอกประจำปี (Annual External Network and Public-Facing Penetration Test - Black-box) รอบที่ 2

4) รายงานผลทดสอบความพร้อมของบุคลากรผ่านการจำลองสถานการณ์ประจำปี (Cyber Drill Testing: Phishing Mail) รอบที่ 2

งวดที่ 5 คิดเป็นเงินร้อยละ 15 ของราคาค่าจ้างทั้งหมดตามสัญญา เมื่อผู้รับจ้างได้ปฏิบัติงานและส่งมอบรายงานการให้บริการ ตั้งแต่วันที่ 1 มิถุนายน 2570 – 31 สิงหาคม 2570 จำนวน 2 ชุด พร้อมไฟล์อิเล็กทรอนิกส์ในรูปแบบ Word และ PDF ให้แล้วเสร็จภายในวันที่ 5 กันยายน 2570 ดังนี้

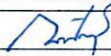
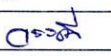
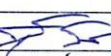
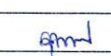
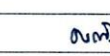
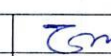
1) รายเดือน: สรุปเหตุการณ์ตามประเภทและระดับความรุนแรง (Incident Report) ได้แก่ สรุป 10 อันดับสูงสุดของการโจมตี สรุป 10 อันดับสูงสุดของเป้าหมายที่โดนโจมตี สรุป 10 อันดับสูงสุดของผู้โจมตี สรุป 10 อันดับสูงสุดของช่องทางที่ถูกใช้โจมตี บทวิเคราะห์แนวโน้มของภัยคุกคามต่าง ๆ ที่เกิดขึ้นในแต่ละเดือนที่ผ่านมา และสรุปคำแนะนำ

2) รายไตรมาส: รายงานระดับคะแนนความปลอดภัยทางไซเบอร์ขององค์กรภาพรวม (Cybersecurity Rating Report) บทวิเคราะห์ความเสี่ยง คำแนะนำและแนวทางการปรับปรุงระดับคะแนน การเปรียบเทียบค่าระดับคะแนนจากไตรมาสที่ผ่านมา

งวดที่ 6 คิดเป็นเงินร้อยละ 5 ของราคาค่าจ้างทั้งหมดตามสัญญา เมื่อผู้รับจ้างได้ปฏิบัติงานและส่งมอบรายงานการให้บริการ ตั้งแต่วันที่ 1 กันยายน 2570 – 30 พฤศจิกายน 2570 จำนวน 2 ชุด พร้อมไฟล์อิเล็กทรอนิกส์ในรูปแบบ Word และ PDF ให้แล้วเสร็จภายในวันที่ 5 ธันวาคม 2570 ดังนี้

1) รายเดือน: สรุปเหตุการณ์ตามประเภทและระดับความรุนแรง (Incident Report) ได้แก่ สรุป 10 อันดับสูงสุดของการโจมตี สรุป 10 อันดับสูงสุดของเป้าหมายที่โดนโจมตี สรุป 10 อันดับสูงสุดของผู้โจมตี สรุป 10 อันดับสูงสุดของช่องทางที่ถูกใช้โจมตี บทวิเคราะห์แนวโน้มของภัยคุกคามต่าง ๆ ที่เกิดขึ้นในแต่ละเดือนที่ผ่านมา และสรุปคำแนะนำ

คณะกรรมการจัดทำขอบเขตของงานฯ วันที่ 9 กรกฎาคม 2569

						
นายจักรกฤษ พรพิทักษ์ ประธานกรรมการ	น.ส.ณัชชา ขยาดาว์ตร กรรมการ	น.ส.วรรณิ นุ่มนวล กรรมการ	นายสุกฤษฎี สรหงษ์ กรรมการ	น.ส.จุฑามาศ อนรรฆกุล กรรมการ	น.ส.ธนัญญ์ หงษ์ทอง กรรมการ	นายชาญนิตี ดีลี กรรมการ

2) รายไตรมาส: รายงานระดับคะแนนความปลอดภัยทางไซเบอร์ขององค์กรภาพรวม (Cybersecurity Rating Report) บทวิเคราะห์ความเสี่ยง คำแนะนำและแนวทางการปรับปรุงระดับคะแนน การเปรียบเทียบค่าระดับคะแนนจากไตรมาสที่ผ่านมา

งวดที่ 7 คิดเป็นเงินร้อยละ 5 ของราคาค่าจ้างทั้งหมดตามสัญญา เมื่อผู้รับจ้างได้ปฏิบัติงานและส่งมอบรายงานผลการดำเนินงาน จำนวน 2 ชุด พร้อมไฟล์อิเล็กทรอนิกส์ในรูปแบบ Word และ PDF ให้แล้วเสร็จภายในวันที่ 5 มีนาคม 2571 ดังนี้

1) รายงานสรุปผลการให้บริการตั้งแต่วันที่ 1 ธันวาคม 2570 – 29 กุมภาพันธ์ 2571 ดังนี้

(1) รายเดือน: สรุปเหตุการณ์ตามประเภทและระดับความรุนแรง (Incident Report) ได้แก่ สรุป 10 อันดับสูงสุดของการโจมตี สรุป 10 อันดับสูงสุดของเป้าหมายที่โดนโจมตี สรุป 10 อันดับสูงสุดของผู้โจมตี สรุป 10 อันดับสูงสุดของช่องทางที่ถูกใช้โจมตี บทวิเคราะห์แนวโน้มของภัยคุกคามต่าง ๆ ที่เกิดขึ้นในแต่ละเดือนที่ผ่านมา และสรุปคำแนะนำ

(2) รายไตรมาส: รายงานระดับคะแนนความปลอดภัยทางไซเบอร์ขององค์กรภาพรวม (Cybersecurity Rating Report) บทวิเคราะห์ความเสี่ยง คำแนะนำและแนวทางการปรับปรุงระดับคะแนน การเปรียบเทียบค่าระดับคะแนนจากไตรมาสที่ผ่านมา

2) รายงานผลการประเมินหาช่องโหว่ประจำปี รอบที่ 1

3) รายงานผลการทดสอบเจาะระบบภายนอกและระบบที่เปิดให้เข้าถึงจากภายนอกประจำปี (Annual External Network and Public-Facing Penetration Test - Black-box) รอบที่ 1

4) รายงานผลทดสอบความพร้อมของบุคลากรผ่านการจำลองสถานการณ์ประจำปี (Cyber Drill Testing: Phishing Mail) รอบที่ 1

งวดที่ 8 คิดเป็นเงินร้อยละ 5 ของราคาค่าจ้างทั้งหมดตามสัญญา เมื่อผู้รับจ้างได้ปฏิบัติงานและส่งมอบรายงานผลการดำเนินงาน จำนวน 2 ชุด พร้อมไฟล์อิเล็กทรอนิกส์ในรูปแบบ Word และ PDF ให้แล้วเสร็จภายในวันที่ 5 มิถุนายน 2571 ดังนี้

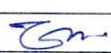
1) รายงานสรุปผลการให้บริการตั้งแต่วันที่ 1 มีนาคม 2571 – 31 พฤษภาคม 2571 ดังนี้

(1) รายเดือน: สรุปเหตุการณ์ตามประเภทและระดับความรุนแรง (Incident Report) ได้แก่ สรุป 10 อันดับสูงสุดของการโจมตี สรุป 10 อันดับสูงสุดของเป้าหมายที่โดนโจมตี สรุป 10 อันดับสูงสุดของผู้โจมตี สรุป 10 อันดับสูงสุดของช่องทางที่ถูกใช้โจมตี บทวิเคราะห์แนวโน้มของภัยคุกคามต่าง ๆ ที่เกิดขึ้นในแต่ละเดือนที่ผ่านมา และสรุปคำแนะนำ

(2) รายไตรมาส: รายงานระดับคะแนนความปลอดภัยทางไซเบอร์ขององค์กรภาพรวม (Cybersecurity Rating Report) บทวิเคราะห์ความเสี่ยง คำแนะนำและแนวทางการปรับปรุงระดับคะแนน การเปรียบเทียบค่าระดับคะแนนจากไตรมาสที่ผ่านมา

2) รายงานผลการประเมินหาช่องโหว่ประจำปี รอบที่ 2

คณะกรรมการจัดทำขอบเขตของงานฯ วันที่ 9 กรกฎาคม 2569

						
นายจักรกฤษ พรพิทักษ์ ประธานกรรมการ	น.ส.ณิชา ชัยธวัช กรรมการ	น.ส.วรรณ นุ่มนวล กรรมการ	นายสุกฤษฎี สรหงษ์ กรรมการ	น.ส.จุฑามาศ อนรรฆกุล กรรมการ	น.ส.ธนัญญ์ หงษ์ทอง กรรมการ	นายชาญนิธิ ดีลี กรรมการ

3) รายงานผลการทดสอบเจาะระบบภายนอกและระบบที่เปิดให้เข้าถึงจากภายนอกประจำปี (Annual External Network and Public-Facing Penetration Test - Black-box) รอบ 2

4) รายงานผลทดสอบความพร้อมของบุคลากรผ่านการจำลองสถานการณ์ประจำปี
(Cyber Drill Testing: Phishing Mail) รอบที่ 2

งวดที่ 9 คิดเป็นเงินร้อยละ 15 ของราคาค่าจ้างทั้งหมดตามสัญญา เมื่อผู้รับจ้างได้ปฏิบัติงานและส่งมอบรายงานการให้บริการตั้งแต่วันที่ 1 มิถุนายน 2571 – 31 สิงหาคม 2571 จำนวน 2 ชุด พร้อมไฟล์อิเล็กทรอนิกส์ในรูปแบบ Word และ Pdf ให้แล้วเสร็จภายในวันที่ 5 กันยายน 2571 ดังนี้

1) รายเดือน: สรุปเหตุการณ์ตามประเภทและระดับความรุนแรง (Incident Report) ได้แก่ สรุป 10 อันดับสูงสุดของการโจมตี สรุป 10 อันดับสูงสุดของเป้าหมายที่โดนโจมตี สรุป 10 อันดับสูงสุดของผู้โจมตี สรุป 10 อันดับสูงสุดของช่องทางที่ถูกใช้โจมตี บทวิเคราะห์แนวโน้มของภัยคุกคามต่าง ๆ ที่เกิดขึ้นในแต่ละเดือนที่ผ่านมา และสรุปคำแนะนำ

2) รายไตรมาส: รายงานระดับคะแนนความปลอดภัยทางไซเบอร์ขององค์กรภาพรวม (Cybersecurity Rating Report) บทวิเคราะห์ความเสี่ยง คำแนะนำและแนวทางการปรับปรุงระดับคะแนน การเปรียบเทียบค่าระดับคะแนนจากไตรมาสที่ผ่านมา

งวดที่ 10 คิดเป็นเงินร้อยละ 5 ของราคาค่าจ้างทั้งหมดตามสัญญา เมื่อผู้รับจ้างได้ปฏิบัติงานและส่งมอบรายงานการให้บริการตั้งแต่วันที่ 1 กันยายน 2571 – 30 พฤศจิกายน 2571 จำนวน 2 ชุด พร้อมไฟล์อิเล็กทรอนิกส์ในรูปแบบ Word และ Pdf ให้แล้วเสร็จภายในวันที่ 5 ธันวาคม 2571 ดังนี้

1) รายเดือน: สรุปเหตุการณ์ตามประเภทและระดับความรุนแรง (Incident Report) ได้แก่ สรุป 10 อันดับสูงสุดของการโจมตี สรุป 10 อันดับสูงสุดของเป้าหมายที่โดนโจมตี สรุป 10 อันดับสูงสุดของผู้โจมตี สรุป 10 อันดับสูงสุดของช่องทางที่ถูกใช้โจมตี บทวิเคราะห์แนวโน้มของภัยคุกคามต่าง ๆ ที่เกิดขึ้นในแต่ละเดือนที่ผ่านมา และสรุปคำแนะนำ

2) รายไตรมาส: รายงานระดับคะแนนความปลอดภัยทางไซเบอร์ขององค์กรภาพรวม (Cybersecurity Rating Report) บทวิเคราะห์ความเสี่ยง คำแนะนำและแนวทางการปรับปรุงระดับคะแนน การเปรียบเทียบค่าระดับคะแนนจากไตรมาสที่ผ่านมา

งวดที่ 11 คิดเป็นเงินร้อยละ 5 ของราคาค่าจ้างทั้งหมดตามสัญญา เมื่อผู้รับจ้างได้ปฏิบัติงานและส่งมอบรายงานผลการดำเนินงาน จำนวน 2 ชุด พร้อมไฟล์อิเล็กทรอนิกส์ในรูปแบบ Word และ Pdf ให้แล้วเสร็จภายในวันที่ 5 มีนาคม 2572 ดังนี้

1) รายงานสรุปผลการให้บริการตั้งแต่วันที่ 1 ธันวาคม 2571 – 28 กุมภาพันธ์ 2572 ดังนี้

(1) รายเดือน: สรุปเหตุการณ์ตามประเภทและระดับความรุนแรง (Incident Report) ได้แก่ สรุป 10 อันดับสูงสุดของการโจมตี สรุป 10 อันดับสูงสุดของเป้าหมายที่โดนโจมตี สรุป 10 อันดับสูงสุดของผู้โจมตี สรุป 10 อันดับสูงสุดของช่องทางที่ถูกใช้โจมตี บทวิเคราะห์แนวโน้มของภัยคุกคามต่าง ๆ ที่เกิดขึ้นในแต่ละเดือนที่ผ่านมา และสรุปคำแนะนำ

คณะกรรมการจัดทำขอบเขตของงานฯ วันที่ 9 กรกฎาคม 2569

นายจักรฤช พรพิทักษ์ ประธานกรรมการ	น.ส.ณัษชา ขยารัตนาวัตร กรรมการ	น.ส.วรรณิ นุ่มนวล กรรมการ	นายสุกฤษฎี ศรีหงษ์ กรรมการ	น.ส.จุฑามาศ อนรรฆกุล กรรมการ	น.ส.ธนวัฒน์ หงษ์ทอง กรรมการ	นายชาญนิธิ ดีลี กรรมการ

(2) รายไตรมาส: รายงานระดับคะแนนความปลอดภัยทางไซเบอร์ขององค์กร ภาพรวม (Cybersecurity Rating Report) บทวิเคราะห์ความเสี่ยง คำแนะนำและแนวทางการปรับปรุงระดับคะแนน การเปรียบเทียบค่าระดับคะแนนจากไตรมาสที่ผ่านมา

- 2) รายงานผลการประเมินหาช่องโหว่ประจำปี รอบที่ 1
- 3) รายงานผลการทดสอบเจาะระบบภายนอกและระบบที่เปิดให้เข้าถึงจากภายนอกประจำปี (Annual External Network and Public-Facing Penetration Test - Black-box) รอบที่ 1
- 4) รายงานผลทดสอบความพร้อมของบุคลากรผ่านการจำลองสถานการณ์ประจำปี (Cyber Drill Testing: Phishing Mail) รอบที่ 1

งวดที่ 12 คิดเป็นเงินร้อยละ 5 ของราคาค่าจ้างทั้งหมดตามสัญญา เมื่อผู้รับจ้างได้ปฏิบัติงานและส่งมอบรายงานผลการดำเนินงาน จำนวน 2 ชุด พร้อมไฟล์อิเล็กทรอนิกส์ในรูปแบบ Word และ PDF ให้แล้วเสร็จภายในวันที่ 5 มิถุนายน 2572 ดังนี้

- 1) รายงานสรุปผลการให้บริการตั้งแต่วันที่ 1 มีนาคม 2572 – 31 พฤษภาคม 2572 ดังนี้
- (1) รายเดือน: สรุปเหตุการณ์ตามประเภทและระดับความรุนแรง (Incident Report) ได้แก่ สรุป 10 อันดับสูงสุดของการโจมตี สรุป 10 อันดับสูงสุดของเป้าหมายที่โดนโจมตี สรุป 10 อันดับสูงสุดของผู้โจมตี สรุป 10 อันดับสูงสุดของช่องทางที่ถูกใช้โจมตี บทวิเคราะห์แนวโน้มของภัยคุกคามต่าง ๆ ที่เกิดขึ้นในแต่ละเดือนที่ผ่านมา และสรุปคำแนะนำ

(2) รายไตรมาส: รายงานระดับคะแนนความปลอดภัยทางไซเบอร์ขององค์กร ภาพรวม (Cybersecurity Rating Report) บทวิเคราะห์ความเสี่ยง คำแนะนำและแนวทางการปรับปรุงระดับคะแนน การเปรียบเทียบค่าระดับคะแนนจากไตรมาสที่ผ่านมา

- 2) รายงานผลการประเมินหาช่องโหว่ประจำปี รอบที่ 2
- 3) รายงานผลการทดสอบเจาะระบบภายนอกและระบบที่เปิดให้เข้าถึงจากภายนอกประจำปี (Annual External Network and Public-Facing Penetration Test - Black-box) รอบที่ 2
- 4) รายงานผลทดสอบความพร้อมของบุคลากรผ่านการจำลองสถานการณ์ประจำปี (Cyber Drill Testing: Phishing Mail) รอบที่ 2

งวดที่ 13 คิดเป็นเงินร้อยละ 15 ของราคาค่าจ้างทั้งหมดตามสัญญา เมื่อผู้รับจ้างได้ปฏิบัติงานและส่งมอบรายงานการให้บริการตั้งแต่วันที่ 1 มิถุนายน 2572 – 31 สิงหาคม 2572 จำนวน 2 ชุด พร้อมไฟล์อิเล็กทรอนิกส์ในรูปแบบ Word และ Pdf และปฏิบัติงานให้แล้วเสร็จตามสัญญา ให้แล้วเสร็จภายในวันที่ 5 กันยายน 2572 ดังนี้

- 1) รายเดือน: สรุปเหตุการณ์ตามประเภทและระดับความรุนแรง (Incident Report) ได้แก่ สรุป 10 อันดับสูงสุดของการโจมตี สรุป 10 อันดับสูงสุดของเป้าหมายที่โดนโจมตี สรุป 10 อันดับสูงสุดของผู้โจมตี สรุป 10 อันดับสูงสุดของช่องทางที่ถูกใช้โจมตี บทวิเคราะห์แนวโน้มของภัยคุกคามต่าง ๆ ที่เกิดขึ้นในแต่ละเดือนที่ผ่านมา และสรุปคำแนะนำ

คณะกรรมการจัดทำขอบเขตของงานฯ วันที่ 9 กรกฎาคม 2569

นายจักรกฤษ พงพิทักษ์ ประธานกรรมการ	น.ส.ณิชา ขยจิธาวัตร กรรมการ	น.ส.วรรณ นุ่มนวล กรรมการ	นายสุกฤษฎี สรหงษ์ กรรมการ	น.ส.จุฑามาศ อนรรฆกุล กรรมการ	น.ส.ธนัญญ์ หงษ์ทอง กรรมการ	นายชาญนิจ ดิติ กรรมการ

2) รายไตรมาส: รายงานระดับคะแนนความปลอดภัยทางไซเบอร์ขององค์กรภาพรวม (Cybersecurity Rating Report) บทวิเคราะห์ความเสี่ยง คำแนะนำและแนวทางการปรับปรุงระดับคะแนน การเปรียบเทียบค่าระดับคะแนนจากไตรมาสที่ผ่านมา

ทั้งนี้หากไม่สามารถเริ่มต้นให้บริการได้ตามกำหนดอันเนื่องมาจากระยะเวลาในการดำเนินการจัดจ้าง และทำสัญญา สำนักเลขาธิการนายกรัฐมนตรีจะพิจารณาระยะเวลาในการดำเนินการจ้างและปรับวงงาน ให้สอดคล้องกับระยะเวลาปัจจุบันที่เหลือในการดำเนินงานต่อไป

9. อัตราค่าปรับ

9.1 กรณีผู้รับจ้างนำงานที่รับจ้างไปจ้างช่วงให้ผู้อื่นทำอีกทอดหนึ่งโดยไม่ได้รับอนุญาตจาก สำนักเลขาธิการนายกรัฐมนตรี จะกำหนดค่าปรับสำหรับการฝ่าฝืนดังกล่าว เป็นจำนวนร้อยละ 10.00 (สิบ) ของวงเงินของงานจ้างช่วงนั้น

9.2 กรณีที่ผู้รับจ้างปฏิบัติผิดสัญญาจ้างนอกเหนือจาก ข้อ 9.1 และข้อ 9.3 จะกำหนดค่าปรับ เป็นรายวันในอัตราร้อยละ 0.10 (ศูนย์จุดหนึ่งศูนย์) ของราคาค่าจ้างทั้งหมดในแต่ละงวด โดยกำหนดค่าปรับ เป็นรายงวด

9.3 กรณีการให้บริการระบบและอุปกรณ์ในโครงการ หากเกิดความเสียหาย ชำรุด บกพร่อง หรือไม่สามารถใช้งานทั้งหมดหรือเพียงบางส่วน ผู้รับจ้างต้องจัดการซ่อมแก้ไขให้แล้วเสร็จภายใน ระยะเวลาที่กำหนดไว้ในข้อ 12.3 รวมถึงหากไม่สามารถให้บริการได้ตามระดับการให้บริการ (Service Level Agreement) ที่กำหนดในข้อ 12.6 และข้อ 12.7 ผู้รับจ้างจะต้องชำระค่าปรับให้แก่สำนักเลขาธิการ นายกรัฐมนตรี เป็นรายวันในอัตราร้อยละ 0.10 ของราคางานจ้างทั้งหมดตามสัญญา ยกเว้นข้อ 12.3.1 คิดอัตราค่าปรับชั่วโมงละ 500 บาท เศษของชั่วโมงคิดเป็น 1 ชั่วโมง

10. แผนการทำงานและเงื่อนไขการให้บริการ

10.1 แผนการทำงาน

ผู้รับจ้างต้องจัดทำแผนการดำเนินงานโดยละเอียด (Project Plan) ประกอบด้วยแผนการ ดำเนินงาน แผนการให้บริการ และแผนผังการติดตั้งอุปกรณ์ จัดส่งให้สำนักเลขาธิการนายกรัฐมนตรี ภายใน 30 วัน นับถัดจากวันที่ลงนามในสัญญา

10.2 เงื่อนไขการให้บริการ

10.2.1 ผู้รับจ้างต้องติดตั้งอุปกรณ์ ซอฟต์แวร์ หรือเครื่องคอมพิวเตอร์แม่ข่าย (Log Collector) ที่ใช้สำหรับบริหารจัดการข้อมูลจราจรทางคอมพิวเตอร์ภายใน 60 วันทำการ นับถัดจากวันที่ ลงนามในสัญญา

10.2.2 ผู้รับจ้างต้องติดตั้ง หรือถอนการติดตั้งกรณีที่มีการเปลี่ยนแปลงภายใน ระยะเวลาสัญญาโครงการแบบออนไลน์ โดยสำนักเลขาธิการนายกรัฐมนตรีเป็นผู้แจ้ง ให้ดำเนินการติดตั้ง หรือถอนการติดตั้ง โดยไม่เสียค่าใช้จ่ายเพิ่ม

คณะกรรมการจัดทำขอบเขตของงานฯ วันที่ 9 กรกฎาคม 2569

						
นายจักรกฤษ พรพิทักษ์ ประธานกรรมการ	น.ส.ณัฏฐา ขยารัตนาวัตร กรรมการ	น.ส.วรรณิ นุ่มนวล กรรมการ	นายสุกฤษฎี สรหงษ์ กรรมการ	น.ส.จุฑามาศ อนรรฆกุล กรรมการ	น.ส.ธนัญญ์ หงษ์ทอง กรรมการ	นายชาญนิจิ ดีลี กรรมการ

10.2.3 ผู้รับจ้างต้องตรวจสอบอุปกรณ์ ซอฟต์แวร์ หรือเครื่องคอมพิวเตอร์แม่ข่าย (Log Collector) ที่ใช้สำหรับบริหารจัดการข้อมูลผ่านระบบของผู้เสนอราคาเพื่อให้สามารถใช้งานได้ตลอด 24 ชั่วโมง 7 วัน

10.2.4 ผู้รับจ้างต้องตรวจสอบข้อมูลจราจรระบบเครือข่ายคอมพิวเตอร์ หากพบว่าไม่มีข้อมูลจราจรทางคอมพิวเตอร์ส่งไปยังที่ตั้งสำนักงานของผู้รับจ้าง หรือระบบวิเคราะห์ข้อมูลจราจรระบบเครือข่ายคอมพิวเตอร์ที่ให้บริการ ต้องแจ้งให้สำนักเลขาธิการนายกรัฐมนตรีทราบโดยเร็วที่สุด ผ่านช่องทางจดหมายอิเล็กทรอนิกส์ หรือช่องทางอื่นๆ ที่ทางสำนักเลขาธิการนายกรัฐมนตรีเห็นสมควร

10.2.5 ผู้รับจ้างต้องมีเจ้าหน้าที่วิเคราะห์ความปลอดภัย (Security Analyst) เพื่อให้บริการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ที่เกิดขึ้น และให้ข้อมูลภัยคุกคามเพื่อใช้สนับสนุนการทำงานของเจ้าหน้าที่เมื่อเกิดเหตุต้องสงสัย เหตุฉุกเฉิน หรือเหตุการณ์ผิดปกติ

10.2.6 ผู้รับจ้างต้องมีเจ้าหน้าที่ให้บริการเฝ้าระวังตอบสนองและแก้ไขต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ (Cyber Security Monitoring Services) ตลอด 24 ชั่วโมง โดยต้องมีผู้เชี่ยวชาญด้านระบบเฝ้าระวังภัยคุกคามทางไซเบอร์ (Security Analyst Tier 1) เพื่อให้บริการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ที่เกิดขึ้นและให้ข้อมูลภัยคุกคามเพื่อสนับสนุนการทำงานของเจ้าหน้าที่ของสำนักเลขาธิการนายกรัฐมนตรี โดยเมื่อเกิดเหตุต้องสงสัย เหตุฉุกเฉิน หรือเหตุความผิดปกติ ให้ปฏิบัติงานร่วมกับเจ้าหน้าที่ของสำนักเลขาธิการนายกรัฐมนตรี เพื่อให้ความช่วยเหลือ ให้คำปรึกษา และแก้ไขปัญหา โดยดำเนินการผ่านช่องทางการเฝ้าระวังระยะไกล (Remote) ตลอดสัญญาของโครงการ

10.2.7 ผู้รับจ้างต้องบริหารจัดการปัญหาที่เกิดขึ้น (Case Management) โดยมีการวัดประสิทธิภาพในการวิเคราะห์และแจ้งเตือนตามข้อกำหนดการให้ข้อบริการตามข้อตกลง (SLA) เวลาเฉลี่ยในการตรวจจับภัยคุกคาม (MTTD) และเวลาที่ใช้ในการแก้ไขปัญหา (MTTR) รวมถึงแนะนำวิธีการแก้ไข พร้อมทั้งระบุรายละเอียดเพิ่มเติมได้

10.2.8 ผู้รับจ้างต้องจัดประชุมเพื่อรายงานผลการดำเนินงานตามโครงการร่วมกับเจ้าหน้าที่สำนักเลขาธิการนายกรัฐมนตรี รวมทั้งจัดทำรายงานสรุปพร้อมเสนอแนะแนวทางการแก้ไขปัญหาต่าง ๆ ที่เกิดขึ้นอย่างน้อย 4 ครั้งต่อเดือน ตามวัน เวลา หัวข้อการประชุม และช่องทางการประชุมที่สำนักเลขาธิการนายกรัฐมนตรีกำหนด

10.2.9 ผู้รับจ้างต้องวิเคราะห์และแก้ไขปัญหาร่วมกับเจ้าหน้าที่ของสำนักเลขาธิการนายกรัฐมนตรีตามการร้องขอ เพื่อทำการตรวจสอบและแก้ไขภัยคุกคามทางไซเบอร์ ในกรณีที่มีผลกระทบรุนแรงเกินกว่าที่สำนักเลขาธิการนายกรัฐมนตรีสามารถดำเนินการแก้ไขได้ ซึ่งอาจจะทำให้เกิดความเสียหายต่อระบบสารสนเทศของสำนักเลขาธิการนายกรัฐมนตรี หรืออาจขยายความรุนแรงส่งผลกระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศเป็นวงกว้าง

คณะกรรมการจัดทำขอบเขตของงานฯ วันที่ 9 กรกฎาคม 2569

						
นายจักรกฤษ พงษ์พิทักษ์ ประธานกรรมการ	น.ส.ณัชชา ขยงจิตต์วาท กรรมการ	น.ส.วรรณิ นุ่มนวล กรรมการ	นายสุกฤษฎี สรหงษ์ กรรมการ	น.ส.จุฑามาศ อนรรฆกุล กรรมการ	น.ส.ธนณัฐ หงษ์ทอง กรรมการ	นายชาญนิธิ ดีลี กรรมการ

12.2 ผู้รับจ้างจะต้องทำ Preventive Maintenance (PM) ระบบและอุปกรณ์ที่ติดตั้งในโครงการทั้งหมดเป็นประจำทุก 3 เดือน ตลอดอายุการรับประกัน เพื่อให้อุปกรณ์ต่าง ๆ อยู่ในสภาพที่ใช้งานได้เป็นปกติและมีประสิทธิภาพ โดยไม่คิดค่าใช้จ่ายใด ๆ ทั้งสิ้น

12.3 ในกรณีระบบและอุปกรณ์ชำรุดเสียหาย ผู้รับจ้างต้องดำเนินการดังนี้

12.3.1 ดำเนินการตรวจสอบและวิเคราะห์ปัญหาเพื่อหาสาเหตุ ณ สถานที่ติดตั้ง ภายในเวลาไม่เกิน 4 ชั่วโมง นับจากเวลาที่ได้รับแจ้งจากผู้ว่าจ้าง

12.3.2 ดำเนินการซ่อมแซมแก้ไขให้แล้วเสร็จภายใน 6 ชั่วโมง นับจากเวลาที่ได้รับแจ้งจากผู้ว่าจ้าง หากไม่สามารถดำเนินการแก้ไขให้แล้วเสร็จภายในเวลาดังกล่าว เนื่องจากต้องนำอะไหล่ ชิ้นส่วน หรืออุปกรณ์อื่นใดกลับไปดำเนินการซ่อมแซมแก้ไข ผู้รับจ้างจะต้องจัดหาอุปกรณ์ทดแทนชั่วคราวเข้ามาให้ใช้งานในทันที ก่อนจะนำอุปกรณ์ที่เกิดปัญหาออกไปซ่อมแซม เพื่อให้ระบบสามารถใช้งานได้ โดยไม่ส่งผลกระทบต่อการทำงานของสำนักเลขาธิการนายกรัฐมนตรี และอุปกรณ์ที่นำกลับไปซ่อมแซมแก้ไขจะต้องใช้เวลาในการซ่อมแซมแก้ไขไม่เกิน 30 วัน นับแต่วันที่นำอุปกรณ์ออกไปซ่อมแซมแก้ไข ในกรณีที่เลยกำหนด 30 วัน จะถือว่าอุปกรณ์นั้นไม่สามารถซ่อมแซมแก้ไขได้ ผู้รับจ้างจะต้องจัดหาอุปกรณ์ที่เป็นของใหม่และไม่เคยใช้งานที่ใดมาก่อน เข้ามาเปลี่ยนทดแทนของเดิมที่นำไปซ่อมแซมแก้ไข ภายใน 60 วันนับถัดจากวันที่ได้รับแจ้ง หากไม่สามารถดำเนินการได้ตามเวลาดังกล่าว ผู้รับจ้างจะต้องจ่ายค่าปรับให้แก่สำนักเลขาธิการนายกรัฐมนตรี เป็นรายวันในอัตราร้อยละ 0.10 ของราคางานจ้าง

12.3.3 การติดตั้งอุปกรณ์ที่นำมาเปลี่ยน ผู้รับจ้างจะต้องติดตั้งอุปกรณ์ที่นำมาเปลี่ยน และทำการทดสอบจนแน่ใจว่าระบบสามารถทำงานได้ตามปกติ จึงจะสามารถนำอุปกรณ์ทดแทนชั่วคราว กลับคืนไปได้

12.4 ผู้รับจ้างต้องจัดให้มีผู้เชี่ยวชาญหรือเจ้าหน้าที่ให้คำปรึกษาและตอบปัญหาแก่นักเลขาธิการนายกรัฐมนตรีทุกวันตลอด 24 ชั่วโมง โดยให้บริการอย่างน้อย ดังนี้

12.4.1 การให้บริการให้คำปรึกษาและแก้ไขปัญหาเบื้องต้นทางโทรศัพท์ กรณีที่ไม่สามารถแก้ไขปัญหาทางโทรศัพท์ได้ ผู้รับจ้างต้องส่งเจ้าหน้าที่เข้าดำเนินการแก้ไขปัญหา ณ จุดเกิดเหตุโดยไม่มีค่าใช้จ่ายเพิ่มเติม

12.4.2 หาก Software เกิดความเสียหายอันเนื่องมาจากการปรับตั้งค่าที่ผิดพลาดจนไม่สามารถทำงานได้ตามปกติ ผู้รับจ้างจะต้องทำการแก้ปัญหาให้แล้วเสร็จภายใน 6 ชั่วโมง นับจากเวลาได้รับแจ้งจากผู้ว่าจ้าง

12.5 ผู้รับจ้างต้องเสนอรายชื่อผู้ประสานงาน และหมายเลขโทรศัพท์ที่สามารถติดต่อได้

12.6 ผู้รับจ้างต้องสามารถให้บริการระบบรักษาความปลอดภัยไซเบอร์แก่นักเรียนเลขาธิการนายกรัฐมนตรีได้ตามเกณฑ์ที่กำหนด ในกรณีที่มีข้อผิดพลาดอันเนื่องมาจากการทำงาน โดยมีระดับการให้บริการ (Service Level Agreement: SLA) อย่างน้อย ดังนี้

นายจักรฤช พงพิทักษ์ ประธานกรรมการ	น.ส.ณิชา ขยริฐดาวัตร์ กรรมการ	น.ส.วรรณีย์ นุ่มนวล กรรมการ	นายสุกฤษฎี สรหงษ์ กรรมการ	น.ส.จุฑามาศ อรรถมงคล กรรมการ	น.ส.ธนัญญ์ หงษ์ทอง กรรมการ	นายชาญนิธิ ตีลี กรรมการ

ระดับ ความรุนแรง	ผลกระทบ	ตอบรับ	แก้ไขแล้ว เสร็จ
ระดับวิกฤติ (Critical)	เหตุคุกคามทางไซเบอร์ส่งผลให้ การบริการทุกระบบงานหยุดชะงัก เช่น เหตุคุกคามทางไซเบอร์ส่งผลให้ระบบหลักหยุดทำงานทั้งหมด ข้อมูลสำคัญรั่วไหลในวงกว้าง เกิดการโจมตี Ransomware การถูกเจาะระบบฐานข้อมูล หรือ DDoS ที่ทำให้เว็บไซต์ล่ม	15 นาที	30 นาที
ระดับสูง (High)	เหตุคุกคามทางไซเบอร์ส่งผลให้ การบริการบางระบบงานหยุดชะงัก เช่น เหตุคุกคามทางไซเบอร์ส่งผลให้บริการบางส่วนหยุดทำงาน มีความพยายามบุกรุกเข้าสู่ระบบงานที่สำคัญ ตรวจพบมัลแวร์ในเครื่อง Server สำคัญ หรือการพยายาม Brute Force ที่ผิดปกติ	30 นาที	1 ชั่วโมง
ระดับกลาง (Medium)	เหตุคุกคามทางไซเบอร์ส่งผลให้ การบริการระบบงานภายในบางระบบหยุดชะงัก เช่น เหตุคุกคามทางไซเบอร์ส่งผลให้มีความผิดปกติเกิดขึ้นยังไม่กระทบต่อระบบงานโดยตรง ตรวจพบช่องโหว่ระดับกลาง หรือพฤติกรรมการใช้งาน User ที่น่าสงสัย	1 ชั่วโมง	4 ชั่วโมง
ระดับต่ำ (Low)	เหตุคุกคามทางไซเบอร์ส่งผลกระทบต่อประสิทธิภาพการทำงานทั่วไป เช่น เหตุคุกคามทางไซเบอร์เหตุการณ์ทั่วไปที่ต้องการการตรวจสอบหรือสอบถามข้อมูล การสแกนพอร์ตทั่วไป (Reconnaissance) หรือการขอคำปรึกษาด้านความปลอดภัย	1 วัน	3 วัน

12.7 ผู้รับจ้างต้องสามารถให้บริการแจ้งเตือนแก่สำนักเลขาธิการนายกรัฐมนตรี สำหรับเหตุการณ์ที่อยู่ในขอบข่ายภัยคุกคามทางไซเบอร์ที่เกิดขึ้นจากข้อมูลจากระบบเครือข่ายคอมพิวเตอร์ที่ได้จัดเก็บตามรายการทรัพย์สินที่สำนักเลขาธิการนายกรัฐมนตรีกำหนด และเหตุคุกคามทางไซเบอร์ได้ตามเกณฑ์ที่กำหนด โดยมีระดับการให้บริการ (Service Level Agreement: SLA) อย่างน้อยดังนี้

คณะกรรมการจัดทำขอบเขตของงานฯ วันที่ 9 กรกฎาคม 2569

นายจักรกฤษ พงพิทักษ์ ประธานกรรมการ	น.ส.ณิชา ชยธิตาวัตร กรรมการ	น.ส.วราณี นุ่มนวล กรรมการ	นายสุกฤษฎี สรหงษ์ กรรมการ	น.ส.จุฑามาศ อนรรฆกุล กรรมการ	น.ส.ธนวัฒน์ หงษ์ทอง กรรมการ	นายชาญนิธิ ดีลี กรรมการ

ระดับ ความรุนแรง	ผลกระทบ	แจ้งเตือน	ให้คำแนะนำ แก้ไขปัญห
ระดับวิกฤติ (Critical)	เหตุคุกคามทางไซเบอร์ส่งผลให้การบริการทุกระบบงาน <u>หยุดชะงัก</u> เช่น เหตุคุกคามทางไซเบอร์ส่งผลให้ระบบ หลักหยุดทำงานทั้งหมด ข้อมูลสำคัญรั่วไหลในวงกว้าง เกิดการโจมตี Ransomware การถูกเจาะระบบฐานข้อมูล หรือ DDoS ที่ทำให้เว็บไซต์ล่ม	15 นาที	30 นาที
ระดับสูง (High)	เหตุคุกคามทางไซเบอร์ส่งผลให้การบริการบางระบบงาน <u>หยุดชะงัก</u> เช่น เหตุคุกคามทางไซเบอร์ส่งผลให้บริการ บางส่วนหยุดทำงาน มีความพยายามบุกรุกเข้าสู่ระบบงาน ที่สำคัญ ตรวจพบมัลแวร์ในเครื่อง Server สำคัญ หรือ การพยายาม Brute Force ที่ผิดปกติ	30 นาที	1 ชั่วโมง
ระดับกลาง (Medium)	เหตุคุกคามทางไซเบอร์ส่งผลให้การบริการระบบงาน <u>ภายในบางระบบหยุดชะงัก</u> เช่น เหตุคุกคามทางไซเบอร์ ส่งผลให้มีความผิดปกติเกิดขึ้นยังไม่กระทบต่อระบบงาน โดยตรง ตรวจพบช่องโหว่ระดับกลาง หรือพฤติกรรมการใช้ งาน User ที่น่าสงสัย	1 ชั่วโมง	4 ชั่วโมง
ระดับต่ำ (Low)	เหตุคุกคามทางไซเบอร์ส่งผลกระทบต่อประสิทธิภาพ การทำงานทั่วไป เช่น เหตุคุกคามทางไซเบอร์เหตุการณ์ ทั่วไปที่ต้องการการตรวจสอบหรือสอบถามข้อมูล การสแกนพอร์ตทั่วไป (Reconnaissance) หรือการขอ คำปรึกษาด้านความปลอดภัย	1 วัน	3 วัน

12.8 เงื่อนไขการให้บริการอื่น ๆ ให้เป็นไปตามเงื่อนไขการรับประกัน (Warranty) และระดับการให้บริการ (Service Level agreement) ตามที่ปรากฏในภาคผนวก

13. บุคลากรผู้มีความรู้ความเชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security)

ผู้รับจ้างต้องยื่นเอกสารรายชื่อบุคลากรผู้จัดการโครงการและผู้มีความรู้ความเชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) เพื่อปฏิบัติงานในด้านต่าง ๆ ดังนี้

13.1 ผู้จัดการโครงการ (Project Manager) อย่างน้อย 1 ราย โดยสำเร็จการศึกษาในระดับปริญญาตรีหรือสูงกว่า สาขาวิศวกรรมคอมพิวเตอร์ หรือวิทยาการคอมพิวเตอร์ หรือวิศวกรรมไฟฟ้าสื่อสาร หรือวิศวกรรมไฟฟ้า หรือสาขาอื่นที่เทียบเท่า

คณะกรรมการจัดทำขอบเขตของงานฯ วันที่ 9 กรกฎาคม 2569

						
นายจักรกฤษ พรทิพย์ ประธานกรรมการ	น.ส.ณัชชา ขยารัตน์ กรรมการ	น.ส.วรรณ นุ่มนวล กรรมการ	นายสุกฤษฎี สรพงษ์ กรรมการ	น.ส.จุฑามาศ อนรรฆกุล กรรมการ	น.ส.ธนัญญ์ หงษ์ทอง กรรมการ	นายชานนธิ์ ดีลี กรรมการ

13.2 ผู้จัดการศูนย์ปฏิบัติการรักษาความปลอดภัยทางไซเบอร์ (CSOC Manager) หรือที่ปรึกษาด้านความปลอดภัย (Security Consultant) หรือผู้จัดการศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ (MDR Manager) ที่มีความสามารถในการจัดการและควบคุมศูนย์ปฏิบัติการรักษาความปลอดภัย และสามารถพัฒนากระบวนการรวมถึงนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ให้เหมาะสมและเป็นปัจจุบัน อย่างน้อย 1 ราย โดยต้องแสดงสำเนาประกาศนียบัตรรับรองความรู้ อย่างน้อย 2 ประกาศนียบัตร ดังนี้

13.2.1 ISO/IEC 27001 Lead Auditor (เวอร์ชันปัจจุบัน)

13.2.2 CISSP (Certified Information System Security Professional)

13.2.3 CISM (Certified Information Security Manager)

13.2.4 CISA (Certified Information System Auditor)

13.2.5 CRISC (Certified in Risk and Information System Control)

13.3 ผู้เชี่ยวชาญด้านระบบเผื่อการรั่วภัยคุกคามทางไซเบอร์ ระดับ 3 (Security Analyst Tier 3) ที่มีความเชี่ยวชาญในการรับมือ การวิเคราะห์เหตุการณ์เชิงลึก และการตอบสนองต่อภัยคุกคามทางไซเบอร์ขั้นสูง อย่างน้อย 1 ราย โดยต้องได้รับใบประกาศนียบัตรรับรองความรู้ ความสามารถอย่างใด อย่างหนึ่ง ดังนี้

13.3.1 Offensive Security Certified Professional (OSCP)

13.3.2 GIAC Certified Intrusion Analyst Certification (GCIA)

13.3.3 GIAC Certified Incident Handler Certification (GCIH)

13.3.4 CompTIA Advanced Security Practitioner (CompTIA SecurityX)

13.4 ผู้เชี่ยวชาญด้านระบบเฝ้าระวังภัยคุกคามทางไซเบอร์ ระดับ2 (Security Analyst Tier 2) ที่มีความเชี่ยวชาญในการวิเคราะห์และรับมือกับภัยคุกคามที่ซับซ้อนมากขึ้น รวมถึงสามารถให้คำปรึกษาและการดำเนินการเกี่ยวกับเหตุการณ์ที่มีความเสี่ยงสูง อย่างน้อย 2 ราย โดยมีคุณสมบัติดังนี้

13.4.1 สำเร็จการศึกษาไม่ต่ำกว่าระดับปริญญาตรี ด้านวิศวกรรมศาสตร์คอมพิวเตอร์ หรือวิทยาศาสตร์คอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศ หรือสาขาอื่นที่เกี่ยวข้อง

13.4.2 ได้รับใบประกาศนียบัตรรับรองความรู้ ความสามารถอย่างใด อย่างหนึ่ง ดังนี้

13.4.2.1 CompTIA Cybersecurity Analyst (CySA+)

13.4.2.2 CEH (Certified Ethical Hacker)

13.4.2.3 OSCP (Offensive Security Certified Professional)

13.4.3 มีประสบการณ์ด้าน Cyber Security อย่างน้อย 3 ปี

13.5 ผู้เชี่ยวชาญวิเคราะห์ความปลอดภัยทางไซเบอร์ ระดับ 1 (Security Analyst Tier 1) ที่มีความเชี่ยวชาญในการพัฒนากระบวนการ การตรวจจับ (Detect) การป้องกันภัยคุกคาม (Prevent) และการตอบสนอง (Response) ต่อภัยคุกคามทางไซเบอร์ อย่างน้อย 3 ราย โดยมีคุณสมบัติดังนี้

13.5.1 สำเร็จการศึกษาไม่ต่ำกว่าระดับปริญญาตรี ด้านวิศวกรรมศาสตร์คอมพิวเตอร์ หรือวิทยาศาสตร์คอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศ หรือสาขาอื่นที่เกี่ยวข้อง

คณะกรรมการจัดทำขอบเขตของงานฯ วันที่ 9 กรกฎาคม 2569

นายจักรกฤษ พรพิทักษ์ ประธานกรรมการ	น.ส.ณัชชา ชัยจิตาวัตร กรรมการ	น.ส.วรรณ นุ่มนวล กรรมการ	นายสุกฤษฎี สรหงษ์ กรรมการ	น.ส.จุฑามาศ อนรรฆกุล กรรมการ	น.ส.ธนณัฐ หงษ์ทอง กรรมการ	นายชาญนิธิ ดีลี กรรมการ

13.5.2 ได้รับใบประกาศนียบัตรรับรองความรู้ ความสามารถอย่างใด อย่างหนึ่ง ดังนี้

13.5.2.1 CompTIA Security+

13.5.2.2 CompTIA Cybersecurity Analyst (CySA+)

13.5.2.3 CEH (Certified Ethical Hacker)

13.5.2.4 OSCP (Offensive Security Certified Professional)

13.5.3 มีประสบการณ์ด้าน Cyber Security อย่างน้อย 2 ปี

13.6 ผู้เชี่ยวชาญด้านระบบเฝ้าระวังภัยคุกคามทางไซเบอร์ ระดับ 1 (Security Analyst Tier 1) ที่มีความเชี่ยวชาญในการตรวจจับและตอบสนอง เพื่อปฏิบัติงานที่สำนักเลขาธิการนายกรัฐมนตรี ในวันและเวลาราชการ อย่างน้อย 1 ราย โดยมีคุณสมบัติดังนี้

13.6.1 สำเร็จการศึกษาไม่ต่ำกว่าระดับปริญญาตรี ด้านวิศวกรรมศาสตร์คอมพิวเตอร์ หรือวิทยาศาสตร์คอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศ หรือสาขาอื่นที่เกี่ยวข้อง

13.6.2 ได้รับใบประกาศนียบัตรรับรองความรู้ ความสามารถอย่างใด อย่างหนึ่ง ดังนี้

13.6.2.1 CompTIA Security+

13.6.2.2 CompTIA Cybersecurity Analyst (CySA+)

13.6.3 มีประสบการณ์ด้าน Cyber Security อย่างน้อย 2 ปี

ทั้งนี้ ต้องเป็นใบประกาศนียบัตรที่ยังไม่หมดอายุ โดยให้นำสำเนาใบประกาศนียบัตร ส่งมอบให้สำนักเลขาธิการนายกรัฐมนตรี ในวันทำสัญญา

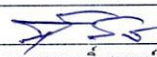
14. การรักษาความลับ

14.1 ผู้รับจ้างต้องตกลงจะไม่เปิดเผยรายละเอียดเกี่ยวกับงาน และจะเก็บรักษาข้อมูล และหรือเอกสารอื่นใดที่เกี่ยวข้องกับโครงการนี้ไว้เป็นความลับ เว้นแต่เป็นการเปิดเผยเพื่อประโยชน์หรือความจำเป็นในการปฏิบัติงานตามสัญญา หรือจำเป็นต้องเปิดเผยตามกฎหมายหรือคำสั่งศาล หรือได้รับความยินยอมจากผู้ว่าจ้างเป็นลายลักษณ์อักษรหรือเป็นข้อมูลและหรือเอกสารที่ได้เปิดเผยต่อสาธารณชนแล้ว

14.2 ผู้รับจ้างต้องตกลงว่าบรรดาข้อมูล เอกสาร และความลับทางธุรกิจของผู้ว่าจ้างทั้งปวง ที่ติดต่อสื่อสารมาจากผู้ว่าจ้างไม่ว่าลักษณะใด ๆ ที่เกี่ยวพันกับโครงการนี้ ถือว่าเป็นข้อมูลความลับของผู้ว่าจ้าง ซึ่งผู้รับจ้างจะต้องนำข้อมูลดังกล่าวไปใช้เพื่อให้บรรลุวัตถุประสงค์ตามสัญญา ผู้รับจ้างมีหน้าที่รับผิดชอบในการควบคุมดูแลพนักงาน ลูกจ้าง ตัวแทนหรือบุคลากรของผู้รับจ้าง ไม่ให้เปิดเผยข้อมูลความลับของผู้ว่าจ้างให้แก่บุคคลที่สาม โดยปราศจากความยินยอมล่วงหน้าจากผู้ว่าจ้างเป็นลายลักษณ์อักษร

14.3 ผู้รับจ้างเข้าใจและยอมรับว่าข้อมูลหรือเอกสารใด ๆ ที่เกี่ยวข้องกับการปฏิบัติงานตามสัญญาฉบับนี้เป็นทรัพย์สินของผู้ว่าจ้าง ผู้รับจ้างจะใช้ข้อมูลและหรือเอกสารดังกล่าว ในการปฏิบัติงานให้เป็นไปตามวัตถุประสงค์ของสัญญานี้เท่านั้น และจะต้องเก็บรักษาข้อมูลหรือเอกสารดังกล่าวไว้เป็นความลับ โดยจะเปิดเผยต่อบุคคลอื่นไม่ได้เป็นอันขาด เว้นแต่จะได้รับความยินยอมจากผู้ว่าจ้างเป็นลายลักษณ์อักษรและ

คณะกรรมการจัดทำขอบเขตของงานฯ วันที่ 9 กรกฎาคม 2569

						
นายจักรกฤษ พรพิทักษ์ ประธานกรรมการ	น.ส.ณัฏฐา ขยาคูวัฒนา กรรมการ	น.ส.วรรณิ นุ่มนวล กรรมการ	นายสุกฤษฎี สรหงษ์ กรรมการ	น.ส.จุฑามาศ อรรถมกุล กรรมการ	น.ส.ธนัญญ์ หงษ์ทอง กรรมการ	นายชาญนิตี ตีลี กรรมการ

ต้องควบคุมดูแลพนักงาน ลูกจ้าง ตัวแทนหรือบุคลากรของผู้รับจ้าง ให้ปฏิบัติเช่นเดียวกันกับผู้รับจ้างด้วย ในกรณีที่สัญญาสิ้นสุดลงไม่ว่าด้วยเหตุใด ๆ ผู้รับจ้างต้องส่งมอบบรรดาข้อมูลและเอกสารดังกล่าวคืนให้แก่ ผู้ว่าจ้างทันที

14.4 ผู้รับจ้างตกลงจะเก็บรักษาข้อมูลใด ๆ ที่ได้รับมา เนื่องจากการปฏิบัติงานตามสัญญา ไว้เป็นความลับตลอดไป แม้ว่าสัญญา จะสิ้นสุดลงไม่ว่าด้วยเหตุใด ๆ ก็ตาม

14.5 ผู้รับจ้างต้องจัดทำสัญญาไม่เปิดเผยข้อมูลพร้อมลงนามให้แก่ผู้ว่าจ้าง โดยข้อมูลและ เอกสารทั้งหมดของโครงการนี้จัดทำขึ้นถือเป็นลิขสิทธิ์ของผู้ว่าจ้าง ผู้รับจ้างจะไม่นำเอกสาร และข้อมูลใด ๆ ที่ได้รับไปทำการเปิดเผย หรือเผยแพร่ โดยไม่ได้รับความเห็นชอบจากผู้ว่าจ้างเป็นลายลักษณ์อักษร

15. เอกสารคู่มือ

ผู้รับจ้างจะต้องส่งมอบเอกสารและคู่มือต่าง ๆ อย่างน้อยดังนี้

15.1 เอกสารหรือคู่มือของอุปกรณ์และซอฟต์แวร์ทั้งหมดที่ได้ดำเนินการติดตั้ง

15.1.1 แบบติดตั้ง (As-Built Drawing) ภายหลังการติดตั้งอุปกรณ์ โดยแบบติดตั้งดังกล่าว ต้องเป็นไฟล์เอกสารที่แก้ไขได้

15.1.2 แผนผังระบบเครือข่ายแสดงการเชื่อมต่อระบบเครือข่ายที่เกี่ยวข้องทั้งหมด

15.1.3 เอกสารหรือคู่มืออุปกรณ์ที่มาพร้อมอุปกรณ์

15.2 คู่มือการปฏิบัติงาน ขั้นตอนการดูแลรักษา และวิธีการตั้งค่าอุปกรณ์ เป็นเอกสารรูปเล่ม ภาษาไทยโดยแสดงรายละเอียดเป็นขั้นตอนที่สามารถใช้ปฏิบัติงานได้จริง จำนวนไม่น้อยกว่า 2 ชุด และ Digital File ในรูปแบบ Microsoft Word และ PDF

15.3 ไฟล์ติดตั้งซอฟต์แวร์รุ่นที่ติดตั้งใช้งานอยู่ ณ วันส่งมอบงาน จำนวนไม่น้อยกว่า 2 ชุด

15.4 ผู้รับจ้างต้องจัดทำฟอร์มเอกสารในการดูแล และการตรวจเช็คค่าต่าง ๆ ของอุปกรณ์ ที่เสนอในลักษณะการตรวจสอบรายวันหรือรายสัปดาห์หรือรายเดือน เพื่อเป็นประโยชน์ในการจดบันทึก และใช้ในการวางแผนสำหรับการซ่อมแซมบำรุงรักษาแก้ไขข้อขัดข้องที่เกิดขึ้น อันเนื่องมาจากการทำงาน ตามปกติหรือข้อผิดพลาดของการใช้งานอุปกรณ์

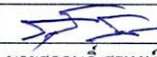
15.5 การส่งมอบไฟล์เอกสารต่าง ๆ ทั้งหมดตามข้อ 15.1 -15.4 จะต้องส่งบันทึกในอุปกรณ์ จัดเก็บข้อมูลแบบ External Storage ชนิด Solid State Drive จำนวนไม่น้อยกว่า 2 ชุด

16. การฝึกอบรม

16.1 ผู้รับจ้างต้องทำแผนการฝึกอบรม พร้อมรายละเอียดของการฝึกอบรมและคุณสมบัติ วิทยากร ส่งมอบให้แก่สำนักเลขาธิการนายกรัฐมนตรีพิจารณา ก่อนดำเนินการฝึกอบรม

16.2 ผู้รับจ้างต้องจัดฝึกอบรมการติดตั้งและใช้งานอุปกรณ์และซอฟต์แวร์ต่าง ๆ ที่ติดตั้ง ในโครงการ ให้กับเจ้าหน้าที่สำนักเลขาธิการนายกรัฐมนตรี จำนวนไม่น้อยกว่า 15 ราย ให้สามารถใช้งานได้ อย่างถูกต้องและมีประสิทธิภาพ

คณะกรรมการจัดทำขอบเขตของงานฯ วันที่ 9 กรกฎาคม 2569

						
นายจักรกฤษ พรพิทักษ์ ประธานกรรมการ	น.ส.ณัฏฐา ขยาฐิตาวัตร กรรมการ	น.ส.วรรณ นุ่มนวล กรรมการ	นายสุกฤษฎี สรพงษ์ กรรมการ	น.ส.จุฑามาศ อนุธรรมกุล กรรมการ	น.ส.ธนัญญ์ หงษ์ทอง กรรมการ	นายชาญนิตี ตีลี กรรมการ

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักเลขาธิการนายกรัฐมนตรี

นายจักรกฤษ พรพิทักษ์ ประธานกรรมการ	น.ส.ณิชา ขยายูธวัตร กรรมการ	น.ส.วรรณ นุ่มนวล กรรมการ	นายสุกฤษฎี สรหงษ์ กรรมการ	น.ส.จุฑามาศ อนรรฆกุล กรรมการ	น.ส.ธนณัฐ หงษ์ทอง กรรมการ	นายชาญนิธิ ดีลี กรรมการ

ภาคผนวก

ขอบเขตของงาน (Terms of Reference: TOR)

จ้างบริหารจัดการระบบรักษาความมั่นคงปลอดภัยไซเบอร์
ของสำนักเลขาธิการนายกรัฐมนตรี

1. บริการศูนย์เฝ้าระวังตรวจสอบการโจมตีทางไซเบอร์ (Cyber Security Operations Center: CSOC Managed Service) จำนวน 1 ระบบ

- 1.1 มีศูนย์ปฏิบัติการ Cybersecurity Operations Center (CSOC) ในประเทศไทยที่ได้รับมาตรฐานสากล ISO/IEC 27001 และมีความพร้อมในการให้บริการเฝ้าระวังและแจ้งเตือนเหตุการณ์ภัยคุกคามตลอด 7 วัน 24 ชั่วโมง (7 x 24)
- 1.2 จัดหาและติดตั้งอุปกรณ์หรือซอฟต์แวร์ หรือจัดหาเครื่องคอมพิวเตอร์แม่ข่าย (Log Collector) ที่เข้ามาบริหารจัดการข้อมูลจราจรทางคอมพิวเตอร์เพื่อใช้ในการดำเนินงานตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และตามประกาศหลักเกณฑ์การเก็บข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564 ให้เพียงพอและครบถ้วนต่อการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ของสำนักเลขาธิการนายกรัฐมนตรี โดยต้องส่งผลการทดสอบการใช้งานหลังการติดตั้งอุปกรณ์ ซอฟต์แวร์ หรือเครื่องคอมพิวเตอร์แม่ข่าย (Log Collector) ภายใน 30 วันทำการ นับถัดจากลงนามในสัญญา
- 1.3 สามารถรับมือต่อเหตุคุกคามทางไซเบอร์ตามรูปแบบ Playbook หรือ Use Case ที่สำนักเลขาธิการนายกรัฐมนตรีใช้งานอยู่ในปัจจุบันได้เป็นอย่างดี
- 1.4 ตรวจสอบ เฝ้าระวังความพร้อมใช้งานของอุปกรณ์ ซอฟต์แวร์ หรือเครื่องคอมพิวเตอร์แม่ข่าย (Log Collector) ที่ให้บริการจัดการข้อมูลจราจรทางคอมพิวเตอร์ตลอดอายุสัญญา
- 1.5 มีผู้เชี่ยวชาญสำหรับดำเนินการเข้าเตรียมพร้อมและส่งผ่านข้อมูลจราจรทางคอมพิวเตอร์ เพื่อใช้ในการเฝ้าระวัง (On-Boarding Process) โดยต้องทำการจัดเก็บ และดำเนินการสำรองข้อมูลจราจรทางคอมพิวเตอร์ให้สอดคล้องตามข้อกำหนดของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และตามประกาศหลักเกณฑ์การเก็บข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564 ตามรายการทรัพย์สินที่ต้องดำเนินการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ หรือข้อมูลจราจรทางคอมพิวเตอร์อื่น ๆ ที่จำเป็นต่อการใช้สืบสวนและสอบสวนการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
- 1.6 ติดตั้งอุปกรณ์ป้องกันเครือข่าย (Firewall) และระบบป้องกันเว็บแอปพลิเคชันและ API เพื่อใช้ในการควบคุมการเชื่อมต่อระบบเครือข่าย

คณะกรรมการจัดทำขอบเขตของงานฯ วันที่ 9 กรกฎาคม 2569

						
นายจักรกฤษ พรพิทักษ์ ประธานกรรมการ	น.ส.ณัฏฐา ชัยธิตะวาท กรรมการ	น.ส.วรรณ นุ่มนวล กรรมการ	นายสุกฤษฎี สรหงษ์ กรรมการ	น.ส.จุฑามาศ อนรรฆกุล กรรมการ	น.ส.ธนัญญ์ หงษ์ทอง กรรมการ	นายชาญนิจ์ ตีลี กรรมการ

- 1.7 ให้บริการพื้นที่ในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ได้ไม่น้อยกว่า 100 GB/Day และจะต้องทำการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า 365 วัน
- 1.8 ประเมินความเสี่ยงทางด้านไซเบอร์ของสำนักเลขาธิการนายกรัฐมนตรี (Security Assessment) ในด้าน Network Security, Endpoint Security, Cloud Security และ Security Operation Center (SOC) หรือเทียบเท่า โดยจัดทำเอกสารแนวทางในการปรับปรุงแต่ละหัวข้อ ให้สอดคล้องกับมาตรฐานต่าง ๆ ที่สำนักเลขาธิการนายกรัฐมนตรีต้องปฏิบัติตาม เช่น พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และแนวปฏิบัติ NIST Cyber Security Framework เป็นต้น
- 1.9 มีผู้เชี่ยวชาญสำหรับจัดทำแผนการเฝ้าระวัง และจัดเก็บข้อมูลการใช้งานระบบเครือข่ายให้ครอบคลุมจากระบบรักษาความปลอดภัยระบบเครือข่ายระดับแอปพลิเคชัน เพื่อนำไปวิเคราะห์ เฝ้าระวัง และป้องกันภัยคุกคามไซเบอร์ โดยต้องรองรับการเก็บข้อมูลเพื่อการวิเคราะห์ไม่น้อยกว่า 100 GB/Day โดยนำข้อมูลดังกล่าวไปจัดทำ Playbook หรือ Use Case เพื่อใช้ตอบสนองต่อเหตุการณ์ทางไซเบอร์ในลักษณะอัตโนมัติ และกึ่งอัตโนมัติ
- 1.10 เฝ้าระวังตรวจสอบการโจมตีทางไซเบอร์ (Cyber Security Operations Center: CSOC Managed Service) แบบ 24x7 โดยอ้างอิงตามขอบข่ายภัยคุกคามที่เกิดขึ้นจากข้อมูลจราจรระบบเครือข่ายคอมพิวเตอร์ที่ได้จัดเก็บตามรายการทรัพย์สินตามที่สำนักเลขาธิการนายกรัฐมนตรีกำหนด ให้ครอบคลุมการใช้งานระบบเครือข่ายทั้งจากระบบรักษาความปลอดภัยระบบเครือข่ายระดับแอปพลิเคชัน และระบบตรวจจับและตอบสนองต่อภัยคุกคามทางไซเบอร์ในระดับ Endpoint และจะต้องจัดให้มีเจ้าหน้าที่ประสานงานกับสำนักเลขาธิการนายกรัฐมนตรี โดยสามารถติดต่อได้ตลอด 24 ชั่วโมง ตลอดอายุสัญญา
- 1.11 แจ้งเตือนเหตุการณ์ที่อยู่ในขอบข่ายภัยคุกคาม ที่เกิดขึ้นจากข้อมูลจราจรระบบเครือข่ายคอมพิวเตอร์ที่ได้จัดเก็บตามรายการทรัพย์สินที่สำนักเลขาธิการนายกรัฐมนตรีกำหนด โดยดำเนินการจัดเก็บข้อมูลจราจรระบบเครือข่ายคอมพิวเตอร์ และการใช้งานระบบเครือข่ายให้ครอบคลุมทั้งจากระบบรักษาความปลอดภัยระบบเครือข่ายระดับแอปพลิเคชัน รวมถึงระบบตรวจจับและตอบสนองต่อภัยคุกคามทางไซเบอร์ในระดับ Endpoint โดยต้องแจ้งเตือนผ่านทาง Email หรือทางโทรศัพท์ หรือช่องทาง Ticket Management หรือช่องทางอื่นใด ตามที่สำนักเลขาธิการนายกรัฐมนตรีเห็นชอบ
- 1.12 ต้องรักษาระดับการตอบสนองแจ้งเตือนภัยคุกคาม เป็นภาพรวมของระดับความรุนแรงในแต่ละเดือน โดยการให้บริการรวมกันในแต่ละระดับความรุนแรงต้องไม่ต่ำกว่า 95 เปอร์เซนต์ (%) ของจำนวนการแจ้งเตือนในแต่ละระดับความรุนแรง

คณะกรรมการจัดทำขอบเขตของงานฯ วันที่ 9 กรกฎาคม 2569

						
นายจักรกฤษ พรพิทักษ์ ประธานกรรมการ	น.ส.ณัฏฐา ขยาลิตดาวัตร กรรมการ	น.ส.วรรณ นุ่มนวล กรรมการ	นายสุกฤษฎี สรหงษ์ กรรมการ	น.ส.จุฑามาศ อนรรฆกุล กรรมการ	น.ส.ธนัญญ์ หงษ์ทอง กรรมการ	นายชาญนิจิ ดิติ กรรมการ

- 1.13 ต้องทำเงื่อนไขการโจมตี เพื่อช่วยในการเฝ้าระวังและแจ้งเตือนภัยคุกคาม ด้วยรูปแบบและมาตรฐานของผู้รับจ้าง (Standard Use Case) รวมทั้งปรับปรุงและจัดการการแจ้งเตือนภัยคุกคามด้วยรูปแบบเงื่อนไขเฉพาะ หรือเงื่อนไขอื่น ๆ เพิ่มเติม (Custom Use Case) โดยเงื่อนไขการโจมตีด้วยรูปแบบและมาตรฐาน ดังนี้
- 1.13.1 Unauthorized Access
 - 1.13.2 Malicious Code
 - 1.13.3 Inappropriate Usage
 - 1.13.4 Web Site Defacement
 - 1.13.5 DDoS Attack
 - 1.13.6 Intrusion Attempts
 - 1.13.7 Information Gathering
 - 1.13.8 Information Content Security
- 1.14 ดำเนินการจัดหาระบบบริหารจัดการภัยและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ (Security Orchestration Automation and Response : SOAR) จำนวน 1 ระบบ โดยมีคุณสมบัติ ดังนี้
- 1.14.1 เป็นระบบที่ถูกออกแบบมาเพื่อให้สามารถบริหารจัดการและตอบสนองต่อเหตุการณ์ภัยคุกคามที่เกิดขึ้นบนระบบเครือข่ายคอมพิวเตอร์ได้อย่างอัตโนมัติ (Security Orchestration Automation and Response : SOAR)
 - 1.14.2 ระบบที่นำเสนอต้องสามารถสร้างกระบวนการทำงานตอบสนองต่อเหตุการณ์ (Playbook) และเรียกใช้งาน ได้ทั้งแบบอัตโนมัติ และกำหนดเอง
 - 1.14.3 ระบบที่นำเสนอต้องสามารถเชื่อมโยงกับอุปกรณ์อื่นจากผู้ผลิตภายนอก (3rd Party) ผ่านการเรียกใช้ API
- 1.15 จัดทำ Playbook เพื่อใช้ตอบสนองต่อเหตุการณ์ทางไซเบอร์ในลักษณะอัตโนมัติ และกึ่งอัตโนมัติ รวมถึงกำหนดระยะเวลาในการตรวจสอบ และวิเคราะห์กระบวนการที่ได้สร้างขึ้น เพื่อนำมาปรับปรุงกระบวนการให้มีความทันสมัยต่อเหตุการณ์ทางไซเบอร์ โดยต้องเป็น Playbook หรือ Use Case ที่มีความสามารถในการดำเนินการอย่างน้อย ดังนี้
- 1.15.1 Malware Attack
 - 1.15.2 Insider Threat
 - 1.15.3 Bot C&C
 - 1.15.4 DoS/DDoS
 - 1.15.5 Brute Force Login

คณะกรรมการจัดทำขอบเขตของงานฯ วันที่ 9 กรกฎาคม 2569

						
นายจักรกฤษ พรพิทักษ์ ประธานกรรมการ	น.ส.ณัฏฐา ขยาดาว์ตร กรรมการ	น.ส.วรรณ นุ่มนวล กรรมการ	นายสุกฤษฎี สรหงษ์ กรรมการ	น.ส.จุฑามาศ อนรรฆกุล กรรมการ	น.ส.ธนัญญ์ หงษ์ทอง กรรมการ	นายชานนธิ์ ตีลี กรรมการ

- 1.15.6 Threat Hunting
- 1.15.7 Bad Destination
- 1.15.8 Vulnerable Attack
- 1.15.9 High Privileged Change Account
- 1.15.10 High Privileged Non-working Hour
- 1.16 ทำรายงานการเฝ้าระวังตรวจสอบการโจมตีทางไซเบอร์ เป็นไฟล์ข้อมูลอิเล็กทรอนิกส์ และจัดส่งให้กับ
สำนักเลขาธิการนายกรัฐมนตรีตามหัวข้อดังต่อไปนี้
 - 1.16.1 รายงานเหตุการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้น (Incident Report) ซึ่งจะต้องสรุป
เหตุการณ์ที่ตรวจพบ พฤติกรรม ภาพรวมภัยคุกคามและระดับความรุนแรงที่เกิดขึ้น
รายละเอียดเหตุการณ์และพฤติกรรมทั้งหมด และคำแนะนำถึงขั้นตอนการดำเนินการแก้ไข
ด้านเทคนิคแบบละเอียด โดยมีหัวข้อการนำเสนออย่างน้อย ดังนี้
 - 1.16.1.1 ระบุประเภทของภัยคุกคาม
 - 1.16.1.2 วัน-เวลา เริ่มต้นของภัยคุกคาม
 - 1.16.1.3 ระบุต้นทาง (Attacker) และปลายทาง (Target)
 - 1.16.1.4 ระบุระดับความรุนแรง (Severity)
 - 1.16.1.5 รายละเอียดเหตุการณ์และพฤติกรรม
 - 1.16.1.6 คำแนะนำและขั้นตอนการดำเนินการแก้ไขด้านเทคนิค (Action &
Recommendation)
 - 1.16.2 รายงานการเฝ้าระวังภัยคุกคามทางไซเบอร์รายวัน (Daily Report) เป็นรายงานสรุปของ
Incident ที่เกิดขึ้นในแต่ละวัน ซึ่งจะต้องสรุปเหตุการณ์ที่ตรวจพบ พฤติกรรม ภาพรวม
ภัยคุกคามที่เกิดขึ้นทั้งหมดในรอบวัน ระดับความรุนแรงที่เกิดขึ้นในรอบวัน และมีหัวข้อ
การนำเสนออย่างน้อย ดังนี้
 - 1.16.2.1 จำนวนและภาพรวมการแจ้งเตือน (Alert Summary)
 - 1.16.2.2 สรุปเหตุการณ์ภัยคุกคาม (Incident Summary)
 - 1.16.2.3 สรุปภาระงานที่ได้รับการร้องขอ (Service Request)
 - 1.16.2.4 สถานะการเชื่อมต่อ (Online/Offline) ของอุปกรณ์ (Log Sources)
 - 1.16.2.5 ปริมาณ Log Source ของแต่ละอุปกรณ์หรือระบบ

คณะกรรมการจัดทำขอบเขตของงานฯ วันที่ 9 กรกฎาคม 2569

						
นายจักรกฤษ พรพิทักษ์ ประธานกรรมการ	น.ส.ณัชชา ชัยธวัชวัตร กรรมการ	น.ส.วรรณิ นุ่มนวล กรรมการ	นายสุกฤษฎี สรหงษ์ กรรมการ	น.ส.จุฑามาศ อนรรฆกุล กรรมการ	น.ส.ธนัญญ์ หงษ์ทอง กรรมการ	นายชาญนิธิ ตีลี กรรมการ

1.16.3 รายงานการเฝ้าระวังภัยคุกคามทางไซเบอร์รายเดือน (Monthly Report) และรายไตรมาส (Quarterly) มีเนื้อหาอย่างน้อย ดังนี้

1.16.3.1 รายเดือน: สรุปเหตุการณ์ตามประเภทและระดับความรุนแรง (Incident Report) ดังนี้

- 1) สรุป 10 อันดับสูงสุดของการโจมตี
- 2) สรุป 10 อันดับสูงสุดของเป้าหมายที่โดนโจมตี
- 3) สรุป 10 อันดับสูงสุดของผู้โจมตี
- 4) สรุป 10 อันดับสูงสุดของช่องทางที่ถูกใช้โจมตี
- 5) บทวิเคราะห์แนวโน้มของภัยคุกคามต่าง ๆ ที่เกิดขึ้นในเดือนที่ผ่านมา
- 6) สรุปคำแนะนำที่สำนักเลขาธิการนายกรัฐมนตรีต้องดำเนินการปรับปรุง

1.16.3.2 รายไตรมาส: สรุปเหตุการณ์ตามประเภทและระดับความรุนแรง (Incident Report) ดังนี้

- 1) รายงานระดับคะแนนความปลอดภัยทางไซเบอร์ภาพรวมขององค์กร (Cybersecurity Rating Report)
- 2) บทวิเคราะห์ความเสี่ยง
- 3) คำแนะนำและแนวทางการปรับปรุงระดับคะแนน
- 4) การเปรียบเทียบค่าระดับคะแนนจากไตรมาสที่ผ่านมา

1.17 ต้องอัปเดตข้อมูลข่าวสารเกี่ยวกับภัยคุกคามร้ายแรงด้านความปลอดภัยสารสนเทศ ที่เกิดขึ้นเป็นรายสัปดาห์เป็นอย่างน้อย ที่คาดว่าจะมีผลกระทบต่อทรัพย์สินและระบบสารสนเทศของสำนักเลขาธิการนายกรัฐมนตรี เป็นภาษาไทยผ่านระบบสรุปผลการดำเนินการเฝ้าระวังและตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ ซึ่งสามารถแสดงภาพรวมและสั่งการระบบได้ ดังนี้

1.17.1 จำนวนของเหตุการณ์ (Incident) ที่เกิดขึ้น โดยแบ่งประเภทตามความรุนแรง (Severity)

1.17.2 จำนวนของเหตุการณ์ (Incident) ที่เกิดขึ้น ในแต่ละเดือน

1.17.3 สามารถแสดงรายการเหตุการณ์ (Incident) ที่เกิดขึ้น โดยแสดงข้อมูลอย่างน้อย ดังนี้ หมายเลข ID ชื่อเหตุการณ์ ความรุนแรง (Severity) สถานะ การตอบสนอง (Action) วันที่เกิดเหตุการณ์ (Created Date) วันที่เหตุการณ์สิ้นสุด (Closed Date) และดูข้อมูลย้อนหลังได้ 7 วัน 15 วัน และ 30 วัน

1.17.4 สามารถแสดงรายการเครื่องปลายทาง (Endpoint) โดยแสดงข้อมูลอย่างน้อย ดังนี้ ชื่อเครื่อง ประเภท OS, IP Address, Mac Address และ Policy ที่ได้รับการใช้งาน

1.17.5 สามารถสั่งการทำงานไปยังเครื่องปลายทาง (Endpoint) โดยสามารถสั่งตัดการเชื่อมต่อจากระบบเครือข่าย (Isolate) และสั่งสแกนเครื่องปลายทาง (Scan) ได้

1.17.6 มีบริการอัปเดตข้อมูลข่าวสารภัยคุกคามให้กับเจ้าหน้าที่เป็นภาษาไทย

คณะกรรมการจัดทำขอบเขตของงานฯ วันที่ 9 กรกฎาคม 2569

						
นายจักรกฤษ พรพิทักษ์ ประธานกรรมการ	น.ส.ณัฏฐา ขยารัฐาวัตร กรรมการ	น.ส.วรรณิ นุ่มนวล กรรมการ	นายสุกฤษฏี สรหงษ์ กรรมการ	น.ส.จุฑามาศ อนรรฆกุล กรรมการ	น.ส.ธนัญญ์ หงษ์ทอง กรรมการ	นายชาญนิจิ ดิล กรรมการ

- 1.17.7 มีการรวบรวมข้อมูล Campaign ที่เกี่ยวข้องกับ Common Vulnerabilities and Exposures (CVE) เพื่อใช้เป็นแหล่งข้อมูลอ้างอิง
 - 1.17.8 มีการรวบรวมข้อมูล Threat Indicator โดยสามารถแบ่งได้ตามประเภทและ Actor
 - 1.17.9 สามารถเปิดเคสเพื่อติดต่อกับผู้เชี่ยวชาญด้านระบบเฝ้าระวังภัยคุกคามทางไซเบอร์ที่ผู้รับจ้างให้บริการได้
 - 1.18 ผู้รับจ้างต้องจัดให้มีการประชุมรายเดือน (Monthly Meeting) ในรูปแบบประชุมทางไกล (Video Conference) เพื่อสรุปผลงานบริการวิเคราะห์เฝ้าระวังภัยคุกคามต่าง ๆ ที่เกิดขึ้นกับผู้ให้บริการตลอดอายุสัญญา
2. บริการตรวจจับและตอบสนองต่อภัยคุกคามทางไซเบอร์ในระดับ Endpoint (Managed Detection and Response: MDR) จำนวน 1 ระบบ
- 2.1 ให้บริการตรวจจับและตอบสนองต่อภัยคุกคามทางไซเบอร์ในระดับ Endpoint เพื่อทำการป้องกัน (Prevent) และตรวจจับ (Detect) ภัยคุกคามทางไซเบอร์สำหรับเครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ลูกข่าย จำนวนเครื่องได้ไม่น้อยกว่า 1,000 สิทธิ์ และให้ครบถ้วนตามรายการทรัพย์สินที่ต้องดำเนินการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ และต้องส่งผลการติดตั้งระบบตรวจจับและตอบสนองต่อภัยคุกคามทางไซเบอร์ในระดับ Endpoint ภายใน 30 วันทำการ หลังจากลงนามในสัญญา รวมทั้งต้องส่งหนังสือรับรองว่าระบบตรวจจับและตอบสนองต่อภัยคุกคามทางไซเบอร์ในระดับ Endpoint เป็นลิขสิทธิ์ซอฟต์แวร์ที่ถูกต้องตามกฎหมายให้สำนักเลขาธิการนายกรัฐมนตรีทราบ
 - 2.2 จัดหาผู้เชี่ยวชาญ และเครื่องมือที่นำมาให้บริการในการตรวจจับและตอบสนองต่อภัยคุกคามทางไซเบอร์ในระดับ Endpoint เพื่อให้สามารถใช้งานได้อย่างต่อเนื่องและมีประสิทธิภาพ โดยเครื่องมือที่ให้บริการต้องมีคุณสมบัติอย่างน้อย ดังนี้
 - 2.2.1 โปรแกรมที่นำเสนอต้องเป็นผลิตภัณฑ์ที่อยู่ในกลุ่ม Leader Gartner Magic Quadrant ด้าน Endpoint Protection Platforms ปี 2025 และ The Forrester Wave™: Extended Detection And Response Platform, Q2 2024
 - 2.2.2 โปรแกรมที่นำเสนอต้องมีคุณสมบัติอย่างน้อย ดังนี้
 - 2.2.2.1 การป้องกันไวรัส (NextGen-AV)
 - 2.2.2.2 Endpoint Detection and Response (EDR)
 - 2.2.2.3 บริการล่าภัยคุกคามเพื่อการป้องกันเชิงรุกโดยผู้เชี่ยวชาญจากเจ้าของผลิตภัณฑ์ (Human Managed Threat Hunting) หรือผู้เชี่ยวชาญที่ได้รับการแต่งตั้งจากเจ้าของผลิตภัณฑ์ตลอด 7 วัน 24 ชั่วโมง (7 x 24)

คณะกรรมการจัดทำขอบเขตของงานฯ วันที่ 9 กรกฎาคม 2569

						
นายจักรกรฤช พรพิทักษ์ ประธานกรรมการ	น.ส.ณิชา ชัยธวัชวาท กรรมการ	น.ส.วรรณ นุ่มนวล กรรมการ	นายสุกฤษฎี สรหงษ์ กรรมการ	น.ส.จุฑามาศ อนรรฆกุล กรรมการ	น.ส.ธนัญญ์ หงษ์ทอง กรรมการ	นายชาญนิตี ตีลี กรรมการ

- 2.2.3 มีระบบบริหารจัดการแบบรวมศูนย์ (Single Console) โดยต้องบริหารจัดการ Policy ของ Endpoint ต่าง ๆ ได้อย่างน้อย ดังนี้ Windows, Linux และ Mac
- 2.2.4 สามารถทำการยืนยันตัวตนร่วมกับระบบ 2 Factor Authentication ได้
- 2.2.5 สามารถทำ Single Sign-On ร่วมกับระบบยืนยันตัวตนภายนอกได้อย่างน้อย ดังนี้ Okta, Ping, AD FS และ Microsoft Entra ID (Azure AD)
- 2.2.6 สามารถติดตั้งได้กับระบบปฏิบัติการอย่างน้อย ดังนี้
 - 2.2.6.1 Windows
 - 2.2.6.2 Windows Server
 - 2.2.6.3 CentOS
 - 2.2.6.4 Debian
 - 2.2.6.5 Oracle Linux
 - 2.2.6.6 Red Hat Enterprise Linux
 - 2.2.6.7 SUSE
 - 2.2.6.8 Ubuntu
- 2.2.7 สามารถตรวจจับ Malware โดยไม่อาศัย Signature และไม่ต้องทำการ Update Signature บนเครื่องลูกข่าย โดยโปรแกรมที่ติดตั้งเป็นแบบ Lightweight Agent
- 2.2.8 โปรแกรมที่นำเสนอต้องทำการ Upgrade Machine Learning และ Indicator of Attack (IOA) หรือ Indicator of Compromise (IOC) โดยแยกจากการ Update Patch ของ Operating System เพื่อให้สามารถทำการ Update ได้อย่างอิสระ
- 2.2.9 โปรแกรมที่นำเสนอต้องสามารถป้องกัน Known and Unknown Malware , Adware และ Potentially Unwanted Programs (PUPs) หรือซอฟต์แวร์ที่ไม่พึงประสงค์ ด้วยเทคโนโลยี Machine Learning
- 2.2.10 สามารถป้องกัน Malware และการโจมตีที่ไม่เกิดจากมัลแวร์ (Malware-Free Attack) ด้วยเทคโนโลยี Machine Learning และ Indicator of Attack (IOA) หรือ Indicator of Compromise (IOC) ได้เป็นอย่างน้อย
- 2.2.11 สามารถแสดงผลของภัยคุกคามที่เกิดขึ้นออกมาเป็นรูปภาพ, Process Tree และ Process Table หรือ Process Activity ได้
- 2.2.12 สามารถกำหนด Policy ตามกลุ่มของเครื่อง (Host Groups) ได้

คณะกรรมการจัดทำขอบเขตของงานฯ วันที่ 9 กรกฎาคม 2569

						
นายจักรกฤษ พรพิทักษ์ ประธานกรรมการ	น.ส.ณัชชา ขยารัตน์ กรรมการ	น.ส.วรรณ นุ่มนวล กรรมการ	นายสุกฤษฎี สรหงษ์ กรรมการ	น.ส.จุฑามาศ อนรรฆกุล กรรมการ	น.ส.ธนัญญ์ หงษ์ทอง กรรมการ	นายชาญนิตี ตีลี กรรมการ

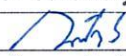
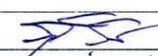
- 2.2.13 สามารถทำการตัดการเชื่อมต่อของระบบเครือข่าย (Network Containment / Network Isolation) บนเครื่องที่มีการติดตั้ง Agent จากระบบบริหารจัดการส่วนกลาง (Centralize Management) บน Windows, MacOS และ Linux ตามจำนวน License ที่เสนอ
- 2.2.14 สามารถเชื่อมต่อกลับไปยังเครื่องต่าง ๆ (Real Time Response) เพื่อทำการ Run Command ต่าง ๆ ไปยังเครื่อง Windows, MacOS, iOS และ Linux ตามจำนวน License ทั้งหมดที่เสนอได้
- 2.2.15 สามารถป้องกันการ Exploit ไปยังช่องโหว่ (Vulnerability) เพื่อยึดเครื่อง (Compromised) ได้
- 2.2.16 ระบบที่นำเสนอต้องสามารถป้องกันการโจมตี เช่น มัลแวร์ หรือไวรัส (Malware Prevention หรือ Antivirus) มัลแวร์ระดับสูง ที่ใช้เทคนิคโจมตีแบบไม่ใช้ไฟล์ (Fileless Attacks) การโจมตีโดยใช้การวิเคราะห์พฤติกรรม (Behavior Threat Prevention) และมัลแวร์เรียกค่าไถ่ (Ransomware Protection)
- 2.2.17 สามารถป้องกันการทำงานของ Registry ที่มีพฤติกรรมที่ต้องสงสัยได้
- 2.2.18 สามารถสร้าง Custom Hash เพื่อทำการ Block List และ Allow List ได้
- 2.2.19 สามารถเปิดการทำงานในรูปแบบ Endpoint Detection and Response (EDR) เพื่อเก็บข้อมูลการใช้งาน (Activity) ของเครื่อง Endpoint ต่าง ๆ และนำมาวิเคราะห์ภัยคุกคามร่วมกับอุปกรณ์ป้องกันเครือข่าย (Firewall) แบบ Real-Time ได้
- 2.2.20 สามารถแสดงข้อมูลการแจ้งเตือนภัยคุกคาม (Alerts) ในรูปแบบ MITRE ATT&CK Framework เพื่อง่ายต่อการทำความเข้าใจ
- 2.2.21 สามารถเก็บข้อมูลภายในระบบปฏิบัติการ (Kernel-Mode หรือ Kernel Module) เพื่อนำมาย้อนรูปแบบหรือตรวจจับภัยคุกคามที่เกิดขึ้น (Incident)
- 2.2.22 สามารถสร้าง Indicator of Attack (IOA) หรือ Indicator of Compromise (IOC) เพื่อตรวจจับพฤติกรรมที่ผิดปกติ (Suspicious Behaviors) หรือต้องการตรวจจับพฤติกรรมการทำงานที่องค์กรต้องการเฝ้าระวังจากเหตุการณ์ที่เคยเกิดขึ้นและคาดว่าจะเกิดได้
- 2.2.23 สามารถค้นหาข้อมูลการใช้งาน Source IP Address, Domain และ Event ที่เกี่ยวข้องกับข้อมูลการใช้งาน (Activity) ได้
- 2.2.24 สามารถค้นหาข้อมูลการใช้งานภายในที่เกี่ยวข้องกับเครื่อง Windows และ Mac (Host Search) ได้
- 2.2.25 สามารถค้นหาข้อมูลการใช้งาน Hash (Hash Search) กับเครื่อง Windows และ Mac ได้

คณะกรรมการจัดทำขอบเขตของงานฯ วันที่ 9 กรกฎาคม 2569

						
นายจักรกฤษ พรพิทักษ์ ประธานกรรมการ	น.ส.ณัษชา ชยาธิตาวัตร กรรมการ	น.ส.วรรณิ นุ่มนวล กรรมการ	นายสุกฤษฎี สรหงษ์ กรรมการ	น.ส.จุฑามาศ อนรรฆกุล กรรมการ	น.ส.ธนัญญ์ หงษ์ทอง กรรมการ	นายชานูนิตี ตีลี กรรมการ

- 2.2.26 สามารถค้นหาข้อมูลการใช้งาน Username (User Search) กับเครื่อง Windows และ Mac ได้
- 2.2.27 สามารถระบุช่องโหว่ (Vulnerability) ของเครื่อง Windows, Mac และ Linux ได้ โดยต้องแสดงผลบน Console อันเดียวกัน โดยไม่จำเป็นต้องลงโปรแกรมอื่นเพิ่มเติม
- 2.3 ให้บริการวิเคราะห์และตรวจจับ (Analysis & Detection) เหตุการณ์ที่ตรวจพบบนระบบและตอบสนองต่อภัยคุกคามทางไซเบอร์ในระดับ Endpoint เป็นอย่างน้อยดังต่อไปนี้
- 2.3.1 บริการวิเคราะห์และตรวจจับ (Analysis & Detection) โดยอาศัยข้อมูลต่าง ๆ ที่ถูกเก็บรวบรวมอยู่ในระบบ Endpoint Protection Platform (EDR Data)
- 2.3.2 ส่งผลวิเคราะห์และคำแนะนำในการแก้ไขปัญหา (Remediation) เป็นภาษาไทยผ่านทาง Email โดยผู้ว่าจ้างสามารถสอบถามหรือค้นหาข้อมูลเพิ่มเติมได้บน Web Portal ของผู้ให้บริการ
- 2.3.3 บริการแก้ไขปัญหาโดยวิธีการเข้าถึงจากระยะไกล (Remote Remediation) ภายใต้ความสามารถของฟังก์ชัน Remote ที่มีอยู่ในระบบ Endpoint Protection Platform เช่น การลบ File หรือแก้ไข Registry ที่น่าสงสัย เป็นต้น
- 2.3.4 บริการสืบค้นข้อมูลในระบบของผู้ใช้บริการ โดยอาศัยข้อมูลต่าง ๆ ที่ถูกเก็บรวบรวมอยู่ในระบบ Endpoint Protection Platform (EDR Data) ตามที่สำนักเลขาธิการนายกรัฐมนตรีเห็นควรให้ดำเนินการ
- 2.3.5 บริหารจัดการ (Managed) และปรับแต่ง (Fine-Tune) ระบบ Endpoint Protection Platform
- 2.3.6 บริการให้คำแนะนำเกี่ยวกับระบบ Endpoint Protection Platform เป็นภาษาไทยทาง Email
- 2.4 ดำเนินการระงับภัยคุกคามทางไซเบอร์ที่มีการติดตั้ง Endpoint โดยต้องสามารถระงับภัยคุกคามได้ทันทีภายใต้ Policy ของระบบ Endpoint ที่สำนักเลขาธิการนายกรัฐมนตรีกำหนด
- 2.5 ดำเนินการระงับภัยคุกคามทางไซเบอร์ที่มีการติดตั้ง Endpoint ภายใน 2 ชั่วโมง ด้วยวิธีการเข้าถึงจากระยะไกล (Remote Remediation) ภายใต้ความสามารถของฟังก์ชัน Remote ที่มีอยู่ในระบบ Endpoint Protection Platform กรณีที่ไม่ตรงกับ Policy ของระบบ Endpoint หรือมีการร้องขอจากสำนักเลขาธิการนายกรัฐมนตรี
- 2.6 ดำเนินการเฝ้าระวังเหตุคุกคามทางไซเบอร์ให้กับทางสำนักเลขาธิการนายกรัฐมนตรีและต้องวิเคราะห์ความเป็นไปได้ของแหล่งที่มาของการโจมตี และสามารถตอบสนองต่อเหตุการณ์ภัยคุกคาม โดยสั่งงานให้ Isolate และ ยกเลิกการ Isolate เครื่องคอมพิวเตอร์ที่เกี่ยวข้องกับเหตุการณ์ภัยคุกคามทั้งหมดได้

คณะกรรมการจัดทำขอบเขตของงานฯ วันที่ 9 กรกฎาคม 2569

						
นายจักรกฤษ พรพิทักษ์ ประธานกรรมการ	น.ส.ณัชชา ชัยธิตาวัตร กรรมการ	น.ส.วรรณิ นุ่มนวล กรรมการ	นายสุกฤษฎี สรพงษ์ กรรมการ	น.ส.จุฑามาศ อนรรณกุล กรรมการ	น.ส.ธนัญญ์ หงษ์ทอง กรรมการ	นายชาญนิติ ตีลี กรรมการ

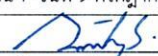
- 2.7 ดำเนินการเพิ่มและแก้ไข Behavior indicators of compromise (BIOC) เพื่อให้สามารถสร้าง Alert จากเหตุการณ์ที่เคยเกิดขึ้นในอดีตย้อนหลังได้ เพื่อใช้ในกรณีที่สำนักเลขาธิการนายกรัฐมนตรีได้รับ ข้อมูลการโจมตี และการแจ้งเตือนจากหน่วยงานที่เกี่ยวข้องเพื่อตรวจสอบข้อมูลที่เกิดขึ้น

3. บริการบุคลากรผู้มีความรู้ความเชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security)

ผู้รับจ้างจะต้องจัดให้มีบุคลากรผู้มีความรู้ความเชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ซึ่งมีคุณสมบัติตาม ข้อ 13. เพื่อปฏิบัติหน้าที่ในการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับสำนักเลขาธิการนายกรัฐมนตรี ดังนี้

- 3.1 ผู้จัดการโครงการ (Project Manager) ทำหน้าที่กำกับ ดูแล และติดตามการดำเนินการบริหารจัดการ การรักษาความปลอดภัยไซเบอร์ของสำนักเลขาธิการนายกรัฐมนตรี ตลอดอายุสัญญา
- 3.2 ผู้จัดการศูนย์ปฏิบัติการรักษาความปลอดภัยทางไซเบอร์ (CSOC Manager) หรือที่ปรึกษา ด้านความปลอดภัย (Security Consultant) หรือ ผู้จัดการศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัย ไซเบอร์ (MDR Manager) อย่างน้อย 1 ราย ทำหน้าที่ควบคุมและบริหารจัดการการรักษา ความปลอดภัยไซเบอร์ รวมทั้งการพัฒนาระบบและกำหนดนโยบายด้านความมั่นคงปลอดภัย ไซเบอร์ให้เหมาะสมและเป็นปัจจุบัน
- 3.3 ผู้เชี่ยวชาญด้านระบบเฝ้าระวังภัยคุกคามทางไซเบอร์ (Security Analyst Tier 3) อย่างน้อย 1 ราย ทำหน้าที่ วิเคราะห์ Root Cause Analysis ของเหตุการณ์ร้ายแรง โดยใช้ข้อมูลเชิงลึก จาก Endpoint, Network, Email และ Cloud Telemetry ที่จัดเก็บจาก EDR หรือ Log Source พร้อม กับปฏิบัติการ Digital Forensics และ Malware Analysis เพื่อตรวจสอบพฤติกรรมของไฟล์ และกระบวนการ (Process) ที่ต้องสงสัย
- 3.4 ผู้เชี่ยวชาญด้านระบบเฝ้าระวังภัยคุกคามทางไซเบอร์ (Security Analyst Tier 2) อย่างน้อย 2 ราย ทำหน้าที่ดำเนินการตรวจสอบค้นหาเหตุการณ์เชิงลึก พร้อมทั้งให้คำแนะนำการแก้ไขปัญหาหรือ การป้องกันเบื้องต้น
- 3.5 ผู้เชี่ยวชาญด้านระบบเฝ้าระวังภัยคุกคามทางไซเบอร์ (Security Analyst Tier 1) อย่างน้อย 3 ราย ทำหน้าที่ตรวจสอบและวิเคราะห์เหตุการณ์ภัยคุกคามที่ได้รับผ่านการแจ้งเตือนจากระบบ จัดเก็บและวิเคราะห์ข้อมูลความปลอดภัย และระบบบริหารจัดการภัยคุกคามโดยการวิเคราะห์ พฤติกรรมภัยคุกคามที่ให้บริการ และแจ้งข้อมูลภัยคุกคามและเหตุการณ์ให้กับผู้ที่เกี่ยวข้อง ตลอด 24 ชั่วโมง โดยกำหนดรอบการทำงานและแบ่งทีมการทำงานให้มีความเหมาะสมต่อการ ให้บริการกับสำนักเลขาธิการนายกรัฐมนตรี

คณะกรรมการจัดทำขอบเขตของงานฯ วันที่ 9 กรกฎาคม 2569

						
นายจักรกรกฎ พรพิทักษ์ ประธานกรรมการ	น.ส.ณัชชา ขยารัตน์ กรรมการ	น.ส.วรรณิ นุ่มนวล กรรมการ	นายสุกฤษฎี สรหงษ์ กรรมการ	น.ส.จุฑามาศ อนรรฆกุล กรรมการ	น.ส.ธนัญญ์ หงษ์ทอง กรรมการ	นายชาญนิตี ตีลี กรรมการ

3.6 ผู้เชี่ยวชาญด้านระบบเฝ้าระวังภัยคุกคามทางไซเบอร์ ระดับ 1 (Security Analyst Tier 1) เพื่อปฏิบัติงานที่สำนักเลขาธิการนายกรัฐมนตรี ในวันและเวลาราชการ อย่างน้อย 1 ราย ทำหน้าที่เฝ้าระวัง (Monitor) ป้องกัน (Prevent) ตรวจจับ (Detect) และตอบสนอง (Response) ต่อภัยคุกคามทางไซเบอร์ ที่แอบแฝงเข้ามาภายในระบบเครือข่ายของสำนักเลขาธิการนายกรัฐมนตรี

4. บริการตรวจสอบและเตรียมความพร้อมด้านความปลอดภัยไซเบอร์ (Cybersecurity Assessment and Readiness Services)

4.1 บริการประเมินหาช่องโหว่ประจำปี (Annual Vulnerability Assessment: VA Scan) จำนวน 1 ครั้ง/ปี

4.1.1 ดำเนินการค้นหาช่องโหว่ ประเมินหาจุดอ่อน ประเมินความเสี่ยงและผลกระทบ (Vulnerability Assessment) พร้อมจัดทำข้อเสนอแนะสำหรับแนวทางแก้ไขช่องโหว่ที่พบบนระบบปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่าย (Server Operating Systems) จำนวนไม่น้อยกว่า 30 IPs โดยใช้โปรแกรมหรือซอฟต์แวร์แบบ Commercial ที่มีความน่าเชื่อถือ และเป็นโปรแกรมที่มีลิขสิทธิ์ถูกต้อง

4.1.2 ต้องแจ้งสำนักเลขาธิการนายกรัฐมนตรี ให้ทราบถึงแผนการเข้าดำเนินงาน เครื่องมือที่ใช้ หรือเทคนิคที่ใช้ในการตรวจสอบระบบ รวมถึงการประเมินผลกระทบที่อาจเกิดขึ้นระหว่างดำเนินงานทุกครั้งก่อนเข้าดำเนินการ ทั้งนี้จะต้องแจ้งให้สำนักเลขาธิการนายกรัฐมนตรีทราบล่วงหน้าเป็นลายลักษณ์อักษร อย่างน้อย 3 วันทำการ และสามารถเข้าดำเนินการได้หลังจากที่ได้รับความเห็นชอบจากสำนักเลขาธิการนายกรัฐมนตรี

4.1.3 ต้องนำส่งรายงานผลการประเมินหาช่องโหว่ประจำปี รอบที่ 1 ประกอบด้วยรายละเอียดช่องโหว่ หรือจุดอ่อนที่พบ โดยแสดงถึงปริมาณช่องโหว่ของระบบ ความเสี่ยงที่พบ และแนวทางการแก้ไข ภายใน 30 วันหลังจากเข้าดำเนินการค้นหาช่องโหว่ และประเมินหาจุดอ่อน ทั้งนี้รายงานดังกล่าวจะต้องลงนามรับรองโดยบุคลากรในข้อ 4.1.7

4.1.4 ต้องรับผิดชอบในข้อเสนอแนะสำหรับแนวทางในการแก้ไขช่องโหว่ให้กับผู้ดูแลระบบ และผู้พัฒนาระบบของสำนักเลขาธิการนายกรัฐมนตรีภายหลังจากการทดสอบการค้นหาช่องโหว่

4.1.5 ดำเนินการตรวจสอบผลการดำเนินการปิดช่องโหว่หรือจุดอ่อนซ้ำ (Revisit) เพื่อยืนยันช่องโหว่ที่พบว่าได้รับการแก้ไขแล้ว และหาช่องโหว่ที่อาจยังเหลืออยู่

4.1.6 จัดส่งรายงานผลการประเมินหาช่องโหว่ประจำปี รอบที่ 2 ประกอบด้วยบทวิเคราะห์คำแนะนำ การแก้ไข และบทสรุปผู้บริหาร ภายใน 30 วัน หลังจากเข้าดำเนินการตรวจสอบการปิดช่องโหว่ซ้ำ (Revisit) ทั้งนี้รายงานดังกล่าวจะต้องลงนามรับรองโดยบุคลากรในข้อ 4.1.7

คณะกรรมการจัดทำขอบเขตของงานฯ วันที่ 9 กรกฎาคม 2569

						
นายจักรกฤษ พรพิทักษ์ ประธานกรรมการ	น.ส.ณัฏฐา ชยาธิ์ดาวัตร กรรมการ	น.ส.วรรณิ นุ่มนวล กรรมการ	นายสุกฤษฎี สรพงษ์ กรรมการ	น.ส.จุฑามาศ อนรรฆกุล กรรมการ	น.ส.ธนัญญ์ หงษ์ทอง กรรมการ	นายชาญนิติ ตีลี กรรมการ

- 4.1.7 บุคลากรที่ดำเนินการประเมินช่องโหว่ ต้องเป็นผู้ที่มีความรู้ความสามารถทางด้านระบบเครือข่าย ระบบคอมพิวเตอร์แม่ข่าย และระบบรักษาความปลอดภัย และจะต้องมีใบประกาศนียบัตรหรือหนังสือรับรอง อย่างใด อย่างหนึ่ง ดังนี้
- 4.1.7.1 GPEN (GIAC Penetration Tester)
 - 4.1.7.2 GSEC (GIAC Security Essentials)
 - 4.1.7.3 OSCP (Offensive Security Certified Professional)
 - 4.1.7.4 CEH (Certified Ethical Hacker)
 - 4.1.7.5 CompTIA CySA+
- 4.1.8 ต้องมีการประชุมร่วมกับผู้ดูแลระบบของสำนักเลขาธิการนายกรัฐมนตรี เพื่อแจ้งแผนการดำเนินการก่อนทำการประเมินช่องโหว่ และรายงานผลหลังการดำเนินการ
- 4.1.9 การประเมินช่องโหว่ต้องไม่ส่งผลกระทบต่อหรือสร้างความเสียหายต่อระบบงานของสำนักเลขาธิการนายกรัฐมนตรี หากมีความเสียหายใด ๆ อันเกิดจากการดำเนินการของผู้รับจ้าง จะต้องรายงานให้สำนักเลขาธิการนายกรัฐมนตรีทราบทันที และผู้รับจ้างต้องเป็นผู้รับผิดชอบต่อความเสียหายนั้น รวมถึงต้องทำให้ระบบงานที่เสียหายหรือได้รับผลกระทบนั้นกลับมาใช้งานได้เป็นปกติดังเดิม โดยไม่มีค่าใช้จ่ายใด ๆ ทั้งสิ้น
- 4.1.10 ผู้รับจ้างจะต้องมีการบริการทางโทรศัพท์ (On Call Service) ในวันและเวลาราชการ
- 4.1.11 มีบุคลากรให้คำปรึกษาเกี่ยวกับรายงานการตรวจสอบช่องโหว่ แนวทางการแก้ไขปัญหา และข้อเสนอแนะที่เป็นประโยชน์ต่อการพัฒนาระบบการรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้กับสำนักเลขาธิการนายกรัฐมนตรีตลอดอายุสัญญา
- 4.2 บริการทดสอบเจาะระบบภายนอกและระบบที่เปิดให้เข้าถึงจากภายนอก (Annual External Network and Public-Facing Penetration Test - Black-box) จำนวน 1 ครั้ง/ปี
- 4.2.1 ดำเนินทดสอบเจาะระบบเครื่องคอมพิวเตอร์แม่ข่ายจากภายนอก โดยแบ่งการทดสอบเป็น 2 รอบ โดยรอบที่ 1 คือการทดสอบเจาะระบบ (Initial Test) และรอบที่ 2 คือการทดสอบเจาะระบบซ้ำ (Revisit Test) โดยมีระบบเป้าหมายที่ต้องทำการทดสอบอย่างน้อย ดังนี้

คณะกรรมการจัดทำขอบเขตของงานฯ วันที่ 9 กรกฎาคม 2569

						
นายจักรกฤษ พรพิทักษ์ ประธานกรรมการ	น.ส.ณัฏฐา ขยาลัฐิวัฒน์ กรรมการ	น.ส.วรรณ นุ่มนวล กรรมการ	นายสุกฤษฎี สรหงษ์ กรรมการ	น.ส.จุฑามาศ อนรรฆกุล กรรมการ	น.ส.ธนัญญ์ หงษ์ทอง กรรมการ	นายชาญนิติ ตีลี กรรมการ

ลำดับ	ชื่อโดเมน	ลำดับ	ชื่อโดเมน
1	thaigov.go.th	8	edoc.thaigov.go.th
2	langban.thaigov.go.th	9	portal.thaigov.go.th
3	archives.thaigov.go.th	10	spm.e-office.cloud
4	media.thaigov.go.th	11	epcos.thaigov.go.th
5	analytics.thaigov.go.th	12	pmone.thaigov.go.th
6	spm.thaigov.go.th	13	dpis6.thaigov.go.th
7	budget.thaigov.go.th	14	acoc.thaigov.go.th

- 4.2.2 ดำเนินการทดสอบเจาะระบบภายนอกและระบบที่เปิดให้เข้าถึงจากภายนอกประจำปี (Annual External Network and Public-Facing Penetration Test - Black-box) จากเครือข่ายภายนอกในรูปแบบ Black Box
- 4.2.3 รายงานผลการทดสอบเจาะระบบภายนอกและระบบที่เปิดให้เข้าถึงจากภายนอกประจำปี (Annual External Network and Public-Facing Penetration Test - Black-box) ประกอบด้วย ผลการประเมินความเสี่ยง ผลการทดสอบอย่างละเอียด วิธีการทดสอบ พร้อมผลการวิเคราะห์ผลกระทบจากความเสี่ยง และข้อเสนอแนะเพื่อใช้ในการแก้ไขปัญหา ทั้ง 2 รอบ ทั้งนี้รายงานดังกล่าวจะต้องลงนามรับรองโดยบุคลากรในข้อ 4.2.4
- 4.2.4 บุคลากรที่ดำเนินการต้องเป็นผู้ที่มีความรู้ความสามารถด้านระบบเครือข่าย ระบบคอมพิวเตอร์ แม่ข่าย และระบบรักษาความปลอดภัย โดยมีใบประกาศนียบัตรหรือหนังสือรับรอง อย่างใดอย่างหนึ่ง ดังนี้
- 4.2.4.1 Offensive Security Certified Professional (OSCP)
- 4.2.4.2 Offensive Security Web Expert (OSWE)
- 4.2.5 ผู้รับจ้างจะต้องมีการบริการทางโทรศัพท์ (On Call Service) ในวันและเวลาราชการ
- 4.2.6 มีบุคลากรให้คำปรึกษาเกี่ยวกับรายงานการทดสอบเจาะระบบภายนอกและระบบที่เปิดให้เข้าถึงจากภายนอก แนวทางการแก้ไขปัญหา และข้อเสนอแนะที่เป็นประโยชน์ต่อการพัฒนาระบบการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ให้กับสำนักเลขาธิการนายกรัฐมนตรี ตลอดจนอายุสัญญา

คณะกรรมการจัดทำขอบเขตของงานฯ วันที่ 9 กรกฎาคม 2569

นายจักรกฤษ พรพิทักษ์ ประธานกรรมการ	น.ส.ณัษชา ชัยธวัชวาท กรรมการ	น.ส.วรรณ นุ่มนวล กรรมการ	นายสุกฤษฎี สรหังษ์ กรรมการ	น.ส.จุฑามาศ อนรรฆกุล กรรมการ	น.ส.ธนัญญ์ หงษ์ทอง กรรมการ	นายชาญนิธิ ดีสี กรรมการ

4.3 บริการทดสอบความพร้อมของบุคลากรผ่านการจำลองสถานการณ์ (Cyber Drill Testing: Phishing Mail) จำนวน 1 ครั้ง/ปี

- 4.3.1 ดำเนินการจัดทำแผนการทดสอบ Cyber Drill ด้วยวิธีการ Phishing Mail 1 ครั้ง จำนวน 2 รอบ แต่ละรอบมีระยะเวลาห่างกันไม่น้อยกว่า 2 เดือน โดยกำหนดกลุ่มเป้าหมายที่เป็นบุคลากร (Staff) ของสำนักเลขาธิการนายกรัฐมนตรี จำนวนไม่น้อยกว่า 800 บัญชีต่อรอบ และสามารถรองรับได้ถึง 1,500 บัญชีต่อรอบ ทั้งนี้ ต้องได้รับความเห็นชอบจากสำนักเลขาธิการนายกรัฐมนตรีก่อนดำเนินการทดสอบดังกล่าว
- 4.3.2 การทดสอบส่ง Phishing Mail จะต้องไม่กระทบต่อระบบงานของสำนักเลขาธิการนายกรัฐมนตรีและไม่ละเมิดลิขสิทธิ์ รวมถึงกฎหมายที่สำนักเลขาธิการนายกรัฐมนตรีต้องปฏิบัติตาม
- 4.3.3 จัดทำรายงานสรุปผลการทดสอบ Cyber Drill พร้อมทั้งระบุวิธีการวัดผล และเปรียบเทียบผลการทดสอบทั้ง 2 รอบ พร้อมข้อเสนอแนะในการปรับปรุงต่อสำนักเลขาธิการนายกรัฐมนตรี และจัดให้มีการประชุมเพื่อรายงานสรุปผลการทดสอบ Cyber Drill
- 4.3.4 จัดให้มีการอบรมความรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์แก่บุคลากรของสำนักเลขาธิการนายกรัฐมนตรี อย่างน้อยปีละ 1 ครั้ง ในรูปแบบตามที่สำนักเลขาธิการนายกรัฐมนตรีเห็นชอบ
- 4.3.5 มีการบริการทางโทรศัพท์ (On Call Service) ในวันและเวลาราชการ
- 4.3.6 มีบุคลากรให้คำปรึกษาเกี่ยวกับรายงานการทดสอบความพร้อมของบุคลากรผ่านการจำลองสถานการณ์ แนวทางการแก้ไขปัญหา และข้อเสนอแนะที่เป็นประโยชน์ต่อการพัฒนาระบบการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ให้กับสำนักเลขาธิการนายกรัฐมนตรีตลอดอายุสัญญา

5. จัดหาอุปกรณ์ป้องกันเครือข่าย (Firewall) จำนวน 1 ระบบ

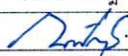
- 5.1 จัดหาและติดตั้งอุปกรณ์ป้องกันเครือข่าย (Firewall) เพื่อให้สามารถทำงานร่วมกับระบบเครือข่ายของสำนักเลขาธิการนายกรัฐมนตรีได้อย่างต่อเนื่องและมีประสิทธิภาพ โดยต้องมีคุณสมบัติอย่างน้อย ดังนี้
- 5.1.1 ต้องได้รับการจัดอันดับให้อยู่ในกลุ่ม Leader ของ Gartner Magic Quadrant ในกลุ่มผลิตภัณฑ์ Enterprise Network Firewalls ปี 2022 หรือปีล่าสุด
- 5.1.2 มี Threat Prevention Throughput ไม่น้อยกว่า 45 Gbps หรือมี IPS Throughput ไม่น้อยกว่า 45 Gbps ในแบบ Appmix หรือ Enterprise Testing Condition หรือ Enterprise Traffic Mix
- 5.1.3 มี Firewall Throughput หรือ NGFW Throughput ไม่น้อยกว่า 45 Gbps ในแบบ Appmix หรือ Enterprise Testing Condition หรือ Enterprise Traffic Mix
- 5.1.4 มี Network Interface อย่างน้อย ดังนี้

คณะกรรมการจัดทำขอบเขตของงานฯ วันที่ 9 กรกฎาคม 2569

						
นายจักรกฤษ พรพิทักษ์ ประธานกรรมการ	น.ส.ณัฏฐา ชัยธวัชวาท กรรมการ	น.ส.วรรณ นุ่มนวล กรรมการ	นายสุกฤษฎี สรหงษ์ กรรมการ	น.ส.จุฑามาศ อนรรฆกุล กรรมการ	น.ส.ธนัญญ์ หงษ์ทอง กรรมการ	นายชาญนิตี ดีลี กรรมการ

- 5.1.4.1 Interface แบบ 1G หรือดีกว่า ไม่น้อยกว่า 8 พอร์ต
- 5.1.4.2 ช่องเชื่อมต่อแบบ 1G/10G SFP/SFP+ หรือดีกว่า ไม่น้อยกว่า 8 พอร์ต
- 5.1.5 สามารถรองรับ Concurrent Connections หรือ Concurrent Sessions หรือ Maximum Sessions อย่างน้อย 16,000,000 Connections และรองรับจำนวน New Sessions/Sec หรือ Connections Per Second ไม่น้อยกว่า 300,000 Connections ต่อวินาที
- 5.1.6 มี Interface HA แบบ 10/100/1000 หรือดีกว่า ไม่น้อยกว่า 1 พอร์ต และมี Interface แบบ 10/100/1000 สำหรับบริหารจัดการโดยเฉพาะ (Out of Band Management) ไม่น้อยกว่า 1 พอร์ต โดยทั้งหมดไม่นับรวมกับ Interface จากข้อ 5.1.4
- 5.1.7 มี Storage ชนิด SSD สำหรับจัดเก็บข้อมูลระบบ (System Storage) ขนาดไม่น้อยกว่า 480 GB หรือดีกว่า
- 5.1.8 มีแหล่งจ่ายไฟฟ้า (Power Supply) แบบ Redundant หรือสามารถถอดเปลี่ยนได้โดยไม่มีผลกระทบต่อการใช้งาน (Without Services Interruption)
- 5.1.9 สามารถทำการติดตั้งเพื่อทำ High Availability แบบ Active-Active หรือ Active-Passive ได้
- 5.1.10 สามารถติดตั้งในรูปแบบ Transparent Inline (Virtual Wire), Non-Inline Monitoring (Tap), L2 และ L3 หรือเทียบเท่าได้
- 5.1.11 สามารถทำ Routing แบบ Static, RIP, BGP, OSPF, Multicast และ Policy Based Forwarding หรือ Policy Based Routing ได้เป็นอย่างดี
- 5.1.12 สามารถทำงานร่วมกับระบบการพิสูจน์ตัวตน (Authentication Systems) เพื่อทำการติดตามผู้ใช้ได้แก่ Active Directory, LDAP และ Radius ได้เป็นอย่างดี
- 5.1.13 ผลิตภัณฑ์ที่นำเสนอต้องได้รับการรับรองมาตรฐานความปลอดภัย FCC, CE และ VCCI เป็นอย่างน้อย
- 5.1.14 ต้องตั้งค่าอุปกรณ์ป้องกันเครือข่าย (Firewall) ให้สามารถส่ง Log ไปยังศูนย์เฝ้าระวังตรวจสอบการโจมตีทางไซเบอร์ (Cyber Security Operations Center: CSOC Managed Service) ที่นำเสนอในโครงการได้อัตโนมัติ
- 5.2 ระบบบริหารจัดการอุปกรณ์ป้องกันเครือข่าย (Firewall) แบบรวมศูนย์ จำนวน 1 ระบบ โดยมีคุณสมบัติอย่างน้อย ดังนี้
 - 5.2.1 ต้องเป็นผลิตภัณฑ์ภายใต้เครื่องหมายการค้าเดียวกันกับอุปกรณ์ป้องกันเครือข่าย (Firewall) เพื่อให้สามารถทำงานร่วมกันได้อย่างมีประสิทธิภาพ
 - 5.2.2 เป็นระบบสำหรับการบริหารจัดการอุปกรณ์รักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์ แบบรวมศูนย์ (Centralized Management)

คณะกรรมการจัดทำขอบเขตของงานฯ วันที่ 9 กรกฎาคม 2569

						
นายจักรกฤษ พรพิทักษ์ ประธานกรรมการ	น.ส.ณัชชา ชัยสุติวารัต กรรมการ	น.ส.วรรณ นุ่มนวล กรรมการ	นายสุกฤษฎี สรพงษ์ กรรมการ	น.ส.จุฑามาศ อนรรฆกุล กรรมการ	น.ส.ธนัญญา หงษ์ทอง กรรมการ	นายชาญนิจ์ ตีลี กรรมการ

- 5.2.3 มีระบบการพิสูจน์ตัวตนของผู้ดูแลระบบ (Administrator) โดยใช้ฐานข้อมูลจาก Local Database หรือ LDAP หรือ RADIUS ได้เป็นอย่างดี
 - 5.2.4 สามารถทำการบริหารจัดการผ่านทาง Web Interface ได้เป็นอย่างดี
 - 5.2.5 สามารถบริหารจัดการและปรับเปลี่ยนค่าต่าง ๆ ของอุปกรณ์ป้องกันเครือข่าย (Firewall) ที่นำเสนอได้จากส่วนกลาง เช่น Policies, Object และ Security Profile
 - 5.2.6 ระบบต้องสามารถเรียกดู Dashboard โดยมีรายละเอียดอย่างน้อย ดังนี้
 - 5.2.6.1 แสดงผลการตรวจสอบการตั้งค่าอุปกรณ์ให้เป็นไปตามมาตรฐานสากล เช่น CIS, NIST, GDPR, PCI-DSS หรือ HIPAA เป็นอย่างน้อย
 - 5.2.6.2 แสดงข้อมูลการใช้งานในภาพรวมสำหรับผู้บริหาร (Executive Summary)
 - 5.2.7 ดำเนินการการย้ายค่า Configuration ของอุปกรณ์ป้องกันเครือข่าย (Firewall) ที่สำนักเลขาธิการนายกรัฐมนตรีใช้งานอยู่เดิม ไปยังอุปกรณ์ป้องกันเครือข่าย (Firewall) ที่นำเสนอได้
 - 5.3 มีการบริการทางโทรศัพท์ (On Call Service) ในวันและเวลาราชการ
 - 5.4 มีบุคลากรให้คำปรึกษาเกี่ยวกับแนวทางการแก้ไขปัญหา และข้อเสนอแนะที่เป็นประโยชน์เกี่ยวกับอุปกรณ์ป้องกันเครือข่าย (Firewall) ให้กับสำนักเลขาธิการนายกรัฐมนตรีตลอดอายุสัญญา
6. จัดหาระบบป้องกันเว็บแอปพลิเคชันและ API จำนวน 1 ระบบ
- 6.1 จัดหาระบบป้องกันเว็บแอปพลิเคชันและ API เพื่อให้สามารถทำงานร่วมกับเว็บเซิร์ฟเวอร์ของสำนักเลขาธิการนายกรัฐมนตรีได้อย่างต่อเนื่อง และมีประสิทธิภาพ
 - 6.2 เชื่อมโยงระบบป้องกันเว็บแอปพลิเคชันและ API ไปยังศูนย์เฝ้าระวังตรวจสอบการโจมตีทางไซเบอร์ (Cyber Security Operations Center: CSOC Managed Service) ที่นำเสนอในโครงการ
 - 6.3 ระบบป้องกันเว็บแอปพลิเคชันและ API จะต้องมีความสมบูรณ์อย่างน้อย ดังนี้
 - 6.3.1 มี Cloud Security ประกอบด้วย Web Application Firewall, API Protection และ DDoS Protection เป็นอย่างน้อย
 - 6.3.2 รองรับการป้องกันได้ไม่น้อยกว่า 30 FQDN
 - 6.3.3 สามารถป้องกันการโจมตีทางไซเบอร์ที่ส่งผลกระทบต่อเว็บแอปพลิเคชันโดยสามารถอ้างอิงกับ OWASP Top 10 ปี 2021 หรือดีกว่า เช่น Broken Access Control, Injection และ Vulnerable and Outdated Components
 - 6.3.4 สามารถตรวจจับการโจมตีแบบ Zero Day Attacks ผ่านช่องทางเว็บแอปพลิเคชันได้
 - 6.3.5 สามารถอัปเดตเพื่อป้องกันการโจมตีแบบเฉพาะเจาะจง โดยไม่ต้องรอรอบการอัปเดตแบบปกติ

คณะกรรมการจัดทำขอบเขตของงานฯ วันที่ 9 กรกฎาคม 2569

						
นายจักรกฤษ พรพิทักษ์ ประธานกรรมการ	น.ส.ณัฏฐา ขยาลูวัฒวรร กรรมการ	น.ส.วรรณ นุ่มนวล กรรมการ	นายสุกฤษฎี สรหงษ์ กรรมการ	น.ส.จุฑามาศ อนรรฆกุล กรรมการ	น.ส.ธนัญญ์ หงษ์ทอง กรรมการ	นายชาญิธิ ดีสี กรรมการ

- 6.3.6 สามารถทำ Load Balancing และ Global Server Load Balancing (GSLB) ในรูปแบบ High Availability พร้อมระบบ Health-Check โดยสามารถกระจาย Traffic ไปยัง Web Application ด้วยวิธี Round-Robin, Least Connections หรือ Least Request, Random และ Ring-Hash หรือเทียบเท่า
- 6.3.7 สามารถปรับแต่ง Web Application เช่น Host Rewrite, Add/Remove HTTP Header และ Route Redirection ได้เป็นอย่างดี
- 6.3.8 สามารถป้องกันการโจมตีฝั่ง Client เพื่อป้องกันการโจรกรรมข้อมูลจากวิธี Formjacking และ Magecart ได้เป็นอย่างดี
- 6.3.9 สามารถสร้างรายงานสรุปผลการใช้งานเป็นรายวัน รายสัปดาห์ และรายเดือน โดยสามารถส่งรายงานผ่านอีเมลได้
- 6.3.10 สามารถป้องกันการโจมตีในรูปแบบของ DDoS ได้ไม่น้อยกว่า 12 Tbps โดยสามารถป้องกันการโจมตีทั้งในระดับ Network (Layer 3 และ 4) และระดับ Application (Layer 7)
- 6.3.10.1 สามารถใช้งาน Peak Bandwidth ได้แบบไม่มีจำกัดค่าสูงสุด โดยใช้วิธีคำนวณตามปริมาณ Cleaned-Bandwidth แบบ 95th Percentile ต่อเดือนได้อย่างน้อย 50 Mbps หรือรูปแบบอื่นที่เทียบเท่า
- 6.3.10.2 สามารถป้องกันการโจมตีได้หลายรูปแบบ เช่น Filtering Traffic, IP Geolocation, HTTP Header, TLS Fingerprint และ Rate Limit ได้เป็นอย่างดี
- 6.3.10.3 สามารถเก็บ Security Log เพื่อใช้สำหรับตรวจสอบข้อมูลย้อนหลังได้ไม่น้อยกว่า 30 วัน
- 6.3.10.4 รองรับการทำ Policy ในรูปแบบ Positive Security และ Negative Security ได้เป็นอย่างดี
- 6.3.10.5 มีระบบ AI หรือ Machine-Learning ที่สามารถเรียนรู้และวิเคราะห์ Traffic ได้หลากหลายและรวดเร็ว เพื่อช่วยในการปรับตั้งค่า Policy เช่น การลด False Positive ได้เป็นอย่างดี
- 6.3.10.6 สามารถแสดงข้อมูล HTTP Request Parameter และ HTTP Request Body บน WAF Log เพื่อช่วยในการวิเคราะห์การโจมตีได้เป็นอย่างดี
- 6.3.10.7 สามารถทำ API Security ได้

คณะกรรมการจัดทำขอบเขตของงานฯ วันที่ 9 กรกฎาคม 2569

						
นายจักรกฤษ พรพิทักษ์ ประธานกรรมการ	น.ส.ณัษชา ขยารัตนาวัตร กรรมการ	น.ส.วรรณ นุ่มนวล กรรมการ	นายสุกฤษฎี สรหงษ์ กรรมการ	น.ส.จุฑามาศ อนรรฆกุล กรรมการ	น.ส.ธนัญญ์ หงษ์ทอง กรรมการ	นายชาญนิธิ ตีลี กรรมการ

- 6.3.10.8 สามารถตรวจจับ Malicious Users จาก TLS Fingerprint, Header Name และ Cookie Name ได้ไม่น้อยกว่า 500k Requests ต่อเดือน หรือตามจำนวน Bandwidth ที่ใช้งาน
 - 6.3.10.9 สามารถตรวจจับ Personally Identifiable Information (PII) และ Sensitive Data จาก API Traffic ได้เป็นอย่างดี
 - 6.3.10.10 สามารถแสดง API และ Shadow API จาก API Traffic ที่เข้ามาในระบบได้เป็นอย่างดี
 - 6.3.10.11 สามารถทำ API Discovery ได้
 - 6.3.10.12 สามารถทำ Synthetic Monitoring เพื่อตรวจสอบประสิทธิภาพของแอปพลิเคชันได้ เช่น มีรายงานความเสี่ยงจากใบรับรองหมดอายุและการเข้ารหัสที่ไม่ปลอดภัย โดยสามารถเสนอผลิตภัณฑ์อื่น ๆ เพิ่มเติมเพื่อให้สามารถดำเนินการตามข้อกำหนดดังกล่าวได้
 - 6.3.10.13 สามารถทำ Exclusion Rules หรือ Managed Rules หรือเทียบเท่าจาก Request Log ได้
 - 6.3.10.14 สามารถทำ Dynamic Application Security Testing (DAST) ให้กับเว็บแอปพลิเคชันได้ไม่จำกัดจำนวนครั้ง หรือนำเสนอบริการ Dynamic Application Security Testing (DAST) จากผู้ให้บริการภายนอกไม่น้อยกว่า 3 Applications ต่อเดือน
 - 6.3.10.15 สามารถตรวจสอบ Attack Surface Management โดยสามารถค้นหา Domains, Services, Software และ Netblocks จาก Root Domain หรือ Apex Domain ที่กำหนดได้ โดยสามารถเสนอผลิตภัณฑ์อื่น ๆ เพิ่มเติมเพื่อให้สามารถดำเนินการตามข้อกำหนดดังกล่าวได้
 - 6.3.10.16 สามารถสร้างรายงานสรุปผลการใช้งานเป็นรายวัน รายสัปดาห์ และรายเดือน โดยสามารถส่งรายงานผ่านอีเมลได้
 - 6.3.10.17 รองรับการยืนยันตัวตนของผู้ดูแลระบบแบบ Two-Factor Authentication ได้เป็นอย่างดี
 - 6.3.10.18 เป็นบริการที่ต้องผ่านมาตรฐานหรือสับสนุน PCI DSS Compliant, ISO27001 และ SOC2 Type 2 เป็นเป็นอย่างดี
- 6.3.11 มีการบริการทางโทรศัพท์ (On Call Service) ในวันและเวลาราชการ

คณะกรรมการจัดทำขอบเขตของงานฯ วันที่ 9 กรกฎาคม 2569

						
นายจักรกฤษ พรพิทักษ์ ประธานกรรมการ	น.ส.ณิชา ชัยธวัชวตร กรรมการ	น.ส.วรรณิ นุ่มนวล กรรมการ	นายสุกฤษฎี สรพงษ์ กรรมการ	น.ส.จุฑามาศ อนุรรณกุล กรรมการ	น.ส.ธนัญญ์ หงษ์ทอง กรรมการ	นายชาญนิตี ดีลี กรรมการ

6.3.12 มีบุคลากรให้คำปรึกษาเกี่ยวกับ การแก้ไขปัญหาและข้อเสนอแนะที่เป็นประโยชน์ เกี่ยวกับระบบป้องกันเว็บแอปพลิเคชันและ API ให้กับสำนักเลขาธิการนายกรัฐมนตรีตลอดอายุสัญญา

7. จัดหาระบบยืนยันตัวตนแบบหลายปัจจัย (Multifactor Authentication: MFA) จำนวน 1 ระบบ

- 7.1 จัดหาระบบยืนยันตัวตนแบบหลายปัจจัย (Multifactor Authentication: MFA) จำนวนไม่น้อยกว่า 100 ผู้ใช้งาน
- 7.2 สามารถป้องกันผู้ใช้งานในการเข้าถึงแอปพลิเคชันที่ติดตั้งบนคลาวด์ และแอปพลิเคชันที่ติดตั้งภายในหน่วยงาน
- 7.3 มีแอปพลิเคชันบนมือถือ (Mobile Application) สำหรับการยืนยันตัวตนผ่านแอปพลิเคชันด้วยวิธี Push (Push Notification)
- 7.4 สามารถส่งรหัสยืนยัน (Security keys หรือ OTP หรือ Passcode) ผ่านทาง Mobile Application และ SMS ได้เป็นอย่างดี
- 7.5 สามารถยืนยันตัวตนแบบไม่ต้องใช้รหัสผ่าน (Password Less) หรือใช้อัตลักษณ์ตัวบุคคล (Biometric) แทนได้
- 7.6 สามารถเพิ่มผู้ใช้งานได้จาก Active Directory (AD), Bulk Enrollment, User Self-Enrollment หรือ Self-Provisioning และผู้ใช้งานสามารถบริหารจัดการ การใช้งานของตนเองได้ (User Self-Management หรือ User Self Service)
- 7.7 สามารถปรับเปลี่ยนนโยบายความปลอดภัย (Policy) เพื่อจำกัดการอนุมัติการเข้าใช้งานได้ตามเงื่อนไขอย่างน้อยดังต่อไปนี้
 - 7.7.1 สามารถตั้งค่าจำกัดการใช้งานตามระบบเครือข่ายได้ (Authorized หรือ Specific Network)
 - 7.7.2 สามารถตั้งค่าจำกัดการใช้งานตามสถานที่ใช้งาน หรือผู้ใช้งาน (User หรือ Specific Location)
 - 7.7.3 สามารถยืนยันตัวตนแบบ Multi-Factor Authentication อย่างน้อยดังนี้
 - 7.7.3.1 On-Premise Application ใช้ Protocol Radius ได้เป็นอย่างดี
 - 7.7.3.2 Native Cloud Application และ Federated Cloud Application ใช้ Protocol SAML2.0 หรือ Open ID Connect (OIDC) ได้เป็นอย่างดี
 - 7.7.4 มีการบริการทางโทรศัพท์ (On Call Service) ในวันและเวลาราชการ
 - 7.7.5 มีบุคลากรให้คำปรึกษาเกี่ยวกับ การแก้ไขปัญหา และข้อเสนอแนะที่เป็นประโยชน์ เกี่ยวกับระบบพิสูจน์ตัวตนแบบหลากหลายปัจจัย (Multifactor Authentication) ให้กับสำนักเลขาธิการนายกรัฐมนตรี ตลอดสัญญาของโครงการ

คณะกรรมการจัดทำขอบเขตของงานฯ วันที่ 9 กรกฎาคม 2569

						
นายจักรกฤษ พรพิทักษ์ ประธานกรรมการ	น.ส.ณัฏฐา ขยาลูตาวัตร กรรมการ	น.ส.วรรณ นุ่มนวล กรรมการ	นายสุกฤษฎี สรหงษ์ กรรมการ	น.ส.จุฑามาศ อนรรฆกุล กรรมการ	น.ส.ธนัญญ์ หงษ์ทอง กรรมการ	นายชาญนิจิ ดีลี กรรมการ

8. รายการทรัพย์สินที่ต้องดำเนินการเชื่อมต่อกับศูนย์เฝ้าระวังตรวจสอบการโจมตีทางไซเบอร์ และจัดเก็บข้อมูลจราจรระบบเครือข่ายคอมพิวเตอร์

- 8.1 ผู้รับจ้างจะต้องให้บริการพื้นที่ในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ได้ไม่น้อยกว่า 100 GB/Day และจะต้องทำการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้นานอย่างน้อย 365 วัน
- 8.2 ผู้รับจ้างจะต้องให้บริการในการเชื่อมต่ออุปกรณ์ และจัดเก็บข้อมูลจราจรระบบเครือข่ายคอมพิวเตอร์ เพื่อให้บริการในการตอบสนองต่อภัยคุกคามทางไซเบอร์ตามรายการทรัพย์สินของสำนักเลขาธิการนายกรัฐมนตรี ดังนี้

ลำดับที่	รายการอุปกรณ์
1	Windows Servers
2	Windows Domain Controller/Active Directory Server
3	Linux / Unix Servers
4	Web Servers
5	Database Servers
6	VPN / SSL VPN
7	Virtual Infrastructure Servers
8	DNS Servers
9	DHCP Servers
10	RSA / 2FA
11	Firewalls
12	Switches
13	Routers
14	Network Access Control (NAC)
15	Wireless Access Points
16	Endpoint Detection and Response (EDR)
17	Wireless Controller

คณะกรรมการจัดทำขอบเขตของงานฯ วันที่ 9 กรกฎาคม 2569

						
นายจักรพงษ์ พรพิทักษ์ ประธานกรรมการ	น.ส.ณัฏฐา ขยาดิชาวัตร กรรมการ	น.ส.วรรณ นุ่มนวล กรรมการ	นายสุกฤษฎี สรหงษ์ กรรมการ	น.ส.จุฑามาศ อนรรฆกุล กรรมการ	น.ส.ธนัญญ์ หงษ์ทอง กรรมการ	นายชาญนิตี ตีลี กรรมการ