ประกาศสำนักข่าวกรองแห่งชาติ

เรื่อง ประกวดราคาซื้อโครงการจัดตั้งและพัฒนาศูนย์ปฏิบัติการความมั่นคงปลอดภัยไซเบอร์

แขวงพญาไท เขตพญาไท กรุงเทพมหานคร

กิจกรรมที่ ๒ จัดซื้อครุภัณฑ์ พัฒนาระบบและเครือข่ายผู้ปฏิบัติงานความมั่นคงปลอดภัยไซเบอร์

กลุ่มหน่วยงานความมั่นคง

ด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding)

สำนักข่าวกรองแห่งชาติ มีความประสงค์จะประกวดราคาซื้อโครงการจัดตั้งและพัฒนาศูนย์ปฏิบัติการความมั่นคงปลอดภัยไซเบอร์ แขวงพญาไท เขตพญาไท กรุงเทพมหานคร กิจกรรมที่ ๒ จัดซื้อครุภัณฑ์ พัฒนาระบบและเครือข่ายผู้ปฏิบัติงานความมั่นคงปลอดภัยไซเบอร์ กลุ่มหน่วยงานความมั่นคง ด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding) ราคากลางของงานซื้อในการประกวดราคาครั้งนี้ เป็นเงินทั้งสิ้น ๘,๖๗๙,๙๔๗.๗๐ บาท (แปดล้านหกแสนเจ็ดหมื่นเก้าพันเก้าร้อยสี่สิบเจ็ดบาทเจ็ดสิบสตางค์) ตามรายการ ดังนี้

๑. ระบบคอมพิวเตอร์แม่ข่ายประสิทธิภาพสูง จำนวน ๑๐ รายการ

๒. พัฒนาระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์ จำนวน ๑ งาน

๓. จัดอบรมและจัดการแข่งขันทักษะความมั่นคงปลอดภัยไซเบอร์ จำนวน ๓ หลักสูตร

ผู้ยื่นข้อเสนอจะต้องมีคุณสมบัติ ดังต่อไปนี้

๑. มีความสามารถตามกฎหมาย

๒. ไม่เป็นบุคคลล้มละลาย

๓. ไม่อยู่ระหว่างเลิกกิจการ

๔. ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

๕. ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

๖. มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

๗. เป็นนิติบุคคล ผู้มีอาชีพให้ขายพัสดุที่ประกวดราคาซื้อด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

๘. ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่สำนักข่าวกรองแห่งชาติ ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

๙. ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์ความคุ้มกันเช่นว่านั้น

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

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

๑๒. ผู้ยื่นข้อเสนอต้องไม่อยู่ในฐานะเป็นผู้ไม่แสดงบัญชีรายรับรายจ่ายหรือแสดงบัญชีรายรับรายจ่ายไม่ถูกต้องครบถ้วนในสาระสำคัญ ตามที่คณะกรรมการ ป.ป.ช. กำหนด

๑๓. ผู้ยื่นข้อเสนอซึ่งได้รับคัดเลือกเป็นคู่สัญญาต้องรับและจ่ายเงินผ่านบัญชีธนาคาร เว้นแต่การจ่ายเงินแต่ละครั้งซึ่งมีมูลค่าไม่เกินสามหมื่นบาทคู่สัญญาอาจจ่ายเป็นเงินสดก็ได้

๑๔. ผู้ยื่นข้อเสนอต้องไม่เป็นที่ปรึกษาของสำนักข่าวกรองแห่งชาติ หรือมีส่วนร่วมในบริษัทที่ปรึกษาของ สำนักข่าวกรองแห่งชาติในการจัดซื้อครั้งนี้ และต้องไม่มีผู้ปฏิบัติงานของสำนักข่าวกรองแห่งชาติเข้าไปมีส่วนร่วมในธุรกิจของผู้ยื่นข้อเสนอในฐานะผู้กระทำการหรือผู้ร่วมงาน

ผู้ยื่นข้อเสนอต้องยื่นข้อเสนอและเสนอราคาทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ในวันที่ ๕ กรกฎาคม ๒๕๖๕ ระหว่างเวลา ๐๘.๓๐ น. ถึง ๑๖.๓๐ น.

ผู้สนใจสามารถขอรับเอกสารประกวดราคาอิเล็กทรอนิกส์ โดยดาวน์โหลดเอกสารผ่านทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ตั้งแต่วันที่ประกาศจนถึงก่อนวันเสนอราคา

ผู้สนใจสามารถดูรายละเอียดได้ที่เว็บไซต์ www.nia.go.th หรือ www.gprocurement.go.th หรือสอบถามทางโทรศัพท์ เกี่ยวกับข้อมูลทางเทคนิคหมายเลข ๐๒๒๘๐๖๘๔๑ เกี่ยวกับงานด้านพัสดุ หมายเลข ๐๒๒๙๘๔๙๐๐ ต่อ ๕๕๔๔ ในวันและเวลาราชการ

ประกาศ ณ วันที่ ๒๙ มิถุนายน พ.ศ. ๒๕๖๕

(นายธนากร บัวรัษฎ์)
ผู้อำนวยการสำนักข่าวกรองแห่งชาติ

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

เอกสารประกวดราคาซื้อด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding)

เลขที่ ๐๐๙/๒๕๖๕

การจัดซื้อโครงการจัดตั้งและพัฒนาศูนย์ปฏิบัติการความมั่นคงปลอดภัยไซเบอร์

แขวงพญาไท เขตพญาไท กรุงเทพมหานคร

กิจกรรมที่ ๒ จัดซื้อครุภัณฑ์ พัฒนาระบบและเครือข่ายผู้ปฏิบัติงานความมั่นคงปลอดภัยไซเบอร์

กลุ่มหน่วยงานความมั่นคง

ตามประกาศ สำนักข่าวกรองแห่งชาติ

ลงวันที่ ๒๙ มิถุนายน ๒๕๖๕

สำนักข่าวกรองแห่งชาติ ซึ่งต่อไปนี้เรียกว่า "สำนักข่าวกรองแห่งชาติ" มีความประสงค์จะประกวดราคาซื้อด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ ตามรายการ ดังนี้

๑. ระบบคอมพิวเตอร์แม่ข่ายประสิทธิภาพสูง จำนวน ๑๐ รายการ

๒. พัฒนาระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์ จำนวน ๑ งาน

๓. จัดอบรมและจัดการแข่งขันทักษะความมั่นคงปลอดภัยไซเบอร์ จำนวน ๓ หลักสูตร

พัสดุที่จะซื้อนี้ต้องเป็นของแท้ ของใหม่ ไม่เคยใช้งานมาก่อน ไม่เป็นของเก่าเก็บ อยู่ในสภาพที่จะใช้งานได้ทันที และมีคุณลักษณะเฉพาะตรงตามที่กำหนดไว้ในเอกสารประกวดราคาซื้อด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ฉบับนี้ โดยมีข้อแนะนำและข้อกำหนด ดังต่อไปนี้

๑. เอกสารแนบท้ายเอกสารประกวดราคาอิเล็กทรอนิกส์

๑.๑ รายละเอียดคุณลักษณะเฉพาะ

๑.๒ แบบใบเสนอราคาที่กำหนดไว้ในระบบการจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์

๑.๓ สัญญาซื้อขายทั่วไป

๑.๔ แบบหนังสือค้ำประกัน

(๑) หลักประกันการเสนอราคา

(๒) หลักประกันสัญญา

๑.๕ บทนิยาม

(๑) ผู้มีผลประโยชน์ร่วมกัน

(๒) การขัดขวางการแข่งขันอย่างเป็นธรรม

๑.๖ แบบบัญชีเอกสารที่กำหนดไว้ในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์

(๑) บัญชีเอกสารส่วนที่ ๑

(๒) บัญชีเอกสารส่วนที่ ๒

๒. คุณสมบัติของผู้ยื่นข้อเสนอ

๒.๑ มีความสามารถตามกฎหมาย

๒.๒ ไม่เป็นบุคคลล้มละลาย

๒.๓ ไม่อยู่ระหว่างเลิกกิจการ

๒.๔ ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

๒.๕ ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

๒.๖ มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

๒.๗ เป็นนิติบุคคลผู้มีอาชีพขายพัสดุที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

๒.๘ ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่ สำนักข่าวกรองแห่งชาติ ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

๒.๙ ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

๒.๑๐ ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ "กิจการร่วมค้า" ต้องมีคุณสมบัติดังนี้

กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงฯจะต้องมีการกำหนดสัดส่วนหน้าที่ และความรับผิดชอบในปริมาณงาน สิ่งของ หรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก กิจการร่วมค้านั้นต้องใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

สำหรับข้อตกลงฯ ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมค้าหลัก ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน

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

๒.๑๒ ผู้ยื่นข้อเสนอซึ่งได้รับคัดเลือกเป็นคู่สัญญาต้องลงทะเบียนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement: e-GP) ของกรมบัญชีกลาง ตามที่คณะกรรมการ ป.ป.ช. กำหนด

๒.๑๓ ผู้ยื่นข้อเสนอต้องไม่อยู่ในฐานะเป็นผู้ไม่แสดงบัญชีรายรับรายจ่ายหรือแสดงบัญชีรายรับรายจ่ายไม่ถูกต้องครบถ้วนในสาระสำคัญ ตามที่คณะกรรมการ ป.ป.ช. กำหนด

๒.๑๔ ผู้ยื่นข้อเสนอซึ่งได้รับคัดเลือกเป็นคู่สัญญาต้องรับและจ่ายเงินผ่านบัญชีธนาคาร เว้นแต่การจ่ายเงินแต่ละครั้งซึ่งมีมูลค่าไม่เกินสามหมื่นบาทคู่สัญญาอาจจ่ายเป็นเงินสดก็ได้

๒.๑๕ ผู้ยื่นข้อเสนอต้องไม่เป็นที่ปรึกษาของสำนักข่าวกรองแห่งชาติ หรือมีส่วนร่วมในบริษัทที่ปรึกษาของ สำนักข่าวกรองแห่งชาติในการจัดซื้อครั้งนี้ และต้องไม่มีผู้ปฏิบัติงานของสำนักข่าวกรองแห่งชาติเข้าไปมีส่วนร่วมในธุรกิจของผู้ยื่นข้อเสนอในฐานะผู้กระทำการหรือผู้ร่วมงาน

๓. หลักฐานการยื่นข้อเสนอ

ผู้ยื่นข้อเสนอจะต้องเสนอเอกสารหลักฐานยื่นมาพร้อมกับการเสนอราคาทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ โดยแยกเป็น ๒ ส่วน คือ

๓.๑ ส่วนที่ ๑ อย่างน้อยต้องมีเอกสารดังต่อไปนี้

(๑) ในกรณีผู้ยื่นข้อเสนอเป็นนิติบุคคล

(ก) ห้างหุ้นส่วนสามัญหรือห้างหุ้นส่วนจำกัด ให้ยื่นสำเนาหนังสือรับรองการจดทะเบียนนิติบุคคล บัญชีรายชื่อหุ้นส่วนผู้จัดการ ผู้มีอำนาจควบคุม (ถ้ามี) พร้อมทั้งรับรองสำเนาถูกต้อง

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

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

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

(๔) เอกสารเพิ่มเติมอื่นๆ

(๔.๑) สำเนาใบทะเบียนภาษีมูลค่าเพิ่ม

(๔.๒) สำเนาใบทะเบียนพาณิชย์

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

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

๓.๒ ส่วนที่ ๒ อย่างน้อยต้องมีเอกสารดังต่อไปนี้

(๑) ในกรณีที่ผู้ยื่นข้อเสนอมอบอำนาจให้บุคคลอื่นกระทำการแทนให้แนบหนังสือมอบอำนาจซึ่งติดอากรแสตมป์ตามกฎหมาย โดยมีหลักฐานแสดงตัวตนของผู้มอบอำนาจและผู้รับมอบอำนาจ ทั้งนี้หากผู้รับมอบอำนาจเป็นบุคคลธรรมดาต้องเป็นผู้ที่บรรลุนิติภาวะตามกฎหมายแล้วเท่านั้น

(๒) แคตตาล็อกและ/หรือแบบรูปรายการละเอียดคุณลักษณะเฉพาะ ตามข้อ ๔.๔

(๓) รายการพิจารณาที่ ๑ ครุภัณฑ์ พัฒนาระบบและเครือข่ายผู้ปฏิบัติงานความมั่นคงปลอดภัยไซเบอร์ กลุ่มหน่วยงานความมั่นคง

(๓.๑) หลักประกันการเสนอราคา ตามข้อ ๕

(๓.๒) สำเนาใบขึ้นทะเบียนผู้ประกอบการวิสาหกิจขนาดกลางและขนาดย่อม (SMEs) (ถ้ามี)

(๓.๓) สำเนาหนังสือรับรองสินค้า Made In Thailand ของสภาอุตสาหกรรมแห่งประเทศไทย (ถ้ามี)

(๔) เอกสารเพิ่มเติมอื่นๆ

(๔.๑) ผู้เสนอราคาต้องแสดงหนังสือรับรองจากเจ้าของผลิตภัณฑ์ หรือสาขาของเจ้าของผลิตภัณฑ์ ว่าผลิตภัณฑ์ที่เสนอขายเป็นของแท้ ของใหม่ ไม่เก่าเก็บ ไม่เคยใช้งานมาก่อน หรือปรับปรุงสภาพขึ้นมาใหม่ หรือดัดแปลงสภาพมาเพื่อใช้ในการเสนอราคาครั้งนี้โดยเฉพาะ และผลิตภัณฑ์ได้รับการบรรจุหีบห่อตามมาตรฐานผู้ผลิต

(๔.๒) ผู้เสนอราคาต้องทำตารางเปรียบเทียบรายละเอียด และเงื่อนไขเฉพาะเป็นรายข้อทุกข้อ (Statement of Compliance) รายละเอียดตามขอบเขตการดำเนินงานโดยใช้ตัวอย่างแบบฟอร์มการเปรียบเทียบ ตามตารางที่ ๑ ในการเปรียบเทียบรายการดังกล่าว หากมีกรณีที่ต้องมีการอ้างอิงข้อความ หรือเอกสารในส่วนอื่นที่จัดทำเสนอมา ผู้เสนอราคาต้องระบุให้เห็นอย่างชัดเจน สามารถตรวจสอบได้โดยง่ายไว้ในเอกสารเปรียบเทียบด้วยว่า สิ่งที่ต้องการอ้างอิงถึงนั้น อยู่ในส่วนใดตำแหน่งใดของเอกสารอื่น ๆ ที่จัดทำเสนอมา สำหรับเอกสารที่อ้างอิงถึงนั้น ให้หมายเหตุ หรือขีดเส้นใต้ หรือระบายสี พร้อมเขียนหัวข้อกำกับไว้ เพื่อให้สามารถตรวจสอบกับเอกสารเปรียบเทียบได้ง่าย และตรงกันด้วย

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

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

๔. การเสนอราคา

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

๔.๒ ในการเสนอราคาให้เสนอราคาเป็นเงินบาท และเสนอราคาได้เพียงครั้งเดียวและราคาเดียวโดยเสนอราคารวม และหรือราคาต่อหน่วย และหรือต่อรายการ ตามเงื่อนไขที่ระบุไว้ท้ายใบเสนอราคาให้ถูกต้อง ทั้งนี้ ราคารวมที่เสนอจะต้องตรงกันทั้งตัวเลขและตัวหนังสือ ถ้าตัวเลขและตัวหนังสือไม่ตรงกัน

ให้ถือตัวหนังสือเป็นสำคัญ โดยคิดราคารวมทั้งสิ้นซึ่งรวมค่าภาษีมูลค่าเพิ่ม ภาษีอากรอื่น ค่าขนส่ง ค่าจดทะเบียน และค่าใช้จ่ายอื่นๆ ทั้งปวงไว้แล้ว จนกระทั่งส่งมอบพัสดุให้ ณ สำนักข่าวกรองแห่งชาติ เลขที่ ๘ ซอยพหลโยธิน ๓ ถนนพหลโยธิน แขวงพญาไท เขตพญาไท กรุงเทพมหานคร

ราคาที่เสนอจะต้องเสนอกำหนดยืนราคาไม่น้อยกว่า ๑๒๐ วัน ตั้งแต่วันเสนอราคาโดยภายในกำหนดยืนราคา ผู้ยื่นข้อเสนอต้องรับผิดชอบราคาที่ตนได้เสนอไว้ และจะถอนการเสนอราคามิได้

๔.๓ ผู้ยื่นข้อเสนอจะต้องเสนอกำหนดเวลาส่งมอบพัสดุไม่เกิน ๒๔๐ วัน นับถัดจากวันลงนามในสัญญาซื้อขาย หรือวันที่ได้รับหนังสือแจ้งจาก สำนักข่าวกรองแห่งชาติ ให้ส่งมอบพัสดุ โดยแบ่งออกเป็น ๕ งวดงาน ดังนี้

๔.๓.๑ งวดที่ ๑ ส่งมอบภายใน ๔๕ วัน นับถัดจากวันลงนามในสัญญา โดยส่งมอบงานในรูปแบบเอกสาร จำนวน ๕ ชุด และรูปแบบไฟล์ที่แก้ไขได้พร้อมไฟล์ PDF ในแฟลชไดร์ฟ (Flash Drive) จำนวน ๑ ชุด ประกอบด้วย

๔.๓.๑.๑ เอกสารแผนการดำเนินงานโครงการ (Project Plan) ที่แสดงระยะเวลาในการทำงานขั้นตอนตามขอบเขตการดำเนินงาน โดยจะต้องระบุชื่อกิจกรรม ความเชื่อมโยงของกิจกรรม ผู้รับผิดชอบ ระยะเวลาที่ใช้ในกิจกรรม ตั้งแต่เริ่มต้นจนถึงวันส่งมอบงาน ผลลัพธ์ที่ได้ในแต่ละกิจกรรม

๔.๓.๑.๒ รายละเอียดบุคลากรทั้งหมดที่รับผิดชอบโครงการ

๔.๓.๒ งวดที่ ๒ ส่งมอบภายใน ๑๒๐ วัน นับถัดจากวันลงนามในสัญญา โดยส่งมอบงานในรูปแบบเอกสาร จำนวน ๕ ชุด และรูปแบบไฟล์ที่แก้ไขได้พร้อมไฟล์ PDF ในแฟลชไดร์ฟ (Flash Drive) จำนวน ๑ ชุด ประกอบด้วย

๔.๓.๒.๑ เอกสารผลการวิเคราะห์ความต้องการใช้งานระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์

๔.๓.๒.๒ เอกสารการวิเคราะห์และออกแบบระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์

๔.๓.๒.๒.๑ ภาพรวมการออกแบบระบบและการทำงานของระบบ

๔.๓.๒.๒.๒ แผนผังโครงสร้างแสดงการเชื่อมโยงภายในและภายนอกของระบบ

๔.๓.๒.๒.๓ แผนผังกิจกรรม (Activity Diagram) ของระบบ

๔.๓.๒.๒.๔ แผนผังแสดงความสัมพันธ์ระหว่างข้อมูล (E-R Diagram) ของระบบและฐานข้อมูล

๔.๓.๒.๒.๕ แผนผังพจนานุกรมฐานข้อมูล (Data Dictionary)

๔.๓.๒.๒.๖ รูปแบบการแสดงผลและการทำงานของฟังก์ชั่นแต่ละหน้า (Web Page)

๔.๓.๒.๓ นำเสนอโครงร่างระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์

๔.๓.๒.๔ ต้นแบบระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์ (Prototype)

๔.๓.๓ งวดที่ ๓ ส่งมอบภายใน ๑๕๐ วัน นับถัดจากวันลงนามในสัญญา โดยส่งมอบงานในรูปแบบเอกสาร จำนวน ๕ ชุด และรูปแบบไฟล์ที่แก้ไขได้พร้อมไฟล์ PDF ในแฟลชไดร์ฟ (Flash Drive) จำนวน ๑ ชุด ประกอบด้วย

๔.๓.๓.๑ ครุภัณฑ์คอมพิวเตอร์ที่จัดหาภายในโครงการประกอบด้วยอุปกรณ์คอมพิวเตอร์ (Hardware) และซอฟต์แวร์ลิขสิทธิ์ (License Software) ในโครงการ

๔.๓.๓.๒ รายงานผลการติดตั้งอุปกรณ์คอมพิวเตอร์ (Hardware) และซอฟต์แวร์ลิขสิทธิ์ (License Software) ในโครงการ

๔.๓.๔ งวดที่ ๔ ส่งมอบภายใน ๑๘๐ วัน นับถัดจากวันลงนามในสัญญา โดยส่งมอบงานในรูปแบบเอกสาร จำนวน ๕ ชุด และรูปแบบไฟล์ที่แก้ไขได้พร้อมไฟล์ PDF ในแฟลชไดร์ฟ (Flash Drive) จำนวน ๑ ชุด ประกอบด้วย

๔.๓.๔.๑ รายงานผลงานอบรมและจัดแข่งขันทักษะความมั่นคงปลอดภัยไซเบอร์

๔.๓.๔.๒ ภาพถ่ายและวีดิโอกิจกรรมการจัดงานแข่งขันทักษะความมั่นคงปลอดภัยไซเบอร์

๔.๓.๕ งวดสุดท้าย ส่งมอบภายใน ๒๔๐ วัน นับถัดจากวันลงนามในสัญญา โดยส่งมอบงานในรูปแบบเอกสาร จำนวน ๕ ชุด และรูปแบบไฟล์ที่แก้ไขได้พร้อมไฟล์ PDF ในแฟลชไดร์ฟ (Flash Drive) จำนวน ๑ ชุด ประกอบด้วย

๔.๓.๕.๑ รายงานผลการทดสอบระบบ (User Acceptance Test) ระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วยการทดสอบการใช้งานของผู้ใช้งาน (Usability Testing) ประสิทธิภาพ (Performance Testing) ความถูกต้องสมบูรณ์โดยรวม (Functional Testing) และการรักษาความปลอดภัยของระบบ (Security Testing)

๔.๓.๕.๒ รายงานผลการทดสอบเจาะระบบ (Penetration Testing) ตามแนวทาง OWASP Top ๑๐ ๒๐๒๑

๔.๓.๕.๓ ผลการพัฒนาระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์ พร้อมการติดตั้งระบบให้สามารถใช้งานได้อย่างถูกต้องสมบูรณ์ตามขอบเขตการดำเนินงาน

๔.๓.๕.๔ รายงานผลการฝึกอบรมผู้ใช้งานและผู้ดูแลระบบของระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์

๔.๓.๕.๕ คู่มือการใช้งานสำหรับผู้ใช้งานและผู้ดูแลระบบของระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์ พร้อมคลิปวีดิโอแนะนำการใช้งานระบบสำหรับผู้ใช้งานทั่วไป

๔.๓.๕.๖ ส่งมอบรหัสชุดคำสั่งโปรแกรม (Source Code) ระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์

๔.๔ ผู้ยื่นข้อเสนอจะต้องส่งแคตตาล็อก และหรือรายละเอียดคุณลักษณะเฉพาะของ

๔.๔.๑ ระบบคอมพิวเตอร์แม่ข่ายประสิทธิภาพสูง จำนวน ๑ ระบบ

๔.๔.๒ พัฒนาระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์ จำนวน ๑ งาน

๔.๔.๓ จัดอบรมและจัดการแข่งขันทักษะความมั่นคงปลอดภัยไซเบอร์ จำนวน ๓ หลักสูตร

ไปพร้อมการเสนอราคาทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ เพื่อประกอบการพิจารณา หลักฐานดังกล่าวนี้ สำนักข่าวกรองแห่งชาติ จะยึดไว้เป็นเอกสารของทางราชการ

๔.๕ ก่อนเสนอราคา ผู้ยื่นข้อเสนอควรตรวจดูร่างสัญญา รายละเอียดคุณลักษณะเฉพาะ ฯลฯ ให้ถี่ถ้วนและเข้าใจเอกสารประกวดราคาอิเล็กทรอนิกส์ทั้งหมดเสียก่อนที่จะตกลงยื่นข้อเสนอตามเงื่อนไขในเอกสารประกวดราคาซื้ออิเล็กทรอนิกส์

๔.๖ ผู้ยื่นข้อเสนอจะต้องยื่นข้อเสนอและเสนอราคาทางระบบการจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ในวันที่ ๕ กรกฎาคม ๒๕๖๕ ระหว่างเวลา ๐๘.๓๐ น. ถึง ๑๖.๓๐ น. และเวลาในการเสนอราคาให้ถือตามเวลาของระบบการจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์เป็นเกณฑ์

เมื่อพ้นกำหนดเวลายื่นข้อเสนอและเสนอราคาแล้ว จะไม่รับเอกสารการยื่นข้อเสนอและการเสนอราคาใดๆ โดยเด็ดขาด

๔.๗ ผู้ยื่นข้อเสนอต้องจัดทำเอกสารสำหรับใช้ในการเสนอราคาในรูปแบบไฟล์เอกสารประเภท PDF File (Portable Document Format) โดยผู้ยื่นข้อเสนอต้องเป็นผู้รับผิดชอบตรวจสอบความครบถ้วน ถูกต้อง และชัดเจนของเอกสาร PDF File ก่อนที่จะยืนยันการเสนอราคา แล้วจึงส่งข้อมูล (Upload) เพื่อเป็นการเสนอราคาให้แก่ สำนักข่าวกรองแห่งชาติ ผ่านทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์

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

หากปรากฏต่อคณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์ว่า ก่อนหรือในขณะที่มีการพิจารณาข้อเสนอ มีผู้ยื่นข้อเสนอรายใดกระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมตามข้อ ๑.๕ (๒) และคณะกรรมการฯ เชื่อว่ามีการกระทำอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรม คณะกรรมการฯ จะตัดรายชื่อผู้ยื่นข้อเสนอรายนั้นออกจากการเป็นผู้ยื่นข้อเสนอ และสำนักข่าวกรองแห่งชาติจะพิจารณาลงโทษผู้ยื่นข้อเสนอดังกล่าวเป็นผู้ทิ้งงาน เว้นแต่ สำนักข่าวกรองแห่งชาติ จะพิจารณาเห็นว่าผู้ยื่นข้อเสนอรายนั้นมิใช่เป็นผู้ริเริ่มให้มีการกระทำดังกล่าวและได้ให้ความร่วมมือเป็นประโยชน์ต่อการพิจารณาของ สำนักข่าวกรองแห่งชาติ

๔.๙ ผู้ยื่นข้อเสนอจะต้องปฏิบัติ ดังนี้

(๑) ปฏิบัติตามเงื่อนไขที่ระบุไว้ในเอกสารประกวดราคาอิเล็กทรอนิกส์

(๒) ราคาที่เสนอจะต้องเป็นราคาที่รวมภาษีมูลค่าเพิ่ม และภาษีอื่นๆ (ถ้ามี) รวมค่าใช้จ่ายทั้งปวงไว้ด้วยแล้ว

(๓) ผู้ยื่นข้อเสนอจะต้องลงทะเบียนเพื่อเข้าสู่กระบวนการเสนอราคา ตามวัน เวลาที่กำหนด

(๔) ผู้ยื่นข้อเสนอจะถอนการเสนอราคาที่เสนอแล้วไม่ได้

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

๕. หลักประกันการเสนอราคา

ผู้ยื่นข้อเสนอต้องวางหลักประกันการเสนอราคาพร้อมกับการเสนอราคาทางระบบการจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ โดยใช้หลักประกันอย่างหนึ่งอย่างใดดังต่อไปนี้ จำนวน ๖๐๗,๔๖๐.๐๐ บาท (หกแสนเจ็ดพันสี่ร้อยหกสิบบาทถ้วน)

๕.๑ เช็คหรือดราฟท์ที่ธนาคารเซ็นสั่งจ่าย ซึ่งเป็นเช็คหรือดราฟท์ลงวันที่ที่ใช้เช็คหรือดราฟท์นั้นชำระต่อเจ้าหน้าที่ในวันที่ยื่นข้อเสนอ หรือก่อนวันนั้นไม่เกิน ๓ วันทำการ โดยระบุผู้รับเงินเป็น "กรมบัญชีกลาง"

๕.๒ หนังสือค้ำประกันอิเล็กทรอนิกส์ของธนาคารภายในประเทศตามแบบที่คณะกรรมการนโยบายกำหนด

๕.๓ พันธบัตรรัฐบาลไทย

๕.๔ หนังสือค้ำประกันของบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยอนุโลมให้ใช้ตามตัวอย่างหนังสือค้ำประกันของธนาคารที่คณะกรรมการนโยบายกำหนด

กรณีที่ผู้ยื่นข้อเสนอนำเช็คหรือดราฟท์ที่ธนาคารสั่งจ่ายหรือพันธบัตรรัฐบาลไทยหรือหนังสือค้ำประกันของบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ มาวางเป็นหลักประกันการเสนอราคาจะต้องส่งต้นฉบับเอกสารดังกล่าวมาให้สำนักข่าวกรองแห่งชาติตรวจสอบความถูกต้องในวันที่ ๘ กรกฎาคม ๒๕๖๕ ระหว่างเวลา ๐๘.๓๐ น. ถึง ๑๖.๓๐ น.

กรณีที่ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ "กิจการร่วมค้า" ประสงค์จะใช้หนังสือค้ำประกันอิเล็กทรอนิกส์ของธนาคารในประเทศเป็นหลักประกันการเสนอราคาให้ระบุชื่อผู้เข้าร่วมค้ารายที่สัญญาร่วมค้ากำหนดให้เป็นผู้เข้ายื่นข้อเสนอกับหน่วยงานของรัฐเป็นผู้ยื่นข้อเสนอ

หลักประกันการเสนอราคาตามข้อนี้ สำนักข่าวกรองแห่งชาติ จะคืนให้ผู้ยื่นข้อเสนอหรือผู้ค้ำประกันภายใน ๑๕ วัน นับถัดจากวันที่สำนักข่าวกรองแห่งชาติได้พิจารณาเห็นชอบรายงานผลคัดเลือกผู้ชนะการประกวดราคาเรียบร้อยแล้ว เว้นแต่ผู้ยื่นข้อเสนอรายที่คัดเลือกไว้ซึ่งเสนอราคาต่ำสุดหรือได้คะแนนรวมสูงสุดไม่เกิน ๓ ราย ให้คืนได้ต่อเมื่อได้ทำสัญญาหรือข้อตกลง หรือผู้ยื่นข้อเสนอได้พ้นจากข้อผูกพันแล้ว

การคืนหลักประกันการเสนอราคา ไม่ว่าในกรณีใด ๆ จะคืนให้โดยไม่มีดอกเบี้ย

๖. หลักเกณฑ์และสิทธิ์ในการพิจารณา

๖.๑ ในการพิจารณาผลการยื่นข้อเสนอประกวดราคาอิเล็กทรอนิกส์ครั้งนี้ สำนักข่าวกรองแห่งชาติจะพิจารณาตัดสินโดยใช้หลักเกณฑ์ ราคา

๖.๒ การพิจารณาผู้ชนะการยื่นข้อเสนอ

กรณีใช้หลักเกณฑ์ราคาในการพิจารณาผู้ชนะการยื่นข้อเสนอ สำนักข่าวกรองแห่งชาติ จะพิจารณาจาก ราคารวม

๖.๓ หากผู้ยื่นข้อเสนอรายใดมีคุณสมบัติไม่ถูกต้องตามข้อ ๒ หรือยื่นหลักฐานการยื่นข้อเสนอไม่ถูกต้อง หรือไม่ครบถ้วนตามข้อ ๓ หรือยื่นข้อเสนอไม่ถูกต้องตามข้อ ๔ คณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์จะไม่รับพิจารณาข้อเสนอของผู้ยื่นข้อเสนอรายนั้น เว้นแต่ ผู้ยื่นข้อเสนอรายใดเสนอเอกสารทางเทคนิคหรือรายละเอียดคุณลักษณะเฉพาะของพัสดุที่จะขายไม่ครบถ้วน หรือเสนอรายละเอียดแตกต่างไปจากเงื่อนไขที่สำนักข่าวกรองแห่งชาติกำหนดไว้ในประกาศและเอกสารประกวดราคาอิเล็กทรอนิกส์ ในส่วนที่มิใช่สาระสำคัญและความแตกต่างนั้นไม่มีผลทำให้เกิดการได้เปรียบเสียเปรียบต่อผู้ยื่นข้อเสนอรายอื่น หรือเป็นการผิดพลาดเล็กน้อย คณะกรรมการฯ อาจพิจารณาผ่อนปรนการตัดสิทธิผู้ยื่นข้อเสนอรายนั้น

๖.๔ สำนักข่าวกรองแห่งชาติ สงวนสิทธิ์ไม่พิจารณาข้อเสนอของผู้ยื่นข้อเสนอโดยไม่มีการผ่อนผัน ในกรณีดังต่อไปนี้

(๑) ไม่ปรากฏชื่อผู้ยื่นข้อเสนอรายนั้นในบัญชีรายชื่อผู้รับเอกสารประกวดราคาอิเล็กทรอนิกส์ทางระบบจัดซื้อจัดจ้างด้วยอิเล็กทรอนิกส์ หรือบัญชีรายชื่อผู้ซื้อเอกสารประกวดราคาอิเล็กทรอนิกส์ทางระบบจัดซื้อจัดจ้างด้วยอิเล็กทรอนิกส์ ของ สำนักข่าวกรองแห่งชาติ

(๒) ไม่กรอกชื่อผู้ยื่นข้อเสนอในการเสนอราคาทางระบบจัดซื้อจัดจ้างด้วยอิเล็กทรอนิกส์

(๓) เสนอรายละเอียดแตกต่างไปจากเงื่อนไขที่กำหนดในเอกสารประกวดราคาอิเล็กทรอนิกส์ที่เป็นสาระสำคัญ หรือมีผลทำให้เกิดความได้เปรียบเสียเปรียบแก่ผู้ยื่นข้อเสนอรายอื่น

๖.๕ ในการตัดสินการประกวดราคาอิเล็กทรอนิกส์หรือในการทำสัญญา คณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์หรือสำนักข่าวกรองแห่งชาติมีสิทธิให้ผู้ยื่นข้อเสนอชี้แจงข้อเท็จจริงเพิ่มเติมได้ สำนักข่าวกรองแห่งชาติ มีสิทธิที่จะไม่รับข้อเสนอ ไม่รับราคา หรือไม่ทำสัญญา หากข้อเท็จจริงดังกล่าวไม่เหมาะสมหรือไม่ถูกต้อง

๖.๖ สำนักข่าวกรองแห่งชาติ ทรงไว้ซึ่งสิทธิที่จะไม่รับราคาต่ำสุด หรือราคาหนึ่งราคาใดหรือราคาที่เสนอทั้งหมดก็ได้ และอาจพิจารณาเลือกซื้อในจำนวน หรือขนาด หรือเฉพาะรายการหนึ่งรายการใดหรืออาจจะยกเลิกการประกวดราคาอิเล็กทรอนิกส์โดยไม่พิจารณาจัดซื้อเลยก็ได้ สุดแต่จะพิจารณา ทั้งนี้เพื่อประโยชน์ของทางราชการเป็นสำคัญ และให้ถือว่าการตัดสินของ สำนักข่าวกรองแห่งชาติ เป็นเด็ดขาด ผู้ยื่นข้อเสนอจะเรียกร้องค่าใช้จ่าย หรือค่าเสียหายใดๆ มิได้ รวมทั้ง สำนักข่าวกรองแห่งชาติ จะพิจารณายกเลิกการประกวดราคาอิเล็กทรอนิกส์และลงโทษผู้ยื่นข้อเสนอเป็นผู้ทิ้งงาน ไม่ว่าจะเป็นผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกหรือไม่ก็ตาม หากมีเหตุที่เชื่อถือได้ว่าการยื่นข้อเสนอกระทำการโดยไม่สุจริต เช่น การเสนอเอกสารอันเป็นเท็จ หรือใช้ชื่อบุคคลธรรมดา หรือนิติบุคคลอื่นมาเสนอราคาแทน เป็นต้น

ในกรณีที่ผู้ยื่นข้อเสนอรายที่เสนอราคาต่ำสุด เสนอราคาต่ำจนคาดหมายได้ว่าไม่อาจดำเนินงานตามเอกสารประกวดราคาอิเล็กทรอนิกส์ได้ คณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์หรือสำนักข่าวกรองแห่งชาติ จะให้ผู้ยื่นข้อเสนอนั้นชี้แจงและแสดงหลักฐานที่ทำให้เชื่อได้ว่าผู้ยื่นข้อเสนอสามารถดำเนินการตามเอกสารประกวดราคาอิเล็กทรอนิกส์ให้เสร็จสมบูรณ์ หากคำชี้แจงไม่เป็นที่รับฟังได้ สำนักข่าวกรองแห่งชาติ มีสิทธิที่จะไม่รับข้อเสนอหรือไม่รับราคาของผู้ยื่นข้อเสนอรายนั้น ทั้งนี้ผู้ยื่นข้อเสนอดังกล่าวไม่มีสิทธิเรียกร้องค่าใช้จ่ายหรือค่าเสียหายใดๆ จากสำนักข่าวกรองแห่งชาติ

๖.๗ ก่อนลงนามในสัญญาสำนักข่าวกรองแห่งชาติอาจประกาศยกเลิกการประกวดราคาอิเล็กทรอนิกส์ หากปรากฏว่ามีการกระทำที่เข้าลักษณะผู้ยื่นข้อเสนอที่ชนะการประกวดราคาหรือที่ได้รับการคัดเลือกมีผลประโยชน์ร่วมกัน หรือมีส่วนได้เสียกับผู้ยื่นข้อเสนอรายอื่น หรือขัดขวางการแข่งขันอย่างเป็นธรรม หรือสมยอมกันกับผู้ยื่นข้อเสนอรายอื่น หรือเจ้าหน้าที่ในการเสนอราคา หรือส่อว่ากระทำการทุจริตอื่นใดในการเสนอราคา

๖.๘ หากผู้ยื่นข้อเสนอซึ่งเป็นผู้ประกอบการ SMEs เสนอราคาสูงกว่าราคาต่ำสุดของผู้ยื่นข้อเสนอรายอื่นที่ไม่เกินร้อยละ ๑๐ ให้หน่วยงานของรัฐจัดซื้อจัดจ้างจากผู้ประกอบการ SMEs ดังกล่าวโดยจัดเรียงลำดับผู้ยื่นข้อเสนอซึ่งเป็นผู้ประกอบการ SMEs ซึ่งเสนอราคาสูงกว่าราคาต่ำสุดของผู้ยื่นข้อเสนอรายอื่นไม่เกินร้อยละ ๑๐ ที่จะเรียกมาทำสัญญาไม่เกิน ๓ ราย

ผู้ยื่นข้อเสนอที่เป็นกิจการร่วมค้าที่จะได้สิทธิตามวรรคหนึ่ง ผู้เข้าร่วมค้าทุกรายจะต้องเป็นผู้ประกอบการ SMEs

๖.๙ หากผู้ยื่นข้อเสนอซึ่งมิใช่ผู้ประกอบการ SMEs แต่เป็นบุคคลธรรมดาที่ถือสัญชาติไทยหรือนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยเสนอราคาสูงกว่าราคาต่ำสุดของผู้ยื่นข้อเสนอซึ่งเป็นบุคคลธรรมดาที่มิได้ถือสัญชาติไทยหรือนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายของต่างประเทศไม่เกินร้อยละ ๓ ให้หน่วยงานของรัฐจัดซื้อหรือจัดจ้างจากผู้ยื่นข้อเสนอซึ่งเป็นบุคคลธรรมดาที่ถือสัญชาติไทยหรือนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยดังกล่าว

ผู้ยื่นข้อเสนอที่เป็นกิจการร่วมค้าที่จะได้สิทธิตามวรรคหนึ่ง ผู้เข้าร่วมค้าทุกรายจะต้องเป็นผู้ประกอบการที่เป็นบุคคลธรรมดาที่ถือสัญชาติไทยหรือนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย

๗. การทำสัญญาซื้อขาย

๗.๑ ในกรณีที่ผู้ชนะการประกวดราคาอิเล็กทรอนิกส์ สามารถส่งมอบสิ่งของได้ครบถ้วนภายใน ๕ วันทำการ นับแต่วันที่ทำข้อตกลงซื้อ สำนักข่าวกรองแห่งชาติ จะพิจารณาจัดทำข้อตกลงเป็นหนังสือแทนการทำสัญญาตามแบบสัญญาดังระบุ ในข้อ ๑.๓ ก็ได้

๗.๒ ในกรณีที่ผู้ชนะการประกวดราคาอิเล็กทรอนิกส์ไม่สามารถส่งมอบสิ่งของได้ครบถ้วนภายใน ๕ วันทำการ หรือ สำนักข่าวกรองแห่งชาติ เห็นว่าไม่สมควรจัดทำข้อตกลงเป็นหนังสือ ตามข้อ ๗.๑ ผู้ชนะการประกวดราคาอิเล็กทรอนิกส์จะต้องทำสัญญาซื้อขายตามแบบสัญญาดังระบุในข้อ ๑.๓ หรือทำข้อตกลงเป็นหนังสือ กับ สำนักข่าวกรองแห่งชาติ ภายใน ๗ วัน นับถัดจากวันที่ได้รับแจ้ง และจะต้องวางหลักประกันสัญญาเป็นจำนวนเงินเท่ากับร้อยละ ๕ ของราคาค่าสิ่งของที่ประกวดราคาอิเล็กทรอนิกส์ให้สำนักข่าวกรองแห่งชาติยึดถือไว้ในขณะทำสัญญา โดยใช้หลักประกันอย่างหนึ่งอย่างใดดังต่อไปนี้

(๑) เงินสด

(๒) เช็คหรือดราฟท์ที่ธนาคารเซ็นสั่งจ่าย ซึ่งเป็นเช็คหรือดราฟท์ลงวันที่ที่ใช้เช็คหรือดราฟท์นั้นชำระต่อเจ้าหน้าที่ในวันทำสัญญา หรือก่อนวันนั้นไม่เกิน ๓ วันทำการ โดยระบุผู้รับเงินเป็น "กรมบัญชีกลาง"

(๓) หนังสือค้ำประกันของธนาคารภายในประเทศ ตามตัวอย่างที่คณะกรรมการนโยบายกำหนด ดังระบุในข้อ ๑.๔ (๒) หรือจะเป็นหนังสือค้ำประกันอิเล็กทรอนิกส์ตามวิธีการที่กรมบัญชีกลางกำหนด

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

(๕) พันธบัตรรัฐบาลไทย

หลักประกันนี้จะคืนให้ โดยไม่มีดอกเบี้ยภายใน ๑๕ วัน นับถัดจากวันที่ผู้ชนะการประกวดราคาอิเล็กทรอนิกส์ (ผู้ขาย) พ้นจากข้อผูกพันตามสัญญาซื้อขายแล้ว

หลักประกันนี้จะคืนให้ โดยไม่มีดอกเบี้ย ตามอัตราส่วนของพัสดุที่ซื้อซึ่งสำนักข่าวกรองแห่งชาติ ได้รับมอบไว้แล้ว

๘. ค่าจ้างและการจ่ายเงิน

สำนักข่าวกรองแห่งชาติ จะจ่ายค่าสิ่งของซึ่งได้รวมภาษีมูลค่าเพิ่ม ตลอดจนภาษีอากรอื่นๆ และค่าใช้จ่ายทั้งปวงแล้วให้แก่ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกให้เป็นผู้ขาย เมื่อผู้ขายได้ส่งมอบสิ่งของได้ครบถ้วนตามสัญญาซื้อขายหรือข้อตกลงเป็นหนังสือ และสำนักข่าวกรองแห่งชาติ ได้ตรวจรับมอบสิ่งของไว้เรียบร้อยแล้ว โดยจะแบ่งจ่ายเป็น ๕ งวด ดังนี้

๘.๑ งวดที่ ๑ ชำระเงินจำนวนร้อยละ ๑๐ ของวงเงินตามสัญญา หลังจากคณะกรรมการตรวจรับพัสดุตรวจรับงานงวดที่ ๑ ของสัญญาเป็นที่เรียบร้อยแล้ว

๘.๒ งวดที่ ๒ ชำระเงินจำนวนร้อยละ ๒๐ ของวงเงินตามสัญญา หลังจากคณะกรรมการตรวจรับพัสดุตรวจรับงานงวดที่ ๒ ของสัญญาเป็นที่เรียบร้อยแล้ว

๘.๓ งวดที่ ๓ ชำระเงินจำนวนร้อยละ ๓๐ ของวงเงินตามสัญญา หลังจากคณะกรรมการตรวจรับพัสดุตรวจรับงานงวดที่ ๓ ของสัญญาเป็นที่เรียบร้อยแล้ว

๘.๔ งวดที่ ๔ ชำระเงินจำนวนร้อยละ ๒๐ ของวงเงินตามสัญญา หลังจากคณะกรรมการตรวจรับพัสดุตรวจรับงานงวดที่ ๔ ของสัญญาเป็นที่เรียบร้อยแล้ว

๘.๕ งวดสุดท้าย ชำระเงินจำนวนร้อยละ ๒๐ ของวงเงินตามสัญญา หลังจากคณะกรรมการตรวจรับพัสดุตรวจรับงานงวดที่ ๕ ของสัญญาเป็นที่เรียบร้อยแล้ว

๙. อัตราค่าปรับ

ค่าปรับตามแบบสัญญาซื้อขายแนบท้ายเอกสารประกวดราคาอิเล็กทรอนิกส์นี้ หรือข้อตกลงซื้อขายเป็นหนังสือ ให้คิดในอัตราร้อยละ ๐.๒๐ ของราคาค่าสิ่งของที่ยังไม่ได้รับมอบต่อวัน

๑๐. การรับประกันความชำรุดบกพร่อง

ผู้ชนะการประกวดราคาอิเล็กทรอนิกส์ ซึ่งได้ทำสัญญาซื้อขายตามแบบดังระบุในข้อ ๑.๓ หรือทำข้อตกลงซื้อเป็นหนังสือ แล้วแต่กรณี จะต้องรับประกันความชำรุดบกพร่องของสิ่งของที่ซื้อขายที่เกิดขึ้นภายในระยะเวลาไม่น้อยกว่า ๑ ปี นับถัดจากวันที่ สำนักข่าวกรองแห่งชาติ ได้รับมอบสิ่งของ โดยต้องรีบจัดการซ่อมแซมแก้ไขให้ใช้การได้ดีดังเดิมภายใน ๓ วัน นับถัดจากวันที่ได้รับแจ้งความชำรุดบกพร่อง

๑๑. ข้อสงวนสิทธิ์ในการยื่นข้อเสนอและอื่นๆ

๑๑.๑ เงินค่าพัสดุสำหรับการซื้อครั้งนี้ ได้มาจากเงินงบประมาณประจำปี พ.ศ. ๒๕๖๕

การลงนามในสัญญาจะกระทำได้ ต่อเมื่อสำนักข่าวกรองแห่งชาติได้รับอนุมัติเงินค่าพัสดุจากเงินงบประมาณประจำปี พ.ศ. ๒๕๖๕ แล้วเท่านั้น

๑๑.๒ เมื่อสำนักข่าวกรองแห่งชาติได้คัดเลือกผู้ยื่นข้อเสนอรายใดให้เป็นผู้ขาย และได้ตกลงซื้อสิ่งของตามการประกวดราคาอิเล็กทรอนิกส์แล้ว ถ้าผู้ขายจะต้องสั่งหรือนำสิ่งของดังกล่าวเข้ามาจากต่างประเทศและของนั้นต้องนำเข้ามาโดยทางเรือในเส้นทางที่มีเรือไทยเดินอยู่ และสามารถให้บริการรับขนได้ตามที่รัฐมนตรีว่าการกระทรวงคมนาคมประกาศกำหนด ผู้ยื่นข้อเสนอซึ่งเป็นผู้ขายจะต้องปฏิบัติตามกฎหมายว่าด้วยการส่งเสริมการพาณิชยนาวี ดังนี้

(๑) แจ้งการสั่งหรือนำสิ่งของที่ซื้อขายดังกล่าวเข้ามาจากต่างประเทศต่อกรมเจ้าท่า ภายใน ๗ วัน นับตั้งแต่วันที่ผู้ขายสั่ง หรือซื้อของจากต่างประเทศ เว้นแต่เป็นของที่รัฐมนตรีว่าการกระทรวงคมนาคมประกาศยกเว้นให้บรรทุกโดยเรืออื่นได้

(๒) จัดการให้สิ่งของที่ซื้อขายดังกล่าวบรรทุกโดยเรือไทย หรือเรือที่มีสิทธิเช่นเดียวกับเรือไทย จากต่างประเทศมายังประเทศไทย เว้นแต่จะได้รับอนุญาตจากกรมเจ้าท่า ให้บรรทุกสิ่งของนั้นโดยเรืออื่นที่มิใช่เรือไทย ซึ่งจะต้องได้รับอนุญาตเช่นนั้นก่อนบรรทุกของลงเรืออื่น หรือเป็นของที่รัฐมนตรีว่าการกระทรวงคมนาคมประกาศยกเว้นให้บรรทุกโดยเรืออื่น

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

๑๑.๓ ผู้ยื่นข้อเสนอซึ่งสำนักข่าวกรองแห่งชาติได้คัดเลือกแล้ว ไม่ไปทำสัญญาหรือข้อตกลงซื้อเป็นหนังสือภายในเวลาที่กำหนด ดังระบุไว้ในข้อ ๗ สำนักข่าวกรองแห่งชาติจะริบหลักประกันการยื่นข้อเสนอ หรือเรียกร้องจากผู้ออกหนังสือค้ำประกันการยื่นข้อเสนอทันที และอาจพิจารณาเรียกร้องให้ชดใช้ความเสียหายอื่น (ถ้ามี) รวมทั้งจะพิจารณาให้เป็นผู้ทิ้งงาน ตามระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ

๑๑.๔ สำนักข่าวกรองแห่งชาติสงวนสิทธิ์ที่จะแก้ไขเพิ่มเติมเงื่อนไข หรือข้อกำหนดในแบบสัญญาหรือข้อตกลงซื้อเป็นหนังสือ ให้เป็นไปตามความเห็นของสำนักงานอัยการสูงสุด (ถ้ามี)

๑๑.๕ ในกรณีที่เอกสารแนบท้ายเอกสารประกวดราคาอิเล็กทรอนิกส์นี้ มีความขัดหรือแย้งกัน ผู้ยื่นข้อเสนอจะต้องปฏิบัติตามคำวินิจฉัยของสำนักข่าวกรองแห่งชาติ คำวินิจฉัยดังกล่าวให้ถือเป็นที่สุด และผู้ยื่นข้อเสนอไม่มีสิทธิเรียกร้องค่าใช้จ่ายใดๆ เพิ่มเติม

๑๑.๖ สำนักข่าวกรองแห่งชาติอาจประกาศยกเลิกการจัดซื้อในกรณีต่อไปนี้ได้ โดยที่ผู้ยื่นข้อเสนอจะเรียกร้องค่าเสียหายใดๆ จากสำนักข่าวกรองแห่งชาติไม่ได้

(๑) สำนักข่าวกรองแห่งชาติไม่ได้รับการจัดสรรเงินที่จะใช้ในการจัดซื้อหรือที่ได้รับจัดสรรแต่ไม่เพียงพอที่จะทำการจัดซื้อครั้งนี้ต่อไป

(๒) มีการกระทำที่เข้าลักษณะผู้ยื่นข้อเสนอที่ชนะการจัดซื้อหรือที่ได้รับการคัดเลือกมีผลประโยชน์ร่วมกัน หรือมีส่วนได้เสียกับผู้ยื่นข้อเสนอรายอื่น หรือขัดขวางการแข่งขันอย่างเป็นธรรม หรือสมยอมกันกับผู้ยื่นข้อเสนอรายอื่น หรือเจ้าหน้าที่ในการเสนอราคา หรือส่อว่ากระทำการทุจริตอื่นใดในการเสนอราคา

(๓) การทำการจัดซื้อครั้งนี้ต่อไปอาจก่อให้เกิดความเสียหายแก่สำนักข่าวกรองแห่งชาติ หรือกระทบต่อประโยชน์สาธารณะ

(๔) กรณีอื่นในทำนองเดียวกับ (๑) (๒) หรือ (๓) ตามที่กำหนดในกฎกระทรวงซึ่งออกตามความในกฎหมายว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ

๑๒. การปฏิบัติตามกฎหมายและระเบียบ

ในระหว่างระยะเวลาการซื้อ ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกให้เป็นผู้ขายต้องปฏิบัติตามหลักเกณฑ์ที่กฎหมายและระเบียบได้กำหนดไว้โดยเคร่งครัด

๑๓. การประเมินผลการปฏิบัติงานของผู้ประกอบการ

สำนักข่าวกรองแห่งชาติ สามารถนำผลการปฏิบัติงานแล้วเสร็จตามสัญญาของผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกให้เป็นผู้ขายเพื่อนำมาประเมินผลการปฏิบัติงานของผู้ประกอบการ

ทั้งนี้ หากผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกไม่ผ่านเกณฑ์ที่กำหนดจะถูกระงับการยื่นข้อเสนอหรือทำสัญญากับสำนักข่าวกรองแห่งชาติ ไว้ชั่วคราว

สำนักข่าวกรองแห่งชาติ
๒๙ มิถุนายน ๒๕๖๕

ขอบเขตของงาน (Terms of Reference : TOR)
โครงการจัดตั้งและพัฒนาศูนย์ปฏิบัติการความมั่นคงปลอดภัยไซเบอร์
แขวงพญาไท เขตพญาไท กรุงเทพมหานคร
กิจกรรมที่ 2 : จัดซื้อครุภัณฑ์ พัฒนาระบบและเครือข่ายผู้ปฏิบัติงานความมั่นคงปลอดภัยไซเบอร์
กลุ่มหน่วยงานความมั่นคง

1. ความเป็นมา

ปัจจุบันภัยคุกคามและการโจมตีทางไซเบอร์ มีแนวโน้มทวีความรุนแรงและมีปริมาณมากขึ้นอย่างยิ่ง ก่อให้เกิดผลกระทบต่อความสงบเรียบร้อยในวงกว้าง ในปัจจุบันหน่วยงานด้านความมั่นคงของประเทศ ได้นำเทคโนโลยีดิจิทัลเข้ามาสนับสนุนการปฏิบัติงานจัดเก็บข้อมูลในข่าวสารที่มีชั้นความลับและเกี่ยวข้องกับความมั่นคงของประเทศในระบบฐานข้อมูลและระบบสารสนเทศ ซึ่งมีความเสี่ยงและอาจได้รับผลกระทบจากภัยคุกคามทางไซเบอร์

ภัยคุกคามทางไซเบอร์ อาทิ การจารกรรมทางไซเบอร์เพื่อขโมยข้อมูล การแสวงประโยชน์จากช่องโหว่ของเทคโนโลยีดิจิทัลเพื่อสอดแนมและขโมยข้อมูล เฉพาะอย่างยิ่งการขโมยข้อมูลและเข้ารหัสข้อมูลเรียกค่าไถ่นั้น ส่งผลต่อข้อมูลที่เกี่ยวข้องกับความมั่นคงของประเทศ ข้อมูลที่ถูกจารกรรมรั่วไหลไปยังบุคคลที่ไม่เกี่ยวข้องหรือฝ่ายตรงข้ามส่งผลกระทบต่อความมั่นคงของประเทศชาติอย่างร้ายแรง

สำนักข่าวกรองแห่งชาติและหน่วยงานด้านความมั่นคงจะต้องเร่งพัฒนาและขยายขีดความสามารถของบุคลากรและหน่วยงานในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้มีความสามารถในการตรวจสอบช่องโหว่ระบบคอมพิวเตอร์และระบบเครือข่าย และการรับมือภัยคุกคามทางไซเบอร์ในระดับประเทศ จึงจำเป็นต้องส่งเสริมให้เกิดความร่วมมือระหว่างหน่วยงานด้านความมั่นคงให้มีเครือข่ายหรือประชาคมผู้ปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์ขึ้น เพื่อให้เกิดความร่วมมือในการประสานงานแก้ไขปัญหาภัยคุกคามทางไซเบอร์

2. วัตถุประสงค์

เพื่อสร้างเครือข่ายและพัฒนาบุคลากรผู้ปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์ในกลุ่มหน่วยงานด้านความมั่นคง ให้เกิดการแลกเปลี่ยนข้อมูลและวิธีการรับมือภัยคุกคามทางไซเบอร์

3. คุณสมบัติผู้เสนอราคา

3.1 มีความสามารถตามกฎหมาย,

3.2 ไม่เป็นบุคคลล้มละลาย ,

3.3 ไม่อยู่ระหว่างเลิกกิจการ ,

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราวเนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าด้วยกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง,

3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย,

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา,

1.	2.	3.	4.	5. .....
ประธานคณะกรรมการ	คณะกรรมการ	คณะกรรมการ	คณะกรรมการ	คณะกรรมการและเลขานุการ

3.7 เป็นนิติบุคคล ผู้มีอาชีพขายพัสดุดังกล่าว

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่สำนักข่าวกรองแห่งชาติ ณ วันที่ยื่นข้อเสนอ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการเสนอราคาครั้งนี้

3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่ รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์ความคุ้มกันเช่นว่านั้น

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

3.11 ผู้ยื่นข้อเสนอซึ่งได้รับคัดเลือกเป็นคู่สัญญาต้องลงทะเบียนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement: e-GP) ของกรมบัญชีกลาง ตามที่คณะกรรมการ ป.ป.ช. กำหนด

3.12 ผู้ยื่นข้อเสนอต้องไม่อยู่ในฐานะเป็นผู้ไม่แสดงบัญชีรายรับรายจ่ายหรือแสดงบัญชีรายรับรายจ่ายไม่ถูกต้องครบถ้วนในสาระสำคัญ ตามที่คณะกรรมการ ป.ป.ช. กำหนด

3.13 ผู้ยื่นข้อเสนอซึ่งได้รับคัดเลือกเป็นคู่สัญญาต้องรับและจ่ายเงินผ่านบัญชีธนาคาร เว้นแต่การจ่ายเงินแต่ละครั้งซึ่งมีมูลค่าไม่เกินสามหมื่นบาทคู่สัญญาอาจจ่ายเป็นเงินสดก็ได้

3.14 ผู้ยื่นข้อเสนอต้องไม่เป็นที่ปรึกษาของสำนักข่าวกรองแห่งชาติ หรือมีส่วนร่วมในบริษัทที่ปรึกษาของสำนักข่าวกรองแห่งชาติในการจัดซื้อครั้งนี้ และต้องไม่มีผู้ปฏิบัติงานของสำนักข่าวกรองแห่งชาติเข้าไปมีส่วนร่วมในธุรกิจของผู้ยื่นข้อเสนอในฐานะผู้กระทำการหรือผู้ร่วมงาน

4. เกณฑ์การพิจารณาคัดเลือก

4.1 ผู้ยื่นข้อเสนอต้องมีคุณสมบัติพร้อมมีเอกสารและหลักฐานต่าง ๆ ครบถ้วนตามที่กำหนดในคุณสมบัติผู้เสนอราคา จึงจะได้รับการพิจารณาคัดเลือกตามเกณฑ์ที่กำหนด

4.2 การพิจารณาผลการยื่นข้อเสนอครั้งนี้ สำนักข่าวกรองแห่งชาติจะพิจารณาตัดสินโดยใช้หลักเกณฑ์ราคา

5. ขอบเขตการดำเนินงาน

5.1 จัดซื้อครุภัณฑ์สำหรับการพัฒนาระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์ จำนวน 10 รายการ รายละเอียดครุภัณฑ์ตามผนวก 1

5.2 พัฒนาระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์ จำนวน 1 ระบบ ตามผนวก 2

5.3 จัดอบรมบุคลากรและจัดการแข่งขันทักษะความมั่นคงปลอดภัยไซเบอร์ จำนวน 1 งาน ตามผนวก 3

6. เงื่อนไขและข้อกำหนดอื่น ๆ

6.1 ผู้เสนอราคาต้องแสดงหนังสือรับรองจากเจ้าของผลิตภัณฑ์ หรือสาขาของเจ้าของผลิตภัณฑ์ ว่าผลิตภัณฑ์ที่เสนอขายเป็นของแท้ ของใหม่ ไม่เก่าเก็บ ไม่เคยใช้งานมาก่อน หรือปรับปรุงสภาพขึ้นมาใหม่ หรือดัดแปลงสภาพมาเพื่อใช้ในการเสนอราคาครั้งนี้โดยเฉพาะ และผลิตภัณฑ์ได้รับการบรรจุหีบห่อตามมาตรฐานผู้ผลิต

6.2 ผู้เสนอราคาต้องทำตารางเปรียบเทียบรายละเอียด และเงื่อนไขเฉพาะเป็นรายข้อทุกข้อ (Statement of Compliance) รายละเอียดตามขอบเขตการดำเนินงานโดยใช้ตัวอย่างแบบฟอร์มการเปรียบเทียบ ตามตารางที่ 1 ในการเปรียบเทียบรายการดังกล่าว หากมีกรณีที่ต้องมีการอ้างอิงข้อความ หรือเอกสารในส่วนอื่นที่จัดทำเสนอมา ผู้เสนอราคาต้องระบุให้เห็นอย่างชัดเจน สามารถตรวจสอบได้โดยง่ายไว้ในเอกสารเปรียบเทียบด้วยว่า สิ่งที่ต้องการอ้างอิงถึงนั้น อยู่ในส่วนใดตำแหน่งใดของเอกสารอื่น ๆ ที่จัดทำเสนอมา

1.	2.	3.	4.	5.
ประธานคณะกรรมการ	คณะกรรมการ	คณะกรรมการ	คณะกรรมการ	คณะกรรมการและเลขานุการ

สำหรับเอกสารที่อ้างอิงถึงนั้น ให้หมายเหตุ หรือขีดเส้นใต้ หรือระบายสี พร้อมเขียนหัวข้อกำกับไว้ เพื่อให้สามารถตรวจสอบกับเอกสารเปรียบเทียบได้ง่าย และตรงกันด้วย

ตารางที่ 1 ตารางเปรียบเทียบคุณสมบัติข้อกำหนด และรายละเอียดข้อเสนอ

อ้างถึงข้อ	ข้อกำหนดที่ต้องการ	ข้อกำหนดที่นำเสนอ	เอกสารอ้างอิง
ระบุหัวข้อให้ตรงกับหัวข้อที่ระบุในเอกสารรายละเอียดคุณลักษณะเฉพาะ	ให้คัดลอกคุณลักษณะเฉพาะที่สำนักข่าวกรองแห่งชาติกำหนด	ให้ระบุคุณลักษณะเฉพาะที่ผู้เสนอราคาเสนอ	ระบุหมายเลขหน้าของเอกสารอ้างอิงของผู้เสนอราคา

6.3 ผู้ขายต้องติดสติ๊กเกอร์ ระบุชื่อบริษัทผู้ขายและบริษัทเจ้าของผลิตภัณฑ์หรือสาขาของบริษัทเจ้าของผลิตภัณฑ์ ระยะเวลาการรับประกัน เริ่มต้น/สิ้นสุด และหมายเลขโทรศัพท์ติดต่อศูนย์บริการหรือตัวแทนผู้ได้รับแต่งตั้งจากบริษัทเจ้าของผลิตภัณฑ์หรือสาขาของบริษัทเจ้าของผลิตภัณฑ์ อย่างชัดเจน

6.4 ต้องบรรจุหีบห่อที่สามารถป้องกันความเสียหายแก่ตัวเครื่องได้เป็นอย่างดี หรือตามมาตรฐานผู้ผลิต

6.5 ราคาที่เสนอเป็นราคารวมภาษีมูลค่าเพิ่ม ภาษีอากรอื่น ๆ และค่าใช้จ่ายทั้งปวงแล้ว

7. การรับประกันความชำรุดบกพร่องและบริการหลังการขาย

7.1 ผู้ขายต้องให้บริการบำรุงรักษาระบบทั้งหมดในโครงการ และสนับสนุนเจ้าหน้าที่สำนักข่าวกรองแห่งชาติให้สามารถใช้งานระบบที่ได้จัดหาและพัฒนาให้สำนักข่าวกรองแห่งชาติได้อย่างต่อเนื่อง ตลอดช่วงเวลาราชการเป็นระยะเวลา 1 ปี นับจากวันตรวจรับพัสดุงวดสุดท้าย

7.2 สำนักข่าวกรองแห่งชาติสามารถขอรับคำปรึกษาด้านเทคนิคทางโทรศัพท์ได้โดยไม่จำกัดจำนวนครั้งตลอดช่วงเวลาราชการเป็นระยะเวลา 1 ปี นับวันตรวจรับพัสดุงวดสุดท้าย

7.3 ผู้ขายต้องเข้ามาตรวจสอบและอัพเกรดเวอร์ชั่น (Version) ระบบที่ได้ส่งมอบให้สำนักข่าวกรองแห่งชาติให้มีความทันสมัยอยู่เสมอ โดยต้องแจ้งให้ผู้ดูแลระบบของสำนักข่าวกรองแห่งชาติทราบเมื่อมีซอฟต์แวร์หรือระบบเวอร์ชั่นใหม่เผยแพร่ ตลอดระยะเวลา 1 ปี นับจากวันตรวจรับพัสดุงวดสุดท้าย

7.4 กรณีเกิดเหตุฉุกเฉินจนระบบคอมพิวเตอร์และระบบเครือข่ายไม่สามารถใช้งานได้ และผู้ขายไม่สามารถแก้ไขปัญหาผ่านทางโทรศัพท์ได้ ผู้เสนอราคาที่ผ่านการคัดเลือกต้องเข้ามาตรวจสอบและให้บริการภายในพื้นที่ที่ติดตั้งอุปกรณ์ (On site services) หรือ ดำเนินการจากภายนอก (Remote) โดยต้องแก้ไขปัญหาให้แล้วเสร็จภายในระยะเวลาที่กำหนด

7.5 กรณีซอฟต์แวร์หรือระบบคอมพิวเตอร์และระบบเครือข่ายมีปัญหาจนไม่สามารถใช้งานได้ ผู้ขายจะต้องจัดส่งเจ้าหน้าที่ด้านเทคนิคเข้ามาตรวจสอบและแก้ไขในพื้นที่ที่ติดตั้งซอฟต์แวร์หรือระบบคอมพิวเตอร์และระบบเครือข่ายของสำนักข่าวกรองแห่งชาติ ภายในระยะเวลา 24 ชั่วโมงนับตั้งแต่เวลาที่ได้รับแจ้งจากสำนักข่าวกรองแห่งชาติ โดย ผู้เสนอราคาที่ผ่านการคัดเลือกจะต้องแก้ไขให้ซอฟต์แวร์และระบบคอมพิวเตอร์และระบบเครือข่ายกลับมาอยู่ในสภาพพร้อมใช้งานได้ตามปกติ และ/หรือจัดการกู้คืนค่าระบบ (Configuration) ให้เทียบเท่าเดิม โดยต้องดำเนินการให้แล้วเสร็จภายในระยะเวลา 72 ชั่วโมงนับตั้งแต่เวลาที่ได้รับแจ้งจากสำนักข่าวกรองแห่งชาติ

8. กรรมสิทธิ์และลิขสิทธิ์ของงาน ข้อมูล เอกสารและโปรแกรมคอมพิวเตอร์

8.1 งาน ข้อมูล เอกสาร และโปรแกรมคอมพิวเตอร์ที่ผู้ขายจัดทำขึ้นและส่งมอบให้แก่สำนักข่าวกรองแห่งชาติในการดำเนินงานโครงการนี้ ให้ตกเป็นกรรมสิทธิ์ของสำนักข่าวกรองแห่งชาติ โดยผู้ขายต้องส่งมอบ Source Code และ Component หรือ Library ทั้งหมดของโปรแกรมคอมพิวเตอร์ที่ผู้ขายจัดทำขึ้นและส่งมอบให้แก่สำนักข่าวกรองแห่งชาติ โดยครบถ้วนสมบูรณ์ และในกรณีที่ผู้ขายนำงาน ข้อมูล เอกสาร และโปรแกรมคอมพิวเตอร์ที่บุคคลอื่นเป็นเจ้าของกรรมสิทธิ์หรือเป็นเจ้าของลิขสิทธิ์มาใช้ในการดำเนินงานที่จัดจ้างนี้ด้วย ผู้ขายจะต้องจัดให้ สำนักข่าวกรองแห่งชาติ ได้สิทธิในการใช้งานโดยไม่มีข้อจำกัดทั้งการติดตั้งบนเครื่องคอมพิวเตอร์ใด ๆ และระยะเวลาการใช้งาน รวมทั้งไม่ต้องเสียค่าใช้จ่ายเพิ่มเติมอีก

8.2 ผู้ขายจะต้องไม่เปิดเผยหรือเผยแพร่งาน ข้อมูล เอกสาร และโปรแกรมคอมพิวเตอร์ที่ผู้ขายส่งมอบให้แก่สำนักข่าวกรองแห่งชาติ ไม่ว่าทั้งหมดหรือเพียงบางส่วนให้แก่บุคคลใด

8.3 ผู้ขายต้องรับประกันว่า งาน ข้อมูล เอกสาร และโปรแกรมคอมพิวเตอร์ทั้งหมดที่นำมาส่งมอบให้แก่ สำนักข่าวกรองแห่งชาติ ในการดำเนินงานตามโครงการนี้ ผู้ขายเป็นผู้จัดทำ สร้างสรรค์ และมีสิทธิโดยชอบด้วยกฎหมายที่จะนำมาใช้ในการดำเนินงานและส่งมอบให้แก่ สำนักข่าวกรองแห่งชาติ ในการดำเนินงานตามโครงการนี้ เพื่อให้สำนักข่าวกรองแห่งชาติสามารถใช้งานได้โดยชอบด้วยกฎหมายและไม่มีข้อจำกัดใด ๆ

8.4 ในกรณีที่มีบุคคลใดกล่าวอ้างว่า สำนักข่าวกรองแห่งชาติ ละเมิดกรรมสิทธิ์หรือลิขสิทธิ์ในงาน ข้อมูล เอกสาร และโปรแกรมคอมพิวเตอร์ทั้งหมดที่ผู้ขายนำมาส่งมอบให้แก่สำนักข่าวกรองแห่งชาติในการดำเนินงานตามโครงการนี้ ผู้เสนอราคาที่ผ่านการคัดเลือกจะต้องรับผิดชอบค่าใช้จ่ายทั้งหมดในการต่อสู้คดี และความเสียหายที่เกิดขึ้นแก่สำนักข่าวกรองแห่งชาติ

8.5 ผู้ขายจะต้องส่งเอกสาร สัญญารักษาความลับ (Non-disclosure Agreement) ที่ลงนามโดยบุคลากรที่เข้าร่วมดำเนินงานในโครงการทั้งหมด กรณีที่มีการเปลี่ยนแปลงหรือเพิ่มบุคลากรผู้เข้าร่วมโครงการจะต้องส่งเอกสารสัญญารักษาความลับของบุคลากรดังกล่าวให้แก่ผู้ว่าจ้างก่อนที่บุคลากรนั้นจะเข้าเริ่มงานในโครงการ

9. ลิขสิทธิ์หรือสิทธิ์ในทรัพย์สินทางปัญญาและการรักษาความลับ

ผู้ขายตกลงให้ลิขสิทธิ์ในรายงานและข้อมูลที่ผู้ขายจัดทำขึ้นจากการทำงานตามโครงการนี้เป็นของสำนักข่าวกรองแห่งชาติ โดยผู้ขายจะต้องไม่นำข้อมูลที่ได้รับจากการทำงาน รวมทั้งรายงานและข้อมูลที่ผู้ขายได้จัดทำขึ้นไปเปิดเผยหรือใช้งานต่อไป เว้นแต่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากสำนักข่าวกรองแห่งชาติ

10. สถานที่ส่งมอบงาน

สำนักข่าวกรองแห่งชาติ เลขที่ 8 ซอยพหลโยธิน 3 ถนนพหลโยธิน แขวงพญาไท เขตพญาไท กรุงเทพมหานคร

11. การส่งมอบงาน

ผู้ขายจะต้องส่งมอบงานในโครงการ ฯ ทั้งหมด ให้แก่สำนักข่าวกรองแห่งชาติภายในระยะเวลา 240 วัน นับถัดจากวันลงนามในสัญญา โดยแบ่งออกเป็น 5 งวดงาน ดังนี้

1.	2.	3.	4.	5. .....
ประธานคณะกรรมการ	คณะกรรมการ	คณะกรรมการ	คณะกรรมการ	คณะกรรมการและเลขานุการ

11.1 งวดที่ 1 ส่งมอบภายใน 45 วัน นับถัดจากวันลงนามในสัญญา โดยส่งมอบงานในรูปแบบเอกสาร จำนวน 5 ชุด และรูปแบบไฟล์ที่แก้ไขได้พร้อมไฟล์ PDF ในแฟลชไดร์ฟ (Flash Drive) จำนวน 1 ชุด ประกอบด้วย

11.1.1 เอกสารแผนการดำเนินงานโครงการ (Project Plan) ที่แสดงระยะเวลาในการทำงานขั้นตอนตามขอบเขตการดำเนินงาน โดยจะต้องระบุชื่อกิจกรรม ความเชื่อมโยงของกิจกรรม ผู้รับผิดชอบ ระยะเวลาที่ใช้ในกิจกรรม ตั้งแต่เริ่มต้นจนถึงวันส่งมอบงาน ผลลัพธ์ที่ได้ในแต่ละกิจกรรม

11.1.2 รายละเอียดบุคลากรทั้งหมดที่รับผิดชอบโครงการ

11.2 งวดที่ 2 ส่งมอบภายใน 120 วัน นับถัดจากวันลงนามในสัญญา โดยส่งมอบงานในรูปแบบเอกสาร จำนวน 5 ชุด และรูปแบบไฟล์ที่แก้ไขได้พร้อมไฟล์ PDF ในแฟลชไดร์ฟ (Flash Drive) จำนวน 1 ชุด ประกอบด้วย

11.2.1 เอกสารผลการวิเคราะห์ความต้องการใช้งานระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์

11.2.2 เอกสารการวิเคราะห์และออกแบบระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์

11.2.2.1 ภาพรวมการออกแบบระบบและการทำงานของระบบ

11.2.2.2 แผนผังโครงสร้างแสดงการเชื่อมโยงภายในและภายนอกของระบบ

11.2.2.3 แผนผังกิจกรรม (Activity Diagram) ของระบบ

11.2.2.4 แผนผังแสดงความสัมพันธ์ระหว่างข้อมูล (E-R Diagram) ของระบบและฐานข้อมูล

11.2.2.5 แผนผังพจนานุกรมฐานข้อมูล (Data Dictionary)

11.2.2.6 รูปแบบการแสดงผลและการทำงานของฟังก์ชั่นแต่ละหน้า (Web Page)

11.2.3 นำเสนอโครงร่างระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์

11.2.4 ต้นแบบระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์ (Prototype)

11.3 งวดที่ 3 ส่งมอบภายใน 150 วัน นับถัดจากวันลงนามในสัญญา โดยส่งมอบงานในรูปแบบเอกสาร จำนวน 5 ชุด และรูปแบบไฟล์ที่แก้ไขได้พร้อมไฟล์ PDF ในแฟลชไดร์ฟ (Flash Drive) จำนวน 1 ชุด ประกอบด้วย

11.3.1 ครุภัณฑ์คอมพิวเตอร์ที่จัดหาภายในโครงการประกอบด้วยอุปกรณ์คอมพิวเตอร์ (Hardware) และซอฟต์แวร์ลิขสิทธิ์ (License Software) ในโครงการ

11.3.2 รายงานผลการติดตั้งอุปกรณ์คอมพิวเตอร์ (Hardware) และซอฟต์แวร์ลิขสิทธิ์ (License Software) ในโครงการ

11.4 งวดที่ 4 ส่งมอบภายใน 180 วัน นับถัดจากวันลงนามในสัญญา โดยส่งมอบงานในรูปแบบเอกสาร จำนวน 5 ชุด และรูปแบบไฟล์ที่แก้ไขได้พร้อมไฟล์ PDF ในแฟลชไดร์ฟ (Flash Drive) จำนวน 1 ชุด ประกอบด้วย

11.4.1 รายงานผลงานอบรมและจัดแข่งขันทักษะความมั่นคงปลอดภัยไซเบอร์

11.4.2 ภาพถ่ายและวีดิโอกิจกรรมการจัดงานแข่งขันทักษะความมั่นคงปลอดภัยไซเบอร์

11.5 งวดที่ 5 ส่งมอบภายใน 240 วัน นับถัดจากวันลงนามในสัญญา โดยส่งมอบงานในรูปแบบเอกสาร จำนวน 5 ชุด และรูปแบบไฟล์ที่แก้ไขได้พร้อมไฟล์ PDF ในแฟลชไดร์ฟ (Flash Drive) จำนวน 1 ชุด ประกอบด้วย

1.	2.	3.	4.	5. .....
ประธานคณะกรรมการ	คณะกรรมการ	คณะกรรมการ	คณะกรรมการ	คณะกรรมการและเลขานุการ

11.5.1 รายงานผลการทดสอบระบบ (User Acceptance Test) ระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วยการทดสอบการใช้งานของผู้ใช้งาน (Usability Testing) ประสิทธิภาพ (Performance Testing) ความถูกต้องสมบูรณ์โดยรวม (Functional Testing) และการรักษาความปลอดภัยของระบบ (Security Testing)

11.5.2 รายงานผลการทดสอบเจาะระบบ (Penetration Testing) ตามแนวทาง OWASP Top 10 2021

11.5.3 ผลการพัฒนาระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์ พร้อมการติดตั้งระบบให้สามารถใช้งานได้อย่างถูกต้องสมบูรณ์ตามขอบเขตการดำเนินงาน

11.5.4 รายงานผลการฝึกอบรมผู้ใช้งานและผู้ดูแลระบบของระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์

11.5.5 คู่มือการใช้งานสำหรับผู้ใช้งานและผู้ดูแลระบบของระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์ พร้อมคลิปวีดิโอแนะนำการใช้งานระบบสำหรับผู้ใช้งานทั่วไป

11.5.6 ส่งมอบรหัสชุดคำสั่งโปรแกรม (Source Code) ระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์

12. เงื่อนไขการชำระเงิน

12.1 **งวดที่ 1** ชำระเงินจำนวนร้อยละ 10 ของวงเงินตามสัญญา หลังจากคณะกรรมการตรวจรับพัสดุตรวจรับงานงวดที่ 1 ของสัญญาเป็นที่เรียบร้อยแล้ว

12.2 **งวดที่ 2** ชำระเงินจำนวนร้อยละ 20 ของวงเงินตามสัญญา หลังจากคณะกรรมการตรวจรับพัสดุตรวจรับงานงวดที่ 2 ของสัญญาเป็นที่เรียบร้อยแล้ว

12.3 **งวดที่ 3** ชำระเงินจำนวนร้อยละ 30 ของวงเงินตามสัญญา หลังจากคณะกรรมการตรวจรับพัสดุตรวจรับงานงวดที่ 2 ของสัญญาเป็นที่เรียบร้อยแล้ว

12.4 **งวดที่ 4** ชำระเงินจำนวนร้อยละ 20 ของวงเงินตามสัญญา หลังจากคณะกรรมการตรวจรับพัสดุตรวจรับงานงวดที่ 4 ของสัญญาเป็นที่เรียบร้อยแล้ว

12.5 **งวดที่ 5** ชำระเงินจำนวนร้อยละ 20 ของวงเงินตามสัญญา หลังจากคณะกรรมการตรวจรับพัสดุตรวจรับงานงวดที่ 5 ของสัญญาเป็นที่เรียบร้อยแล้ว

13. วงเงินในการจัดหา

วงเงินทั้งสิ้น 8,678,000 บาท (แปดล้านหกแสนเจ็ดหมื่นแปดพันบาทถ้วน)

14. อัตราค่าปรับ

ในกรณีผู้ขายไม่สามารถส่งมอบงานได้ตามกำหนด และสำนักข่าวกรองแห่งชาติยังไม่ใช้สิทธิบอกเลิกสัญญา ผู้เสนอราคาที่ผ่านการคัดเลือกจะต้องชำระค่าปรับเป็นรายวัน ในอัตราร้อยละ 0.2 ของวงเงินสัญญาจ้างที่จะเกิดขึ้น นับถัดจากวันครบกำหนดตามสัญญาจนถึงวันที่ผู้ขายได้ส่งมอบงานทั้งหมด

15. ผู้รับผิดชอบโครงการ

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักข่าวกรองแห่งชาติ

---

1.	2.	3.	4.	5. .....
ประธานคณะกรรมการ	คณะกรรมการ	คณะกรรมการ	คณะกรรมการ	คณะกรรมการและเลขานุการ

ภาคผนวก 1

กิจกรรมที่ 2 : จัดซื้อครุภัณฑ์ พัฒนาระบบและเครือข่ายผู้ปฏิบัติงานความมั่นคงปลอดภัยไซเบอร์ กลุ่มหน่วยงานความมั่นคง

1. ระบบคอมพิวเตอร์แม่ข่ายประสิทธิภาพสูง จำนวน 1 ระบบ มีคุณลักษณะดังนี้

1.1 เป็นเครื่องคอมพิวเตอร์แม่ข่ายที่มีสถาปัตยกรรมแบบ Hyper-Converged Infrastructure โดยเฉพาะ จำนวน 3 โหนด (Node) หรือดีกว่า

1.2 มีหน่วยประมวลผลกลาง (CPU) แบบ 20 แกนหลัก (20 Core) หรือดีกว่า สำหรับคอมพิวเตอร์แม่ข่าย (Server) โดยเฉพาะ มีความเร็วสัญญาณนาฬิกาพื้นฐานไม่น้อยกว่า 2.1 GHz จำนวนไม่น้อยกว่า 1 หน่วยต่อโหนด (Node)

1.3 มีหน่วยความจำหลักขนาดไม่น้อยกว่า 192 GB แบบ DDR4 RDIMM

1.4 มีหน่วยจัดเก็บข้อมูล M.2 SSD ที่มีความจุไม่น้อยกว่า 240GB จำนวน 2 หน่วย สามารถทำ Hardware RAID1 ได้

1.5 มีหน่วยจัดเก็บข้อมูล SSD แบบ SAS Interface ขนาดความจุไม่น้อยกว่า 800 GB จำนวนไม่น้อยกว่า 1 หน่วย

1.6 มีหน่วยจัดเก็บข้อมูล HDD แบบ SATA หรือ SAS Interface ที่มีความเร็วรอบไม่น้อยกว่า 7,200 RPM ขนาดความจุไม่น้อยกว่า 4 TB จำนวนไม่น้อยกว่า 4 หน่วย

1.7 ต้องติดตั้งระบบแม่ข่ายคอมพิวเตอร์เสมือน (Hypervisor) ที่เป็น VMware ESXi 7.0 หรือดีกว่า มาพร้อมใช้งาน

1.8 มีระบบจัดเก็บข้อมูลแบบเสมือนสำหรับระบบแม่ข่ายคอมพิวเตอร์เสมือน ที่สามารถนำ HDD หรือ SSD บน Server มาสร้างเป็น Shared Storage สำหรับเครื่องคอมพิวเตอร์เสมือนและใช้ SSD ที่มีอยู่บน Server เป็น Cache เพื่อช่วยเพิ่มความเร็วในการอ่าน/เขียนข้อมูลได้

1.9 รองรับการขยายหน่วยจัดเก็บข้อมูลโดยไม่ต้องหยุดระบบและรองรับการขยายได้อย่างน้อย 64 Nodes Server

1.10 ระบบสามารถทำการอัพเกรดเพื่อเพิ่มประสิทธิภาพและฟังก์ชันการใช้งานโดยไม่ต้องหยุดการทำงานของระบบได้

1.11 มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10/25GbE SFP28 จำนวนไม่น้อยกว่า 4 พอร์ต พร้อมสาย 10GbE SFP+ Direct Attach Cable ระยะสาย 3 เมตร หรือ Transceiver 10GbE ชนิด SR ครบตามจำนวนพอร์ต

1.12 มี Power Supply แบบ Hot Plug หรือ Hot Swap ขนาดไม่น้อยกว่า 1,100 Watt. จำนวน 2 ชุด ต่อ 1 Node แบบ Redundant

1.13 รองรับ Wi-Fi หรือ Bluetooth ในการจัดการเครื่องแม่ข่ายผ่านอุปกรณ์สื่อสารเคลื่อนที่ได้โดยตรงเพื่อความปลอดภัย

1.14 ระบบที่เสนอต้องสามารถทำการสำรองข้อมูลหรือมีซอฟต์แวร์สำหรับสำรองข้อมูลและกู้คืนข้อมูลได้ โดยมีคุณสมบัติอย่างน้อยดังนี้

1.14.1 สามารถทำการกู้คืนข้อมูลแบบ VM โดยเลือก version ของ backup ได้

1.14.2 สามารถทำการ Replicate ข้อมูลระหว่าง Site ได้ และสามารถทำได้แบบ Synchronous และ Asynchronous และสามารถเลือก version ของ backup ที่จะ fail over ได้

1.14.3 เปลี่ยน IP Address ของเครื่องคอมพิวเตอร์แม่ข่ายเสมือนที่ fail over ขึ้นปลายทางได้

1.14.4 รองรับการทำสำรองข้อมูล (Backup) ร่วมกับ Public Cloud ได้

1.14.5 สามารถทำ VM Replicate แบบ Continuous Data Protection (CDP)

1.14.6 ลิขสิทธิ์ถูกต้องและครอบคลุมตามเครื่องคอมพิวเตอร์แม่ข่ายเสมือน ไม่ต่ำกว่า 15 VM

1.15 มี Remote Management Port แบบ 1GbE Ethernet RJ-45 จำนวน 1 พอร์ตต่อ Node เพื่อช่วยในการจัดการ กับ Server จากระยะไกล ผ่าน Web Base Application (Remote) สามารถสั่ง Power ON, Power OFF, Restart เครื่อง Server และตั้งค่าใน BIOS ได้

1.16 มีเครื่องมือบริหารจัดการส่วนกลาง (Centralize Management) ที่สามารถบริหารจัดการเครื่องคอมพิวเตอร์แม่ข่ายและคอมพิวเตอร์แม่ข่ายเสมือน (Virtual Machine) ผ่าน web browser แบบ HTML5 ได้ โดยไม่จำกัดจำนวนเครื่อง

1.17 มี License vSphere Standard subscription 3 ปี ครอบคลุมตาม Hardware ที่เสนอ

1.18 มี License VMware vCenter Standard ลิขสิทธิ์ถูกต้อง

1.19 มีเงื่อนไขการรับประกันเป็นเวลา 3 ปี ในกรณีที่เกิดปัญหาทางด้าน Hardware จะมีการติดต่อกลับภายใน 4 ชั่วโมง (4 Hours Response) โดยเข้ามาทำการแก้ไข / ซ่อมแซม ณ ที่ติดตั้งเครื่อง (On-Site Service) โดยมีศูนย์บริการมาตรฐาน ISO 9001 พร้อม Call Center ที่ให้บริการแบบ 7 วัน x 24 ชั่วโมง ที่มีเบอร์โทรศัพท์รับแจ้งปัญหาทางเทคนิคแบบเบอร์โทรฟรีทั้งโทรศัพท์พื้นฐานและโทรศัพท์เคลื่อนที่

1.20 ผู้เสนอราคาต้องมีหนังสือแต่งตั้งการเป็นตัวแทนจำหน่ายจากบริษัทเจ้าของผลิตภัณฑ์ที่มีสาขาในประเทศไทยโดยตรง และมีเอกสารรับรองว่าอุปกรณ์ที่เสนอเป็นอุปกรณ์ใหม่ ไม่เคยถูกใช้งานมาก่อนและยังอยู่ในสายการผลิต

1.21 มีอุปกรณ์กระจายสัญญาณเครือข่าย 10 Gigabit Switches จำนวน 2 หน่วย มีคุณสมบัติอย่างน้อยดังนี้

1.21.1 เป็นอุปกรณ์สวิตช์ที่สามารถทำงานในระดับ Layer 2 และ Layer 3 ได้

1.21.2 มีขนาดของ Switching Fabric capacity ไม่น้อยกว่า 840Gbps (Full-duplex)

1.21.3 มีความสามารถในการส่งข้อมูลได้ไม่น้อยกว่า 630Mpps

1.21.4 มีพอร์ตแบบ 10G SFP+ ที่สนับสนุนความเร็ว 10G จำนวนไม่น้อยกว่า 12 พอร์ต

1.21.5 มีพอร์ตแบบ 100 Gigabit Ethernet (QSFP28) จำนวนไม่น้อยกว่า 3 พอร์ต พร้อมทั้งเสนอสายสำเร็จรูปแบบ 100GbE QSFP28 Direct Attach Cable จำนวนไม่น้อยกว่า 1 เส้น

1.21.6 มี Transceiver SFP to Base-T จำนวนไม่น้อยกว่า 2 หน่วย

1.21.7 มีพอร์ตสำหรับบริหารจัดการตัวอุปกรณ์แบบ RJ45 console และ management port

1.21.8 สนับสนุนจำนวน MAC Address ได้สูงสุดไม่น้อยกว่า 160,000 Addresses

1.21.9 สนับสนุน Jumbo frames ขนาดไม่น้อยกว่า 9,416 bytes

1.21.10 สามารถรองรับจำนวน Layer 2 VLAN ได้ไม่น้อยกว่า 4,000 VLAN รวมทั้งสนับสนุนมาตรฐาน IEEE 802.1Q VLAN Tagging และ GVRP ได้

1.21.11 สนับสนุนมาตรฐาน DCB ได้แก่ 802.1Qaz Enhanced Transmission Selection (ETS), IEEE 802.1Qbb Priority-based Flow Control (PFC) และ DCBx เป็นอย่างน้อย

1.21.12 สนับสนุนการทำ Link aggregation ตามมาตรฐาน IEEE 802.3ad ได้

1.21.13 สนับสนุนมาตรฐานดังต่อไปนี้ได้ IEEE 802.1D, IEEE 802.1w, IEEE 802.1S, PVST+, IEEE 802.3ae และ IEEE802.3ba ได้

1.21.14 สามารถบริหารจัดการได้ดังต่อไปนี้ Command Line Interface (CLI), telnet และ SSH เป็นต้น

1.21.15 สนับสนุนการ Monitor ของ Traffic แบบ sFlow หรือ NetFlowได้

1.21.16 มีระบบจ่ายไฟแบบ Redundant, hot-swappable Power Supply

1.21.17 ได้รับมาตรฐานจาก FCC, UL, EN, VCCI และ RoHS เป็นอย่างน้อย

1.21.18 เป็นผลิตภัณฑ์ภายใต้เครื่องหมายการค้าเดียวกันกับเครื่องคอมพิวเตอร์แม่ข่ายชนิด Hyper-Converged

1.21.19 มีเงื่อนไขการรับประกันเป็นเวลา 3 ปี ในกรณีที่เกิดปัญหาทางด้าน Hardware จะมีการติดต่อกลับภายใน 4 ชั่วโมง (4 Hours Response) โดยเข้ามาทำการแก้ไข / ซ่อมแซม ณ ที่ติดตั้งเครื่อง (On-Site Service) โดยมีศูนย์บริการมาตรฐาน ISO 9001 พร้อม Call Center ที่ให้บริการแบบ 7 วัน x 24 ชั่วโมง ที่มีเบอร์โทรศัพท์รับแจ้งปัญหาทางเทคนิคแบบเบอร์โทรฟรีทั้งโทรศัพท์พื้นฐานและโทรศัพท์เคลื่อนที่

1.21.20 ผู้เสนอราคาต้องมีหนังสือแต่งตั้งการเป็นตัวแทนจำหน่ายจากบริษัทเจ้าของผลิตภัณฑ์ที่มีสาขาในประเทศไทยโดยตรง และมีเอกสารรับรองว่าอุปกรณ์ที่เสนอเป็นอุปกรณ์ใหม่ ไม่เคยถูกใช้งานมาก่อน และยังอยู่ในสายการผลิต

2. อุปกรณ์กระจายสัญญาณ (L3 Switch) ขนาด 24 ช่อง จำนวน 1 เครื่อง มีคุณลักษณะดังนี้

2.1 มีลักษณะการทำงานไม่น้อยกว่า Layer 3 ของ OSI Model

2.2 สามารถค้นหาเส้นทางเครือข่ายโดยใช้โปรโตคอล (Routing Protocol) RIPv2, OSPFv3 ได้เป็นอย่างน้อย

2.3 มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10/100/1000Base-T จำนวนไม่น้อยกว่า 24 ช่อง

2.4 มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 1/10G SFP จำนวนไม่น้อยกว่า 4 ช่อง

2.5 มีช่องสำหรับเชื่อมต่อ USB Console จำนวน 1 ช่อง

2.6 รองรับ MAC Address ได้ไม่น้อยกว่า 16,000 MAC Address

2.7 มี Switching Capacity ไม่น้อยกว่า 128 Gbps และ Throughput ไม่น้อยกว่า 95.2 Mpps

2.8 สามารถนำอุปกรณ์ 2 ตัวขึ้นไปมาทำ High Availability โดยวิธีการ Virtual Switching Framework (VSF) หรือเทียบเท่า ได้สูงสุด 8 ตัว (Stacking members)

2.9 มีหน่วยความจำภายในขนาดไม่น้อยกว่า 8 GB และมี Flash ขนาดไม่น้อยกว่า 16 GB

2.10 สามารถทำงานได้ตามมาตรฐาน IPv6 และ Dual stack (IPv4 and IPv6) ได้

2.11 สามารถทำการยืนยันตัวตนในรูปแบบ IEEE 802.1X, Web, MAC authentication ได้

2.12 สามารถทำงานร่วมกับ RADIUS และ TACACS+ ได้

2.13 อุปกรณ์จะต้องมี Network Analytics Engine ที่สามารถวิเคราะห์และแจ้งเตือนผู้ใช้งานเวลาเกิดข้อผิดพลาดในระบบได้

2.14 อุปกรณ์จะต้องสามารถเก็บข้อมูล time series database ภายในตัวอุปกรณ์ได้

2.15 สามารถทำงานร่วมกับ REST API และ Python ได้

2.16 สามารถทำงานได้ตามมาตรฐาน sFlow หรือ NetFlow ได้

2.17 สามารถทำ VLAN ตามมาตรฐาน IEEE 802.1Q ได้ไม่น้อยกว่า 4000 VLAN IDs

2.18 สามารถทำ Link Aggregation ตามมาตรฐาน IEEE 802.3ad ได้ไม่น้อยกว่า 32 LAGs

2.19 สามารถทำ Spanning Tree ได้ตามมาตรฐาน IEEE 802.1s, IEEE 802.1d, IEEE 802.1w

2.20 สามารถทำ Protocol Independent Multicast (PIM) แบบ Sparse Mode (SM) และ Dense Mode (DM) ได้เป็นอย่างน้อย

2.21 สามารถบริหารจัดการอุปกรณ์ผ่านทาง Web GUI, SNMPv3 และ SSHv2 ได้เป็นอย่างน้อย

2.22 รองรับการทำ Centralized configuration ผ่านซอฟต์แวร์ได้

2.23 สามารถส่งข้อมูล Log File ในรูปแบบ Syslog ได้เป็นอย่างน้อย

2.24 สามารถทำ Control Plane Policing เพื่อป้องกัน CPU overload ได้

2.25 อุปกรณ์จะต้องได้รับมาตรฐาน EN, FCC, VCCI Class A เป็นอย่างน้อย

2.26 ต้องมีการรับประกันตัวเครื่องแบบ Limited Lifetime Warranty

2.27 ผู้เสนอราคาต้องมีหนังสือแต่งตั้งการเป็นตัวแทนจำหน่ายจากบริษัทเจ้าของผลิตภัณฑ์ที่มีสาขาในประเทศไทยโดยตรง และมีเอกสารรับรองว่าอุปกรณ์ที่เสนอเป็นอุปกรณ์ใหม่ ไม่เคยถูกใช้งานมาก่อน และยังอยู่ในสายการผลิต

3. อุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall) แบบที่ 1 จำนวน 1 เครื่อง มีคุณลักษณะดังนี้

3.1 เป็นอุปกรณ์ Next Generation Firewall แบบ Appliance ที่ใช้ตัวประมวลผลสำหรับงานเฉพาะทาง

3.2 มีช่องต่อ GE RJ45 ไม่น้อยกว่า 16 ช่อง มีช่องต่อ GE SFP ไม่น้อยกว่า 8 ช่อง และช่องต่อ 10G SFP+ ไม่น้อยกว่า 4 ช่อง

3.3 มีประสิทธิภาพการทำงาน (throughput) ของ Firewall ไม่น้อยกว่า 27 Gbps และได้รับการรับรองมาตรฐานด้าน Firewall จากหน่วยงาน ICSA Labs

3.4 รองรับการเชื่อมต่อพร้อมกัน (Concurrent Sessions) ได้ไม่น้อยกว่า 3,000,000 การเชื่อมต่อ และรองรับการเชื่อมต่อใหม่ (New Sessions) ไม่น้อยกว่า 280,000 การเชื่อมต่อต่อวินาที

3.5 มีประสิทธิภาพการทำงาน (throughput) ของ IPS ไม่น้อยกว่า 5 Gbps และได้รับการรับรองมาตรฐานด้าน IPS จากหน่วยงาน ICSA Labs

3.6 มีประสิทธิภาพการทำงาน (throughput) ของการป้องกันการบุกรุก (Threat Protection) ไม่น้อยกว่า 3 Gbps

3.7 มีประสิทธิภาพการทำงาน (throughput) ของ IPSec VPN ได้ไม่น้อยกว่า 13 Gbps รองรับ IPSec VPN Tunnel แบบ Gateway-to-Gateway พร้อมกันได้ไม่น้อยกว่า 2,000 Tunnels และได้รับการรับรองมาตรฐานด้าน IPSec จากหน่วยงาน ICSA Labs

3.8 มีความสามารถทำ SSL VPN มีประสิทธิภาพการทำงาน (throughput) ของ SSL VPN ไม่น้อยกว่า 2 Gbps รองรับการเชื่อมต่อพร้อมกันได้ไม่น้อยกว่า 500 users และได้รับการรับรองมาตรฐานด้าน SSL VPN จากหน่วยงาน ICSA Labs

3.9 ได้รับการรับรองมาตรฐานด้าน Antivirus จากหน่วยงาน ICSA Labs

3.10 สามารถทำงานในลักษณะของไฟล์วอลล์เสมือน (Logical System, Virtual System, Virtual Domain หรือ Security Context) ได้ไม่น้อยกว่า 10 ระบบ

3.11 มีความสามารถเป็น Wireless Controller รองรับการเชื่อมต่ออุปกรณ์ Access Point ที่อยู่ภายใต้เครื่องหมายการค้าเดียวได้ไม่น้อยกว่า 128 ตัว

3.12 มีความสามารถในการทำ Software-Defined WAN (SD-WAN) โดยตรวจสอบ WAN SLA ตาม latency, jitter และ packet loss ได้

3.13 มีความสามารถในการตรวจสอบ Application ได้ไม่น้อยกว่า 1,000 รายการ

3.14 ป้องกันการเข้าถึง Web ตาม Categories และตาม URL ที่กำหนดได้

3.15 รองรับการทำงานแบบ High Availability (HA) แบบ Active/Active และ Active/Passive ได้

3.16 สามารถใช้งานกับไฟฟ้ากระแสสลับ (AC) ขนาด 220 Volts 50/60 Hz

3.17 อุปกรณ์ได้รับรองมาตรฐาน FCC Part 15B Class A, VCCI, CE, CB และ UL/cUL

3.18 มี Redundant power supply

3.19 มีการรับประกันสินค้าระยะเวลาไม่น้อยกว่า 1 ปี จากเจ้าของผลิตภัณฑ์

3.20 ผู้เสนอราคาต้องมีหนังสือแต่งตั้งการเป็นตัวแทนจำหน่ายจากบริษัทเจ้าของผลิตภัณฑ์ที่มีสาขาในประเทศไทยโดยตรง และมีเอกสารรับรองว่าอุปกรณ์ที่เสนอเป็นอุปกรณ์ใหม่ ไม่เคยถูกใช้งานมาก่อน และยังอยู่ในสายการผลิต

4. อุปกรณ์ป้องกันและตรวจจับการบุกรุก (Intrusion Prevention System) แบบที่ 1 จำนวน 1 เครื่อง มีคุณลักษณะดังนี้

4.1 เป็นอุปกรณ์ Intrusion Prevention System (IPS) หรือ Threat Protection System (TPS) โดยเฉพาะแบบ Appliance ที่ออกแบบมาเพื่อทำหน้าที่ป้องกันการบุกรุกและการโจมตี และต้องไม่เป็นอุปกรณ์ลักษณะ UTM (Unified Threat Management)

4.2 สามารถประมวลผล โดยมีค่า Latency น้อยกว่า 60 microseconds

4.3 มี IPS Inspection Throughput ไม่น้อยกว่า 1 Gbps

4.4 อุปกรณ์ที่นำเสนอสามารถทำ SSL Inspection โดยมี Throughput ได้ไม่น้อยกว่า 1 Gbps

4.5 มี SSL Connections per second ไม่น้อยกว่า 3,500 Connections per second หากอุปกรณ์ที่นำเสนอไม่สามารถทำงานในลักษณะดังกล่าวได้สามารถเสนออุปกรณ์ SSL Inspection หรือ SSL Orchestration เพิ่มเติมได้

4.6 อุปกรณ์ที่นำเสนอสามารถรับปริมาณ Concurrent Session ได้ไม่น้อยกว่า 30,000,000 Concurrent Sessions และสามารถรับปริมาณ Connection ได้ไม่น้อยกว่า 400,000 Connections per Second

4.7 มี Network Interface แบบ 4 Segments Gig-T Bypass จำนวนไม่น้อยกว่า 8 ports พร้อมคุณสมบัติ Bypass ได้บนตัวอุปกรณ์

4.8 มี Interface สำหรับบริหารจัดการอุปกรณ์ (Out of band management) แบบ 10/100/1000 RJ-45 อย่างน้อย 1 พอร์ต

4.9 ต้องมี Power supply แบบ Dual redundant hot-swappable

4.10 รองรับการทำ High Availability แบบ Active-Active และ Active-Passive ได้

4.11 สามารถรองรับการตรวจจับการบุกรุก Tunnel Traffic ได้ ดังต่อไปนี้

4.11.1 Generic Routing Encapsulation (GRE)

4.11.2 GPRS Tunneling Protocol (GTP)

4.11.3 Mobile IPv4 (IP-in-IP)

4.11.4 IPv6 (6-in-4, 4-in-6, และ 6-in-6)

4.12 สามารถตรวจจับวิธีการบุกรุกและป้องกันเครือข่ายได้ดังต่อไปนี้เป็นอย่างน้อย Exploits, Identity Theft, Spyware, Virus, Vulnerabilities, Network Equipment (Malicious attacks through printers, modems, routers and integrated phone systems), Traffic Normalization (improper or malformed traffic), Instant Messaging, Peer-to-Peer (P2P), Streaming Media และ DDoS ได้เป็นอย่างน้อย

4.13 สามารถทำการตรวจสอบ Geolocation ของ IP Address ที่ทำการบุกรุกหรือโจมตีระบบเครือข่ายผ่านอุปกรณ์ IPS ได้

4.14 สามารถตรวจจับ DNS request โดยใช้เทคนิค Domain Generation Algorithms (DGAs) ได้

4.15 สามารถ Update reputation feed เพื่อป้องกันการติดต่อสื่อสารจาก IP address ทั้ง IPv4, IPv6 และ Domain names ของ malicious ได้ เพื่อเพิ่มความปลอดภัยให้ระบบเครือข่าย

4.16 รองรับการแสดงข้อมูลเกี่ยวกับ Signature หรือ Filter เพื่อประโยชน์ในการจัดการเหตุการณ์ที่เกิดขึ้นของผู้ใช้งานได้ เช่น Geo Map, Source IP, Source/Destination Port เป็นต้น

4.17 เจ้าของผลิตภัณฑ์จะต้องมีหน่วยงานเฉพาะที่ทำหน้าที่ในการติดตามความเคลื่อนไหวของการบุกรุกเพื่อจะได้ปรับปรุงฐานข้อมูลการบุกรุกระบบเครือข่ายได้

4.18 รองรับการทำงานร่วมกับ Vulnerability Assessment อย่างน้อยดังนี้ Qualys, Rapid7 หรือ Tenable เพื่อช่วยปรับแต่งระบบความปลอดภัยให้เหมาะสมกับองค์กร

4.19 รองรับการทำงานร่วมกับระบบศึกษาและวิเคราะห์การทำงานของ unknown malware และ advanced malware ด้วยระบบ sandboxing ที่เป็น on-premise appliance ได้

4.20 ได้รับการรับรองมาตรฐาน CSA, UL, IEC, EN, VCCI, CISPR และ RoHS ได้เป็นอย่างน้อย

4.21 มีเงื่อนไขการรับประกันเป็นเวลาอย่างน้อย 1 ปี

4.22 ผู้เสนอราคาต้องมีหนังสือแต่งตั้งการเป็นตัวแทนจำหน่ายจากบริษัทเจ้าของผลิตภัณฑ์ที่มีสาขาในประเทศไทยโดยตรง และมีเอกสารรับรองว่าอุปกรณ์ที่เสนอเป็นอุปกรณ์ใหม่ ไม่เคยถูกใช้งานมาก่อน และยังอยู่ในสายการผลิต

5. อุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall) จำนวน 1 ชุด มีคุณลักษณะดังนี้

5.1 เป็นอุปกรณ์ Web Application Firewall (WAF) ที่สามารถป้องกัน Web Application จากภัยคุกคามได้

5.2 มีช่องการเชื่อมต่อระบบเครือข่าย (Network Interfaces) อย่างน้อย ดังนี้

5.2.1 แบบ 1G (RJ45) จำนวนไม่น้อยกว่า 4 พอร์ต

5.2.2 แบบ 1G (SFP) จำนวนไม่น้อยกว่า 4 พอร์ต

5.3 มีหน่วยเก็บข้อมูล Storage ไม่น้อยกว่าขนาด 480 GB

5.4 สามารถรองรับ throughput ได้ไม่น้อยกว่า 250 Mbps

5.5 สามารถป้องกันการโจมตีผ่านทางเว็บไซต์ ได้ตาม OWASP Top 10 รวมถึง Cross Site Scripting, SQL Injection, Cross Site Request Forgery, Session Hijacking, Web Service Signature, XML and JSON protocol conformance, Protocol validation, Brute force protection, Cookie signing and encryption, Data Leak Prevention, OpenAPI 3.0 verification, Virtual Patching, CAPTCHA และ Real Browser Enforcement (RBE)

5.6 มีความสามารถในการเฝ้าระวังการเปลี่ยนแปลงเว็บไซต์ (Anti-defacement)

5.7 มีความสามารถในการทำ File อัปโหลด Scanning ด้วย Antivirus (AV) ได้

5.8 มีความสามารถในการตรวจสอบ IP Reputation เพื่อป้องกัน Botnets, Malicious Hosts และ Anonymous Proxies ได้

5.9 สามารถทำงานแบบ Dual-Layer Machine learning เพื่อตรวจจับการร้องขอไม่ปกติ (Anomaly) และป้องกันการใช้งานที่เป็นอันตราย (Threats) ได้

5.10 สามารถทำ High Availability ได้ทั้งแบบ Active/Passive และ Active/Active Clustering ได้

5.11 รองรับการใช้งานได้ทั้งแบบ Reverse proxy, Inline Transparent, Span (sniffing) หรือ WCCP ได้เป็นอย่างน้อย

5.12 สามารถตรวจสอบช่องโหว่ของเว็บแอปพลิเคชัน (Vulnerability Scan) จากตัวอุปกรณ์ได้ และรองรับการทำงานร่วมกับ 3rd Party vulnerability scanner เช่น Acunetix, HP WebInspect, IBM AppScan, Qualys ได้เป็นอย่างน้อย

5.13 สามารถทำ SSL Offloading หรือ SSL Inspection เพื่อลดภาระงาน web server ได้

5.14 รองรับการตรวจสอบข้อมูล API ในรูปแบบ XML, JSON และ RESTful ได้เป็นอย่างน้อย

5.15 อุปกรณ์ที่เสนอต้องผ่านการรับรองมาตรฐานด้านความปลอดภัยจาก FCC, VCCI, CE และ UL เป็นอย่างน้อย

5.16 มีเงื่อนไขการรับประกันเป็นเวลาอย่างน้อย 1 ปี

5.17 ผู้เสนอราคาต้องมีหนังสือแต่งตั้งการเป็นตัวแทนจำหน่ายจากบริษัทเจ้าของผลิตภัณฑ์ที่มีสาขาในประเทศไทยโดยตรง และมีเอกสารรับรองว่าอุปกรณ์ที่เสนอเป็นอุปกรณ์ใหม่ ไม่เคยถูกใช้งานมาก่อน และยังอยู่ในสายการผลิต

6. ชุดโปรแกรมระบบปฏิบัติการ Windows Server จำนวน 1 ชุด มีคุณลักษณะดังนี้

6.1 จัดหาลิขสิทธิ์ซอฟต์แวร์ Microsoft Server Standard เวอร์ชั่นใหม่กว่า ที่ถูกต้องตามกฎหมาย สำหรับเครื่องคอมพิวเตอร์แม่ข่าย

6.2 รองรับหน่วยประมวลผลกลาง (CPU) ไม่น้อยกว่า 60 แกนหลัก (Core) และรองรับการสร้างเครื่องคอมพิวเตอร์เสมือนได้จำนวนอย่างน้อย 6 เครื่อง

7. เครื่องคอมพิวเตอร์โน้ตบุ๊คแบบประมวลผลขั้นสูง จำนวน 10 เครื่อง มีคุณลักษณะดังนี้

7.1 มีหน่วยประมวลผลกลาง (CPU) ไม่น้อยกว่า 4 แกนหลัก (4 cores) ความเร็วไม่ต่ำกว่า 2.4 GHz และมีเทคโนโลยี Turbo boost ไม่น้อยกว่า 4.2 GHz และ Cache ไม่ต่ำกว่า 6 MB

7.2 มีหน่วยจัดเก็บข้อมูลชนิด NVMe Solid State Drive หรือดีกว่า ขนาดความจุไม่น้อยกว่า 1TB

7.3 มีจอภาพที่รองรับความละเอียดไม่น้อยกว่า 1920 x 1080 จุด หรือดีกว่า

7.4 มีหน่วยความจำแบบ DDR4 ขนาดไม่น้อยกว่า 32 GB

7.5 จอภาพเป็นแบบ OLED หรือ IPS มีขนาดไม่น้อยกว่า 14 นิ้ว

7.6 มีหน่วยประมวลผลกราฟิกเทียบเท่า Intel HD Graphics หรือ UHD หรือ Intel Iris Xe

7.7 มีกล้อง Webcam ในตัว

7.8 มีช่องเชื่อมต่อ (Interface) แบบ USB หรือดีกว่า ไม่น้อยกว่า 2 ช่อง

7.9 มีช่องเชื่อมต่อแบบ HDMI จำนวนไม่น้อยกว่า 1 ช่อง

7.10 มีช่องเชื่อมต่อแบบ USB Type-C หรือ Display Port จำนวนไม่น้อยกว่า 1 ช่อง

7.11 มีช่องเชื่อมต่อระบบเครือข่าย (LAN) แบบ 10/100/1000Base-T หรือดีกว่า จำนวนไม่น้อยกว่า 1 ช่อง กรณีไม่มีช่องเชื่อมต่อ LAN โดยเฉพาะต้องมีอุปกรณ์แปลงสัญญาณ LAN ผ่าน USB

7.12 รองรับการเชื่อมต่อเครือข่ายไร้สาย (Wi-Fi) ไม่น้อยกว่า 802.11b/g/n/ax และ Bluetooth
7.13 มีน้ำหนักไม่เกิน 2 กิโลกรัม
7.14 สนับสนุนมาตรฐาน Trusted Platform Module 2.0 (TPM 2.0) หรือดีกว่า
7.15 ได้รับรองมาตรฐาน Energy Star และ EPEAT ไม่ต่ำกว่า Silver
7.16 มีเมาส์และแป้นพิมพ์แยกแบบไร้สายซึ่งรองรับการเชื่อมต่อแบบ Bluetooth
7.17 มีอุปกรณ์สนับสนุนการเชื่อมต่อพ่วงภายนอกแบบ Docking ผ่าน USB 3.0 Type-C ให้สามารถใช้งานพอร์ตชนิด RJ-45, USB 3.0 , HDMI, และ PD 3.0 และสามารถแสดงผลบนจอภาพที่ต่อพ่วงได้
7.18 มีระบบปฏิบัติการ Windows 10 Pro หรือ Windows 11 Pro แบบมีลิขสิทธิ์ถูกต้องตามกฎหมาย
7.19 มีเงื่อนไขการรับประกันอย่างน้อย 3 ปี ในกรณีที่เกิดปัญหาทางด้าน Hardware โดยเข้ามาทำการแก้ไข / ซ่อมแซม ณ ที่ตั้ง หรือ นอกสถานที่ตั้ง (On-Site Service) ภายในวันทำการถัดไป (Next Business Day Response)
7.20 มีกระเป๋าจัดเก็บเครื่องคอมพิวเตอร์โน้ตบุ๊คผลิตภัณฑ์เดียวกันกับตัวเครื่อง 1 ใบ

8. จอคอมพิวเตอร์ จำนวน 10 จอ มีคุณลักษณะดังนี้

8.1 มีขนาดหน้าจอตามแนวเส้นทแยงมุม 26.2 นิ้วหรือใหญ่กว่า
8.2 ความละเอียดของหน้าจอ (Resolution) สามารถปรับได้ละเอียดสูงสุด 3840 x 2160 จุด หรือละเอียดกว่า ทำงานที่ความถี่ 60 Hz หรือมากกว่า
8.3 หน้าจอผลิตโดยเทคโนโลยี In-Plane Switching หรือดีกว่า
8.4 หน้าจอเคลือบสารลดการสะท้อนแสง
8.5 ใช้เทคโนโลยีการเปล่งแสงจอภาพแบบ LED หรือดีกว่า
8.6 มีอัตราส่วนจอภาพขนาด 16:9 หรือ 16:10
8.7 รองรับมุมมองตามตั้ง/แนวราบ 178 °/ 178 ° หรือดีกว่า
8.8 อัตราส่วนคอนทราส (Dynamic Contrast Ratio) 1000 :1 (Typical) หรือสูงกว่า
8.9 ค่าความสว่าง (Brightness) 320 cd/m2 หรือสูงกว่า
8.10 รองรับการติดตั้งแบบ VESA
8.11 รองรับการปรับหมุนจอภาพแบบ Pivot (หมุนตามเข็มหรือหมุนทวนเข็มนาฬิกา)
8.12 มีช่องทางการสื่อสารกับอุปกรณ์ภายนอก ดังนี้
8.13 มี HDMI อย่างน้อย 1 ช่อง
8.14 มี DisplayPort อย่างน้อย 1 ช่อง
8.15 มี USB Type-C with DisplayPort หรือ Thunderbolt หรือเทียบเท่า หรือดีกว่า อย่างน้อย 1 ช่อง
8.16 รับประกันจอภาพอย่างน้อย 3 ปี
8.17 มีสายเคเบิ้ลพร้อมใช้งาน เช่น สายเคเบิ้ล HDMI หรือสายเคเบิ้ล DisplayPort หรือสาย USB Type-C
8.18 มีลำโพงแบบ Soundbar ที่มีระบบเสียง Stereo ติดตั้งมากับจอ หรือยึดติดกับขาจอได้ จำนวน 1 ชุด

9. ชุดโปรแกรมสำนักงาน จำนวน 10 ชุด มีคุณลักษณะดังนี้

9.1 จัดหาลิขสิทธิ์ซอฟต์แวร์ Microsoft Office Home & Business 2021 หรือเวอร์ชั่นใหม่กว่า ที่ถูกต้องตามกฎหมาย จำนวน 10 ชุด
9.2 สามารถติดตั้งบนระบบปฏิบัติการ Microsoft Windows ทั้งแบบ 32 Bit และ 64 Bit ได้

10. อุปกรณ์กระจายการทำงานบนเครือข่าย (Load Balance Router)

10.1 เป็นอุปกรณ์ (Hardware Application) ที่ออกแบบมาเพื่อใช้กระจายการทำงานสำหรับเครือข่ายโดยเฉพาะ

10.2 มี Router Throughput ไม่น้อยกว่า 12 Gbps และ VPN Throughput ไม่น้อยกว่า 1 Gbps

10.3 มีช่องเชื่อมต่อระบบเครือข่าย (WAN Interface) แบบ 10G SFP+ จำนวน 2 ช่อง

10.4 มีช่องเชื่อมต่อระบบเครือข่าย (WAN Interface) แบบ 1000Base-T จำนวน 2 ช่อง

10.5 มีช่องเชื่อมต่อระบบเครือข่าย (LAN Interface) แบบ 1000Base-T PoE+ จำนวน 8 ช่อง

10.6 มีช่องเชื่อมต่อ USB 3.0 Port จำนวน 2 ช่อง

10.7 รองรับจำนวนผู้ใช้งานได้ไม่น้อยกว่า 2,000 users

10.8 รองรับการเชื่อมต่อ VPN ได้ไม่น้อยกว่า 300 Peers

10.9 สามารถบริหารจัดการอุปกรณ์ผ่าน Local Web GUI มาตรฐาน HTTPS ได้เป็นอย่างน้อย

10.10 สามารถบริหารจัดการอุปกรณ์ผ่าน Cloud Management ได้

10.11 สามารถทำ High Availability ในรูปแบบ VRRP ได้

10.12 สามารถทำงานเป็น Controller ได้ โดยรองรับ Access Point ได้ไม่น้อยกว่า 250 ตัว

10.13 สามารถใช้งานตามมาตรฐาน IPv6 ได้

10.14 สามารถทำงานแบบ IPsec VPN เพื่อเชื่อมต่อระหว่าง Site ได้

10.15 สามารถเข้ารหัสข้อมูลแบบ 256-bit AES Encryption ได้

10.16 สามารถค้นหาเส้นทางเครือข่ายโดยใช้โปรโตคอล (Routing Protocol) RIPv2, OSPF, BGP ได้เป็นอย่างน้อย

10.17 สามารถทำการยืนยันตัวตน (Authentication) ร่วมกับ RADIUS และ LDAP ได้

10.18 สามารถกำหนด Outbound Policy ได้แก่ Weighted Balance, Persistence, Enforced, Priority, Overflow, Least Used, Lowest Latency เป็นอย่างน้อย

10.19 สามารถทำ Bandwidth Aggregation และ Hot Failover ได้

10.20 สามารถทำ WAN Smoothing เพื่อช่วยลดปัญหาที่เกิดจาก packet loss ได้

10.21 สามารถทำงานในรูปแบบ DHCP, Static IP, PPPoE, NAT ได้เป็นอย่างน้อย

10.22 สามารถติดตั้งในรูปแบบ Drop-in Mode หรือ LAN Bypass ได้

10.23 สามารถทำ Stateful Firewall, DoS Prevention และ Web Blocking ได้

10.24 สามารถส่งข้อมูล Log File แบบ Syslog ได้เป็นอย่างน้อย

10.25 สามารถทำ QoS เพื่อกำหนด Priority ให้แก่การใช้งานที่สำคัญได้ เช่น VoIP

10.26 สามารถทำ Bandwidth Control สำหรับผู้ใช้งานในแต่ละกลุ่มได้ (Per-User Bandwidth Control)

10.27 สามารถแสดง Event Log, WAN Quality ผ่านทาง Web GUI ได้

10.28 อุปกรณ์จะต้องผ่านการรับรองตามมาตรฐาน FCC และ CE เป็นอย่างน้อย

10.29 มีการรับประกันไม่น้อยกว่า 1 ปีจากบริษัทเจ้าของผลิตภัณฑ์

10.30 ผู้เสนอราคาต้องมีหนังสือแต่งตั้งการเป็นตัวแทนจำหน่ายจากบริษัทเจ้าของผลิตภัณฑ์ที่มีสาขาในประเทศไทยโดยตรง และมีเอกสารรับรองว่าอุปกรณ์ที่เสนอเป็นอุปกรณ์ใหม่ ไม่เคยถูกใช้งานมาก่อน และยังอยู่ในสายการผลิต

ภาคผนวก 2
พัฒนาระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์

---

1. ขอบเขตงาน

1.1 ผู้ขายต้องมีรายละเอียดของบุคลากรทั้งหมดซึ่งเป็นทีมปฏิบัติงานของผู้ขาย พร้อมประวัติการทำงาน และคุณวุฒิการศึกษาโดยบุคลากรในแต่ละสาขา แต่ละคนจะต้องส่งประวัติการศึกษา ประวัติการทำงาน ประวัติประสบการณ์ตามความเชี่ยวชาญ พร้อมรูปถ่ายขนาด 1 นิ้ว จำนวน 1 รูป และแนบแผนผังแสดงหน้าที่และความรับผิดชอบของบุคลากรที่ทำงานตามโครงการฯ ในครั้งนี้ หากมีบุคลากรที่ไม่ได้เป็นเจ้าหน้าที่ประจำของผู้เสนอราคาต้องมีหนังสือยืนยันการร่วมดำเนินการด้วย ซึ่งทีมปฏิบัติงานของผู้ขายอย่างน้อยต้องประกอบด้วย

1.1.1 ผู้จัดการโครงการ (Project Manager) จำนวน 1 คน วุฒิการศึกษาระดับปริญญาโท ประสบการณ์ 5 - 10 ปี

1.1.2 นักวิเคราะห์ระบบ (System Analyst) จำนวน 1 คน วุฒิการศึกษาระดับปริญญาตรี ประสบการณ์ 5 - 10 ปี

1.1.3 นักพัฒนาฐานข้อมูล (Database Developer) จำนวน 1 คน วุฒิการศึกษาระดับปริญญาตรี ประสบการณ์ 5 - 10 ปี

1.1.4 นักออกแบบเว็ปไซต์ (Web Designer) จำนวน 1 คน วุฒิการศึกษาระดับปริญญาตรี ประสบการณ์ 5 - 10 ปี

1.1.5 นักพัฒนาระบบ (Programmer) จำนวน 2 คน วุฒิการศึกษาระดับปริญญาตรี ประสบการณ์ 5 - 10 ปี

1.1.6 นักทดสอบระบบ (Tester) จำนวน 1 คน วุฒิการศึกษาระดับปริญญาตรี ประสบการณ์ 5 - 10 ปี

1.1.7 เลขานุการโครงการ จำนวน 1 คน

1.2 ผู้ขายต้องวิเคราะห์ความต้องการของผู้ใช้งาน (Requirement Analysis) ทั้งความต้องการเชิงฟังก์ชัน (Functional requirements) ความต้องการไม่เป็นเชิงฟังก์ชัน (Non-functional requirements) ความต้องการของผู้ใช้ (User requirements) ความต้องการของระบบ (System requirements) และข้อกำหนดความต้องการ (Requirement specification) คัดเลือกส่วนที่เป็นสาระสำคัญเพื่อให้อยู่ในขอบเขตของการพัฒนา

1.3 ผู้ขายต้องเป็นผู้ออกแบบและจัดทำภาพที่ใช้ประกอบในระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์ ทั้งที่เป็นภาพนิ่งและภาพเคลื่อนไหว

1.4 ผู้ขายต้องจัดทำระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์ให้มีคุณสมบัติในการปรับขนาดตัวอักษรในหน้าเว็บ ให้สามารถปรับขนาดตัวหนังสือใหญ่-เล็กได้อย่างน้อย 3 ระดับ โดยเมื่อปรับขนาดตัวหนังสือแล้วจะไม่กระทบกับโครงสร้าง (Layout) ที่ได้ออกแบบไว้

1.5 ผู้ขายต้องศึกษาและวิเคราะห์โครงร่างข้อมูล และเนื้อหา (Content) ที่น่าสนใจนำเสนอแก่สำนักข่าวกรองแห่งชาติเพื่อใช้พิจารณาเผยแพร่บนระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์

1.6 ผู้ขายต้องออกแบบและพัฒนาระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์ให้มีความสามารถในการจัดทำเป็นเว็บท่า (Web Portal) มีความสวยงาม ทันสมัย น่าสนใจ ใช้งานง่าย แสดงถึงภาพลักษณ์ที่ดี สามารถค้นหาข้อมูลและแก้ไขข้อมูลผ่านเครื่องมือบริหารจัดการข้อมูลได้ และเป็นไปตามข้อกำหนดรายละเอียดคุณลักษะเฉพาะทางเทคนิคงานพัฒนาระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์ในข้อ 2

1.7 ผู้ขายต้องนำหลักการบูรณาการของกลศาสตร์เกมหรือเกมิฟิเคชัน (Gamification) เข้าไปในการออกแบบและพัฒนาระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์ โดยอาจพิจารณาพัฒนาระบบกำหนดคะแนน (Point) รางวัล (Award) การแสดงผู้มีคะแนนนำ (Leader board) หรืออื่น ๆ เพื่อกระตุ้นหรือส่งเสริมให้ผู้ใช้งานเกิดความสนใจในเนื้อหาหรือข้อมูลที่อยู่บนระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์ และเกิดการมีส่วนร่วมในการแบ่งปันหรือแลกเปลี่ยนข่าวสารความมั่นคงปลอดภัยไซเบอร์ หรือปฏิสัมพันธ์กับผู้ใช้งานอื่นผ่านระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์

1.8 ผู้ขายต้องออกแบบพัฒนาและติดตั้งระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายของที่สำนักข่าวกรองแห่งชาติกำหนด

1.9 ผู้ขายต้องพัฒนาระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์ตามหลัก SEO (Search Engine Optimization) เพื่อเพิ่มประสิทธิภาพในการถูกค้นหาด้วย Google Search Engine และอธิบายวิธีการเพิ่มประสิทธิภาพในการถูกค้นหาดังกล่าว ลงในรายงานผลการออกแบบและพัฒนาระบบระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์

1.10 ผู้ขายต้องพัฒนาระบบให้รองรับการทำงานร่วมกับเครือข่ายสังคมออนไลน์ (Social Network) ของผู้ใช้บริการที่มี Youtube, Facebook, Twitter หรือ อื่นๆ (ถ้ามี) สามารถแสดงความคิดเห็น (Comment), กดไลค์ (Like) หรือ ถูกใจ แบ่งปัน (Share) หรือ เผยแพร่ ข่าวและบทความภายในระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์กับเครือข่ายสังคมออนไลน์ของผู้ใช้บริการเองได้

1.11 ผู้ขายต้องออกแบบและพัฒนาโครงร่างระบบ (Template)

1.12 ผู้ขายจัดทำต้นแบบ (Prototype) ของระบบในโครงการ พร้อมนำเสนอต่อสำนักข่าวกรองแห่งชาติ ให้ความเห็นชอบก่อนการพัฒนาต่อไป

1.13 ผู้ขายต้องจดทะเบียนโดเมนเนมสำหรับระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์อย่างน้อย 5 ปี จำนวน 2 โดเมน ตามที่สำนักข่าวกรองแห่งชาติกำหนด

1.14 ผู้ขายต้องพัฒนาระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์ให้มีความมั่นคงปลอดภัยอย่างน้อยดังนี้

1.14.1 มีมาตรการรักษาความปลอดภัยตามมาตรฐาน Secure Socket Layer (SSL) ที่ทันสมัย

1.14.2 ป้องกันการโจมตีทางไซเบอร์ตามแนวทาง OWASP Top 10 2021 เป็นอย่างน้อย

1.14.3 มีการใช้เทคนิคตรวจสอบผู้ใช้งานผ่านเว็บ (CAPTCHA)

1.15 ผู้ขายต้องพัฒนาระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์ให้สามารถจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์และกิจกรรมความเคลื่อนไหวในระบบของแต่ละบัญชีผู้ใช้งาน (Account) ซึ่งเข้าถึงข้อมูลได้เฉพาะผู้ที่ถูกกำหนดสิทธิไว้เท่านั้น

1.16 ผู้ขายต้องทำการทดสอบระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์อย่างน้อย ดังนี้

1.16.1 การทดสอบการใช้งานของผู้ใช้งาน (Usability Testing) ประสิทธิภาพ (Performance Testing) ความถูกต้องสมบูรณ์โดยรวม (Functional Testing) การรักษาความปลอดภัย (Security Testing) และนำผลที่ได้จากการทดสอบปรับปรุงแก้ไขระบบงาน เพื่อตรวจสอบการทำงานของระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์ว่าสามารถรองรับกระบวนการทำงานตามที่ต้องการได้

1.16.2 การทดสอบความมั่นคงปลอดภัยระบบ (Penetration Testing) โดยจะต้องทดสอบความเสี่ยงตามแนวทาง OWASP Top 10 2021 เป็นอย่างน้อย

1.16.3 การทดสอบการทำงานของระบบทั้งหมด (System Integration Testing)

1.17 ผู้ขายต้องจัดทำคู่มือการใช้งานระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์ อย่างน้อย ดังนี้

1.17.1 คู่มือการใช้งานสำหรับผู้ใช้งานที่เป็นเจ้าหน้าที่ของสำนักข่าวกรองแห่งชาติ ตามสิทธิ์ที่กำหนด

1.17.2 คู่มือสำหรับผู้ดูแลระบบงานระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์

2. ข้อกำหนดรายละเอียดคุณลักษะเฉพาะทางเทคนิคงานพัฒนาระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์

2.1 ข้อกำหนดทั่วไป

2.1.1 ออกแบบ และพัฒนาระบบให้สามารถใช้งานได้ในรูปแบบผ่านเว็บ Web-based Application

2.1.2 ระบบสามารถแสดงผลแบบปรับขนาดตามขนาดหน้าจอ (Web Responsive) บนสมาร์ทโฟน (Smart Phone) และแท็บเล็ต (Tablet) ได้อย่างมีประสิทธิภาพ

2.1.3 ระบบสามารถแสดงผลผ่านโปรแกรมเว็บบราวเซอร์ (Web Browser) บนเครื่องคอมพิวเตอร์อย่างน้อยประกอบด้วย เว็บบราวเซอร์ Google Chrome, Safari, FireFox, Opera และ Microsoft Edge เวอร์ชั่นปัจจุบัน ได้อย่างถูกต้อง

2.1.4 ระบบอยู่ภายใต้หน้าจอ (Interface) เดียวกันกับทุกระบบที่พัฒนาขึ้นในโครงการ ซึ่งผู้ใช้งานเข้าสู่ระบบ (Log in) เพียงครั้งเดียว

2.1.5 สามารถเข้าสู่ระบบล็อกอิน (Login) เข้าใช้ระบบได้ด้วยการยืนยันตัวตนแบบ 2 ชั้น (Two-Factor Authentication) โดยใช้รหัสลับเฉพาะส่วนบุคคล (Pin Code) และแอปพลิเคชันยืนยันตัวตน เช่น Google Authenticator, Microsoft Authenticator เป็นต้นได้

2.2 ระบบจัดการข้อมูลสมาชิก

2.2.1 การสมัครสมาชิก

2.2.1.1 สามารถสมัครสมาชิกผ่านแบบฟอร์มการสมัครสมาชิกทางหน้าระบบได้

2.2.1.2 สามารถแก้ไขข้อมูลส่วนตัว เปลี่ยนแปลงรหัสผ่านได้

2.2.1.3 สามารถแจ้งให้ระบบสร้างรหัสผ่านใหม่ และส่งรหัสผ่านใหม่นั้นไปยังอีเมลของสมาชิกได้

2.2.2 การจัดการข้อมูลการติดตามกิจกรรมและการสมัครรับรายงานข่าวสารความมั่นคงปลอดภัยไซเบอร์

2.2.2.1 สามารถยกเลิกการติดตามกิจกรรมและรายงานข่าวสารความมั่นคงปลอดภัยไซเบอร์

2.2.2.2 สามารถค้นหาการติดตามกิจกรรมและรายงานข่าวสารความมั่นคงปลอดภัยไซเบอร์และสามารถแสดงรายละเอียดการใช้งานของสมาชิก ได้อย่างน้อย ดังนี้ ชื่อกิจกรรม กิจกรรมสมัครเข้าร่วมกิจกรรม และรายงานข่าวสารความมั่นคงปลอดภัยไซเบอร์ที่ติดตาม รวมถึงสถานะต่าง ๆ วันและเวลา

2.2.2.3 สามารถแสดงรายงานรายละเอียดการติดตามกิจกรรม รายงานข่าวสารความมั่นคงปลอดภัยไซเบอร์สมาชิก โดยพิมพ์เป็นรูปแบบแฟ้มข้อมูลตามที่สำนักข่าวกรองแห่งชาติกำหนด

2.2.3 การจัดการข้อมูลสมาชิก

2.2.3.1 สามารถเพิ่มข้อมูลสมาชิกใหม่ แก้ไข ลบข้อมูลสมาชิกและกู้คืนสมาชิกกลับมาได้

2.2.3.2 สามารถกำหนดสิทธิการเข้าใช้ระบบและจัดการข้อมูลได้ตามระดับและกลุ่มของสมาชิก

2.2.3.3 สามารถเลือกการอนุมัติสถานะการเป็นสมาชิก หรือปรับปรุงระดับการใช้งานของสมาชิกได้

2.2.3.4 สามารถกำหนดได้ว่าข้อมูลส่วนใดที่สมาชิกสามารถแก้ไขได้และส่วนใดแก้ไขไม่ได้

2.2.3.5 สามารถค้นหาสมาชิกแยกตามคำสำคัญ กลุ่มสมาชิก สถานะ หรือวันเวลาได้

2.2.3.6 สามารถแสดงรายงาน รายละเอียดสมาชิก ประวัติการใช้งานของสมาชิก โดยพิมพ์หรือส่งออกเป็นรูปแบบแฟ้มข้อมูลตามที่สำนักข่าวกรองแห่งชาติกำหนด

2.2.4 การจัดการข้อมูลกลุ่มสมาชิก

2.2.4.1 สามารถทำการเพิ่มกลุ่มสมาชิก แก้ไข ลบข้อมูลกลุ่มสมาชิกและกู้คืนกลุ่มสมาชิกกลับมาได้

2.2.4.2 สามารถกำหนดสถานะกลุ่มสมาชิกได้

2.2.4.3 สามารถค้นหากลุ่มสมาชิกแยกตามคำสำคัญ สถานะ หรือวันเวลาได้เป็นอย่างน้อย

2.2.4.4 สามารถแสดงรายละเอียดกลุ่มสมาชิก ประวัติการใช้งานของกลุ่มสมาชิก

2.2.4.5 สจมารถกำหนดค่าเริ่มต้นของกลุ่มสมาชิกได้เพียง 1 รายการ

2.2.5 การจัดการข้อมูลการติดตามกิจกรรมและรายงานข่าวสารความมั่นคงปลอดภัยไซเบอร์

2.2.5.1 สามารถกำหนดการเลือกประเภทการติดตามกิจกรรมและรายงานข่าวสารความมั่นคงปลอดภัยไซเบอร์ได้

2.2.5.2 สามารถเพิ่มอีเมลและเลือกสถานะติดตามกิจกรรมและรายงานข่าวสารความมั่นคงปลอดภัยไซเบอร์

2.2.5.3 สามารถลบสมาชิกและเปลี่ยนสถานการณ์ติดตามกิจกรรมและรายงานข่าวสารความมั่นคงปลอดภัยไซเบอร์ได้

2.2.5.4 สามารถค้นหาการติดตามกิจกรรมและรายงานข่าวสารความมั่นคงปลอดภัยไซเบอร์ และแสดงรายละเอียดการใช้งานของสมาชิก ได้อย่างน้อย ดังนี้ ชื่อ กิจกรรมที่เข้าร่วมกิจกรรม รายงานข่าวสารความมั่นคงปลอดภัยไซเบอร์ที่ติดตาม รวมถึงสถานะต่างๆ วันและเวลา ไอพีแอดเดรส

2.2.5.5 สามารถแสดงรายงานรายละเอียดการติดตามกิจกรรมและรายงานข่าวสารความมั่นคงปลอดภัยไซเบอร์ โดยพิมพ์หรือส่งออกเป็นรูปแบบแฟ้มข้อมูลตามที่สำนักข่าวกรองแห่งชาติกำหนด

2.2.6 การจัดการแบบฟอร์มการสมัครสมาชิก

2.2.6.1 สามารถเพิ่ม ลบ และแก้ไขแบบฟอร์มการสมัครสมาชิกได้

2.2.6.2 สามารถตั้งค่าหน้าสมัครสมาชิก โดยกำหนดว่าจะให้ผู้สมัครสมาชิกกรอกข้อมูลตามที่กำหนด ข้อมูลที่จำเป็นต้องกรอก และสลับตำแหน่งข้อมูลที่ประสงค์ให้สมาชิกกรอกได้

2.2.6.3 สามารถส่งผลการสมัครสมาชิกไปยังอีเมลที่ใช้ในการสมัครได้โดยอัตโนมัติ

2.2.7 ประวัติการใช้งานของสมาชิก

2.2.7.1 สามารถแสดงรายละเอียดการใช้งานของสมาชิกเป็นรายบุคคล โดยแสดงชื่อผู้ใช้ ไอพีแอดเดรส วันเวลาเข้าใช้ระบบและออกจากระบบ เวลาการใช้งาน เป็นอย่างน้อย

2.2.7.2 สามารถค้นหาการใช้งานจากชื่อผู้ใช้ ประเภทสมาชิก วันที่เข้าและออกจากระบบได้

2.2.7.3 สามารถพิมพ์และส่งออกรายงานในลักษณะรูปแบบแฟ้มข้อมูลตามที่สำนักข่าวกรองแห่งชาติกำหนด

2.3 การสร้างและแสดงเนื้อหาทางเว็บเพจ

2.3.1 สามารถแสดงบทความหรือเนื้อหาต่าง ๆ ทางหน้าระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์

2.3.2 สามารถแสดงข้อมูลมัลติมีเดีย คลิปเสียง คลิปวิดีโอ รูปภาพ ในหน้าบทความหรือเนื้อหาได้

2.3.3 สามารถส่งบทความหรือเนื้อหาในระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์ผ่านทาง email และ Social Media ได้

2.3.4 สามารถแปลงเนื้อหาในหน้าระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์จาก HTML ให้เป็น PDF ได้

2.3.5 สามารถค้นหาข้อมูล ตามคำสำคัญได้เป็นอย่างน้อย

2.3.6 สามารถเปลี่ยนรูปภาพป้ายประชาสัมพันธ์ ให้เหมาะกับงานตามเทศกาลต่าง ๆ

2.3.7 สามารถ อัปโหลด ไฟล์วิดีโอและเสียง อย่างน้อยดังนี้ WMV, MP3, MP4, AVI, MKV บนระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์ผ่านทาง Web Browser ได้

2.3.8 รูปแบบของตัวอักษรและข้อความต่างๆ จะต้องเป็นรูปแบบเดียวกันทั้งระบบ

2.3.9 สามารถใส่ลิงก์เชื่อมโยง (Link) และแนบเอกสารได้

2.3.10 การจัดการข่าวและบทความ

2.3.10.1 สามาถเพิ่ม ลบ แก้ไข ข่าวและบทความ พร้อมกู้คืนข่าวและบทความกลับมาได้

2.3.10.2 สามารถย้ายกลุ่มข่าวและบทความได้

2.3.10.3 สามารถจัดลำดับข่าวและบทความได้

2.3.10.4 สามารถตั้งเวลาและกำหนดการเผยแพร่ข่าวและบทความได้

2.3.10.5 สามารถคัดลอกข่าวและบทความได้

2.3.10.6 สามารถค้นหาบทความได้จาก คำสำคัญ ประเภทข่าวและบทความ สถานะต่างๆ ได้เป็นอย่างน้อย

2.3.10.7 สามารถแสดงรายละเอียดของข่าวและบทความ จำนวนการอ่าน วันที่แก้ไขข้อมูลล่าสุด สถานะของข่าวและบทความ ได้เป็นอย่างน้อย

2.3.10.8 สามารถให้ความเห็นบทความที่เผยแพร่ และแสดงรายเอียดความเห็นของแต่ละบทความ รวมทั้งผู้ให้ความได้เป็นอย่างน้อย

2.3.11 การจัดการประเภทข่าวและบทความ

2.3.11.1 สามารถแบ่งประเภทข่าวและบทความได้อย่างน้อย 3 ระดับ

2.3.11.2 สามารถลบ แก้ไข ประเภทข่าวและบทความ พร้อมกู้คืนกลับมาได้

2.3.11.3 สามารถจัดลำดับประเภทข่าวและบทความได้

2.3.11.4 สามารถตั้งเวลาและกำหนดการเผยแพร่ประเภทข่าวและบทความได้

2.3.11.5 สามารถคัดลอกประเภทข่าวและบทความได้

2.3.11.6 สามารถค้นหาบทประเภทข่าวและบทความได้จาก คำค้น คำสำคัญ ประเภทข่าวและบทความสถานะประเภทข่าวและบทความได้เป็นอย่างน้อย

2.3.11.7 สามารถแสดงรายละเอียดของประเภทข่าวและบทความจำนวนการอ่านประเภทข่าวและบทความวันที่แก้ไขข้อมูลประเภทข่าวและบทความล่าสุด สถานะของประเภทข่าวและบทความได้เป็นอย่างน้อย

2.3.12 การตั้งค่าการแสดงข่าวและบทความ

2.3.12.1 สามารถกำหนดรายการแสดงผลในหน้าของข่าวและบทความโดยเรียงตามสถานะต่างๆ ได้

2.3.12.2 สามารถเลือกรูปแบบได้ตามต้องการ โดยมีการกำหนดอัตราส่วนของรูปภาพที่ใช้แสดงได้

2.3.12.3 สามารถกำหนดจำนวนรายการที่จะแสดงในหนึ่งหน้าได้

2.3.12.4 สามารถกำหนดวันและเวลาในการแสดงข่าวและบทความได้

2.3.12.5 สามารถกำหนดข่าวและบทความที่จะแสดงในหน้าแรกได้

2.3.12.6 สามารถกำหนดให้แสดงข่าวและบทความล่าสุด ยอดนิยม ในหน้าแรกหน้าเว็บเพจอื่นๆในพื้นที่กำหนดไว้ได้

2.3.13 สามารถตั้งเวลาในการเผยแพร่ในสถานะข่าวและบทความใหม่ได้

2.4 ระบบค้นหาข้อมูล (Search) ทั้งภาษาไทยและภาษาอังกฤษ

2.4.1 ค้นหาโดยตรงจากเนื้อหาและข้อมูลข่าวสารที่มีทั้งหมด (Simple Search)

2.4.2 ค้นหาข้อมูลแบบเฉพาะเจาะจงโดยกำหนดเงื่อนไขในการค้นหา (Advance Search) เช่น ตามกลุ่มเนื้อหา ตามช่วงวันที่ ตามคำสำคัญ ตามผู้เขียน

2.4.3 สามารถสร้างคำสำคัญเพื่อใช้ในการค้นหาได้

2.4.4 สามารถประมวลผลข้อมูลสถิติของคำและเงื่อนไขที่ถูกใช้ในการค้นหาบ่อย จำนวนครั้งของการค้นหา

2.4.5 จัดพิมพ์ออกเป็นรายงานได้

2.5 ระบบจัดการข้อมูลแผนผังเว็บไซต์ที่เปลี่ยนแปลงตามข้อมูล (Dynamic Sitemap)

2.5.1 สามารถแสดงลิงก์เชื่อมโยง (Link) แผนผังไปยังเนื้อหาส่วนต่าง ๆ ของระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์ได้อัตโนมัติ

2.5.2 ผู้ดูแลระบบสามารถแก้ไขแผนผังระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์ได้

2.6 ระบบจัดการข้อมูลกิจกรรม (Event) ซึ่งเป็นกิจกรรมที่เกี่ยวข้องกับการประชุม สัมมนา และอบรม

2.6.1 สมาชิกสมัครและยกเลิกการสมัครเข้าร่วมกิจกรรมได้

2.6.2 สามารถแสดงการแจ้งเตือนกิจกรรมผ่านทางอีเมลได้

2.6.3 สามารถดาวน์โหลดเอกสาร วิดีโอ ของกิจกรรมได้

2.6.4 สามารถแสดงรายละเอียดและค้นหาการเข้าร่วมกิจกรรม ได้อย่างน้อย ดังนี้

2.6.5 สามารถส่งอีเมลตอบรับการเข้าร่วมกิจกรรมของสมาชิกได้

2.6.6 สามารถเพิ่ม แก้ไข ลบ ประเภทกิจกรรมได้

2.6.7 สามารถสร้างกิจกรรม กำหนดวันเวลา รายละเอียด โดยเชื่อมโยงกับ Google Calendar พร้อมกำหนดสถานะของกิจกรรมได้

2.6.8 สามารถอัปโหลดไฟล์ ได้อย่างน้อย ดังนี้ PDF, JPG, WMA, WMV, WAV MP3, MP4

2.6.9 สามารถส่งอีเมลแจ้งเตือนผู้เข้าร่วมกิจกรรมได้หลายลักษณะ อย่างน้อยดังนี้

2.6.9.1.1 ส่งถึงสมาชิกตามประเภทกิจกรรมได้

2.6.9.1.2 ส่งโดยระบุสมาชิกครั้งละ 1 คน หรือมากกว่า 1 คน หรือทั้งหมดได้

2.6.10 สามารถแสดงรายละเอียดสมาชิกที่เข้าร่วมกิจกรรมเป็นรายบุคคล และรายกิจกรรมได้

2.6.11 สามารถค้นหารายละเอียดกิจกรรม ประเภท ผู้เข้าร่วม เวลา สถานะกิจกรรมได้เป็นอย่างน้อย

2.6.12 สามารถพิมพ์และส่งออกรายงานในลักษณะรูปแบบแฟ้มข้อมูลตามที่สำนักข่าวกรองแห่งชาติกำหนด

2.7 ระบบลงทะเบียนรับรายงานข่าวสารความมั่นคงปลอดภัยไซเบอร์

2.7.1 สมาชิกสมัครและยกเลิกการรับรายงานข่าวสารความมั่นคงปลอดภัยไซเบอร์ได้

2.7.2 สามารถแสดงการแจ้งเตือนสมาชิกผ่านทางอีเมลได้

2.7.3 สามารถแสดงรายละเอียดและค้นหารายงาน ตามประเภท คำสำคัญได้เป็นอย่างน้อย

2.7.4 สามารถส่งอีเมลตอบรับรายงานข่าวสารความมั่นคงปลอดภัยไซเบอร์

2.7.5 สามารถเพิ่ม แก้ไข ลบ ประเภทรายงานข่าวสารความมั่นคงปลอดภัยไซเบอร์

2.7.6 สามารถสร้างรายงานสำหรับรายงานข่าวสารความมั่นคงปลอดภัยไซเบอร์ กำหนดวันเวลาได้เป็นอย่างน้อย

2.7.7 สามารถอัปโหลดไฟล์ ได้ตามที่สำนักข่าวกรองแห่งชาติกำหนด

2.7.8 สามารถส่งอีเมลแจ้งเตือนผู้รับรายงานข่าวสารความมั่นคงปลอดภัยไซเบอร์ได้หลายลักษณะอย่างน้อยดังนี้

2.7.8.1.1 ส่งถึงสมาชิกตามประเภทรายงานได้

2.7.8.1.2 ส่งโดยระบุสมาชิกครั้งละ 1 คน หรือมากกว่า 1 คน หรือทั้งหมดได้

2.7.9 สามารถแสดงรายล่ะเอียดการรายงานข่าวสารความมั่นคงปลอดภัยไซเบอร์เป็นรายบุคคล และตามรายงานข่าวสารความมั่นคงปลอดภัยไซเบอร์ได้

2.7.10 สามารถค้นหารายละเอียดรายงาน ประเภท สถานะรายงานข่าวสารความมั่นคงปลอดภัยไซเบอร์ได้เป็นอย่างน้อย

2.7.11 สามารถพิมพ์และส่งออกรายงานในลักษณะรูปแบบแฟ้มข้อมูลตามที่สำนักข่าวกรองแห่งชาติกำหนด

2.7.12 สามารถแสดงข้อมูลสถิติในรูปแบบแผนภูมิ กราฟ พร้อมส่งออกและพิมพ์ตามรูปแบบที่สำนักข่าวกรองแห่งชาติกำหนด

2.8 ระบบแลกเปลี่ยนความคิดเห็น (Forum)

2.8.1 การจัดการกระทู้ของผู้ใช้งาน

2.8.1.1 สามารถเลือกดู เพิ่มและแสดงความคิดเห็นกระทู้แต่ละห้องแลกเปลี่ยนความเห็นได้ตามสิทธิ์การใช้งาน

2.8.1.2 สามารถแสดงรายการกระทู้พร้อมความคิดเห็นในแต่ละห้องแลกความคิดเห็นทั้งหมด โดยเรียงตามกระทู้ล่าสุด โดยกระทู้ที่มีความเคลื่อนไหวในการตอบบ่อยครั้ง ให้แสดงที่ด้านบนสุดของห้องแลกความคิดเห็นนั้นๆ พร้อมแสดงสัญลักษณ์

2.8.1.3 สามารถแสดงรายละเอียดกระทู้ เช่น จำนวนครั้งที่เปิดอ่าน จำนวนผู้ตอบ วันเวลาที่มีผู้ตอบล่าสุด และชื่อผู้เขียนกระทู้

2.8.1.4 สามารถค้นหากระทู้จากคำสำคัญ คำค้น วันเวลา ได้เป็นอย่างน้อย

2.8.2 การจัดการห้องแลกเปลี่ยนความเห็น

2.8.2.1 สามารถเพิ่ม แก้ไข ลบ หรือซ่อนห้องแลกความคิดเห็นได้ตามสิทธิ์การใช้งาน

2.8.2.2 สามารถกำหนดหรือระงับสิทธิ์สมาชิก ผู้ดูแลประจำห้องแลกความคิดเห็นได้

2.8.2.3 สามารถแสดงรายการห้องแลกความคิดเห็นทั้งหมด โดยแสดงรายละเอียดของแต่ละห้องแลกความคิดเห็น เช่น จำนวนกระทู้, เวลาที่มีความเคลื่อนไหวล่าสุด

2.8.2.4 สามารถค้นหากระทู้จากคำสำคัญ คำค้น วันเวลา ได้เป็นอย่างน้อย

2.8.2.5 สามารถแสดงรายละเอียดของห้องแลกเปลี่ยนความเห็น เช่น จำนวนกระทู้ จำนวนความเห็น พร้อมสถานะของห้องแลกเปลี่ยนความเห็นได้เป็นอย่างน้อย

2.8.3 การจัดการกระทู้สำหรับผู้ดูแลระบบ

2.8.3.1 สามารถเพิ่ม แก้ไข ลบ หรือซ่อนกระทู้และแสดงความคิดเห็นแต่ละกระทู้ได้ตามสิทธิ์การใช้งาน

2.8.3.2 สามารถกำหนดหรือระงับสิทธิ์สมาชิกในการเข้าถึงกระทู้ได้

2.8.3.3 สามารถแสดงรายการกระทู้ในแต่ละห้องแลกความคิดเห็นทั้งหมด โดยเรียงตามกระทู้ล่าสุด โดยกระทู้ที่มีความเคลื่อนไหวในการตอบบ่อยครั้ง ให้แสดงที่ด้านบนสุดของห้องแลกความคิดเห็นนั้นๆ พร้อมแสดงสัญลักษณ์

2.8.3.4 สามารถแสดงรายละเอียดกระทู้ เช่น จำนวนครั้งที่เปิดอ่าน จำนวนผู้ตอบ วันเวลาที่มีผู้ตอบล่าสุด และชื่อผู้เขียนกระทู้

2.8.3.5 สามารถอนุมัติการเผยแพร่กระทู้ได้

2.8.3.6 สามารถส่งอีเมลอัตโนมัติแจ้ง เมื่อมีการอนุมัติ ไม่อนุมัติ หรือลบ ถึงสมาชิกเจ้าของกระทู้นั้นๆ ได้

2.8.3.7 สามารถค้นหากระทู้จากคำสำคัญ คำค้น วันเวลา ได้เป็นอย่างน้อย

2.8.3.8 สามารถแสดงรายละเอียดของกระทู้ ไอพีแอดเดรสของผู้ตั้งและผู้ให้ความเห็น จำนวนการอ่าน จำนวนความเห็น วันที่ตั้งกระทู้ และให้ความเห็น พร้อมสถานะของกระทู้และความเห็นแต่ละรายการ รวมถึงข้อมูลกระทู้ที่ยังไม่ได้ตอบและพิมพ์รายงาน

2.8.4 การตั้งค่าการแลกเปลี่ยนความเห็น

2.8.4.1 สามารถกำหนดรายการกระทู้ที่ต้องแสดงภายใน 1 หน้าได้

2.8.4.2 สามารถตั้งค่าการแสดงห้องแลกเปลี่ยนความเห็นและกระทู้ยอดนิยมได้

2.8.4.3 สามารถตั้งเวลาในการเผยแพร่ในสถานะกระทู้ใหม่ได้

2.8.4.4 สามารถกำหนดการแสดงข้อมูลสมาชิกในบนกระทู้ได้

2.8.4.5 สามารถกำหนดสิทธิ์สมาชิกในการตั้งกระทู้ได้

2.8.4.6 สามารถกำหนดการให้ผู้ใช้เห็นกระทู้ได้

2.8.4.7 สามารถกำหนดการแจ้งเตือนเมื่อมีการตั้งหรือตอบกระทู้ได้

2.8.4.8 สามารถประมวลผลข้อมูลกระทู้ที่ผู้ดูแลห้องสนทนายังไม่ได้ตอบคำถามและพิมพ์รายงานได้

2.8.5 ระบบเกมมิฟิเคชัน (Gamification) สำหรับการใช้งานกระดานสนทนาอย่างน้อย ดังนี้

2.8.5.1 มีระบบสะสมแต้ม (Point)

2.8.5.2 มีระบบเหรียญตรา (Badge)

2.8.5.3 มีระบบแสดงข้อมูลรางวัล (Award)

2.8.5.4 มีระบบแสดงผู้มีคะแนนนำ (Leader board)

2.9 ระบบแสดงไฟล์วิดีโอและเสียง

2.9.1 สามารถแสดงไฟล์ Multimedia อย่างน้อยดังนี้ WMA, WMV, WAV MP3, MP4, Youtube

2.9.2 สามารถดาวน์โหลดไฟล์และแสดงจำนวนการดาวน์โหลดได้

2.9.3 สามารถกำหนด Category เพื่อแบ่งกลุ่มไฟล์วิดีโอและเสียงได้อย่างน้อย 2 ระดับ

2.9.4 สามารถเพิ่ม แก้ไข ลบกลุ่มไฟล์วิดีโอและเสียงได้

2.9.5 สามารถอัปโหลดไฟล์เสียงและไฟล์วิดีโอ พร้อมปกภาพของไฟล์ ได้มากกว่า 1 ไฟล์ต่อครั้ง โดยเลือกกลุ่มเพื่อจัดเก็บ ได้อย่างน้อยดังนี้ WMA, WMV, WAV, MP3, MP4

2.9.6 สามารถใส่ embed code จาก Youtube ได้

2.9.7 สามารถกำหนดขนาดไฟล์ที่จะอัปโหลดได้

2.9.8 สามารถใส่ชื่อไฟล์ได้อัตโนมัติ

2.9.9 สามารถกำหนดจำนวนไฟล์ ที่จะแสดงต่อ 1 หน้าได้

2.9.10 สามารถกำหนดลำดับการแสดงไฟล์ได้

2.9.11 สามารถกำหนดอนุญาตหรือไม่อนุญาตให้ดาวน์โหลดไฟล์ได้

2.9.12 สามารถย้ายกลุ่มของไฟล์ได้

2.9.13 สามารถค้นหาไฟล์ได้ตามคำสำคัญ ได้เป็นอย่างน้อย

2.9.14 สามารถแสดงรายการ รายละเอียดมีเดีย จำนวนการดาวน์โหลด วันและเวลาได้เป็นอย่างน้อย

2.10 ระบบจัดการไฟล์

2.10.1 สามารถแสดงไฟล์ อย่างน้อยดังนี้ PDF, JPG

2.10.2 สามารถดาวน์โหลดไฟล์และแสดงจำนวนการดาวน์โหลดได้

2.10.3 สามารถกำหนดหมวดหมู่ (Category) เพื่อแบ่งกลุ่มไฟล์ได้อย่างน้อย 2 ระดับ

2.10.4 สามารถเพิ่ม แก้ไข ลบกลุ่มไฟล์ได้

2.10.5 สามารถอัปโหลดไฟล์ พร้อมปกภาพของไฟล์ ได้มากกว่า 1 ไฟล์ต่อครั้ง โดยเลือกกลุ่มเพื่อจัดเก็บได้อย่างน้อยดังนี้ อย่างน้อยดังนี้ PDF, JPG และจัดเก็บใน Category ที่เลือก

2.10.6 สามารถปรับลดขนาดไฟล์ PDF (Reduce file size) ให้มีขนาดเล็กลง เมื่อนำเข้า File server ได้

2.10.7 สามารถกำหนดชื่อไฟล์ได้อัตโนมัติ

2.10.8 สามารถกำหนดจำนวนไฟล์ ที่จะแสดงต่อ 1 หน้าได้

2.10.9 สามารถกำหนดลำดับการแสดงไฟล์ได้

2.10.10 สามารถกำหนดอนุญาตหรือไม่อนุญาตให้ดาวน์โหลดไฟล์ได้

2.10.11 สามารถย้ายกลุ่มของไฟล์ได้

2.10.12 สามารถค้นหาไฟล์ได้ตามคำสำคัญ ได้เป็นอย่างน้อย

2.10.13 สามารถแสดงรายการ รายละเอียดไฟล์ จำนวนการดาวน์โหลด วันและเวลาได้เป็นอย่างน้อย

2.11 ระบบภาพกิจกรรม (Gallery)

2.11.1 สามารถแสดงรูปภาพตามกลุ่มที่กำหนดพร้อมชื่อและรายละเอียดภาพได้

2.11.2 สามารถแสดงภาพแบบ Slide show ได้

2.11.3 สามารถดาวน์โหลดภาพและแสดงจำนวนการดาวน์โหลดได้

2.11.4 สามารถกำหนดหมวดหมู่ (Category) เพื่อแบ่งกลุ่มได้อย่างน้อย 2 ระดับ

2.11.5 สามารถเพิ่ม แก้ไข ลบกลุ่มได้

2.11.6 สามารถอัปโหลดภาพได้มากกว่า 1 ภาพต่อครั้งและจัดเก็บใน Category ที่เลือก

2.11.7 สามารถปรับลดขนาดไฟล์ภาพ ให้มีขนาดเล็กลง เมื่อนำเข้า File server ได้

2.11.8 สามารถกำหนดขนาดไฟล์ที่อนุญาตให้อัปโหลดเข้า File Server ได้

2.11.9 สามารถสามารถใส่ชื่อและรายละเอียดภาพได้

2.11.10 กำหนดจำนวนกลุ่มที่แสดงต่อหน้าได้

2.11.11 สามารถกำหนดลำดับการแสดงไฟล์ได้

2.11.12 สามารถกำหนดอนุญาตหรือไม่อนุญาตให้ดาวน์โหลดไฟล์ได้

2.11.13 สามารถย้ายกลุ่มของไฟล์ได้

2.11.14 สามารถค้นหาไฟล์ได้ตามความค้น คำสำคัญ

2.11.15 สามารถแสดงรายการและรายละเอียดไฟล์ได้

2.11.16 สามารถกำหนดรายการแสดงผลในหน้าของแกลอรี โดยเรียงตามสถานะต่างๆ ได้

2.11.17 สามารถเลือกรูปแบบได้ตามต้องการ โดยมีการกำหนดอัตราส่วนของรูปภาพที่ใช้แสดงได้

2.11.18 สามารถกำหนดจำนวนรายการที่จะแสดงในหนึ่งหน้าได้

2.11.19 สามารถตั้งเวลาในการเผยแพร่ในสถานะแกลอรีใหม่ได้

2.12 ระบบแบบสำรวจ (Poll)

2.12.1 แสดงหัวข้อการ Vote

2.12.2 แสดงตัวเลือกการ Vote ทั้งแบบข้อความและรูปภาพ

2.12.3 แสดงสรุปผลการ Vote ในรูปแบบกราฟ
2.12.4 สามารถเพิ่มหัวข้อคำถามคำตอบที่ใช้สำรวจได้ไม่จำกัด
2.12.5 กำหนดจำนวนการ Vote ต่อคนในแต่ละหัวข้อคำถามได้
2.12.6 กำหนดตำแหน่งการแสดง Poll ได้ ทั้งที่เป็นหน้า Webpage และ/หรือหน้าบทความ
2.12.7 สรุปผล Vote ในรูปแบบตารางและกราฟ และจัดพิมพ์เป็นรายงานได้

2.13 ระบบข้อมูลติดต่อเรา (Contact) เพื่อใส่รายละเอียดการติดต่อกับหน่วยงานหรือเจ้าหน้าที่ได้
2.13.1 แสดงรายการกลุ่ม Contact
2.13.2 แสดงรายละเอียดในกลุ่ม
2.13.3 แสดงรายละเอียดของแต่ละรายการ
2.13.4 กำหนดกลุ่มของ Contact ได้
2.13.5 ใส่รายละเอียดได้อย่างน้อยดังนี้ ชื่อ, ตำแหน่ง, อีเมล, ที่อยู่, หมายเลขโทรศัพท์, หมายเลข, โทรสาร, ข้อมูลเพิ่มเติม, ภาพ

2.14 ระบบบริหารข้อมูลลิงก์ที่เกี่ยวข้อง (Web link)
2.14.1 แสดงรายการลิงก์ที่เกี่ยวข้อง
2.14.2 สามารถเพิ่ม/แก้ไข/ลบ หรือปรับเปลี่ยนการแสดงผลหมวดหมู่ลิงก์ที่เกี่ยวข้องกับระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์ได้
2.14.3 สามารถเพิ่ม/แก้ไข/ลบ หรือปรับเปลี่ยนการแสดงผลลิงก์ที่เกี่ยวข้องกับระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์ได้
2.14.4 แสดงผลข้อมูลที่มีอยู่ในรูปแบบแบ่งหน้า (Pagination) โดยสามารถเลือกจำนวนการแสดงผลต่อหน้าได้

2.15 ระบบบริหารป้ายโฆษณา (Banner)
2.15.1 แสดง Banner ในตำแหน่งที่กำหนดได้
2.15.2 กำหนดกลุ่ม Banner ได้
2.15.3 รองรับภาพอย่างน้อยดังนี้ JPEG, GIF, PNG
2.15.4 กำหนดตำแหน่งที่จะวาง Banner ได้
2.15.5 Banner แต่ละกลุ่มสามารถกำหนดให้วางในตำแหน่งต่างกันได้
2.15.6 กำหนดระยะเวลาในการเผยแพร่ banner ได้
2.15.7 กำหนดจำนวน Banner ที่จะแสดงได้
2.15.8 กำหนดลำดับความสำคัญของ Banner ได้
2.15.9 แสดง banner ในลักษณะเลื่อนวน และกำหนดความเร็วในการเลื่อนได้
2.15.10 สร้าง Link สำหรับ Banner ได้
2.15.11 ประมวลผลสถิติการคลิก Banner เป็นรายวัน รายเดือน รายปี โดยมีข้อมูลแสดงอย่างน้อยดังนี้ Unique IP, Unique Session

2.16 ระบบบริหารจัดการเมนู
2.16.1 สามารถแสดงข้อมูลได้จากเมนูได้
2.16.2 สามารถจัดการ เพิ่ม ลบ แก้ไขเมนูหลักในแต่ละเมนูได้อย่างน้อย 2 ระดับชั้น
2.16.3 สามารถอัพเดทข้อมูลไปยัง Site Map ได้อัตโนมัติเมื่อมีการเพิ่มลบหรือแก้ไขเมนู

1.	2.	3.	4.	5. .....
ประธานคณะกรรมการ	คณะกรรมการ	คณะกรรมการ	คณะกรรมการ	คณะกรรมการและเลขานุการ

2.16.4 สามารถเชื่อมต่อกับระบบอื่นๆ โดยใส่เป็น URL ได้

2.16.5 สามารถกำหนดให้ซ่อนแสดงและสลับลำดับของเมนูได้

2.16.6 สามารถเลือกเมนูที่ต้องการให้แสดงผลได้โดยเชื่อมโยงข้อมูลจากระบบได้โดยตรง

2.16.7 สามารถเลือกเมนูที่ต้องการให้แสดงผลให้สอดคล้องกับเทมเพลตที่สำนักข่าวกรองแห่งชาติกำหนด

2.17 ระบบจัดการข้อมูลเว็บไซต์ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์

2.17.1 สามารถเพิ่ม แก้ไข ลบและแสดงผลข้อมูลเกี่ยวกับการประชาสัมพันธ์ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ อาทิ วิสัยทัศน์ พันธกิจ สมาชิก และการติดต่อเจ้าหน้าที่ได้

2.17.2 สามารถจัดการข้อมูล เพิ่ม ลบ แก้ไขเมนูหลักในแต่ละเมนูได้อย่างน้อย 2 ระดับชั้น และสามารถสามารถแสดงผลเมนูหลักและเมนูย่อยบนหน้าเว็บไซต์ได้ รวมทั้งอัพเดทข้อมูลไปยัง Site Map ได้อัตโนมัติเมื่อมีการเพิ่ม ลบ หรือแก้ไขเมนู

2.17.3 สามารถแสดงข้อมูลรายงานแจ้งเตือนภัยคุกคามทางไซเบอร์ รายงานวิเคราะห์เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และข่าวสารสถานการณ์ทางไซเบอร์ และข่าวสารกิจกรรมทั่วไปได้จากฐานข้อมูลระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์ที่กำหนดได้

3. ข้อกำหนดด้านการฝึกอบรมและการสนับสนุนการใช้งานระบบ

3.1 ผู้ขายต้องให้การสนับสนุนด้านวิชาการ โดยส่งมอบเอกสารทั้งหมดที่เกี่ยวข้องกับระบบงาน ดังนี้

3.1.1 เอกสารการออกแบบระบบ และพจนานุกรมข้อมูล (Data Dictionary)

3.1.2 รหัสชุดคำสั่งโปรแกรมระบบ (Source Code)

3.1.3 คู่มือการใช้งานและการดูแลระบบ (User & Administrator Manual)

3.2 ผู้ขายต้องจัดการฝึกอบรมเจ้าหน้าที่ของสำนักข่าวกรองแห่งชาติอย่างน้อย 10 คน ทั้งด้านวิชาการและด้านปฏิบัติการแก่เจ้าหน้าที่ของสำนักข่าวกรองแห่งชาติ ให้มีความรู้และความเข้าใจจนสามารถปฏิบัติงานได้อย่างมีประสิทธิภาพ อย่างน้อยดังต่อไปนี้

3.2.1 หลักสูตรที่เกี่ยวกับการออกแบบและการเขียนชุดคำสั่งโปรแกรมที่ใช้พัฒนาระบบของโครงการ

3.2.2 หลักสูตรที่เกี่ยวกับการบริหารจัดการระบบสำหรับผู้ดูแลระบบ

3.3 ผู้ขายรับผิดชอบค่าใช้จ่ายใด ๆ ที่เกิดขึ้นในการฝึกอบรม รวมทั้งค่าอาหารว่าง ค่าเอกสาร และอุปกรณ์ในการฝึกอบรม ถือเป็นค่าใช้จ่ายของผู้ขายทั้งสิ้น

3.4 ผู้ขายต้องเสนอรายชื่อผู้ชำนาญการที่รับผิดชอบการให้คำแนะนำเกี่ยวกับการใช้โปรแกรมและการแก้ไขปัญหาระบบแลกเปลี่ยนข้อมูลข่าวสารความมั่นคงปลอดภัยไซเบอร์ของสำนักข่าวกรองแห่งชาติ และข้อมูลการติดต่อที่สามารถติดต่อได้ตลอดระยะเวลาตามสัญญา

4. ระยะเวลาดำเนินการ

ระยะเวลาดำเนินการ ทั้งสิ้น 240 วัน นับถัดจากวันลงนามในสัญญา

---

1.	2.	3.	4.	5. .....
ประธานคณะกรรมการ	คณะกรรมการ	คณะกรรมการ	คณะกรรมการ	คณะกรรมการและเลขานุการ

ภาคผนวก 3
จัดอบรมและจัดการแข่งขันทักษะความมั่นคงปลอดภัยไซเบอร์

1. จัดอบรมหลักสูตรความมั่นคงปลอดภัยไซเบอร์เชิงรุก (Offensive Security Certified Professional) โดยมีรายละเอียด ดังนี้

1.1 ความเป็นมา

1.1.1 ปัจจุบันภัยคุกคามและการโจมตีทางไซเบอร์ มีแนวโน้มทวีความรุนแรงและมีปริมาณมากขึ้นอย่างยิ่ง ก่อให้เกิดผลกระทบต่อความสงบเรียบร้อยในวงกว้าง ในปัจจุบันหน่วยงานด้านความมั่นคงของประเทศได้นำเทคโนโลยีดิจิทัลเข้ามาสนับสนุนการปฏิบัติงานจัดเก็บข้อมูลในข่าวสารที่มีชั้นความลับและเกี่ยวข้องกับความมั่นคงของประเทศในระบบฐานข้อมูลและระบบสารสนเทศ ซึ่งมีความเสี่ยงและอาจได้รับผลกระทบจากภัยคุกคามทางไซเบอร์

1.1.2 การศึกษาวิธีการเจาะช่องโหว่และทดสอบความปลอดภัยระบบคอมพิวเตอร์และระบบเครือข่ายจะทำให้ผู้ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในหน่วยงานด้านความมั่นคงของรัฐสามารถนำความรู้และทักษะที่ได้รับไปตรวจสอบและประเมินช่องโหว่ระบบคอมพิวเตอร์และระบบเครือข่ายของหน่วยงานตนเอง เพื่อนำไปสู่การป้องกัน แก้ไข และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ

1.1.3 สำนักข่าวกรองแห่งชาติและหน่วยงานด้านความมั่นคงของรัฐจึงต้องเร่งพัฒนาและขยายขีดความสามารถของบุคลากรผู้ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้มีความสามารถในตรวจประเมินช่องโหว่และทดสอบเจาะระบบคอมพิวเตอร์ รวมถึงส่งเสริมให้เกิดความร่วมมือระหว่างหน่วยงานด้านความมั่นคงของรัฐให้มีเครือข่ายหรือประชาคมผู้ปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์ขึ้น เพื่อให้เกิดความร่วมมือในการประสานงานแก้ไขปัญหาภัยคุกคามทางไซเบอร์ในอนาคตต่อไป

1.2 วัตถุประสงค์

1.2.1 เพื่อเสริมสร้างองค์ความรู้เกี่ยวกับการปฏิบัติการทางไซเบอร์เชิงรุกแก่ผู้ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในกลุ่มหน่วยงานด้านความมั่นคงของรัฐ ให้เกิดความรู้ความเข้าใจและเทคนิควิธีการเจาะระบบคอมพิวเตอร์และระบบเครือข่าย

1.2.2 เพื่อสร้างเครือข่ายผู้ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในกลุ่มหน่วยงานด้านความมั่นคงของรัฐ อันจะเป็นรากฐานการประสานงานและปฏิบัติงานร่วมกันในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ

1.3 กลุ่มเป้าหมาย ผู้ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จำนวนไม่เกิน 30 คน

1.4 ระยะเวลา จำนวน 8 วัน

1.5 สถานที่ สำนักข่าวกรองแห่งชาติเป็นผู้กำหนดสถานที่จัดอบรม

1.6 รายละเอียดเนื้อหาหลักสูตรแสดงดังตารางที่ 1

ตารางที่ 1 รายละเอียดเนื้อหาหลักสูตรความมั่นคงปลอดภัยไซเบอร์เชิงรุก (Offensive Security)

เวลา	หัวข้อการอบรม
วันที่ 1	
09.00 – 12.00 น.	**Penetration Testing with Kali Linux** • About The PWK Course • Overall Strategies for Approaching the Course • Obtaining Support • About Penetration Testing • Legal • The MegaCorpone.com and Sandbox. local • Domains • About the PWK VPN Labs • Reporting • About the OSCP Exam
	Getting Comfortable with Kali Linux • Booting Up Kali Linux • The Kali Menu • Kali Documentation • Finding Your Way Around Kali • Managing Kali Linux Services • Searching, Installing, and Removing Tools
12.00 – 13.00 น.	**พักรับประทานอาหารกลางวัน**
13.00 – 16.00 น.	**Command Line Fun** • The Bash Environment • Piping and Redirection • Text Searching and Manipulation • Editing Files from the Command Line • Comparing Files • Managing Processes • File and Command Monitoring • Downloading Files

เวลา	หัวข้อการอบรม
	• Customizing the Bash Environment
วันที่ 2	
09.00 – 12.00 น.	**Practical Tools** • The Bash Environment • Piping and Redirection • Text Searching and Manipulation • Editing Files from the Command Line • Comparing Files • Managing Processes • File and Command Monitoring • Downloading Files • Customizing the Bash Environment
	Bash Scripting • Intro to Bash Scripting • Variables • If, Else, Elif Statements • Boolean Logical Operations • Loops • Functions • Practical Examples
12.00 – 13.00 น.	**พักรับประทานอาหารกลางวัน**
13.00 – 16.00 น.	**Passive Information Gathering** • Website Recon • Whois Enumeration • Google Hackig • Netcraft • Recon-ng • Open-Source Code

1. ..... ประธานคณะกรรมการ
2. ..... คณะกรรมการ
3. ..... คณะกรรมการ
4. ..... คณะกรรมการ
5. ..... คณะกรรมการและเลขานุการ

เวลา	หัวข้อการอบรม
	• Shodan • Security Headers Scanner • SSL Server Test • Pastebin • User Information Gathering • Social Media Tools • Stack Overflow • Information Gathering Frameworks
วันที่ 3	
09.00 – 12.00 น.	**Active Information Gathering** • DNS Enumeration • Port Scanning • SMB Enumeration • NFS Enumeration • SMTP Enumeration • SNMP Enumeration
	Vulnerability Scanning • Vulnerability Scanning Overview and • Considerations • Vulnerability Scanning with Nessus • Vulnerability Scanning with Nmap
12.00 – 13.00 น.	**พักรับประทานอาหารกลางวัน**
13.00 – 16.00 น.	**Web Application Attacks** • Web Application Assessment Methodology • Web Application Enumeration • Web Application Assessment Tools • Exploiting Web-based Vulnerabilities • Extra Miles

1. ..... ประธานคณะกรรมการ
2. ..... คณะกรรมการ
3. ..... คณะกรรมการ
4. ..... คณะกรรมการ
5. ..... คณะกรรมการและเลขานุการ

เวลา	หัวข้อการอบรม
วันที่ 4	
09.00 – 12.00 น.	**Introduction to Buffer Overflows** • Introduction to the x Architecture • Buffer Overflow Walkthrough

	Windows Buffer Overflows
	• Discovering the Vulnerability
	  ○ Fuzzing the HTTP Protocol
	• Win Buffer Overflow Exploitation
	  ○ A Word About DEP, ASLR, and CFG
	  ○ Replicating the Crash
	  ○ Controlling EIP
	  ○ Locating Space for Our Shellcode
	  ○ Checking for Bad Characters
	  ○ Redirecting the Execution Flow
	  ○ Finding a Return Address
	  ○ Generating Shellcode with Metasploit
	  ○ Getting a Shell
	  ○ Improving the Exploit

12.00 – 13.00 น.	**พักรับประทานอาหารกลางวัน**
13.00 – 16.00 น.	**Linux Buffer Overflows** • About DEP, ASLR, and Canaries • Replicating the Crash • Controlling EIP • Locating Space for Our Shellcode • Checking for Bad Characters • Finding a Return Address • Getting a Shell
วันที่ 5	
09.00 – 12.00 น.	**Client-Side Attacks** • Know Your Target

เวลา	หัวข้อการอบรม
	• Leveraging HTML Applications • Exploiting Microsoft Office
	Locating Public Exploits • A Word of Caution • Searching for Exploits • Putting It All Together
12.00 – 13.00 น.	**พักรับประทานอาหารกลางวัน**
13.00 – 16.00 น.	**Fixing Exploits** • Fixing Memory Corruption Exploits • Fixing Web Exploits
	File Transfers • Considerations and Preparations • Transferring Files with Windows Hosts
วันที่ 6	
09.00 – 12.00 น.	**Antivirus Evasion** • What is Antivirus Software • Methods of Detecting Malicious Code • Bypassing Antivirus Detection
	Privilege Escalation • Information Gathering • Windows Privilege Escalation Examples • Linux Privilege Escalation Examples
12.00 – 13.00 น.	**พักรับประทานอาหารกลางวัน**
13.00 – 16.00 น.	**Password Attacks** • Wordlists • Brute Force Wordlists • Common Network Service Attack Methods Leveraging Password Hashes

เวลา	หัวข้อการอบรม
วันที่ 7	
09.00 – 12.00 น.	**Port Redirection and Tunneling** • Port Forwarding • SSH Tunneling • PLINK.exe • NETSH • HTTPTunnel-ing Through Deep Packet • Inspection
	Active Directory Attacks • Active Directory Theory • Active Directory Enumeration • Active Directory Authentication • Active Directory Lateral Movement • Active Directory Persistence
12.00 – 13.00 น.	**พักรับประทานอาหารกลางวัน**
13.00 – 16.00 น.	**The Metasploit Framework** • Metasploit User Interfaces and Setup • Exploit Modules • Metasploit Payloads • Building Our Own MSF Module • Post-Exploitation with Metasploit • Metasploit Automation
วันที่ 8	
09.00 – 12.00 น.	**PowerShell Empire** • Installation, Setup, and Usage • PowerShell Modules • Switching Between Empire and Metasploit
	Assembling the Pieces: Penetration Test Breakdown

เวลา	หัวข้อการอบรม
	• Public Network Enumeration • Targeting the Web Application • Targeting the Database • Deeper Enumeration of the Web Application Server • Targeting the Database Again • Targeting Poultry • Internal Network Enumeration • Targeting the Jenkins Server • Targeting the Domain Controller
12.00 – 13.00 น.	**พักรับประทานอาหารกลางวัน**
13.00 – 16.00 น.	**Trying Harder: The Labs** • Real Life Simulations • Machine Dependencies • Cloned Lab Machines • Unlocking Networks • Routing • Machine Ordering & Attack Vectors • Firewall / Routers / NAT • Passwords

หมายเหตุ *กำหนดการอาจมีการปรับเปลี่ยนตามความเหมาะสม*

1.7 วิทยากร ต้องมีคุณวุฒิไม่ต่ำกว่าปริญญาโท ในสาขาวิศวกรรมคอมพิวเตอร์ หรือวิศวกรรมไฟฟ้า หรือวิทยาศาสตร์คอมพิวเตอร์ หรือ วิทยาศาสตร์เทคโนโลยีสารสนเทศ หรือ สาขาวิชาอื่นที่เกี่ยวข้อง และมีประสบการณ์ปฏิบัติงานในสาขาดังกล่าวมาแล้วไม่ต่ำกว่า 10 ปี จำนวนไม่น้อยกว่า 1 คน

1.8 การจัดเตรียมบุคลากรเพื่อปฏิบัติหน้าที่ต่าง ๆ ตลอดระยะเวลาการฝึกอบรม ดังนี้

1.8.1 ผู้ประสานงานหลัก จำนวน 1 คน ทำหน้าที่ประสานงานหลักและบริหารจัดการกิจกรรมโดยรวมทั้งหมดให้เป็นไปด้วยความเรียบร้อย ตลอดระยะเวลาตามสัญญาจ้าง

1.8.2 เจ้าหน้าที่เทคนิคจำนวน 2 คน สนับสนุนวิทยากรภาคปฏิบัติ ตลอดจนอำนวยความสะดวกต่าง ๆ ระหว่างการฝึกอบรมให้แก่ผู้เข้ารับการอบรม

1.9 การจัดการฝึกอบรม

1.9.1 จัดให้มีอุปกรณ์สำหรับการฝึกอบรมในภาคปฏิบัติ ตลอดจนสื่อการสอน/เอกสารประกอบการเรียนการสอนที่เหมาะสมสำหรับผู้เข้ารับการอบรม อย่างน้อย 30 ชุด

1.9.2 จัดให้มีอาหารและเครื่องดื่มสำหรับผู้เข้ารับการอบรมและผู้ที่เกี่ยวข้องทุกวันตลอดการอบรม ได้แก่ (1) อาหารว่างวันละ 2 มื้อ เช้า-บ่าย รวม 16 มื้อ (2) อาหารกลางวัน 8 มื้อ

1.9.3 จัดให้มีประกาศนียบัตรพร้อมปกประกาศสำหรับผู้เข้ารับการอบรม

1.9.4 จัดให้มีการประเมินความพึงพอใจและประโยชน์ที่ได้รับจากการอบรม เมื่อสิ้นสุดการอบรม

1.10 งบประมาณ จำนวน 394,000 บาท (สามแสนเก้าหมื่นสี่พันบาทถ้วน) ดังตารางที่ 2

ตารางที่ 2 รายละเอียดค่าใช้จ่ายในการจัดอบรมความมั่นคงปลอดภัยไซเบอร์เชิงรุก

รายละเอียดค่าใช้จ่าย	จำนวนเงิน (บาท)
1. ค่าใช้จ่ายของวิทยากรที่มีความรู้ มีความสามารถเฉพาะทาง และประสบการณ์พิเศษ - ค่าวิทยากรบรรยายและฝึกปฏิบัติ จำนวน 1 คน 48 ชั่วโมง ชั่วโมงละ 3,500 บาท	168,000.00
2. ค่าใช้จ่ายของบุคลากร - ผู้ประสานงานหลัก จำนวน 1 คน - เจ้าหน้าที่ทางเทคนิค จำนวน 2 คน	120,000.00
3. ค่าใช้จ่ายด้านพาหนะ - ค่าเดินทางของวิทยากร จำนวน 1 คน โดยจ่ายตามจริงหรือในอัตรา กิโลเมตรละ 4 บาท หรือไม่เกิน 1,000 บาทต่อเที่ยว	16,000.00
4. ค่าใช้จ่ายด้านฝึกอบรม - ค่าประกาศนียบัตร - ค่าเอกสาร - ค่าวัสดุอุปกรณ์ - ค่าอาหาร จำนวน 8 วัน วันละ 200 บาทต่อคน - ค่าอาหารว่างและเครื่องดื่ม จำนวน 8 วัน วันละ 70 บาทต่อคน	90,000.00
รวมเป็นเงินทั้งสิ้น	**394,000.00**

1.11 การประเมินผล

1.11.1 ร้อยละ 80 ของผู้เข้าร่วมการอบรม มีทักษะด้านความปลอดภัยและการเจาะช่องโหว่ของระบบเครือข่ายเพิ่มขึ้นในระดับมาก – มากที่สุด

1.11.2 ร้อยละ 80 ของผู้เข้าร่วมการอบรม มีความพึงพอใจต่อประโยชน์ที่ได้รับของหลักสูตร

1.12 ผลที่คาดว่าจะได้รับ

1.12.1 ผู้เข้าร่วมการอบรม ได้รับทักษะการเจาะช่องโหว่ของระบบคอมพิวเตอร์และระบบเครือข่าย

1.12.2 เสริมสร้างและพัฒนาสัมพันธ์ระหว่างผู้ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในกลุ่มหน่วยงานด้านความมั่นคงของรัฐ ให้สามารถประสานงานและปฏิบัติงานร่วมกันในการป้องกันรับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ

2. จัดอบรมหลักสูตรการบริหารจัดการและการรับมือกับภัยคุกคามทางไซเบอร์ (Cyber Security Incident Management - CSM) โดยมีรายละเอียด ดังนี้

2.1 ความเป็นมา

2.1.1 ปัจจุบันภัยคุกคามและการโจมตีทางไซเบอร์ มีแนวโน้มทวีความรุนแรงและมีปริมาณมากขึ้นอย่างยิ่ง ก่อให้เกิดผลกระทบต่อความสงบเรียบร้อยในวงกว้าง ในปัจจุบันหน่วยงานด้านความมั่นคงของประเทศได้นำเทคโนโลยีดิจิทัลเข้ามาสนับสนุนการปฏิบัติงานจัดเก็บข้อมูลในข่าวสารที่มีชั้นความลับและเกี่ยวข้องกับความมั่นคงของประเทศในระบบฐานข้อมูลและระบบสารสนเทศ ซึ่งมีความเสี่ยงและอาจได้รับผลกระทบจากภัยคุกคามทางไซเบอร์

2.1.2 ภัยคุกคามทางไซเบอร์ อาทิ การจารกรรมทางไซเบอร์เพื่อขโมยข้อมูล การแสวงประโยชน์จากช่องโหว่ของเทคโนโลยีดิจิทัลเพื่อสอดแนมและขโมยข้อมูล เฉพาะอย่างยิ่งการขโมยข้อมูลและเข้ารหัสข้อมูลเรียกค่าไถ่นั้น ส่งผลต่อข้อมูลที่เกี่ยวข้องกับความมั่นคงของประเทศ ข้อมูลที่ถูกจารกรรมรั่วไหลไปยังบุคคลที่ไม่เกี่ยวข้องหรือฝ่ายตรงข้ามส่งผลกระทบต่อความมั่นคงของประเทศชาติอย่างร้ายแรง

2.1.3 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กำหนดให้หน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำแผนรับมือเหตุการณ์ภัยคุกคามทางไซเบอร์เพื่อเตรียมความพร้อมบุคลากร เครื่องมือ และกระบวนการให้สามารถรับมือภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ

2.1.4 สำนักข่าวกรองแห่งชาติและหน่วยงานด้านความมั่นคงจะต้องเร่งพัฒนาและขยายขีดความสามารถของบุคลากรและหน่วยงานในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้มีความสามารถในการรับมือภัยคุกคามทางไซเบอร์ในระดับประเทศ และจำเป็นต้องส่งเสริมให้เกิดความร่วมมือระหว่างหน่วยงานด้านความมั่นคงให้มีเครือข่ายหรือประชาคมผู้ปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์ขึ้น เพื่อให้เกิดความร่วมมือในการประสานงานแก้ไขปัญหาภัยคุกคามทางไซเบอร์อย่างยั่งยืน

2.2 วัตถุประสงค์

2.2.1 เพื่อให้ผู้เข้าร่วมฝึกอบรมมีความรู้และความเข้าใจในสาระสำคัญของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และปฏิบัติตามความข้อกำหนดของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ได้อย่างสอดคล้อง

2.2.2 เพื่อให้ผู้เข้าร่วมฝึกอบรมมีความรู้และความเข้าใจมาตรการที่จำเป็นในการรับมือภัยคุกคามทางไซเบอร์ สามารถจัดทำแผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ และจัดเตรียมทรัพยากรที่จำเป็นสำหรับการบริหารจัดการภัยคุกคามทางไซเบอร์ได้

2.2.3 เพื่อให้ผู้เข้าร่วมฝึกอบรมเข้าใจแนวทางในการจัดตั้งทีมบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยและ สามารถวิเคราะห์และรับมือกับภัยคุกคามทางไซเบอร์ได้

2.3 กลุ่มเป้าหมาย ผู้ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จำนวนไม่เกิน 30 คน

2.4 ระยะเวลา จำนวน 4 วัน

2.5 สถานที่ สำนักข่าวกรองแห่งชาติกำหนดสถานที่จัดอบรม

2.6 รายละเอียดเนื้อหาหลักสูตรแสดงดังตารางที่ 3

1.	2.	3.	4.	5. .....
ประธานคณะกรรมการ	คณะกรรมการ	คณะกรรมการ	คณะกรรมการ	คณะกรรมการและเลขานุการ

ตารางที่ 3 กำหนดการอบรมหลักสูตรการบริหารจัดการและการรับมือกับภัยคุกคามทางไซเบอร์

เวลา	หัวข้อการอบรม
วันที่ 1	
09.00 – 12.00 น.	**พระราชบัญญัติและกรอบมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์** • สาระสำคัญพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ • กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
12.00 – 13.00 น.	พักรับประทานอาหารกลางวัน
13.00 – 16.00 น.	**การจัดตั้งทีมบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์** • ทีมบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ • ฝึกปฏิบัติครั้งที่ 1 การจัดตั้งทีมบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ • แผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ • ฝึกปฏิบัติ ครั้งที่ 2 การจัดทำแผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์
วันที่ 2	
09.00 – 12.00 น.	**การจัดเตรียมทรัพยากรแผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์** • การจัดสรรทรัพยากรเพื่อสนับสนุนและรองรับแผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ • ฝึกปฏิบัติครั้งที่ 3 การกำหนดทรัพยากรที่จำเป็นในการสนับสนุนแผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ • การซ้อมแผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ • ฝึกปฏิบัติครั้งที่ 4 การซ้อมแผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์
12.00 – 13.00 น.	พักรับประทานอาหารกลางวัน
13.00 – 16.00 น.	**กรณีศึกษากรณีที่ 1 วิเคราะห์ผู้ประสงค์ร้ายสแกนช่องโหว่ระบบคอมพิวเตอร์**
วันที่ 3	
09.00 – 12.00 น.	**กรณีศึกษากรณีที่ 2 วิเคราะห์ผู้ประสงค์ร้ายปฏิบัติการสุ่มรหัสผ่านระบบเป้าหมาย**
12.00 – 13.00 น.	พักรับประทานอาหารกลางวัน

เวลา	หัวข้อการอบรม
13.00 – 16.00 น.	**กรณีศึกษากรณีที่ 3 วิเคราะห์ผู้ประสงค์ร้ายโจมตีระบบจนระบบระงับการให้บริการ** **กรณีศึกษากรณีที่ 4 วิเคราะห์ผู้ประสงค์ร้ายเจาะระบบจากช่องโหว่ของระบบ**
วันที่ 4	
09.00 – 12.00 น.	**กรณีศึกษากรณีที่ 5 วิเคราะห์ผู้ประสงค์ร้ายเปลี่ยนแปลงหน้าเว็บไซต์**
12.00 – 13.00 น.	พักรับประทานอาหารกลางวัน
13.00 – 16.00 น.	**กรณีศึกษากรณีที่ 6 วิเคราะห์การโจมตีระบบแบบ SQL Injection** **กรณีศึกษากรณีที่ 7 วิเคราะห์กรณีมัลแวร์โจมตีระบบคอมพิวเตอร์**

หมายเหตุ กำหนดการอาจมีการปรับเปลี่ยนตามความเหมาะสม

2.7 วิทยากร ต้องมีคุณวุฒิไม่ต่ำกว่าปริญญาโท ในสาขาวิศวกรรมคอมพิวเตอร์ หรือวิศวกรรมไฟฟ้า หรือวิทยาศาสตร์คอมพิวเตอร์ หรือ วิทยาศาสตร์เทคโนโลยีสารสนเทศ หรือ สาขาวิชาอื่นที่เกี่ยวข้อง และมีประสบการณ์ปฏิบัติงานในสาขาดังกล่าวมาแล้วไม่ต่ำกว่า 10 ปี จำนวนไม่น้อยกว่า 1 คน

2.8 การจัดเตรียมบุคลากรเพื่อปฏิบัติหน้าที่ต่าง ๆ ตลอดระยะเวลาการฝึกอบรม ดังนี้

2.8.1 ผู้ประสานงานหลัก จำนวน 1 คน ทำหน้าที่ประสานงานหลักและบริหารจัดการกิจกรรมโดยรวมทั้งหมดให้เป็นไปด้วยความเรียบร้อย ตลอดระยะเวลาตามสัญญาจ้าง

2.8.2 เจ้าหน้าที่เทคนิคจำนวน 3 คน สนับสนุนวิทยากรภาคปฏิบัติ ตลอดจนอำนวยความสะดวกต่าง ๆ ระหว่างการฝึกอบรมให้แก่ผู้เข้ารับการอบรม

2.9 การจัดการฝึกอบรม

2.9.1 จัดให้มีอุปกรณ์สำหรับการฝึกอบรมในภาคปฏิบัติ ตลอดจนสื่อการสอน/เอกสารประกอบการเรียนการสอนที่เหมาะสมสำหรับผู้เข้ารับการอบรม อย่างน้อย 30 ชุด

2.9.2 จัดให้มีอาหารและเครื่องดื่มสำหรับผู้เข้ารับการอบรมและผู้ที่เกี่ยวข้องทุกวันตลอดการอบรม ได้แก่ (1) อาหารว่างวันละ 2 มื้อ เช้า-บ่าย รวม 8 มื้อ และ (2) อาหารกลางวัน 4 มื้อ

2.9.3 จัดให้มีประกาศนียบัตรพร้อมปกประกาศสำหรับผู้เข้ารับการอบรม โดยทางผู้ขายต้องออกแบบให้ผู้ว่าจ้างคัดเลือก

2.9.4 จัดให้มีการประเมินความพึงพอใจและประโยชน์ที่ได้รับจากการอบรม เมื่อสิ้นสุดการอบรม

2.10 งบประมาณ จำนวน 260,000 บาท (สองแสนหกหมื่นบาทถ้วน) ดังตารางที่ 4

ตารางที่ 4 รายละเอียดค่าใช้จ่ายในการจัดอบรมหลักสูตรการบริหารจัดการและการรับมือกับภัยคุกคามทางไซเบอร์

รายละเอียดค่าใช้จ่าย	จำนวนเงิน (บาท)
1. ค่าใช้จ่ายของวิทยากรที่มีความรู้ มีความสามารถเฉพาะทาง และประสบการณ์พิเศษ - ค่าวิทยากรบรรยายและฝึกปฏิบัติ จำนวน 1 คน จำนวน 24 ชั่วโมง ชั่วโมงละ 3,500 บาท	84,000.00

1. ..... ประธานคณะกรรมการ
2. ..... คณะกรรมการ
3. ..... คณะกรรมการ
4. ..... คณะกรรมการ
5. ..... คณะกรรมการและเลขานุการ

รายละเอียดค่าใช้จ่าย	จำนวนเงิน (บาท)
2. ค่าใช้จ่ายของบุคลากร - ผู้ประสานงานหลัก จำนวน 1 คน - เจ้าหน้าที่ทางเทคนิค จำนวน 3 คน	120,000.00
3. ค่าใช้จ่ายด้านพาหนะ - ค่าเดินทางของวิทยากร จำนวน 1 คน โดยจ่ายตามจริงหรือในอัตรากิโลเมตรละ 4 บาท หรือไม่เกิน 1,000 บาทต่อเที่ยว	8,000.00
4. ค่าใช้จ่ายด้านฝึกอบรม - ค่าประกาศนียบัตร - ค่าเอกสาร - ค่าวัสดุอุปกรณ์ - ค่าอาหาร จำนวน 4 วัน วันละ 200 บาทต่อคน - ค่าอาหารว่างและเครื่องดื่ม จำนวน 4 วัน วันละ 70 บาทต่อคน	48,000.00
รวมเป็นเงินทั้งสิ้น	260,000.00

2.11 การประเมินผล

2.11.1 ร้อยละ 80 ของผู้เข้าร่วมการอบรม มีทักษะด้านจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์เพิ่มขึ้นในระดับมาก – มากที่สุด

2.11.2 ร้อยละ 80 ของผู้เข้าร่วมการอบรม มีความพึงพอใจต่อประโยชน์ที่ได้รับของหลักสูตร

2.12 ผลที่คาดว่าจะได้รับ

2.12.1 ผู้เข้าร่วมการอบรม ได้รับทักษะการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์

2.12.2 เสริมสร้างและพัฒนาสัมพันธ์ระหว่างผู้ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในกลุ่มหน่วยงานด้านความมั่นคงของรัฐ ให้สามารถประสานงานและปฏิบัติงานร่วมกันในการป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ

3. จัดการแข่งขันทักษะด้านความมั่นคงปลอดภัยไซเบอร์ โดยมีรายละเอียดดังนี้

3.1 ความเป็นมา

3.1.1 ปัจจุบันภัยคุกคามและการโจมตีทางไซเบอร์ มีแนวโน้มทวีความรุนแรงและมีปริมาณมากขึ้นอย่างยิ่ง ก่อให้เกิดผลกระทบต่อความสงบเรียบร้อยในวงกว้าง ในปัจจุบันหน่วยงานด้านความมั่นคงของประเทศได้นำเทคโนโลยีดิจิทัลเข้ามาสนับสนุนการปฏิบัติงานจัดเก็บข้อมูลในข่าวสารที่มีชั้นความลับและเกี่ยวข้องกับความมั่นคงของประเทศในระบบฐานข้อมูลและระบบสารสนเทศ ซึ่งมีความเสี่ยงและอาจได้รับผลกระทบจากภัยคุกคามทางไซเบอร์

3.1.2 สำนักข่าวกรองแห่งชาติและหน่วยงานด้านความมั่นคงจะต้องเร่งพัฒนาและขยายขีดความสามารถของบุคลากรและหน่วยงานในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้มีความสามารถในการรับมือภัยคุกคามทางไซเบอร์ในระดับประเทศ และจำเป็นต้องส่งเสริมให้เกิดความร่วมมือระหว่างหน่วยงานด้านความมั่นคงให้มีเครือข่ายหรือประชาคมผู้ปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์ขึ้น เพื่อให้เกิดความร่วมมือในการประสานงานแก้ไขปัญหาภัยคุกคามทางไซเบอร์

3.1.3 การจัดการแข่งขันทักษะด้านความมั่นคงปลอดภัยไซเบอร์ในกลุ่มผู้ปฏิบัติงานด้านความมั่นคงของรัฐจะเป็นการเสริมสร้างความสัมพันธ์ระหว่างผู้ปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์ในหน่วยงานด้านความมั่นคงของรัฐให้สามารถผนึกกำลังผสานความรู้และความสามารถระหว่างผู้ปฏิบัติงานต่างหน่วยงานในการแก้ไขปัญหาโจทย์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีความท้าทายและมีลักษณะเดียวกันกับปัญหาภัยคุกคามทางไซเบอร์ที่เกิดขึ้นจริง

3.2 วัตถุประสงค์

3.2.1 เพื่อเสริมสร้างและทดสอบทักษะผู้เข้าการแข่งขันทักษะความมั่นคงปลอดภัยไซเบอร์เกี่ยวกับปฏิบัติการทางไซเบอร์เชิงรุกและเชิงรับ

3.2.2 เพื่อให้ผู้เข้าการแข่งขันทักษะความมั่นคงปลอดภัยไซเบอร์สร้างเครือข่ายผู้ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในกลุ่มหน่วยงานด้านความมั่นคงของรัฐ อันจะเป็นรากฐานการประสานงานและปฏิบัติงานร่วมกันในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ

3.3 กลุ่มเป้าหมาย ผู้ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จำนวนไม่เกิน 30 คน

3.4 ระยะเวลา จำนวน 3 วัน

3.5 รายละเอียดการออกแบบโจทย์การแข่งขันทักษะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

3.5.1 รูปแบบการแข่งขันทักษะด้านความมั่นคงปลอดภัยไซเบอร์เป็นการแข่งขันชิงธงสะสมคะแนน (Capture The Flag - CTF) จากการแก้ไขปัญหาโจทย์ (Jeopardy)

3.5.2 ผู้ขายต้องจัดเตรียมสถานการณ์ภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อหน่วยงานด้านความมั่นคงของรัฐควบคู่กับการออกแบบโจทย์การแข่งขันทักษะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จะต้องครอบคลุมเรื่องดังต่อไปนี้ (1) การรหัส (Cryptography) (2) การตรวจประเมินและเจาะช่องโหว่เว็บแอปพลิเคชัน (Web Application Exploitation) (3) การถอดชุดคำสั่งโปรแกรมคอมพิวเตอร์ด้วยวิธีการวิศวกรรมย้อนกลับ (Reverse Engineering) (4) การโจมตีช่องโหว่โปรแกรมไบนารี (Binary Exploitation) (5) การพิสูจน์พยานหลักฐานดิจิทัล (Digital Forensics) (6) การเขียนโปรแกรม (Programming) (7) หมวดอื่น ๆ (Miscellaneous)

3.5.3 ผู้ขายต้องจัดเตรียมระบบจัดเก็บข้อมูลผู้เข้าร่วมการแข่งขันทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์ โจทย์ทดสอบทักษะ และธง (Flag) โดยระบบสามารถแสดงผลคะแนนของผู้เข้าร่วมการแข่งขันทักษะด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ได้

3.5.4 ผู้ขายต้องจัดเตรียมระบบคอมพิวเตอร์และระบบเครือข่ายที่ใช้ในการแข่งขันทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์ให้สามารถใช้งานได้อย่างมีประสิทธิภาพ

3.5.5 ผู้ขายต้องอธิบายหรือเฉลยโจทย์การแข่งขันทักษะด้านความมั่นคงปลอดภัยไซเบอร์หลังจากเสร็จสิ้นการแข่งขันให้แก่ผู้เข้าร่วมการแข่งขันให้เกิดความเข้าใจในวิธีการตอบโจทย์

3.6 รายละเอียดการจัดงานการแข่งขันทักษะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

3.6.1 จัดทำสื่อประชาสัมพันธ์ก่อนกำหนดการแข่งขันอย่างน้อย 30 วัน เพื่อประชาสัมพันธ์กิจกรรมการแข่งขันทักษะด้านความมั่นคงปลอดภัยไซเบอร์ ดังนี้ (1) โปสเตอร์ ขนาด A3 จำนวน 5 แผ่น (2) สแตนดี้ ขนาด 60 x 160 ซม. จำนวน 5 ชิ้น

3.6.2 จัดหาสถานที่สำหรับการจัดการแข่งขันทักษะด้านความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสม โดยเป็นโรงแรมไม่น้อยกว่า 3 ดาว มีห้องประชุมพร้อมสิ่งอำนวยความสะดวกสำหรับการแข่งขันทักษะด้านความมั่นคงปลอดภัยไซเบอร์ เช่น เครื่องคอมพิวเตอร์สำหรับจัดการแข่งขัน เครื่องฉายภาพ/จอแสดงภาพ ระบบเครื่องขยายเสียง มีปลั๊กไฟรองรับการใช้คอมพิวเตอร์ในการแข่งขันทักษะด้านความมั่นคงปลอดภัยไซเบอร์อย่างเพียงพอ มีสัญญาณอินเทอร์เน็ตไร้สาย (Wi-Fi) โต๊ะและเก้าอี้ โดยเป็นสถานที่ที่มีความปลอดภัยและเดินทางได้สะดวกในเขตพื้นที่ภาคตะวันออก ทั้งนี้ การจัดห้องประชุมจะต้องจัดในรูปแบบวิถีชีวิตใหม่ (New Normal) สามารถรองรับผู้เข้าร่วมกิจกรรมได้ไม่ต่ำกว่า 50 คน

3.6.3 จัดสถานที่สำหรับแข่งขันทักษะด้านความมั่นคงปลอดภัยไซเบอร์ให้มีจุดลงทะเบียน ป้ายฉากหลัง (backdrop) และป้ายอื่นๆ ประดับตกแต่งภายในสถานที่ฝึกอบรมและจุดอื่นๆ ให้เหมาะสมตามมาตรฐาน ตลอดระยะเวลาการแข่งขันทักษะด้านความมั่นคงปลอดภัยไซเบอร์

3.6.4 จัดให้มีอุปกรณ์สำหรับการแข่งขันทักษะด้านความมั่นคงปลอดภัยไซเบอร์ ตลอดจนสื่อการสอนหรือเอกสารประกอบการแข่งขันทักษะด้านความมั่นคงปลอดภัยไซเบอร์

3.6.5 จัดหาพิธีกรดำเนินงานในช่วงการแข่งขัน 1 คน และเจ้าหน้าที่ประสานงาน 5 คน

3.6.6 จัดทำเสื้อโปโลอย่างน้อย 1 สี ปักโลโก้ขนาดอย่างน้อย 1 นิ้ว จำนวนอย่างน้อย 1 ตำแหน่ง สำหรับผู้ร่วมงาน จำนวน 50 ตัว

3.6.7 จัดทำป้ายมอบรางวัล จำนวน 3 ป้ายและป้ายผ้าถือถ่ายรูปสำหรับผู้เข้าร่วมงาน 1 ป้าย

3.6.8 จัดทำป้ายประชาสัมพันธ์ Roll up ขนาด 80 x 200 ซม. จำนวน 2 ป้าย

3.6.9 จัดทำ Pull Frame Backdrop ขนาดอย่างน้อย 3 x 3 เมตร จำนวน 1 ชิ้น

3.6.10 จัดเตรียมอาหารและเครื่องดื่มสำหรับผู้เข้าแข่งขันทักษะด้านความมั่นคงปลอดภัยไซเบอร์และผู้ที่เกี่ยวข้องทุกวันตลอดการอบรม ได้แก่ (1) อาหารว่างวันละ 2 มื้อ เช้า-บ่าย รวม 5 มื้อ (2) อาหารมื้อเช้า 2 มื้อ (3) อาหารกลางวัน 3 มื้อ และ (4) อาหารเย็น 2 มื้อ

3.6.11 จัดให้มียานพาหนะปรับอากาศคุณภาพดี มีความปลอดภัยสูง พร้อมคนขับและน้ำมันเชื้อเพลิงเพื่อใช้ในการเดินทางของผู้จัดและผู้เข้าร่วมการแข่งขัน ในพื้นที่ระหว่างกรุงเทพมหานครและสถานที่จัดการแข่งขันทักษะด้านความมั่นคงปลอดภัยไซเบอร์ วันละ 1 - 2 คันตามจำนวนคนที่เหมาะสมในแต่ละวัน ตั้งแต่วันก่อนอบรม 1 วันจนถึงวันสิ้นสุดการอบรม รวม 3 วัน

3.6.12 จัดให้มีเข็มกลัดที่ระลึกการเข้าร่วมการแข่งขันทักษะด้านความมั่นคงปลอดภัยไซเบอร์แก่ผู้เข้าร่วมงานอย่างน้อย 100 ชิ้น โดยผู้ว่าจ้างเป็นผู้กำหนดรูปแบบเข็มกลัดที่ระลึก

3.6.13 จัดให้มีประกาศนียบัตรพร้อมปกประกาศสำหรับผู้เข้ารับการแข่งขันทักษะด้านความมั่นคงปลอดภัยไซเบอร์ โดยทางผู้ขายต้องออกแบบให้ผู้ว่าจ้างคัดเลือก

3.6.14 จัดให้มีรางวัลสำหรับการแข่งขัน ดังนี้ (1) อันดับ 1 เงินสด 30,000 บาท จำนวน 1 รางวัล พร้อมโล่และเกียรติบัตร (2) อันดับ 2 เงินสด 20,000 บาท จำนวน 1 รางวัล พร้อมโล่และเกียรติบัตร และ (3) อันดับ 3 เงินสด 10,000 บาท จำนวน 1 รางวัล พร้อมโล่และเกียรติบัตร

3.6.15 จัดให้มีการบันทึกวิดีโอตลอดการแข่งขันทักษะด้านความมั่นคงปลอดภัยไซเบอร์ และมีภาพถ่ายในพิธีเปิด พิธีปิด และภาพถ่ายระหว่างการแข่งขันทักษะด้านความมั่นคงปลอดภัยไซเบอร์เป็นระยะ ไว้ใช้เผยแพร่ประชาสัมพันธ์หลังการจัดงาน (ตัดต่อเป็นวิดีโอความยาวไม่เกิน 3 นาที)

3.6.16 วิทยากรออกแบบโจทย์การแข่งขัน ต้องมีคุณวุฒิไม่ต่ำกว่าปริญญาโท ในสาขาวิศวกรรมคอมพิวเตอร์ หรือวิศวกรรมไฟฟ้า หรือวิทยาศาสตร์คอมพิวเตอร์ หรือ วิทยาศาสตร์เทคโนโลยีสารสนเทศ หรือสาขาวิชาอื่นที่เกี่ยวข้อง และมีประสบการณ์ปฏิบัติงานในสาขาดังกล่าวมาแล้วไม่ต่ำกว่า 10 ปี จำนวนไม่น้อยกว่า 1 คน

3.6.17 การจัดเตรียมบุคลากรเพื่อปฏิบัติหน้าที่ต่าง ๆ ตลอดระยะเวลาการจัดการแข่งขัน ดังนี้

3.6.17.1 ผู้ประสานงานหลัก จำนวน 2 คน ทำหน้าที่ประสานงานหลักและบริหารจัดการกิจกรรมโดยรวมทั้งหมดให้เป็นไปด้วยความเรียบร้อย ตลอดระยะเวลาตามสัญญาจ้าง

3.6.17.2 เจ้าหน้าที่เทคนิคจำนวน 3 คน สนับสนุนวิทยากรภาคปฏิบัติ ตลอดจนอำนวยความสะดวกต่าง ๆ ระหว่างการจัดการแข่งขันให้แก่ผู้เข้าร่วมการแข่งขัน

3.6.17.3 พิธีกร จำนวน 1 คน ทำหน้าที่ดำเนินรายการ ตั้งแต่การลงทะเบียนเข้าร่วมกิจกรรมการศึกษาดูงาน การแข่งขันทักษะด้านความมั่นคงปลอดภัยไซเบอร์ และการจัดกิจกรรมสันทนาการ

3.6.17.4 ช่างภาพและช่างกล้องวิดีโอ จำนวน 1 คน ทำหน้าที่ถ่ายภาพและบันทึกวิดีโอตลอดการจัดกิจกรรมการแข่งขันทักษะด้านความมั่นคงปลอดภัยไซเบอร์ รวมทั้งนำภาพและวิดีโอที่ได้บันทึกไปจัดทำสื่อประชาสัมพันธ์การจัดกิจกรรมของงานหลังเสร็จสิ้นการแข่งขัน

3.6.18 จัดให้มีกิจกรรมศึกษาดูงานให้กับผู้เข้าร่วมการแข่งขันทักษะด้านความมั่นคงปลอดภัยไซเบอร์นอกสถานที่ อย่างน้อย 1 ชั่วโมง ตามที่สำนักข่าวกรองแห่งชาติกำหนด โดยจะต้องจัดหายานพาหนะปรับอากาศพร้อมคนขับ จำนวนไม่น้อยกว่า 2 คัน เพื่อใช้เดินทางไปยังสถานที่ดูงาน และจะต้องจัดหาของที่ระลึกให้เหมาะสม เพื่อมอบให้กับสถานที่ดูงาน

3.6.19 จัดให้มีที่พักที่เดียวกับสถานที่จัดการแข่งขันทักษะด้านความมั่นคงปลอดภัยไซเบอร์ จำนวนไม่ต่ำกว่า 25 ห้อง ในอัตราห้องละไม่เกิน 1,500 บาทต่อคืน (จำนวน 2 คืน รวมอาหารเช้า) สำหรับผู้เข้าร่วมการแข่งขันและคณะของผู้ว่าจ้าง (เจ้าหน้าที่อำนวยการและผู้บริหารของสำนักข่าวกรองแห่งชาติ รวมถึงทีมวิทยากร) โดยพักสองคนต่อหนึ่งห้อง เว้นแต่เป็นกรณีที่ไม่เหมาะสมจะพักรวมกันหรือมีเหตุจำเป็นที่ไม่สามารถพักรวมกับผู้อื่นได้ ซึ่งขนาดห้องพักจะต้องมีพื้นที่ไม่น้อยกว่า 30 ตารางเมตร

3.6.20 จัดให้มีกิจกรรมสันทนาการระหว่างหรือหลังอาหารเย็นในวันแข่งขันทักษะด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อเป็นการสร้างความสัมพันธ์ระหว่างผู้เข้าร่วมการแข่งขัน

3.6.21 จัดให้การตรวจหาเชื้อไวรัสโคโรนา 2019 (COVID-19) แบบ Antigen Test Kit (ATK) สำหรับผู้เข้าร่วมการแข่งขันทักษะด้านความมั่นคงปลอดภัยไซเบอร์ก่อนเดินทาง

3.6.22 จัดทำทำเนียบรุ่นผู้เข้าร่วมการแข่งขัน ประกอบด้วย ชื่อ นามสกุล รูปถ่าย หน่วยงาน ชื่อทีม และข้อมูลติดต่อ อาทิ ที่อยู่ เบอร์โทรศัพท์ social media account ในรูปแบบไฟล์ดิจิทัล โดยดำเนินการให้แล้วเสร็จ พร้อมเผยแพร่ก่อนสิ้นสุดการแข่งขัน

3.6.23 จัดให้มีการประเมินความพึงพอใจและประโยชน์ที่ได้รับจากการแข่งขัน เมื่อสิ้นสุดการแข่งขัน

3.7 กำหนดการกิจกรรมการแข่งขันทักษะด้านความมั่นคงปลอดภัยไซเบอร์ดังตารางที่ 5

ตารางที่ 5 กำหนดการแข่งขันทักษะด้านความมั่นคงปลอดภัยไซเบอร์

เวลา	กำหนดการ
วันที่ 1	
07.30 – 08.30 น.	ลงทะเบียนเข้าร่วมกิจกรรมและตรวจเชื้อไวรัสโคโรนา 2019 (COVID-19)
08.30 – 10.00 น.	เดินทางไปยังสถานที่ศึกษาดูงาน
10.00 – 12.00 น.	ศึกษาดูงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ภาคตะวันออก
12.00 – 14.00 น.	พักรับประทานอาหารกลางวันและเดินทางไปยังสถานที่จัดการแข่งขัน
14.00 – 17.00 น.	บรรยายพิเศษ และชี้แจงกำหนดการ กฎ กติการ การแข่งขัน
17.00 – 18.30 น.	จัดเตรียมอุปกรณ์ที่ใช้ในการแข่งขัน
18.30 – 20.00 น.	รับประทานอาหารเย็น
วันที่ 2	
07.00 – 08.30 น.	รับประทานอาหารเช้า
08.00 – 08.30 น.	ลงทะเบียนเข้าร่วมการแข่งขัน
08.30 – 09.00 น.	พิธีเปิดการแข่งขัน
09.00 – 12.00 น.	การแข่งขันทักษะด้านความมั่นคงปลอดภัยไซเบอร์แบบ CTF
12.00 – 13.00 น.	พักรับประทานอาหารกลางวัน
13.00 – 17.00 น.	การแข่งขันทักษะด้านความมั่นคงปลอดภัยไซเบอร์แบบ CTF (ต่อ)
17.00 – 18.30 น.	สรุปผลการแข่งขัน
18.30 – 21.00 น.	รับประทานอาหารเย็นและกิจกรรมสันทนาการ
วันที่ 3	
07.00 – 08.30 น.	รับประทานอาหารเช้า
08.30 – 10.30 น.	บรรยายสรุป อธิบายเฉลยโจทย์ปัญหา CTF
10.30 – 11.30 น.	พิธีมอบรางวัล ประกาศนียบัตร และปิดการแข่งขัน
11.30 – 13.00 น.	รับประทานอาหารกลางวัน
13.00 – 16.00 น.	เดินทางกลับสำนักข่าวกรองแห่งชาติ

หมายเหตุ *กำหนดการอาจมีการปรับเปลี่ยนตามความเหมาะสม*

1. ..... ประธานคณะกรรมการ
2. ..... คณะกรรมการ
3. ..... คณะกรรมการ
4. ..... คณะกรรมการ
5. ..... คณะกรรมการและเลขานุการ

3.8 งบประมาณ จำนวน 746,000 บาท (เจ็ดแสนสี่หมื่นหกพันบาทถ้วน) ดังตารางที่ 6

ตารางที่ 6 รายละเอียดค่าใช้จ่ายการจัดกิจกรรมการแข่งขันทักษะด้านความมั่นคงปลอดภัยไซเบอร์

ลำดับ	รายละเอียดค่าใช้จ่าย	จำนวนเงิน (บาท)
1.	ค่าใช้จ่ายด้านสถานที่ - ค่าอุปกรณ์ ระบบขยายเสียง จอภาพ เครือข่ายอินเตอร์เน็ต - ค่าเช่าห้องประชุม	200,000
2.	ค่าอุปกรณ์ประชาสัมพันธ์และค่าตกแต่งสถานที่	61,000
3.	ค่าใช้จ่ายบุคลากร 3.1 ทีมวิทยากรที่มีความรู้ มีความสามารถเฉพาะทาง และประสบการณ์พิเศษ - วิทยากรบรรยายและฝึกปฏิบัติ จำนวน 1 คน จำนวน 9 ชั่วโมง ชั่วโมงละ 3,500 บาท - เจ้าหน้าที่ทางเทคนิค จำนวน 3 คน 3.2 ทีมงาน - ผู้ควบคุมงาน จำนวน 1 คน - ช่างภาพและวีดีโอ จำนวน 1 คน - ผู้ประสานงาน จำนวน 4 คน - พิธีกร จำนวน 1 คน	167,500
4.	ค่าที่พักรวมอาหารเช้า จำนวน 22 ห้อง 2 คืน คืนละ 1,500 บาท	66,000
5.	ค่าอาหาร จำนวน 3 วัน วันละ 700 บาทต่อคน ค่าอาหารว่าง จำนวน 4 มื้อ มื้อละ 50 บาทต่อคน	101,200
6.	ค่าใช้จ่ายด้านพาหนะ - ค่าเช่ารถบัสปรับอากาศพร้อมคนขับ รวมค่าน้ำมัน ค่าผ่านทางพิเศษและที่จอด - ค่าเดินทางของวิทยากรและเจ้าหน้าที่สนับสนุนทางด้านเทคนิคโดยจ่ายตามจริง หรือในอัตรากิโลเมตรละ 4 บาท หรือไม่เกิน 1,000 บาทต่อเที่ยว	28,800
7.	ค่าใช้จ่ายอื่นๆ - เงินรางวัล - เสื้อโปโล 50 ตัว - เข็มกลัด 100 อัน - โล่ห์และเกียรติบัตร 3 ชุด	121,500

1. ..... ประธานคณะกรรมการ
2. ..... คณะกรรมการ
3. ..... คณะกรรมการ
4. ..... คณะกรรมการ
5. ..... คณะกรรมการและเลขานุการ

ลำดับ	รายละเอียดค่าใช้จ่าย	จำนวนเงิน (บาท)
	- ค่าเอกสารและวัสดุอุปกรณ์ - ค่าบริการตรวจหาเชื้อไวรัสโคโรนา - 2019	
	รวมเป็นเงินทั้งสิ้น	746,000

3.9 การประเมินผล

3.9.1 ร้อยละ 80 ของผู้เข้าร่วมการแข่งขันมีทักษะด้านความมั่นคงปลอดภัยไซเบอร์เพิ่มขึ้นในระดับมาก – มากที่สุด

3.9.2 ร้อยละ 80 ของผู้เข้าร่วมการแข่งขันมีความพึงพอใจต่อประโยชน์ที่ได้รับของการจัดกิจกรรมการแข่งขันทักษะด้านความมั่นคงปลอดภัยไซเบอร์

3.10 ผลที่คาดว่าจะได้รับ

3.10.1 ผู้เข้าร่วมการแข่งขันได้รับการพัฒนาทักษะด้านความมั่นคงปลอดภัยไซเบอร์

3.10.2 เสริมสร้างและพัฒนาสัมพันธ์ระหว่างผู้ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในกลุ่มหน่วยงานด้านความมั่นคงของรัฐ ให้สามารถประสานงานและปฏิบัติงานร่วมกันในการป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ

---

1. ..... ประธานคณะกรรมการ
2. ..... คณะกรรมการ
3. ..... คณะกรรมการ
4. ..... คณะกรรมการ
5. ..... คณะกรรมการและเลขานุการ