ขอบเขตงาน (Term of Reference : TOR)
โครงการซื้อระบบจัดเก็บข้อมูลการจราจรคอมพิวเตอร์ จำนวน 1 ระบบ

1. หลักการและเหตุผล

ฝ่ายเทคโนโลยีดิจิทัล สถาบันเทคโนโลยีนิวเคลียร์แห่งชาติ (องค์การมหาชน) เป็นมีหน้าที่รับผิดชอบด้านการให้บริการระบบสารสนเทศและโครงสร้างพื้นฐานและความมั่นคงปลอดภัยสารสนเทศ เนื่องด้วยระบบจัดเก็บข้อมูลจราจรทางระบบเครือข่ายคอมพิวเตอร์ของสถาบัน มีอายุการใช้งานเกิน 5 ปีแล้ว และมีฟังก์ชันการทำงานไม่ครอบคลุมตาม พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 ทำให้ระบบสารสนเทศและระบบเครือข่ายของสถาบันมีความเสี่ยงจากภัยคุกคามด้านไซเบอร์ อาจจะสร้างความเสียหายต่อการดำเนินงานด้านดิจิทัลและภาพลักษณ์ขององค์กร เพื่อให้มีความพร้อมในการรับมือ และลดผลกระทบต่อองค์กรโดยรวม เพื่อป้องกันภัยคุกคามที่จะเกิดขึ้น จึงมีความประสงค์จัดหาระบบที่สามารถจัดเก็บข้อมูลจราจรระบบเครือข่ายคอมพิวเตอร์ ตรวจจับและตอบสนองต่อภัยคุกคาม (Security Information and Event Management :SIEM) รวมไปถึงผู้ให้บริการ Security Operation Center :SOC พร้อม เพื่อให้เป็นตามข้อกำหนดของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 และให้เป็นไปตามนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ ของสถาบัน

2. วัตถุประสงค์

2.1 เพื่อเพิ่มประสิทธิภาพด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศขององค์กร

2.2 เพื่อจัดทำการตามข้อกำหนดของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 และพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยทาง ไซเบอร์ พ.ศ. 2562 ตามหน่วยงานโครงสร้างพื้นฐานที่ได้มีการประกาศไว้ในกฎหมาย

2.3 เพื่อจัดทำการบันทึก Log File แบบศูนย์กลาง (Centralized Log Management System) ของระบบเทคโนโลยีสารสนเทศและอุปกรณ์เครือข่ายของทางองค์กร โดยสามารถสืบค้นย้อนหลัง เพื่อระบุหาสาเหตุของปัญหาในกรณีที่เกิดภัยคุกคามทางไซเบอร์ได้

2.4 เพื่อจัดเก็บข้อมูลจราจรคอมพิวเตอร์ให้ครบถ้วนทุกโซนที่มีความสำคัญในองค์กร และสามารถรองรับข้อมูลขนาดใหญ่ได้อย่างมีประสิทธิภาพ

2.5 เพื่อบริการเฝ้าระวังและแจ้งเตือนภัยคุกคามทางไซเบอร์ หากพบเหตุการณ์ที่ผิดปกติและมีความรุนแรงระบบเทคโนโลยีสารสนเทศ

2.6 เพื่อป้องกันความเสียหายและลดผลกระทบที่จะเกิดขึ้นจากภัยคุกคามทางไซเบอร์ พร้อมบริการจัดการเหตุการณ์ความมั่นคงปลอดภัยให้ระบบสามารถให้บริการได้อย่างต่อเนื่องและมีประสิทธิภาพ

3. คุณสมบัติของผู้ยื่นข้อเสนอ

3.1 คุณสมบัติทั่วไป

3.1.1 มีความสามารถตามกฎหมาย

3.1.2 ไม่เป็นบุคคลล้มละลาย

3.1.3 ไม่อยู่ระหว่างเลิกกิจการ

3.1.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.1.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอานาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.1.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกาหนดในราชกิจจานุเบกษา

3.1.7 เป็นนิติบุคคลผู้มีอาชีพในงานที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

3.1.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่หน่วยงานของรัฐ ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

3.1.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์ความคุ้มกันเช่นว่านั้น

3.1.10 ผู้รับจ้างที่ยื่นข้อเสนอในรูปแบบของ "กิจการร่วมค้า" ต้องมีคุณสมบัติดังนี้

(1) กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงฯจะต้องมีการกำหนดสัดส่วนหน้าที่ และความรับผิดชอบในปริมาณงาน สิ่งของ หรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

(2) กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก กิจการร่วมค้านั้นต้องใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

(3) สำหรับข้อตกลงฯ ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมค้าหลัก ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน

3.1.11 ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ ดังนี้

(1) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยซึ่งได้จดทะเบียนเกินกว่า 1 ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิ ที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก 1 ปีสุดท้ายก่อนวันยื่นข้อเสนอ

(2) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ให้พิจารณาการกำหนดมูลค่าของทุนจดทะเบียน โดยผู้ยื่นข้อเสนอจะต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอไม่ต่ำกว่า 1 ล้านบาท

(3) สำหรับการจัดซื้อจัดจ้างครั้งหนึ่งที่มีวงเงินเกิน 500,000 บาทขึ้นไป กรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดา ให้พิจารณาจากหนังสือรับรองบัญชีเงินฝากไม่เกิน 90 วัน ก่อนวันยื่น ข้อเสนอ โดยต้องมีเงินฝากคงเหลือในบัญชีธนาคารเป็นมูลค่า 1 ใน 4 ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง และหากเป็นผู้ชนะการจัดซื้อจัดจ้าง หรือเป็นผู้ได้รับการคัดเลือกจะต้องแสดงหนังสือรับรองบัญชีเงินฝากที่มีมูลค่าดังกล่าวอีกครั้งหนึ่งในวันลงนามสัญญา

(4) กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ 1 ใน 4 ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง (สินเชื่อที่ธนาคารภายในประเทศหรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้าประกันตามประกาศของธนาคารแห่งประเทศไทยตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรอง หรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอนับถึงวันยื่นข้อเสนอไม่เกิน 90 วัน)

(5) กรณีตาม (1) – (4) ยกเว้นสำหรับกรณีดังต่อไปนี้

(5.1) กรณีที่ผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐ

(5.2) นิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการตามพระราชบัญญัติล้มละลาย (ฉบับที่ 10) พ.ศ. 2561

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

3.2 คุณสมบัติอื่นๆ

ผู้ยื่นข้อเสนอต้องมีผลงานประเภทระบบจัดเก็บข้อมูลจราจรทางระบบเครือข่ายคอมพิวเตอร์หรือระบบการจัดการรักษาความปลอดภัยขององค์กร Security Information & Event Management (SIEM) หรือบริการ Security Operation Center :SOC หรือผลงานอื่นที่เกี่ยวข้องกับการบำรุงรักษาความมั่นคงปลอดภัยระบบเครือข่าย หรือช่องโหว่ระบบสารสนเทศ กับหน่วยงานราชการหรือรัฐวิสาหกิจหรือเอกชนที่น่าเชื่อถือได้ จำนวนไม่น้อยกว่า 1 ผลงาน ดังนี้

3.2.1 ผลงานการซื้อหรือเช่าต้องมีวงเงินไม่น้อยกว่า 1,00,000 บาท (หนึ่งล้านบาทถ้วน) ต่อสัญญา และจะต้องเป็นผลงานที่แล้วเสร็จจำนวน ไม่เกิน 3 ปี นับถึงวันยื่นเสนอราคา

3.2.2 ทั้งนี้ผู้ยื่นข้อเสนอจะต้องจัดส่งหนังสือรับรองผลงาน ดังกล่าวแนบมาในวันที่ยื่นเสนอราคา

4. รายละเอียดคุณลักษณะทั่วไปหรือขอบเขตของงานจ้าง

ผู้ยื่นข้อเสนอจะต้องดำเนินการตามโครงการซื้อระบบจัดเก็บข้อมูลจราจรทางระบบเครือข่ายคอมพิวเตอร์ มีรายละเอียดดังต่อไปนี้

4.1 คุณลักษณะทั่วไป

4.1.1 ผู้ยื่นข้อเสนอจะต้องมีการเฝ้าระวังแบบ 24x7 SOC มีทีมงานและระบบที่ทำงานอย่างต่อเนื่อง 24 ชั่วโมงต่อวัน 7 วันต่อสัปดาห์ ในการตรวจสอบและตอบสนองต่อภัยคุกคามที่เกิดขึ้นในเครือข่ายและระบบเทคโนโลยีสารสนเทศ ของสถาบัน

4.1.2 มีระบบแจ้งเตือนขั้นสูง โดยใช้เทคโนโลยีและอัลกอริทึมที่ทันสมัยในการวิเคราะห์ข้อมูล หากพบกิจกรรมที่ผิดปกติหรือตรงตามเกณฑ์ที่กำหนด SOC จะส่งการแจ้งเตือนไปยังทีมผู้ดูแลระบบทันที

4.1.3 มีทีมผู้เชี่ยวชาญด้านความปลอดภัย SOC ประกอบด้วยทีมงานที่มีความรู้ความเชี่ยวชาญในด้านความปลอดภัยทางไซเบอร์ ซึ่งมีการฝึกอบรมและพัฒนาความรู้อย่างต่อเนื่อง เพื่อรับมือกับภัยคุกคามใหม่ๆ

4.1.4 มีการทำงานร่วมกับหน่วยงานอื่น เพื่อให้การดำเนินการตอบสนองเป็นไปอย่างมีประสิทธิภาพ SOC สามารถทำงานร่วมกับหน่วยงานภายนอก เช่น ผู้ให้บริการเครือข่าย หน่วยงานบริการด้านความปลอดภัย หรือหน่วยงานรัฐบาล

4.1.5 ระบบ SIEM ที่นำเสนอ ต้องสามารถใช้งานได้ตามข้อเสนอของโครงการทุกฟังก์ชันหลังหมดระยะเวลาสัญญาโดยไม่มีค่าใช้จ่ายเพิ่มเติมใดๆ

4.1.6 ผู้ยื่นข้อเสนอจะต้องจัดส่งเอกสารรายละเอียดตามข้อกำหนดที่ 4 และ 5 แนบมาในวันที่ยื่นเสนอราคา

4.2 รายละเอียดคุณลักษณะเฉพาะของระบบ

ระบบ Security Information and Event Management (SIEM) จำนวน 1 ระบบ มีคุณสมบัติอย่างน้อยดังนี้

4.2.1 ระบบ SIEM ที่นำเสนอต้องสามารถรองรับการติดตั้งและสามารถใช้งานได้อย่างมีประสิทธิภาพภาพ บนระบบเครื่องแม่ข่ายแบบเสมือน VMWare หรือ Nutanix หรือ Proxmox ได้เป็นอย่างน้อย โดยเครื่องแม่ข่ายแบบเสมือน และระบบเครือข่ายจัดเตรียมโดยสถาบัน

4.2.2 ระบบ SIEM ต้องเป็นแพลตฟอร์มที่รองรับการวิเคราะห์ข้อมูลแบบเรียลไทม์และสามารถบันทึกเหตุการณ์ย้อนหลังได้ไม่น้อยกว่า 90 วัน ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560

4.2.3 สามารถเก็บรวบรวม (Ingest) และประมวลผลข้อมูลจากหลายแหล่ง เช่น Syslog, Windows Event Log, Network Traffic, และ Security Events

4.2.4 รองรับการค้นหาข้อมูลด้วยภาษา Query ที่ทรงพลัง เช่น Query DSL

4.2.5 สามารถวิเคราะห์ข้อมูลเชิงลึกด้วย Machine Learning และมีฟีเจอร์ Anomaly Detection

4.2.6 รองรับการแสดงผลข้อมูลและสร้าง Dashboard แบบ Interactive Visualization ผ่าน Web-based UI

4.2.7 มีความสามารถในการตั้งค่า Rule-based Alerting และ Threshold Alerting สำหรับการแจ้งเตือนเหตุการณ์ที่น่าสงสัย

4.2.8 รองรับการปรับขนาด (Scalability) ตามปริมาณข้อมูลที่เพิ่มขึ้น โดยใช้โครงสร้างพื้นฐานที่สามารถขยายตัวได้ (Distributed Cluster Architecture)

4.2.9 รองรับการทำ Data Enrichment เพื่อนำข้อมูลเสริมมาใช้ในการวิเคราะห์ภัยคุกคาม

4.2.10 มี API สำหรับการเชื่อมต่อกับระบบภายนอกและรองรับการ Integrate กับ Threat Intelligence Feeds

4.2.11 ผู้ยื่นข้อเสนอต้องจัดทำคู่มือการใช้งานสำหรับผู้ดูแลระบบ และจัดให้มีการอบรมการใช้งานระบบ โดยรองรับผู้เข้าอบรมไม่น้อยกว่า 3 คน

4.2.12 การอบรมสามารถดำเนินการได้ทั้ง Online หรือ มาอบรม ณ สถาบัน ทั้งนี้ขึ้นอยู่กับสถาบันเป็นผู้กำหนด โดยไม่คิดค่าใช้จ่ายใดๆเพิ่มกับสถาบัน

5. ขอบเขตการดำเนินงาน

ผู้ยื่นข้อเสนอต้องดำเนินการจัดทำเอกสารกระบวนการรองรับเหตุการณ์หรือภัยคุกคามทางไซเบอร์ โดยอ้างอิงจาก เอกสาร Cybersecurity Operations Center จากหน่วยงาน MITRE และเอกสาร NIST Special Publication 800-61 Computer Security Incident Handling Guide และต้องประกอบด้วยการกำหนด Procedure และ คู่มือ ของผู้ปฏิบัติงานแต่ละคน ในแต่ละ tier รวมถึง กระบวนการรองรับและตอบสนอง ดังนี้

5.1 เหตุการณ์ทางไซเบอร์เมื่อมีการตรวจพบหรือแจ้งเหตุการณ์บุกรุกระบบสารสนเทศของสถาบันจากหน่วยงานภายนอก หรือหน่วยงานด้านความมั่นคงอื่นๆ

5.2 เหตุการณ์ทางไซเบอร์เมื่อตรวจพบการโจมตีแบบ DDoS กับอุปกรณ์รักษาความปลอดภัยอุปกรณ์เครือข่าย เว็บไซต์ รวมทั้งระบบงานสารสนเทศภายในสถาบัน

5.3 เหตุการณ์ทางไซเบอร์เมื่อตรวจพบการโจมตีด้วยโปรแกรมมัลแวร์ต่างๆ กับอุปกรณ์รักษาความปลอดภัยอุปกรณ์เครือข่าย เว็บไซต์ รวมทั้งระบบงานสารสนเทศภายในสถาบัน

5.4 เหตุการณ์ทางไซเบอร์เมื่อตรวจพบการโจมตีด้วยแรนซัมแวร์ (Ransomware) กับระบบคอมพิวเตอร์ในศูนย์ข้อมูลหลัก (Data Center) เว็บไซต์ รวมทั้งระบบงานสารสนเทศ ภายในสถาบัน

5.5 เหตุการณ์ทางไซเบอร์เมื่อตรวจพบการโจมตีหรือถูกบุกรุกเพื่อการเปลี่ยนแปลงหน้าเว็บเพจ (Web Defacement) กับระบบเว็บไซต์ ของสถาบัน

5.6 เหตุการณ์ทางไซเบอร์เมื่อตรวจพบการโจมตีแบบ SQL Injection และ Cross Site Script กับระบบเว็บไซต์ของสถาบัน

5.7 เหตุการณ์ทางไซเบอร์เมื่อตรวจพบการโจมตีหรือบุกรุกระบบฐานข้อมูล ได้แก่ Oracle, MySQL และ MS-SQL Server กับระบบงานสารสนเทศภายในสถาบัน

5.8 เหตุการณ์ทางไซเบอร์เมื่อตรวจพบการโจมตีหรือบุกรุกเครื่องแม่ข่ายภายในสถาบัน ด้วยวิธีการเดาสุ่ม password (brute force)

5.9 เหตุการณ์ทางไซเบอร์เมื่อตรวจพบการที่อุปกรณ์รักษาความปลอดภัย อุปกรณ์เครือข่าย มีปัญหาการส่งข้อมูลให้กับระบบจัดเก็บและวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ (Security Incident Event Management: SIEM)

5.10 ดำเนินการตั้งค่าระบบเฝ้าระวังภัยคุกคามไซเบอร์ของสถาบัน ให้สามารถกำหนดเงื่อนไขรูปแบบการเฝ้าระวังและตรวจจับภัยคุกคาม (Use Case) ตามที่ได้ทำการประเมินและตกลง

ร่วมกับสถาบัน ได้ไม่น้อยกว่า 10 Use Case พร้อมจัดทำรายงานสรุปรูปแบบการเฝ้าระวังและตรวจจับภัยคุกคาม (Use Case)

5.11 ผู้รับจ้างต้องดำเนินการกำหนดกระบวนการปฏิบัติของเจ้าหน้าที่ ในรูปแบบของแผนรองรับเหตุการณ์หรือภัยคุกคามทางไซเบอร์ (Known Threat Incident Response Plan) ซึ่งรวมถึงแนวทางการประสานการปฏิบัติกับหน่วยงานที่เกี่ยวข้อง เพื่อรองรับและตอบสนองต่อเหตุการณ์หรือภัยคุกคามทางไซเบอร์ โดยมีรายละเอียดอย่างน้อย ดังนี้

5.11.1 ขั้นตอนการตรวจจับการวิเคราะห์ภัยคุกคาม (Detection and Analysis) ประกอบด้วยการเฝ้าระวัง การตรวจสอบรายละเอียดเกี่ยวกับเหตุการณ์หรือภัยคุกคามทางไซเบอร์การวิเคราะห์เหตุการณ์หรือภัยคุกคาม กระบวนการบันทึกผลการวิเคราะห์เหตุการณ์หรือภัยคุกคาม การจัดลำดับความสำคัญของเหตุการณ์หรือภัยคุกคาม ที่ต้องจัดการ การรายงานเบื้องต้นเกี่ยวกับเหตุการณ์หรือภัยคุกคามให้ผู้ที่เกี่ยวข้องทราบ

5.11.2 ขั้นตอนการจำกัดความเสียหาย การกำจัดภัยคุกคาม การกู้คืนระบบ (Containment, Eradication and Recovery) อันประกอบด้วยการเก็บและรวบรวมหลักฐานเกี่ยวกับเหตุการณ์หรือภัยคุกคาม การจำกัดเหตุการณ์หรือภัยคุกคามไม่ให้สร้างความเสียหายเพิ่มเติม การกำจัดเหตุการณ์หรือภัยคุกคาม การกู้คืนระบบ จากความเสียหายที่เกิดจากเหตุการณ์หรือภัยคุกคาม

5.11.3 ขั้นตอนการปฏิบัติหลังจากการตอบสนองต่อเหตุการณ์เสร็จสิ้น (Post-incident Activity) ประกอบด้วยการจัดทำรายงานผลการดำเนินการตอบสนองกับเหตุการณ์หรือ ภัยคุกคามการเรียนรู้บทเรียนจากการตอบสนองต่อเหตุการณ์หรือภัยคุกคาม การจัดทำชุดข้อมูลสำหรับใช้ฝึกกระบวนการรองรับและตอบสนอง ต่อ เหตุการณ์ (Known Threat Incident Response Drill) การปรับปรุงข่าวกรองด้านภัยคุกคามทางไซเบอร์

5.11.4 รวบรวมข้อมูลความเสี่ยงของระบบสารสนเทศของสถาบัน จากเหตุการณ์หรือภัยคุกคาม การปรับปรุง มาตรวัดประสิทธิภาพ และประสิทธิผลในการดำเนินการ

5.11.5 ผู้ยื่นข้อเสนอต้องดำเนินการ Vulnerability Assessment (VA Scan) ตรวจสอบและระบุช่องโหว่ของระบบเครือข่าย เว็บไซต์ รวมถึงระบบสารสนเทศ ตามที่สถาบันกำหนด พร้อมจัดทำรายงาน ตลอดจนแนะนำ เป็นที่ปรึกษาในการแนะนำ การแก้ไขช่องโหว่ให้กับเจ้าหน้าที่ดูแลระบบของสถาบัน จำนวนไม่น้อยกว่า 2 ครั้งต่อปี ตลอดจนสิ้นสุดสัญญา

5.11.6 ผู้ยื่นข้อเสนอต้องดำเนินการทดสอบเจาะระบบ (Penetration Testing) เพื่อประเมินความเสี่ยงด้วยการเพื่อค้นหาจุดอ่อนของระบบเครือข่าย เว็บไซต์ รวมถึงระบบสารสนเทศ ตามที่สถาบันกำหนด พร้อมจัดทำรายงาน ตลอดจนแนะนำ เป็นที่ปรึกษาในการแนะนำ การแก้ไขช่องโหว่ให้กับเจ้าหน้าที่ดูแลระบบของสถาบัน จำนวนไม่น้อยกว่า 1 ครั้งต่อปี ตลอดจนสิ้นสุดสัญญา

5.11.7 ผู้ยื่นข้อเสนอจะต้องมีเจ้าหน้าที่ปฏิบัติงาน แบบ Out Source ทำงานร่วมกับเจ้าหน้าที่ดูแลระบบของสถาบัน โดยทำงานร่วมกันปรับปรุงกระบวนการปฏิบัติงานที่เกี่ยวข้องกับการรับมือภัยคุกคามทางไซเบอร์ ได้แก่ แผนการรับมือภัยคุกคามทางไซเบอร์ กระบวนการพัฒนาและเสริมสร้างความรู้ แผนการจัดหาและรักษาบุคลากร

ไว้ในองค์กร กระบวนการในการบริหารจัดการผู้ให้บริการภายนอก กระบวนการในการบริหารจัดการ รายงานผลการปฏิบัติงานศูนย์รับมือภัยคุกคามทางไซเบอร์ โดยอ้างอิงจากมาตรฐานที่น่าเชื่อถือในระดับสากล พร้อมจัดทำเป็นเอกสารให้เรียบร้อย โดยเจ้าหน้าที่ปฏิบัติงานที่เป็น Out Source ในศูนย์ปฏิบัติการความมั่นคงปลอดภัยทางไซเบอร์ (SOC) ของผู้ยื่นข้อเสนอ ต้องมีเจ้าหน้าที่ประจำประกอบด้วยดังต่อไปนี้

5.11.7.1 เจ้าหน้าที่ปฏิบัติงานศูนย์ปฏิบัติการความมั่นคงปลอดภัยทางไซเบอร์ (SOC) ระดับงานขั้นตัน (Level-1)

5.11.7.2 เจ้าหน้าที่ปฏิบัติงานศูนย์ปฏิบัติการความมั่นคงปลอดภัยทางไซเบอร์ (SOC) ระดับงานระดับ 2 (Level-2)

5.11.7.3 เจ้าหน้าที่ปฏิบัติงานศูนย์ปฏิบัติการความมั่นคงปลอดภัยทางไซเบอร์ (SOC) ระดับหัวหน้าศูนย์ (SOC Leader)

5.11.8 เจ้าหน้าที่ปฏิบัติงานศูนย์ปฏิบัติการความมั่นคงปลอดภัยทางไซเบอร์ (CSOC) ระดับงานขั้นต้น (Level-1) จำนวนไม่น้อยกว่า 2 คน จะต้องมีคุณสมบัติ ดังต่อไปนี้

5.11.8.1 จบการศึกษาระดับปริญญาตรี หรือสูงกว่าในสาขาเทคโนโลยีสารสนเทศ วิศวกรรมคอมพิวเตอร์ หรือสาขาที่เกี่ยวข้อง

5.11.8.2 มีประสบการณ์การทำงานด้าน Cyber Security ไม่น้อยกว่า 1 ปี

5.11.9 เจ้าหน้าที่ปฏิบัติงานศูนย์ปฏิบัติการความมั่นคงปลอดภัยทางไซเบอร์ (CSOC) ระดับงานระดับ 2 (Level-2) จำนวนไม่น้อยกว่า 2 คน จะต้องมีคุณสมบัติ ดังต่อไปนี้

5.11.9.1 จบการศึกษาระดับปริญญาตรี หรือสูงกว่าในสาขา เทคโนโลยีสารสนเทศ วิศวกรรมคอมพิวเตอร์ หรือสาขาที่เกี่ยวข้อง

5.11.9.2 มีประสบการณ์การทำงานด้าน Cyber Security ไม่น้อยกว่า 2 ปี

5.11.9.3 ได้รับใบรับรอง Certificate CEH หรือ CompTIA SEC+ หรือ CompTIA CySA+ เป็นอย่างน้อย

5.11.10 เจ้าหน้าที่ปฏิบัติงานศูนย์ปฏิบัติการความมั่นคงปลอดภัยทางไซเบอร์ (CSOC) ระดับหัวหน้าศูนย์ (CSOC Leader) จำนวนไม่น้อยกว่า 1 คน จะต้องมีคุณสมบัติ ดังต่อไปนี้

5.11.10.1 จบการศึกษาระดับปริญญาตรี หรือสูงกว่าในสาขา เทคโนโลยีสารสนเทศ วิศวกรรมคอมพิวเตอร์ หรือสาขาอื่นๆ

5.11.10.2 มีประสบการณ์การทำงานด้าน Cyber Security ไม่น้อยกว่า 4 ปี

5.11.10.3 ได้รับใบรับรอง Certificate CompTIA SEC+ และ CompTIA CySA+ เป็นอย่างน้อย

5.11.11 ที่ปรึกษาและวางแผนการปฏิบัติงาน ศูนย์ปฏิบัติการความมั่นคงปลอดภัยทางไซเบอร์ (CSOC) (CSOC Consultant) จะต้องมีคุณสมบัติ ดังต่อไปนี้

5.11.11.1 จบการศึกษาระดับปริญญาโท หรือสูงกว่าในสาขา เทคโนโลยีสารสนเทศ วิศวกรรมคอมพิวเตอร์ หรือสาขาที่เกี่ยวข้อง

5.11.11.2 มีประสบการณ์การทำงานด้าน Cyber Security ไม่น้อยกว่า 9 ปี

5.11.12 มีเจ้าหน้าที่ปฏิบัติงานในศูนย์ปฏิบัติการของผู้รับจ้างตลอด 24 ชั่วโมง อย่างน้อย 2 คน มีบทบาทหน้าที่ดังต่อไปนี้

5.11.12.1 ดำเนินการวิเคราะห์เหตุการณ์ผิดปกติทางด้านบริหารจัดการระบบคอมพิวเตอร์ ระบบเครือข่ายสื่อสารและอินเทอร์เน็ต ในเรื่องที่เกี่ยวข้องกับความผิดปกติของภัยคุกคามด้านความปลอดภัยสารสนเทศ (Security Monitoring) ตลอดเวลา 24 ชั่วโมง แบบ Remote site พร้อมให้คำปรึกษาและร่วมกับเจ้าหน้าที่ดูแลระบบของสถาบัน ในการแก้ไขอุปกรณ์ที่เกี่ยวข้องเพื่อหาแนวทางการป้องกันไม่ให้เกิดเหตุการณ์ขึ้นอีก

5.11.12.2 ดำเนินการตั้งค่าระบบเฝ้าระวังภัยคุกคามไซเบอร์ของสถาบัน ให้สามารถแจ้งเตือนภัยคุกคามด้านความมั่นคงปลอดภัยผ่านทางระบบจดหมายอิเล็กทรอนิกส์ (E-Mail) หรือ Application Line หรือช่องทางการสื่อสารอื่นตามที่สถาบัน กำหนด

5.11.13 ดำเนินการจัดทำรายงานเฝ้าระวังภัยคุกคามทางไซเบอร์ (Incident Response Report) ตามที่สถาบันกำหนดหรืออย่างน้อยไม่เกิน เดือนละ 1 ครั้ง ตลอดระยะสัญญา ภายในวันที่ 7 ของเดือนถัดไป โดยต้องครอบคลุมเนื้อหาอย่างน้อยดังต่อไปนี้

5.11.13.1 ระบุประเภทของภัยคุกคาม

5.11.13.2 วัน-เวลา เริ่มต้นและสิ้นสุดของภัยคุกคาม

5.11.13.3 ระบุต้นทาง (Attacker) และปลายทาง (Target)

5.11.13.4 ให้คำแนะนำพร้อมขั้นตอนการดำเนินการแก้ไขเชิงเทคนิคและแนวทางในการป้องกันไม่ให้เกิดเหตุการณ์เดิมซ้ำอีก

5.12 การระบุระดับความรุนแรง (Severity) อ้างอิง Service Level Agreement (SLA) ตามเงื่อนไข ต่อไปนี้

ระดับความรุนแรง	เวลาในการวิเคราะห์และแจ้งเตือน
Critical	30 นาที
High	2 ชั่วโมง
Medium	6 ชั่วโมง
Low	24 ชั่วโมง

5.12.1 ดำเนินการตั้งค่าระบบเฝ้าระวังภัยคุกคามไซเบอร์ของ สถาบัน ให้สามารถกำหนดเงื่อนไขรูปแบบการเฝ้าระวังและตรวจจับภัยคุกคาม (Use Case) ตามที่ได้ทำการประเมินและตกลงร่วมกับทาง สถาบันเทคโนโลยีนิวเคลียร์แห่งชาติ ได้ไม่น้อยกว่า 10 Use Case พร้อมจัดทำรายงานสรุปรูปแบบการเฝ้าระวังและตรวจจับภัยคุกคาม (Use Case) ตามข้อกำหนด

5.12.2 ผู้รับจ้าง Out Source ในการเฝ้าระวังภัยคุกคามทางไซเบอร์ ต้องการสรุปข่าวสารที่น่าสนใจ และเป็นประโยชน์ต่อสถาบัน ทางด้าน cyber security อย่างน้อยเดือนละ 1 ครั้ง พร้อมทั้งการนำเสนอร่วมกับรายงานการตรวจจับภัยคุกคาม

5.13 การดำเนินงานทั่วไป

5.13.1 ผู้ยื่นข้อเสนอดำเนินการติดตั้งระบบและโปรแกรมตรวจจับภัยคุกคาม และ Integrate กับระบบต่างๆของทางสถาบัน พร้อมรายงานผลการดำเนินงาน เป็น

ประเภท .PDF หรือ MS-Word ในรูปแบบอิเล็กทรอนิกส์ และเอกสาร จำนวน 1 ชุด ภายใน 60 วัน นับถัดจากวันลงนามสัญญา

5.13.2 ผู้ยื่นข้อเสนอต้องให้บริการเฝ้าระวังและตรวจสอบภัยคุกคาม เป็นระยะเวลา 36 เดือน นับถัดจากวันที่ส่งมอบงานงวดที่ 1 โดยดำเนินการเฝ้าระวังและตรวจสอบภัยคุกคาม แบบ 24x7 (24 ชั่วโมง 7 วัน) และสรุปรายงานพร้อมทั้งการนำเสนอร่วมกับรายงานการตรวจจับภัยคุกคามให้กับสถาบัน อย่างน้อยเดือนละ 1 ครั้ง กำหนดส่งไม่เกินวันที่ 7 ของทุกเดือน ตลอดระยะเวลาในการดูแล

6. ระยะเวลากำหนดส่งมอบและเบิกจ่ายเงิน

การส่งมอบงานให้ส่งมอบมอบที่สถาบันเทคโนโลยีนิวเคลียร์แห่งชาติ (องค์การมหาชน) องครักษ์ และเบิกจ่ายเงินดังนี้

งวดที่ 1 ส่งมอบงานตามข้อกำหนด 5.13.1 ภายใน 60 วัน นับถัดจากวันลงนามสัญญาและให้เบิกจ่ายเงิน 20 % ของโครงการ หลังจากคณะกรรมการได้ดำเนินการตรวจรับเรียบร้อย

งวดที่ 2 ถึง 13 ส่งมอบงานตามข้อกำหนด 5.13.2 เมื่อคณะกรรมการตรวจรับพัสดุดำเนินการตรวจรับเรียบร้อย ให้แบ่งจ่ายเงินทุก 3 เดือน งวดละเท่าๆกันในวงเงิน คงเหลือของโครงการ

7. วงเงินในการจัดหา

วงเงินงบประมาณ 3,000,000 บาท (สามล้านบาทถ้วน)

8. หลักเกณฑ์การพิจารณาข้อเสนอ

เกณฑ์ราคา

9. อัตราค่าปรับ

กรณีที่ผู้ยื่นข้อเสนอไม่สามารถดำเนินการตามเวลาที่กำหนดได้ ผู้เสนอราคาจะต้องเสียค่าปรับให้แก่สถาบันเทคโนโลยีนิวเคลียร์แห่งชาติ (องค์การมหาชน) เป็นรายวันในอัตราร้อยละ 0.20 ของราคาพัสดุที่ยังไม่ได้ส่งมอบ นับถัดจากวันครบกำหนดจนถึงวันที่ผู้เสนอราคา ปฏิบัติตามสัญญาถูกต้องครบถ้วน และสถาบันได้ตรวจรับงานแล้ว

10. การรับประกันความชำรุดบกพร่องของงาน

10.1 ผู้ยื่นข้อเสนอจะต้องจัดให้มีการรับประกันผลงาน และการบริการบำรุงรักษา เป็นระยะเวลา 36 เดือน ณ สถานที่ติดตั้ง ในเวลาทำการแบบ 8 x 5 (5 วันทำการ x 8 ชั่วโมง) โดยต้องดำเนินการแก้ไขปัญหาภายใน 6 ชั่วโมง

10.2 การทำ Preventive Maintenance (PM)

10.2.1 ดำเนินการบำรุงรักษาระบบหรือซอฟต์แวร์เชิงป้องกัน ตามข้อกำหนดขอบเขตให้อยู่ในสภาพที่ใช้งานได้ตลอดอายุของสัญญา โดยยื่นข้อเสนอต้องจัดส่งเจ้าหน้าที่เข้ามาตรวจสอบดูแล ตามที่สถาบันกำหนด แบบ Online หรือ มาดำเนินงานที่สถาบัน โดยกำหนดให้ดำเนินการทุกๆ 6 เดือน ตลอดอายุของสัญญา

10.2.2 ดำเนินการตรวจสอบการแจ้งเตือนและข้อผิดพลาดจาก Bug/Error ของระบบ และแจ้งสถาบัน เพื่อร่วมดำเนินการแก้ไข

10.2.3 ดำเนินการ Update Patch/Firmware และปิดช่องโหว่ภัยคุกคามทางไซเบอร์ กรณีมีความจำเป็น เพื่อแก้ไขปัญหาหรือข้อบกพร่อง โดยได้รับความเห็นชอบจากสถาบันก่อนการดำเนินงาน พร้อมทดสอบการทำงานของระบบ

10.2.4 ดำเนินการสำรอง Logs, Configuration และฐานข้อมูลของระบบ ก่อนทุกครั้งที่มีการเปลี่ยนแปลง และส่งมอบให้สถาบัน

10.2.5 ผู้ยื่นข้อเสนอต้องจัดทำรายงานการบำรุงรักษา (Preventive Maintenance Report) โดยรายงานจะต้องมีรายละเอียด ดังนี้

10.2.5.1 ระบุวัน/เดือน/ปี เวลา และผู้ดำเนินงาน

10.2.5.2 รายละเอียดผลการดำเนินงานหรือตรวจสอบ (Service Report)

10.2.5.3 ความคิดเห็นและข้อเสนอแนะ (ถ้ามี)

10.3 การทำ Corrective Maintenance (CM)

10.3.1 ดำเนินการบำรุงรักษาเชิงแก้ไขปรับปรุงให้กับอุปกรณ์ และระบบต่างๆ ตามข้อกำหนดขอบเขต ให้อยู่ในสภาพที่ใช้งานได้ ตลอดอายุของสัญญา โดยยื่นข้อเสนอต้องจัดส่งเจ้าหน้าที่เข้ามาตรวจสอบ ดูแล ณ สถาบัน หรือด้วยวิธีการ Remote Desktop ผ่านช่องทาง VPN ที่สถาบันกำหนดให้ เดือนละ 1 ครั้งเป็นอย่างน้อย ตลอดอายุของสัญญาในกรณีที่อุปกรณ์ตามข้อกำหนดขอบเขตงาน มีปัญหาด้านการใช้งาน สถาบัน สามารถแจ้งเหตุทางโทรศัพท์, Email, Application Line, ทางวาจา หรือเป็นลายลักษณ์อักษร

10.3.2 เมื่อได้รับแจ้งเหตุขัดข้อง จะต้องดำเนินการตรวจสอบปัญหา และแก้ไขปัญหาด้วยวิธีการ Remote Desktop ผ่านช่องทาง VPN ของหน่วยงาน หรือจัดส่งเจ้าหน้าที่เข้ามาดำเนินการแก้ไขปัญหา ณ สถาบัน

10.3.3 กรณีที่ระบบหรือซอฟต์แวร์เกิดความชำรุดเสียหาย และไม่สามารถดำเนินการแก้ไขให้กลับมาใช้งานตามปกติได้ ผู้ยื่นข้อเสนอต้องดำเนินการจัดหาระบบหรือซอฟต์แวร์สำรองมาให้บริการชั่วคราว โดยระบบหรือซอฟต์แวร์ดังกล่าวต้องมีคุณสมบัติเทียบเท่าหรือดีกว่าระบบหรือซอฟต์แวร์เดิม จนกว่าสามารถแก้ไขระบบหรือซอฟต์แวร์ที่ชำรุดเสียหายกลับมาใช้งานได้ตามปกติ

11. เงื่อนไขการดำเนินงาน

11.1 อำนวยความสะดวกให้เจ้าหน้าที่ของสถาบัน ที่รับผิดชอบโครงการเข้าร่วมโครงการตลอดระยะเวลาที่มาดำเนินงานหรือตามความเหมาะสม

11.2 หากผลการดำเนินงานไม่มีคุณภาพ หรือมีข้อผิดพลาดใด ๆ ผู้ยื่นข้อเสนอจะต้องแก้ไขจัดทำให้เรียบร้อยตามความเห็นชอบของคณะกรรมการตรวจรับพัสดุของสถาบัน

11.3 สถาบัน สามารถปรับรายละเอียดเกี่ยวกับการออกแบบและติดตั้งอุปกรณ์ในโครงการได้ตามที่เห็นสมควร

11.4 หากมีการเปลี่ยนแปลงใดๆ หรือผู้ยื่นข้อเสนอไม่สามารถเข้ามาดำเนินงานได้ตามระยะเวลาที่กำหนดไว้ จะต้องแจ้งให้สถาบัน ทราบอย่างเป็นลายลักษณ์อักษรทุกครั้ง

11.5 หากผู้ยื่นข้อเสนอไม่ดำเนินการให้แล้วเสร็จตามกรอบระยะเวลาส่งมอบงานที่กำหนด ตามขอบเขตงานที่ได้กำหนดไว้ สถาบัน ขอสงวนสิทธิ์ไม่จ่ายเงินจนกว่าผู้ยื่นข้อเสนอได้ส่งมอบงานและคณะกรรมการตรวจรับงานของสถาบัน ให้ความเห็นชอบแล้ว

11.6 ผู้ยื่นข้อเสนอต้องปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศ และสัญญารักษาความลับของข้อมูล ของสถาบัน

ผู้สนใจสามารถ วิจารณ์ เสนอข้อคิดเห็น และข้อเสนอแนะเกี่ยวกับร่างขอบเขตการจัดซื้อวัสดุดังกล่าว ด้วยวิธีการดำเนินโครงการ e-bidding สามารถแจ้งให้ความเห็นทาง e-mail ที่ suphachai@tint.or.th, danai @tint.or.th หรือ udomsak@tint.or.th และส่ง e-mail โดยระบุชื่อ ที่อยู่ และหมายเลขโทรศัพท์ที่สามารถติดต่อได้

(ลงชื่อ)_____ประธานกรรมการ

(นายศุภชัย โรยแก้ว)

(ลงชื่อ) _____กรรมการ

(นายดนัย วงษ์เนตร)

(ลงชื่อ) _____กรรมการ

(นายอุดมศักดิ์ สุขสวัสดิ์)