ร่าง ขอบเขตของงาน (Terms of Reference: TOR)
จ้างเหมาบริการป้องกันการโจมตีประเภท DDoS พร้อม Cloud WAAP
สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

1. หลักการและเหตุผล

การโจมตีทางไซเบอร์ในปัจจุบันมุ่งเป้าไปที่ทุกช่องทางตั้งแต่โครงสร้างพื้นฐานสำคัญระดับชาติไปจนถึงข้อมูลส่วนบุคคลที่ละเอียดอ่อน จากสถิติล่าสุดการโจมตีประเภท DDoS (Distributed Denial of Service) ในปี พ.ศ. 2566 พบว่ามีการโจมตีประเภท DDoS ทั่วโลกจำนวนมาก ส่งผลกระทบต่อภาคเศรษฐกิจและสังคมอย่างมหาศาล แสดงให้เห็นถึงแนวโน้มที่เพิ่มขึ้นอย่างต่อเนื่อง ในช่วงไม่กี่ปีที่ผ่านมา การโจมตีเหล่านี้กลายเป็นภัยคุกคามที่ต้องให้ความสำคัญในการป้องกันสำหรับหน่วยงานทั่วโลก ซึ่งมีความซับซ้อนมากยิ่งขึ้น มีความแพร่หลายและสร้างความเสียหายมากกว่าที่ผ่านมา เช่น เว็บไซต์และระบบออนไลน์ของธนาคารแห่งหนึ่งในประเทศไทย ถูกโจมตีด้วย DDoS โดยมีการส่งข้อมูลจำนวนมหาศาลเข้าไปในระบบพร้อมกัน ทำให้เครื่องคอมพิวเตอร์แม่ข่าย (Server) ของธนาคารไม่สามารถรองรับปริมาณข้อมูลที่เข้ามาได้ ผลที่ตามมาคือเว็บไซต์ของธนาคารล่ม และลูกค้าไม่สามารถเข้าถึงบริการออนไลน์ได้เป็นระยะเวลาหนึ่ง ทำให้ชื่อเสียงของธนาคารได้รับผลกระทบ ลูกค้าสูญเสียความเชื่อมั่นในระบบความปลอดภัยของธนาคาร รวมถึงค่าใช้จ่ายในการกู้คืนระบบ และมีเหตุการณ์เว็บไซต์ของหน่วยงานภาครัฐแห่งหนึ่งในประเทศไทย ถูกโจมตีด้วย DDoS ทำให้เว็บไซต์ไม่สามารถใช้งานได้เป็นระยะเวลาหลายชั่วโมง โดยการโจมตีครั้งนี้เป็นส่วนหนึ่งของการประท้วงทางออนไลน์ที่มีการโจมตีเว็บไซต์ของหน่วยงานรัฐหลายแห่งพร้อมกัน โดยกลุ่มผู้โจมตีพยายามแสดงความไม่พอใจต่อการดำเนินการของหน่วยงานรัฐผ่านการโจมตีทางไซเบอร์ ทำให้บริการหยุดชะงักไม่สามารถให้บริการแก่ประชาชนได้ ประชาชนบางส่วนเกิดความไม่มั่นใจในความสามารถของรัฐในการป้องกันการโจมตีทางไซเบอร์ ส่งผลต่อภาพลักษณ์ด้านความมั่นคงและความปลอดภัยของหน่วยงานรัฐ

จากที่กล่าวมาข้างต้นนั้น ปัญหาภัยคุกคามทางไซเบอร์จึงเป็นเรื่องสำคัญที่หน่วยงานต้องให้ความสำคัญเกี่ยวกับระบบป้องกันภัยคุกคามทางไซเบอร์ โดยเฉพาะการโจมตีภายในเครือข่ายซึ่งเป็นระบบให้บริการและรองรับการใช้งาน ซึ่งระบบป้องกันการโจมตีประเภท DDoS (Distributed Denied of Service) เป็นระบบที่ป้องกันไม่ให้ระบบหรือเว็บไซต์ของหน่วยงานหยุดชะงักจากการโจมตี พร้อมทั้งนำเทคโนโลยี Cloud Web Application and API Protection (Cloud WAAP) มาร่วมกับการป้องกันการโจมตีประเภท DDoS เพื่อเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์ให้กับหน่วยงาน Cloud WAAP ไม่เพียงแต่ช่วยป้องกันการโจมตีประเภท DDoS แต่ยังสามารถป้องกันการโจมตีที่มุ่งเป้าไปที่ Web Application และ API ซึ่งเป็นช่องทางที่สำคัญในการทำงานของระบบดิจิทัลในปัจจุบัน การรวมเทคโนโลยีทั้งสองนี้จะช่วยให้หน่วยงานสามารถป้องกันภัยคุกคามได้อย่างมีประสิทธิภาพ ลดความเสี่ยงจากการถูกโจมตีและการสูญเสียข้อมูล ซึ่งเป็นปัจจัยสำคัญต่อการดำเนินงานตามภารกิจของหน่วยงานในยุคดิจิทัล

ดังนั้น สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานจึงมีความจำเป็นต้องดำเนินจ้างบริการป้องกันการโจมตีประเภท DDoS พร้อม Cloud WAAP ปรับปรุงและพัฒนาระบบให้สอดรับกับหลักการทางไซเบอร์ในปัจจุบัน

2. วัตถุประสงค์

2.1 เพื่อเพิ่มประสิทธิภาพการป้องกันการโจมตีประเภท DDoS (Distributed Denied of Service) ให้กับระบบและเว็บไซต์ของหน่วยงานต่าง ๆ ที่ติดตั้งอยู่ภายในศูนย์ข้อมูล (Data Center) ของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

2.2 เพื่อเพิ่มความปลอดภัยให้กับ Web Application และ API ของหน่วยงานต่าง ๆ ที่ติดตั้งอยู่ภายในศูนย์ข้อมูล (Data Center) ของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

2.3 เพื่อจ้างผู้ที่มีความเชี่ยวชาญด้านมาตรฐานความปลอดภัยทางไซเบอร์ ในการศึกษา วิเคราะห์และออกแบบการป้องกันการโจมตีประเภท DDoS และ Cloud WAAP ที่มีประสิทธิภาพและเหมาะกับสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

3. คุณสมบัติผู้เสนอราคา

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วน ผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 เป็นนิติบุคคลผู้มีอาชีพรับจ้างงานที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

3.9 ไม่เป็นผู้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทยเว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

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

3.11 ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ "กิจการร่วมค้า" ต้องมีคุณสมบัติดังนี้

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงระหว่างผู้เข้าร่วมค้าจะต้องมีการกำหนดสัดส่วนหน้าที่และความรับผิดชอบในปริมาณงาน สิ่งของ หรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก กิจการร่วมค้านั้นต้องใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

สำหรับข้อตกลงระหว่างผู้เข้าร่วมค้าที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมค้าหลัก ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้มีการมอบหมายผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอ ในนามกิจการร่วมค้า การยื่นข้อเสนอดังกล่าวไม่ต้องมีหนังสือมอบอำนาจ

สำหรับข้อตกลงระหว่างผู้เข้าร่วมค้าที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้ยื่นข้อเสนอ ผู้เข้าร่วมค้าทุกรายจะต้องลงลายมือชื่อในหนังสือมอบอำนาจให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า

3.12 ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ ดังนี้

3.12.1 กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยซึ่งได้จดทะเบียนเกินกว่า 1 ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก 1 ปีสุดท้ายก่อนวันยื่นข้อเสนอ

3.12.2 กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ให้พิจารณาการกำหนดมูลค่าของทุนจดทะเบียน โดยผู้ยื่นข้อเสนอจะต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอ ดังนี้ ต้องมีทุนจดทะเบียนไม่ต่ำกว่า 3 ล้านบาท

3.12.3 สำหรับการจัดซื้อจัดจ้างครั้งหนึ่งที่มีวงเงินเกิน 500,000 บาทขึ้นไป กรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดา โดยพิจารณาจากบัญชีเงินฝากธนาคาร ณ วันยื่นข้อเสนอ โดยต้องมีเงินฝากคงเหลือในบัญชีธนาคารเป็นมูลค่า 1 ใน 4 ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง และหากเป็นผู้ชนะการจัดซื้อจัดจ้างหรือเป็นผู้ได้รับการคัดเลือกจะต้องแสดงบัญชีเงินฝากที่มีมูลค่าดังกล่าวอีกครั้งหนึ่งในวันลงนามในสัญญา

3.12.4 กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียนหรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ 1 ใน 4 ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง (สินเชื่อที่ธนาคารภายในประเทศหรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้าประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรองหรือที่สำนักงานสาขารับรอง (กรณีที่ได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอนับถึงวันยื่นข้อเสนอไม่เกิน 90 วัน

3.12.5 กรณีตาม (3.12.1) - (3.12.4) ยกเว้นสำหรับกรณีดังต่อไปนี้

3.12.5.1 กรณีที่ผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐ

3.12.5.2 นิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการตามพระราชบัญญัติล้มละลาย (ฉบับที่ 10) พ.ศ. 2561

3.13 ผู้ยื่นข้อเสนอต้องเป็นนิติบุคคลที่มีผลงานประเภทเดียวกันในการจัดหาครั้งนี้หรือเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยเป็นผลงานที่เสร็จสมบูรณ์แล้วอย่างน้อย 1 สัญญา และมีวงเงินต่อสัญญาไม่น้อยกว่า 10 ล้านบาท รวมภาษีมูลค่าเพิ่มแล้ว และเป็นผลงานที่เป็นคู่สัญญาโดยตรงกับหน่วยงานภาครัฐ รัฐวิสาหกิจ หรือเอกชนที่สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานเชื่อถือ โดยผู้เสนอราคาต้องแนบสำเนาหลักฐานสัญญาโครงการ หรือหนังสือรับรองผลงานของหน่วยงานในวันที่ยื่น

4. ขอบเขตการดำเนินงาน

ผู้รับจ้างต้องดำเนินการให้ครอบคลุมงาน โดยมีรายละเอียดของขอบเขตการดำเนินงาน ดังนี้

4.1 การศึกษา วิเคราะห์และออกแบบการป้องกันการโจมตีประเภท DDoS และ Cloud WAAP พร้อมจัดทำแผนการบริหารโครงการ (Project Plan) อย่างน้อยดังนี้

4.1.1 แผนการบริหารโครงการ (Project Management Plan)

4.1.2 แผนการดำเนินการโครงการ (Implementation Plan)

4.1.3 เอกสารการวิเคราะห์และออกแบบการป้องกันการโจมตีประเภท DDoS และ Cloud WAAP

4.2 การป้องกันการโจมตีประเภท DDoS โดยให้บริการอย่างน้อยดังนี้

4.2.1 ตรวจจับการทำงานได้ทั้ง Internet Protocol Version 4 (IPv4) และ Version 6 (IPv6)

4.2.2 มีความสามารถรองรับปริมาณข้อมูลการใช้งาน จากการโจมตีประเภท DDoS ได้ไม่น้อยกว่า 10 Gbps และมีความสามารถในการกรองทราฟฟิก (Traffic) ที่ดี ได้ไม่น้อยกว่า 1 Gbps

4.2.3 มีความสามารถรองรับความเร็วในการป้องกันการโจมตีประเภท DDoS (DDoS Flood Prevention Rate) ได้ไม่น้อยกว่า 14 Mpps (Millions Packets Per Second) และมีค่า Latency ไม่เกิน 60 Micro Seconds

4.2.4 ป้องกันการโจมตีประเภท DoS/DDoS แบบ Behavioral Based และ Signature Based ได้เป็นอย่างน้อย

4.2.5 ป้องกันการโจมตีประเภท DDoS ในระดับ Application Layer ได้แก่ HTTPS Flood, DNS Flood Attacks, SIP Flood Attacks, Brute Force ได้เป็นอย่างน้อย

4.2.6 ตรวจจับและป้องกันการโจมตีแบบ Signature Protection สำหรับ Web-Amplification Application, Mail Servers Vulnerabilities, FTP Servers Vulnerabilities, SQL Server Vulnerabilities, DNS Servers Vulnerabilities, SIP Servers Vulnerabilities ได้เป็นอย่างน้อย

4.2.7 สามารถทำ HTTPS Challenge แบบ RSA 2k keys จำนวนไม่น้อยกว่า 43,000 CPS (Connection Per Second)

4.2.8 สามารถแสดง Dashboard Traffic Statistics ผ่าน Network Analytic และสามารถแสดง Top Source, Top Destination, Top Applications, Top Protocols, Top Countries ได้เป็นอย่างน้อย

4.2.9 สามารถป้องกันด้วยการกำหนด Subnet หรือ IP Range Internet ได้

4.2.10 สามารถรองรับ Scrubbing Center Capacity ได้ไม่น้อยกว่า 10 Tbps

4.2.11 สามารถสร้าง Real Time Signature เพื่อป้องกันการโจมตี Layer 3 – Layer 4 ได้โดยอัตโนมัติ

4.2.12 สามารถรับ Threat Intelligence ที่สามารถป้องกัน Bad Actor เช่น Botnet, C&C, Anonymized Proxies, และ Dormant

4.3 การให้บริการ Cloud Web Application and API Protection (Cloud WAAP) สามารถให้บริการอย่างน้อยดังนี้

4.3.1 สามารถป้องกันภัยคุกคาม Web Application อย่างน้อยดังนี้

4.3.1.1 Cross-side Request Forgery (CSRF)

4.3.1.2 Server-side Request Forgery (SSRF)

4.3.1.3 Cross Site Scripting (XSS)

4.3.1.4 Injection Flaws

4.3.1.5 Command Execution

4.3.1.6 Database Sabotage

4.3.1.7 Stealth Commanding

4.3.1.8 Client Side Protection Detection และ Mitigation

4.3.2 ป้องกัน Bad Bot Traffic โดยอ้างอิงจาก OWASP Automated Threat Top 21 ได้ และสามารถทำ Mitigation Technique ได้เป็นอย่างน้อยดังนี้ Allow, Block, Throttle, Feed Fake Data, Crypto Challenge, Redirect Loop

4.3.3 ป้องกันการโจมตีแบบ Supply Chain Attack, Formjacking Attack, Magecart Attack และ Web DDoS Attack โดยสามารถสร้าง Signature แบบ Real-Time ในระดับ Layer 7 ได้

4.3.4 ป้องกันการโจมตีที่ส่งผลกระทบต่อ Application Programming Interface (API Protection) โดยต้องสามารถทำ API Catalogue Validation, API Quota และ API Discovery ได้เป็นอย่างน้อย

4.3.5 รองรับปริมาณข้อมูลการใช้งานได้อย่างน้อย 10 Mbps

4.3.6 ทำงานแบบ Content Delivery Network (CDN) ได้

4.3.7 สามารถใช้งาน Threat Intelligence ได้ไม่น้อยกว่า 50 Queries ต่อเดือน

4.4 ต้องจัดทำรายงานการโจมตีทางไซเบอร์เป็นรายเดือน อย่างน้อยดังต่อไปนี้

4.4.1 รายงานสรุปผลการโจมตีและการป้องกันภัยคุกคามการโจมตีประเภท DDoS

4.4.2 รายงานแสดงรายละเอียดปริมาณการใช้ข้อมูล อย่างน้อยดังนี้ Traffic Received, Dropped, Excluded, Challenged

4.4.3 รายงานแสดงรายละเอียดปริมาณการโจมตี อย่างน้อยดังนี้ Top Attack Source, Top Attack Destination, Top Applications, Top Attack Geolocation

4.4.4 รายงานแสดงรายละเอียดผลการป้องกันโจมตี เช่น Signature, Threat Category, Mitigation Action, Protection Policy, Risk Level เป็นต้น

4.4.5 รายงานผลการโจมตีและการป้องกันภัยคุกคามการโจมตีประเภท WAF

4.4.6 รายงานแสดงรายละเอียดผลการป้องกันโจมตีผ่านทาง Website ตาม OWASP TOP 10

4.4.7 รายงานแสดงรายละเอียดผลการป้องกันโจมตีรูปแบบ Application Attack Distribution

4.4.8 รายงานแสดงรายละเอียดผลการป้องกันโจมตีจำนวน Application Security Event ที่เกิดขึ้น

5. ระยะเวลาดำเนินงาน

ระยะเวลาในการดำเนินการ 360 วัน นับถัดจากวันลงนามในสัญญาจ้าง

6. หลักเกณฑ์ในการพิจารณาข้อเสนอ

6.1 การพิจารณาผลการยื่นข้อเสนอครั้งนี้ สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานจะใช้หลักเกณฑ์การประเมินค่าประสิทธิภาพต่อราคา (Price Performance) โดยพิจารณาจากราคารวมตามปัจจัยหลักและน้ำหนักที่กำหนดดังต่อไปนี้

6.1.1 ราคาที่ยื่นข้อเสนอ (Price) กำหนดค่าน้ำหนักเท่ากับร้อยละ 20

6.1.2 คุณภาพและคุณสมบัติ (Performance) ที่เป็นประโยชน์ต่อทางราชการกำหนดน้ำหนักเท่ากับร้อยละ 80 รวม 100 คะแนน ดังต่อไปนี้

ลำดับ	เกณฑ์การพิจารณา	เกณฑ์ย่อย	คะแนนเต็ม
1. ผลงานและประสบการณ์ และบุคลากรหลัก คะแนนเต็ม 50 คะแนน			
1.1	ผลงานของผู้เสนอราคา *(หลักฐานสำเนาสัญญาจ้างหรือหนังสือรับรองผลงานหรือใบสั่งจ้าง)*	โดยพิจารณาจากผลงานของผู้เสนอราคา ดังนี้ 1) มีผลงานการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ จำนวน 1 - 2 ผลงาน ได้คะแนน 10 คะแนน 2) มีผลงานการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ จำนวน 3 - 4 ผลงาน ได้คะแนน 15 คะแนน 3) มีผลงานการดำเนินงานด้าน ความมั่นคงปลอดภัยทางไซเบอร์ จำนวน 5 ผลงานขึ้นไป ได้คะแนน 20 คะแนน	20
1.2	ประสบการณ์ของบุคลากรหลัก	โดยพิจารณาจากประสบการณ์บุคลากรของผู้เสนอราคา ดังนี้ 1) บุคลากรหลักที่มีประสบการณ์ตรงตามข้อ 10.1 ได้คะแนน 5 คะแนน 2) บุคลากรหลักที่มีประสบการณ์สูงกว่าข้อ 10.1 ได้คะแนน 10 คะแนน	10
1.3	ใบเอกสารรับรอง (Certificate) ที่เกี่ยวข้องกับด้านความมั่นคงปลอดภัยไซเบอร์และบริการที่นำเสนอ ดังนี้ 1) CompTIA Security+ 2) CompTIA Cybersecurity Analyst (CySA+) 3) CISSP (Certified Information Systems Security Professional) 4) Certified Red Team Master (CRTM)	โดยพิจารณาจากใบเอกสารรับรอง (Certificate) ของบุคลากรของผู้เสนอราคา ดังนี้ 1) มีใบเอกสารรับรองอย่างใดอย่างหนึ่งอย่างน้อย 2 รายการ ได้คะแนน 5 คะแนน 2) มีใบเอกสารรับรองอย่างใดอย่างหนึ่งอย่างน้อย 3 รายการ ได้คะแนน 10 คะแนน 3) มีใบเอกสารรับรองอย่างใดอย่างหนึ่งอย่างน้อย 4 รายการ ได้คะแนน 15 คะแนน 4) มีใบเอกสารรับรองครบทุกรายการ ได้คะแนน 20 คะแนน	20

ลำดับ	เกณฑ์การพิจารณา	เกณฑ์ย่อย	คะแนนเต็ม
	5) Certified เกี่ยวกับบริการการป้องกันการโจมตีประเภท DDoS และ Cloud WAAP ที่นำเสนอ		
2. วิธีการบริหารและวิธีปฏิบัติงาน คะแนนเต็ม 20 คะแนน			
2.1	วิธีการบริหารและวิธีปฏิบัติงาน	วิธีการบริหารและวิธีการปฏิบัติงานพิจารณาจาก 1) วิธีการบริหาร (โครงสร้างทีมงาน การจัดบุคลากรการทำงานตามขอบเขตงาน) คะแนนเต็ม 10 คะแนน 2) ขั้นตอนการปฏิบัติงาน กรอบการดำเนินการตามวัตถุประสงค์ของโครงการ แนวคิด วิธีการศึกษา วิเคราะห์ข้อมูล วิธีดำเนินการ คะแนนเต็ม 10 คะแนน	20
3. มาตรฐานของระบบที่นำเสนอในการให้บริการ คะแนนเต็ม 30 คะแนน			
3.1	ระบบ Cloud Web Application and API Protection (Cloud WAAP) ที่เสนอต้องอยู่ภายใต้ตามมาตราฐานความปลอดภัยด้านไซเบอร์ ตามมาตรฐานดังนี้ 1) ISO/IEC 27001 2) ISO/IEC 27018 3) ISO/IEC 27017 4) ISO/IEC 27032 5) US SSAE16 SOC-2 Type II หรือ US SSAE16 SOC-3 Type II	ระบบที่นำเสนอพิจารณามีมาตรฐานดังนี้ 1) มีมาตราฐานอย่างใดอย่างหนึ่งอย่างน้อย 1 รายการ ได้คะแนน 5 คะแนน 2) มีมาตราฐานอย่างใดอย่างหนึ่งอย่างน้อย 3 รายการ ได้คะแนน 10 คะแนน 3) มีมาตราฐานครบทุกรายการ ได้คะแนน 15 คะแนน	15
3.2	ระบบการป้องกันการโจมตีประเภท DDoS ที่นำเสนอต้องได้รับการรับรองจาก Forrester DDoS Mitigation ปี 2021 หรือปีล่าสุด	ระบบที่นำเสนอพิจารณามีมาตรฐานดังนี้ 1) ถูกจัดอันดับในระดับ Contenders ได้คะแนน 5 คะแนน 2) ถูกจัดอันดับในระดับ Strong Performers ได้คะแนน 10 คะแนน 3) ถูกจัดอันดับในระดับ Leaders ได้คะแนน 15 คะแนน	15
คะแนนรวมทั้งหมด			**100**

7. งบประมาณโครงการ

งบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. 2567 จำนวนทั้งสิ้น 20,000,000 บาท (ยี่สิบล้านบาทถ้วน)

<u>หมายเหตุ</u> ราคากลางเป็นราคาที่ได้จากการอ้างอิงจากหลักเกณฑ์ อัตราค่าใช้จ่าย และแนวทางการพิจารณางบประมาณรายจ่ายประจำปี ของสำนักงบประมาณ ธันวาคม 2566

8. การส่งมอบงาน ค่าจ้าง และการจ่ายเงิน

8.1 งวดที่ 1 ภายใน 60 วัน นับถัดจากวันที่ลงนามในสัญญา เบิกจ่ายเงินร้อยละ 10 ของวงเงินค่าจ้างตามสัญญา และคณะกรรมการตรวจรับพัสดุได้ทำการตรวจรับเรียบร้อยแล้ว โดยผู้รับจ้างต้องส่งมอบเอกสารอย่างน้อยดังนี้

8.1.1 แผนการบริหารโครงการ (Project Management Plan)

8.1.2 แผนการดำเนินการโครงการ (Implementation Plan)

8.1.3 เอกสารการวิเคราะห์และออกแบบระบบป้องกันการโจมตีประเภท DDoS และ Cloud WAAP

8.1.4 คู่มือการใช้งานบริการ

8.2 งวดที่ 2 ภายใน 150 วัน นับถัดจากวันที่ลงนามในสัญญา เบิกจ่ายเงินร้อยละ 30 ของวงเงินค่าจ้างตามสัญญา โดยผู้รับจ้างต้องบริการป้องกันการโจมตี DDoS พร้อม Cloud WAAP พร้อมส่งมอบรายงาน ตามขอบเขตของงาน ข้อ 4.4

8.3 งวดที่ 3 ภายใน 240 วัน นับถัดจากวันที่ลงนามในสัญญา เบิกจ่ายเงินร้อยละ 30 ของวงเงินค่าจ้างตามสัญญา โดยผู้รับจ้างต้องบริการป้องกันการโจมตี DDoS พร้อม Cloud WAAP พร้อมส่งมอบรายงาน ตามขอบเขตของงาน ข้อ 4.4

8.4 งวดที่ 4 ภายใน 360 วัน นับถัดจากวันที่ลงนามในสัญญา เบิกจ่ายเงินร้อยละ 30 ของวงเงินค่าจ้างตามสัญญา โดยผู้รับจ้างต้องบริการป้องกันการโจมตี DDoS พร้อม Cloud WAAP พร้อมส่งมอบรายงาน ตามขอบเขตของงาน ข้อ 4.4

<u>หมายเหตุ</u> ผู้รับจ้างต้องส่งมอบเอกสารในแต่ละงวดงาน ในรูปแบบสื่อสิ่งพิมพ์ อย่างน้อย 3 ชุด พร้อมไฟล์อิเล็กทรอนิกส์ที่สามารถแก้ไขได้ และ PDF พร้อมบันทึกลงใน Flash Drive หรือ External Hard Disk

9. อัตราค่าปรับ

กรณีที่ผู้รับจ้างไม่ส่งมอบงานงวดสุดท้ายให้เป็นไปตามกำหนดระยะเวลาการส่งมอบงาน ผู้ว่าจ้างจะดำเนินการปรับเป็นรายวัน ในอัตราร้อยละ 0.1 (ศูนย์จุดหนึ่ง) ของวงเงินค่าจ้างตามงวดงานที่ยังไม่แล้วเสร็จ นับถัดจากวันที่กำหนดแล้วเสร็จตามสัญญา จนถึงวันที่ผู้รับจ้างปฏิบัติตามสัญญาถูกต้องครบถ้วน และผู้ว่าจ้างได้ตรวจรับงานแล้ว

10. ข้อกำหนดทั่วไป

10.1 จัดหาบุคลากรต้องเสนอบุคลากรหลักที่มีความรู้ ประสบการณ์ และคุณสมบัติเฉพาะของตำแหน่งต่าง ๆ อย่างน้อยดังต่อไปนี้

ตำแหน่ง	วุฒิการศึกษา	จำนวน (คน)
1. ผู้จัดการโครงการ (Project Manager)	ปริญญาโท ด้านคอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศ หรือสื่อสารโทรคมนาคม หรือด้านอื่น ๆ ที่เกี่ยวข้อง และประสบการณ์อย่างน้อย 10 ปี ซึ่งมีประสบการณ์ในด้านที่เกี่ยวข้องกับตำแหน่ง	1
2. ผู้เชี่ยวชาญด้านมาตรฐานความปลอดภัยทางไซเบอร์	ปริญญาตรี ด้านคอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศ หรือสื่อสารโทรคมนาคม หรือด้านอื่น ๆ ที่เกี่ยวข้อง และประสบการณ์อย่างน้อย 10 ปี ซึ่งมีประสบการณ์ในด้านที่เกี่ยวข้องกับตำแหน่ง	1
3. บุคลากรสนับสนุน	ปริญญาตรี ด้านคอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศ หรือสื่อสารโทรคมนาคม หรือด้านอื่น ๆ ที่เกี่ยวข้อง และประสบการณ์อย่างน้อย 3 ปี	1
4. เลขานุการโครงการ	ปริญญาตรี	1

หลักฐานการแสดงความรู้และความสามารถของบุคลากรปฏิบัติงานในโครงการนี้ โดยบุคลากรต้องลงลายมือชื่อรับรองเอกสารว่าเป็นความจริงทุกประการ ตามแบบฟอร์ม (เอกสารแนบ 1)

10.2 จัดให้มีช่องทางรับแจ้งเหตุขัดข้องทุกวันตลอด 24 ชั่วโมง ไม่เว้นวันหยุดราชการ

10.3 ต้องให้คำปรึกษา แนะนำ ชี้แจง และตอบปัญหาทางโทรศัพท์ รวมทั้งกรณีที่ผู้ว่าจ้างร้องขอ โดยจะต้องสนับสนุนและปฏิบัติตามการร้องขอดังกล่าว ภายใน 24 ชั่วโมงหลังจากได้รับแจ้ง

11. หน่วยงานที่รับผิดชอบ

สำนักเทคโนโลยีเพื่อการเรียนการสอน สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน
อีเมล์ obecict@obecmail.obec.go.th โทรศัพท์ 02-288-5906

เอกสารแนบ 1

จ้างเหมาบริการป้องกันการโจมตีประเภท DDoS พร้อม Cloud WAAP

สำหรับสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

<u>ประวัติส่วนตัว</u>

ชื่อ – นามสกุล.....

ตำแหน่งที่เสนอในโครงการ.....

ที่อยู่ปัจจุบัน.....

.....

<u>ประวัติการศึกษา</u>

1. ปริญญาตรี : มหาวิทยาลัย..... คณะ .....
   สาขา..... ปีที่สำเร็จ .....
2. ปริญญาโท : มหาวิทยาลัย..... คณะ .....
   สาขา..... ปีที่สำเร็จ .....
3. ปริญญาเอก : มหาวิทยาลัย..... คณะ .....
   สาขา..... ปีที่สำเร็จ .....

<u>ประวัติการทำงาน (ปัจจุบัน ถึง อดีต)</u>

1. ระบุปี ถึง ปัจจุบัน ตำแหน่ง..... หน่วยงาน.....
   รายละเอียด.....
2. ระบุปี ถึง ปัจจุบัน ตำแหน่ง..... หน่วยงาน.....
   รายละเอียด.....
3. ระบุปี ถึง ปัจจุบัน ตำแหน่ง..... หน่วยงาน.....
   รายละเอียด.....

<u>การฝึกอบรม (ปัจจุบัน ถึง อดีต)</u>

1. ปี.....หลักสูตร.....
2. ปี.....หลักสูตร.....
3. ปี.....หลักสูตร.....

<u>เอกสารประกอบ</u>

1. สำเนาใบรายงานผลการศึกษา (Transcript) พร้อมลงนามรับรองสำเนาถูกต้อง (ถ้ามี)
2. สำเนาใบรับรองการฝึกอบรม (Certification) พร้อมลงนามรับรองสำเนาถูกต้อง (ถ้ามี)