ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและราคากลาง (ราคาอ้างอิง)

ในการจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง

1. ชื่อโครงการ **การจ้างผู้ให้บริการป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์**
2. หน่วยงานเจ้าของโครงการ ฝ่ายปฏิบัติการเทคโนโลยีสารสนเทศ
3. วงเงินงบประมาณที่ได้รับจัดสรร **2,400,000.00 บาท (สองล้านสี่แสนบาทถ้วน)**
4. วันที่กำหนดราคากลาง (ราคาอ้างอิง) **30 ก.ค. 2567**

   เป็นเงิน 1,318,000.00 บาท (หนึ่งล้านสามแสนหนึ่งหมื่นแปดพันบาทถ้วน)
5. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)

   บริษัท อาสค์โฟร์คีย์ จำกัด
6. รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง) ทุกคน

6.1 นายฉัตรชัย	อาศรมเงิน	ผู้ช่วยผู้บริหารฝ่ายปฏิบัติการเทคโนโลยีสารสนเทศ /ฝ่าย ปส.
6.2 นายจรัส	ขวัญพิเชษฐ์สกุล	ผู้บริหารส่วนรักษาความปลอดภัยเทคโนโลยีสารสนเทศ /ฝ่าย ปส.
6.3 นางสาววิลาสินี	คำเพ็ง	ผู้ช่วยผู้บริหารส่วนบริหารจัดการโครงสร้างพื้นฐานและระบบเครือข่าย /ฝ่าย ปส.

ผนวก 1

ขอบเขตการดำเนินงาน

การจ้างผู้ให้บริการป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์

ผู้ยื่นข้อเสนอต้องจัดหาบริการป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์ โดยมีขอบเขตการดำเนินงานดังต่อไปนี้

1. **ข้อกำหนดความต้องการทั่วไป**
   - 1.1 ต้องเสนอบริการป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์ ที่มีคุณสมบัติที่สามารถใช้งานร่วมกับระบบเครือข่าย และระบบคอมพิวเตอร์ที่ธนาคารใช้งานอยู่ในปัจจุบันได้
   - 1.2 สามารถแจ้งเตือนเหตุการณ์ที่เกิดขึ้นได้ตามเงื่อนไขที่ได้กำหนดไว้ ผ่านทาง SNMP หรือ Syslog หรือ Email หรือ SMS ได้
   - 1.3 สามารถบริหารจัดการผ่าน Web Browser ได้
   - 1.4 หากมีส่วนประกอบเพิ่มเติมใดที่มิได้ระบุไว้ในเอกสารรายละเอียดของคุณลักษณะเฉพาะและขอบเขตการดำเนินงาน แต่มีความจำเป็นต่อการใช้งานของบริการป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์ เพื่อให้งานแล้วเสร็จ สามารถใช้งานบริการป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์ได้ครบถ้วน ถูกต้อง ผู้ยื่นข้อเสนอต้องจัดหาหรือจัดทำมาให้เพียงพอต่อการใช้งานของธนาคาร และต้องส่งมอบให้เป็นกรรมสิทธิ์ หรือสิทธิ์ หรือลิขสิทธิ์ของธนาคารทั้งหมด โดยไม่คิดค่าใช้จ่ายใด ๆ เพิ่มเติม

2. **ข้อกำหนดคุณสมบัติเฉพาะของบริการป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์**

   บริการป้องกันเว็บไซต์ของธนาคารจากการโจมตีในระดับเว็บแอปพลิเคชัน จำนวนไม่น้อยกว่า 1 โดเมน (exim.go.th) และ Sub-domain แบบไม่จำกัดตามที่ธนาคารเป็นผู้กำหนด ต้องมีความสามารถคุณสมบัติขั้นต่ำดังนี้

   - 2.1 ความสามารถในการป้องกันการโจมตีประเภท DDoS (DDoS Protections)
     - 2.1.1 สามารถป้องกันการโจมตีจากในระดับเครือข่าย (DDoS attack) ที่ระดับ Network layer 3, 4 และ 7
     - 2.1.2 สามารถป้องกันการโจมตีในระดับเครือข่าย (DDoS attack) แบบไม่จำกัดจำนวนครั้ง และขนาดของการโจมตี โดยไม่มีค่าใช้จ่ายเพิ่มเติม (Unlimited DDOS protection)
     - 2.1.3 มีเครือข่ายที่มีความสามารถในการป้องกันการโจมตีจากประเภท DDoS ขนาดไม่น้อยกว่า 20 Tbps
     - 2.1.4 มี Node หรือ Point of Presence (PoP) จำนวนไม่น้อยกว่า 250 จุดทั่วโลก และมีจำนวนไม่น้อยกว่า 6 จุด ในประเทศไทยที่มีการเชื่อมต่อกับโครงข่ายอินเทอร์เน็ตระหว่างประเทศ (International Internet Gateway: IIG)
     - 2.1.5 Node หรือ Point of Presence (POP) ที่อยู่ในประเทศไทยจะต้องมีความสามารถในการป้องกัน DDoS, Web Application Firewall (WAF) และ Content Delivery Network (CDN) ได้
     - 2.1.6 เป็นผลิตภัณฑ์ที่ถูกจัดอยู่ในกลุ่ม Leader ของ The Forrester Wave ในหัวข้อของ Web Application Firewall ปี 2022 หรือ ปีล่าสุด
   - 2.2 ความสามารถในการป้องกันเว็บแอพพลิเคชัน (Web Security Functions)
     - 2.2.1 สามารถป้องกันการโจมตีผ่านทาง Website ตามเงื่อนไขของ OWASP Top10 ดังนี้
       - 2.2.1.1 SQL injection
       - 2.2.1.2 Broken Authentication
       - 2.2.1.3 Sensitive Data Exposure

2.2.1.4 XML External Entities (XEE)

2.2.1.5 Broken Access Control

2.2.1.6 Security Misconfiguration

2.2.1.7 Cross-Site Scripting

2.2.1.8 Insecure Deserialization

2.2.1.9 Using Components with Known Vulnerabilities

2.2.1.10 Insufficient Logging and Monitoring

2.2.2 สามารถกำหนดค่าของ Web Application Firewall (WAF) ได้แบบไม่จำกัดจำนวน (Unlimited Custom WAF rules) และตั้งค่าการเปิดปิด WAF Rule ให้มีผลบังคับใช้ (Effective) ภายในระยะเวลาไม่เกิน 30 วินาที

2.2.3 สามารถกำหนดค่า IP Firewall ด้วยเงื่อนไข Source IP address, Source IP address range, Autonomous System Number (ASN) และประเทศได้

2.2.4 สามารถกำหนดค่า Rate Limit Rules ในการป้องกันการเข้าถึง Website ได้ไม่น้อยกว่า 100 rules

2.2.5 สามารถทำการตรวจสอบการออกใบรับรอง SSL (Certificate transparency monitoring) โดยสามารถแจ้งเตือนเมื่อมีผู้ทำการออกใบรับรองภายใต้ชื่อโดเมนเดียวกันกับของธนาคาร

2.2.6 สามารถตรวจจับและระบุการใช้งาน Javascript ได้ด้วยเงื่อนไขว่ามีการใช้งาน Javascript นั้นๆ ครั้งแรกและครั้งล่าสุดเมื่อใด และทำการแจ้งเตือนได้ดังนี้

2.2.6.1 มีการเรียกใช้งาน Javascript ใหม่ที่เกิดขึ้น

2.2.6.2 Javascript ที่ใช้งานอยู่มีการเปลี่ยนแปลง (Page attribution)

2.2.6.3 มีการเรียกใช้งาน Javascript จากโดเมนใหม่

2.2.7 เป็นผลิตภัณฑ์ที่จัดอยู่ในกลุ่ม Leader ของ Gartner Magic Quadrant ในหัวข้อ Web Application and API Protection (WAAP) ปี 2022 หรือ ปีล่าสุด

2.2.8 สามารถเพิ่มความปลอดภัยให้กับ DNS จากการถูกปลอมแปลงข้อมูลจากผู้ไม่หวังดีผ่านระบบ DNS ด้วยการทำ DNSSEC (DNS Security Extensions) ได้

2.3 ความสามารถในการเพิ่มประสิทธิภาพเว็บแอพพลิเคชัน (Content Delivery Network : CDN & Optimization)

2.3.1 มีบริการ Authoritative DNS services สำหรับโดเมนสาธารณะ และต้องมี Host Domains ทุกภูมิภาคทั่วโลก โดยต้องมี node ในประเทศไทยไม่น้อยกว่า 6 จุด

2.3.2 มีระบบ Caching ในการจัดเก็บเนื้อหาของเว็บไซต์ โดยสามารถทำ Static Content Caching ดังต่อไปนี้ได้

2.3.2.1 ประเภทรูปภาพ

2.3.2.2 ประเภทวีดีโอ

2.3.2.3 ประเภทตัวอักษร

2.3.2.4 ประเภทไฟล์บีบอัด

2.3.3 สามารถลบ Cache (Purge cache) ทั้งหมดได้ทันที หรือกำหนดเงื่อนไขการลบ Cache เฉพาะ URL, Host name และ Tag ได้

2.3.4 สามารถใช้ API ในการอัพเดท Cache ในกรณีที่มีการอัพเดท Content ใหม่

2.3.5 บริการต้องรองรับการใช้ Bandwidth Consumption ได้ไม่น้อยกว่า 7 TB ต่อเดือน

2.3.6 สามารถลดขนาด บีบอัด และลบ Metadata ของไฟล์ ด้วยเทคโนโลยี ดังต่อไปนี้

2.3.6.1 Lossless

2.3.6.2 Lossy

2.3.6.3 WebP

2.3.7 สามารถทำการลบตัวอักษรที่ไม่จำเป็นใน Source code เช่น Whitespace และ Comments ได้

2.3.8 มีระบบ Always-on ที่สามารถทำการแสดง static content ในกรณีที่ Server ต้นทาง ไม่สามารถใช้งานได้

2.3.9 สามารถลด Latency time ให้กับ Dynamic content และแสดงผลในรูปแบบของประสิทธิภาพที่เพิ่มขึ้น และเวลาที่ตอบสนองได้

2.3.10 สามารถทำการเก็บ Payload logging เมื่อมี request traffic ที่ตรงกับ Web Application Firewall Rule ที่ได้ทำการสร้างไว้

2.3.11 สามารถทำ Load Balancing โดยสามารถทำ Automatic Failover, Geographic routing และ Active health check ได้ไม่น้อยกว่า 8 Origins

2.4 ความสามารถในการแสดงรายงาน (Dashboard Functions)

2.4.1 มี Dashboard แสดงรายงานประเภท Security แบบ Real-time หรือ Near Real-time โดยสามารถแสดงถึงข้อมูลแหล่งที่มาของการโจมตี เช่น IP Address, Browser, Country และ Autonomous System Number (ASN) ได้

2.4.2 มี Dashboard แสดงรายงานประเภท Analytic แบบ Real-time หรือ Near Real-time โดยมีรายละเอียด Total Requests, Cached Request, Bandwidth Saved, Threat Sources, Top Threat Origin และ Top Traffic Origin ได้

2.4.3 สามารถส่ง Raw log และ Event log การใช้งาน ไปยังสถานที่เก็บ log ของธนาคารได้

2.4.4 สามารถกำหนดสิทธิผู้ใช้งาน (RBAC) และยืนยันตัวตนด้วยวิธี Two-Factor Authentication ได้

3. การรับประกันคุณภาพ (Warranty)

ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกจะต้องจัดให้มีการรับประกันการอนุญาตให้ใช้สิทธิในโปรแกรมเป็นระยะเวลา 1 ปี เริ่มตั้งแต่วันที่ 1 พฤศจิกายน 2567 – 31 ตุลาคม 2568

4. การให้บริการสนับสนุนของการใช้บริการตลอดระยะเวลาการใช้บริการ (Support)

4.1 ดำเนินการดูแลพร้อมให้บริการแก้ไขปัญหาเกี่ยวกับบริการป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์ ตลอดระยะเวลา 1 ปี พร้อมจัดทำรายงานสรุปสถิติภัยคุกคามประจำเดือน (Monthly Report)

4.2 จัดให้มีเจ้าหน้าที่เข้าตรวจสอบสถานะการทำงานของระบบ (Preventive Maintenance) ไม่น้อยกว่า 4 ครั้ง/ปี พร้อมจัดทำรายงานสรุปการดำเนินการ และสถานะของระบบ รวมถึงเหตุการณ์ที่น่าสนใจ โดยต้องแจ้งให้ธนาคารทราบล่วงหน้าในการเข้าดำเนินการไม่น้อยกว่า 1 วัน และต้องได้รับความเห็นชอบจากธนาคารก่อนเข้าดำเนินการ และส่งมอบรายงานให้ธนาคารภายใน 15 วันของเดือนถัดไป ตามรายละเอียด ดังต่อไปนี้

4.2.1 รายงานสรุปผลการตรวจสอบสถานะของระบบ (Health Check Report) สรุปผลการตรวจสอบและสถานะของบริการป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์

4.2.2 รายงานสรุปเหตุการณ์ที่น่าสนใจ (Events Report) ซึ่งได้ตรวจพบจาก Traffic log บน Dashboard ของบริการป้องกันภัยคุกคาม WAF DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์

ครั้งที่ 1 ภายในเดือนมกราคม 2568

ครั้งที่ 2 ภายในเดือนเมษายน 2568

ครั้งที่ 3 ภายในเดือนกรกฎาคม 2568

ครั้งที่ 4 ภายในเดือนตุลาคม 2568

4.3 ตลอดระยะเวลาการให้บริการจะต้องจัดให้มีทีมงานที่มีความรู้ความชำนาญเกี่ยวกับบริการป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์ พร้อมหมายเลขโทรศัพท์ที่สามารถติดต่อได้เพื่อให้คำปรึกษา และให้ความช่วยเหลือเบื้องต้น (On Phone Support) ทุกวันตลอด 24 ชั่วโมง (7x24)

4.4 ในกรณีที่บริการป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์ เกิดเหตุขัดข้องชำรุด หรือมีข้อบกพร่องที่ไม่สามารถใช้งานได้ ผู้ยื่นข้อเสนอที่ได้รับคัดเลือกจะต้องจัดส่งเจ้าหน้าที่เข้ามาให้บริการตรวจสอบ และแก้ไขปัญหาให้กับทางธนาคาร รวมทั้งต้องดำเนินการตรวจสอบแก้ไขหรือปรับปรุงให้แล้วเสร็จภายในกำหนดระยะเวลานับถัดจากที่ได้รับแจ้งเหตุขัดข้องหรือความชำรุดบกพร่องจากธนาคาร ตามระดับผลกระทบที่มีต่อธุรกิจ หรือการทำงาน (Severity) ดังนี้

ระดับผลกระทบ (Severity)	ระยะเวลาติดต่อกลับ	ระยะเวลาการแก้ไขปัญหาเสร็จสิ้นนับจากที่ได้รับแจ้ง
Urgent บริการป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์ ไม่สามารถใช้งานได้	30 นาที	4 (สี่) ชั่วโมง
High บริการป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์ ทำงานผิดพลาดซึ่งเป็นส่วนสำคัญที่ส่งผลกระทบต่อการดำเนินงานของธนาคาร	1 ชั่วโมง	8 (แปด) ชั่วโมง
Medium บริการป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์ ทำงานผิดพลาดซึ่งไม่เป็นส่วนสำคัญที่กระทบต่อการดำเนินงานของธนาคาร	2 ชั่วโมง	48 (สี่สิบแปด) ชั่วโมง
Low บริการป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์ ทำงานผิดพลาด ซึ่งไม่เป็นส่วนสำคัญที่ไม่กระทบต่อการดำเนินงานของธนาคาร	4 ชั่วโมง	96 (เก้าสิบหก) ชั่วโมง

4.5 ในกรณีที่ธนาคารร้องขอให้ติดตั้ง Sub-domain เพิ่มเติม ทางผู้ยื่นข้อเสนอจะต้องดำเนินการติดตั้ง แก้ไขปัญหา และทดสอบความพร้อมใช้งานของบริการป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์ โดยไม่มีค่าใช้จ่ายเพิ่มเติม

4.6 จัดทำรายละเอียดและขั้นตอนการเข้ามาดำเนินการแก้ไขปัญหาหรือเหตุขัดข้องหรือความชำรุดบกพร่องของบริการป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์ ให้กับธนาคารในทันทีที่สามารถดำเนินการได้

4.7 ดำเนินการ Review Policy ตาม Best Practice เพื่อปรับปรุงระบบความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ตามที่ธนาคารได้มีการร้องขอ โดยไม่คิดค่าใช้จ่ายเพิ่มเติม

4.8 ดำเนินการ Configure บริการป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์ ตามที่ธนาคารได้มีการร้องขอ

5. การ Upgrade โปรแกรม

ในระหว่างดำเนินการติดตั้งหรือภายในระยะเวลารับประกัน หาก Application Software หรือ Firmware หรือ Patch หรือระบบปฏิบัติการของบริการป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์ มีการออก Version ใหม่ หรือพัฒนาปรับปรุง (Upgrade) ผู้ยื่นข้อเสนอที่ได้รับเลือกจะต้องแจ้งรายละเอียดการเปลี่ยนแปลงและผลกระทบที่เกิดขึ้นจากการเปลี่ยนแปลงดังกล่าวให้ธนาคารทราบ เพื่อใช้เป็นข้อมูลประกอบการตัดสินใจของธนาคาร และหากธนาคารประสงค์จะดำเนินการพัฒนาปรับปรุง (Upgrade) ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกต้องดำเนินการพัฒนาปรับปรุง (Upgrade) ให้กับธนาคารโดยไม่คิดค่าใช้จ่าย