ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและรายละเอียดค่าใช้จ่าย

การจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง

1. ชื่อโครงการ การจ้างผู้ให้บริการ VA Scan & Penetration Test

2. หน่วยงานเจ้าของโครงการ ฝ่ายปฏิบัติการเทคโนโลยีสารสนเทศ

3. วงเงินงบประมาณที่ได้รับจัดสรร 1,500,000.00 บาท (หนึ่งล้านห้าแสนบาทถ้วน)

4. วันที่กำหนดราคากลาง (ราคาอ้างอิง) ณ วันที่ 4 ก.ย. 2568
   เป็นเงิน 1,495,975.33 บาท (หนึ่งล้านสี่แสนเก้าหมื่นห้าพันเก้าร้อยเจ็ดสิบห้าบาทสามสิบสามสตางค์)

5. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)
   5.1. บริษัท แบงคอค เอ็มเอสพี จำกัด
   5.2 บริษัท อี-ซี.โอ.พี (ประเทศไทย) จำกัด
   5.3 บริษัท โซ ซีเคียว จำกัด

6. รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง) ทุกคน
   6.1 นายจรัส ขวัญพิเชษฐ์สกุล ผู้บริหารส่วนรักษาความปลอดภัยเทคโนโลยีสารสนเทศ / ฝ่ายปส.
   6.2 นายกิตติ์ธเนศ วงศ์ประสิทธิ์ ผู้ช่วยผู้บริหารส่วนบริการและปฏิบัติการเทคโนโลยีสารสนเทศ / ฝ่าย ปส.
   6.3 นางสาวเยาวลักษณ์ กำเนิดกาญจน์ เจ้าหน้าที่ธุรการส่วนจัดซื้อเทคโนโลยีสารสนเทศ / ฝ่าย จธ.

รายละเอียดและขอบเขตของงาน
การจ้างผู้ให้บริการ VA Scan & Penetration Test

1. ความเป็นมาและวัตถุประสงค์

1.1 ความเป็นมา

เนื่องด้วยธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย ซึ่งต่อไปนี้จะเรียกว่า "ธนาคาร" มีความประสงค์จะดำเนินการตรวจสอบความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ เพื่อประเมินสถานะความมั่นคงปลอดภัยด้านสารสนเทศ ลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากภัยคุกคามไซเบอร์ รวมถึงการเตรียมความพร้อมในการรับมือภัยคุมคามที่อาจเกิดขึ้น เพื่อป้องกันความเสี่ยงและผลกระทบต่อการดำเนินธุรกิจของธนาคาร จึงจำเป็นต้องจัดจ้างผู้ให้บริการเข้าดำเนินการประเมินช่องโหว่ และทดสอบเจาะระบบ พร้อมวิเคราะห์และให้คำแนะนำในการปิดช่องโหว่และตรวจสอบผลการปิดช่องโหว่ เพื่อป้องกันไม่ได้เกิดความเสียหายต่อข้อมูลของลูกค้าหรือระบบงานของธนาคาร ซึ่งการจ้างในครั้งนี้รวมถึงการให้สิทธิการใช้งาน ตลอดจนการดำเนินงานอื่นๆ ที่จำเป็น เพื่อให้ธนาคารใช้บริการได้ตามขอบเขตงานที่ต้องการ

1.2 วัตถุประสงค์

1.2.1 เพื่อดำเนินการตรวจสอบ ประเมินช่องโหว่ด้านความมั่นคงปลอดภัย (Vulnerability Assessment: VA) ของอุปกรณ์ในระบบเครือข่าย เครื่องคอมพิวเตอร์แม่ข่าย (Server) หรืออุปกรณ์ในระบบเครือข่าย (Network Equipment) หรืออุปกรณ์ในระบบรักษาความปลอดภัยสารสนเทศ (Security Device) จากเครือข่ายภายใน (Internal Vulnerability Assessment)

1.2.2 เพื่อดำเนินการทดสอบการเจาะระบบ (Penetration Test) ระบบคอมพิวเตอร์และระบบเครือข่ายจากเครือข่ายภายในและเครือข่ายภายนอกที่ธนาคารใช้งานในปัจจุบัน

1.2.3 เพื่อป้องกันความเสี่ยงและผลกระทบต่อการดำเนินธุรกิจของธนาคาร เฝ้าระวังและรับมือกับภัยคุมคาม และปรับปรุงการรักษาความมั่นคงปลอดภัยทางไซเบอร์

2. วงเงินงบประมาณ / วงเงินที่ได้รับการจัดสรร

1,500,000.00 บาท (หนึ่งล้านห้าแสนบาทถ้วน) (รวมภาษีมูลค่าเพิ่มแล้ว)

3. ข้อกำหนดความต้องการทั่วไป

3.1 ผู้ยื่นข้อเสนอต้องเสนอบริการประเมินช่องโหว่ (Vulnerability Assessment: VA) และทดสอบเจาะระบบ (Penetration Test) ที่มีคุณสมบัติสามารถทำงานร่วมกับระบบคอมพิวเตอร์และระบบเครือข่าย ของธนาคารที่ใช้งานอยู่ในปัจจุบันได้

3.2 หากอุปกรณ์หรือโปรแกรมหรือส่วนประกอบเพิ่มเติมที่ธนาคารไม่ได้กำหนดและมีความจำเป็นต้องนำมาใช้งานร่วมกันเพื่อให้เกิดประสิทธิภาพสูงสุด ผู้ยื่นข้อเสนอจะต้องจัดหาและส่งมอบให้กับธนาคารได้อย่างครบถ้วน

3.3 ผู้ยื่นข้อเสนอต้องมีสิทธิในการใช้งานอุปกรณ์หรือโปรแกรมที่ใช้ในการให้บริการอย่างถูกต้องตามกฎหมาย และจัดให้ธนาคารมีสิทธิใช้งานได้โดยไม่ละเมิดสิทธิ์ของผู้อื่น รวมทั้งรับผิดชอบในกรณีที่มีการกล่าวหาฟ้องร้องหรือเรียกค่าเสียหายใดๆ จากเจ้าของลิขสิทธิ์

4. ขอบเขตของงาน

4.1 ดำเนินการตรวจสอบและวิเคราะห์ความเสี่ยงของช่องโหว่ด้านความมั่นคงปลอดภัย (Vulnerability Assessment) เพื่อสำรวจสถานภาพด้านความปลอดภัยของเครื่องคอมพิวเตอร์แม่ข่าย (Server) หรืออุปกรณ์ในระบบเครือข่าย (Network Equipment) หรืออุปกรณ์ในระบบรักษาความปลอดภัยสารสนเทศ (Security Device) จากเครือข่ายภายใน (Internal Vulnerability Assessment) ของธนาคาร จำนวนไม่น้อยกว่า 400 อุปกรณ์ หรือ 400 IP Address พร้อมทั้งจัดทำรายงานผลการตรวจสอบและวิเคราะห์ความเสี่ยงของช่องโหว่ด้านความมั่นคงปลอดภัย ซึ่งต้องประกอบด้วยความเสี่ยงและผลกระทบของช่องโหว่ที่ตรวจพบ และแนะนำวิธีการแก้ไขหรือป้องกัน

ในการตรวจสอบและวิเคราะห์ความเสี่ยงของช่องโหว่ด้านความมั่นคงปลอดภัย (Vulnerability Assessment) ผู้ยื่นข้อเสนอต้องดำเนินการใช้โปรแกรมหรือซอฟท์แวร์แบบ Commercial และ Non-Commercial ที่มีความน่าเชื่อถืออย่างน้อยแบบละ 1 โปรแกรม และเป็นโปรแกรมที่ผู้ยื่นข้อเสนอมีลิขสิทธิ์การใช้งานถูกต้อง

4.2 ต้องจัดให้ธนาคารได้รับสิทธิการใช้งาน License Tenable Nessus Professional และเพิ่ม Nessus Fundamentals จำนวน 1 License ระยะเวลา 1 ปี (เริ่มใช้บริการตั้งแต่วันที่ 1 ตุลาคม 2568 – 30 กันยายน 2569) เพื่อให้ทางธนาคารสามารถตรวจสอบช่องโหว่ซ้ำได้

4.3 ดำเนินการตรวจสอบและวิเคราะห์ความเสี่ยงของการทดสอบเจาะระบบเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์ที่เกี่ยวข้องดังต่อไปนี้

4.3.1 ทดสอบเจาะระบบจากเครือข่ายภายนอก แบบ Black-box (External Black-box Penetration Testing) ผ่านช่องทาง Web Application จำนวนไม่เกิน 11 website โดยดำเนินการทดสอบไม่เกิน 3 ครั้ง เพื่อเปรียบเทียบผลการดำเนินการปิดช่องโหว่ (Pentest 1 ครั้ง Revisit ไม่เกิน 2 ครั้ง)

4.3.2 ทดสอบเจาะระบบจากเครือข่ายภายนอก แบบ Black-box (External Black-box Penetration Testing) ผ่านช่องทาง Mobile Application 1 application โดยดำเนินการทดสอบไม่เกิน 3 ครั้ง เพื่อเปรียบเทียบผลการดำเนินการปิดช่องโหว่ (Pentest 1 ครั้ง Revisit ไม่เกิน 2 ครั้ง) ดังรายละเอียดต่อไปนี้

- MY EXIM (IOS)
- MY EXIM (Android)

4.3.3 ทดสอบเจาะระบบจากเครือข่ายภายใน แบบ Black-box (External Black-box Penetration Testing) ผ่านช่องทาง Web Application จำนวนไม่เกิน 2 website โดยดำเนินการทดสอบไม่เกิน 3 ครั้ง เพื่อเปรียบเทียบผลการดำเนินการปิดช่องโหว่ (Pentest 1 ครั้ง Revisit ไม่เกิน 2 ครั้ง)

4.3.4 ทดสอบเจาะระบบจากเครือข่ายภายใน โดยอ้างอิงจากผลการทดสอบที่ผ่านมา (Revisit) ผ่านช่องทาง Web API จำนวนไม่เกิน 10 ช่องโหว่ โดยดำเนินการทดสอบไม่เกิน 3 ครั้ง

4.3.5 ทดสอบเจาะระบบเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์ที่เกี่ยวข้องจากเครือข่ายภายในแบบ Black-box (Internal Black-box Network/Infrastructure Penetration Testing) จำนวน 50 อุปกรณ์ หรือ 50 IP Address

4.3.6 ดำเนินการทดสอบเจาะระบบในรูปแบบการแบบผสมผสานโดยใช้โปรแกรมเจาะระบบแบบอัตโนมัติ (Automate Tool) ทั้งที่เป็น Commercial Tool และที่เป็น Open Source Tool รวมกับความเชี่ยวชาญของบุคลากร (Human Skill) ที่ทำการทดสอบเจาะระบบ พร้อมเก็บหลักฐานจากการทดสอบ

4.3.7 ดำเนินการจัดทำรายงานผลการทดสอบการเจาะระบบ พร้อมนำเสนอจุดอ่อน ผลกระทบและระดับความเสี่ยง ตลอดจนให้คำแนะนำในการปรับปรุงแก้ไข

4.3.8 ผู้ยื่นข้อเสนอจะต้องแจ้งธนาคารให้ทราบทุกครั้งก่อนเข้าดำเนินการต่างๆ โดยจะต้องทำการประเมินผลกระทบที่อาจเกิดขึ้นระหว่างดำเนินงาน และได้รับความยินยามจากธนาคารก่อนการดำเนินการ

4.3.9 ผู้ยื่นข้อเสนอสามารถดำเนินการนอกเวลาทำการของธนาคารได้ โดยเป็นข้อกำหนดหรือความต้องการของธนาคาร เช่น หลังระบบพ้นช่วง Peak hour หรือวันหยุดทำการ ทั้งนี้ ขึ้นอยู่กับการตกลงร่วมกันของทั้งสองฝ่าย

4.3.10 ผู้ยื่นข้อเสนอจะต้องทำงานในสภาวะแวดล้อมที่ปลอดภัย ในขณะทำการทดสอบระบบจากภายนอก

4.3.11 ดำเนินการทดสอบเจาะระบบตามมาตรฐาน OWAPS Top 10 หรือ CWE/SANS TOP 25

4.4 บุคลากรที่เสนอให้ดำเนินการโครงการ ต้องเป็นบุคคลที่มีคุณสมบัติตามที่ธนาคารกำหนด ตั้งแต่ช่วงเสนอราคาจนกระทั่งสิ้นสุดโครงการ และจะต้องเป็นบุคคลเดียวกัน หากมีความจำเป็นต้องเปลี่ยนแปลงบุคลากร ผู้ยื่นข้อเสนอต้องเสนอบุคลากรที่มีคุณสมบัติไม่น้อยกว่าบุคลากรเดิม โดยแจ้งเป็นลายลักษณ์อักษรล่วงหน้าอย่างน้อย 1 วันทำการ และต้องได้รับความเห็นชอบจากธนาคาร ทั้งนี้การพิจารณาดังกล่าวให้อยู่ในดุลยพินิจของธนาคาร

4.5 จัดให้มีบุคลากรที่มีความรู้ความเชี่ยวชาญเข้าร่วมประชุมกับธนาคาร ในการดำเนินการงานดังกล่าว

4.6 ผู้ยื่นข้อเสนอต้องจัดทำและเสนอแผนการดำเนินการให้ธนาคารเห็นชอบก่อนดำเนินการ

4.7 การดำเนินการงานดังกล่าว ต้องไม่ส่งผลกระทบหรือสร้างความเสียหายต่อระบบงานของธนาคาร หากเกิดความเสียหาย ผู้ยื่นข้อเสนอต้องรับผิดชอบในการดำเนินการให้ระบบงานนั้นใช้งานได้เป็นปกติดังเดิม โดยไม่คิดค่าใช้จ่ายใดๆ เพิ่มเติม

4.8 ต้องจัดให้มีบุคลากรเข้ามากรณีเรียกใช้บริการเพิ่มเติมตามที่ตกลงกัน ที่นอกเหนือจากข้อ 4.1 และ 4.3 รวมกันไม่เกิน 10 Man day ภายในระยะเวลาสัญญา พร้อมทั้งจัดทำรายงานผลการทดสอบ พร้อมนำเสนอจุดอ่อน ผลกระทบและระดับความเสี่ยง ตลอดจนให้คำแนะนำในการปรับปรุงแก้ไข (ถ้ามี)

4.9 ต้องมีผลงานในการตรวจสอบด้านความมั่นคงปลอดภัยของระบบเครือข่ายการสื่อสารและระบบคอมพิวเตอร์ (Vulnerability / Penetration Testing) ให้กับสถาบันการเงิน หรือหน่วยงานภาครัฐ รัฐวิสาหกิจ หรือ บริษัทเอกชนในประเทศไทย ที่ดำเนินการแล้วเสร็จ อย่างน้อย 1 ผลงาน ภายในระยะเวลาย้อนหลังไม่เกิน 3 ปี นับถัดจากวันที่ส่งมอบงานที่แล้วเสร็จ จนถึงวันยื่นเอกสารประกวดราคาจ้างด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ครั้งนี้ มีมูลค่าไม่น้อยกว่า 5 แสนบาท (ห้าแสนบาทถ้วน) ต่อผลงาน และต้องเป็นผลงานที่ผู้ยื่นข้อเสนอเป็นคู่สัญญาโดยตรง โดยแสดงหนังสือรับรองผลงาน หรือหนังสือตรวจรับงาน หรือเอกสารอื่นใดที่แสดงถึงผลงาน และการส่งมอบที่แล้วเสร็จทั้งโครงการมาแสดงในวันยื่นเอกสารประกวดราคาจ้างด้วยวิธีประกวดราคาอิเล็กทรอนิกส์

4.10 ต้องมีบุคลากรผู้ดำเนินงาน ซึ่งได้รับรองมาตรฐานความรู้ความสามารถทางด้านความปลอดภัยคอมพิวเตอร์ จำนวนไม่น้อยกว่า 1 คน ตามที่ระบุด้านล่างนี้ (นำเสนอ 1 คน ต่อ 1 ตำแหน่ง) โดยต้องยื่นเอกสารรับรอง (Certificate) ที่ยังมีผลบังคับใช้ของบุคลากร พร้อมกับการเสนอเอกสารประกวดราคา

4.10.1 ผู้ควบคุมการดำเนินการ ต้องมีใบรับรองมาตรฐานความรู้ความสามารถทางด้านความปลอดภัยคอมพิวเตอร์อย่างใดอย่างหนึ่ง ดังนี้

4.10.1.1 CISSP (Certified Information System Security Professional) หรือ CISA (Certified Information Systems Auditor)

4.10.1.2 GPEN (GIAC Penetration Tester) หรือ GCIH (GIAC Certified Incident Handler) หรือ OSCP (Offensive Security Certified Professional) หรือ GWAPT (GIAC Web Application Penetration Tester) หรือ CEH (Certified Ethical Hacker)

4.10.2 ผู้ดำเนินการทดสอบ

CEH (Certified Ethical Hacker) หรือ GPEN (GIAC Penetration Tester) หรือ GCIH (GIAC Certified Incident Handler) หรือ OSCP (Offensive Security Certified Professional) หรือ GWAPT (GIAC Web Application Penetration Tester)

5. กำหนดเวลาส่งมอบพัสดุ

ผู้ยื่นข้อเสนอราคาที่ได้รับการคัดเลือกต้องดำเนินการตามรายละเอียดและขอบเขตการดำเนินการที่กำหนดในสัญญาได้อย่างถูกต้องครบถ้วน และการดำเนินการอื่นๆ ที่จำเป็น เพื่อให้งานดังกล่าวแล้วเสร็จ ภายในระยะเวลา 330 วัน นับถัดจากวันที่ลงนามในสัญญา

6. หลักเกณฑ์ในการพิจารณาคัดเลือกข้อเสนอ

ธนาคารจะพิจารณาตัดสินโดยใช้หลักเกณฑ์ราคา

7. งวดงานและการจ่ายเงิน

ธนาคารจะจ่ายค่าจ้างแบบเหมาจ่าย ซึ่งได้รวมภาษีมูลค่าเพิ่มตลอดจนภาษีอากรอื่นๆ และค่าใช้จ่ายทั้งปวงด้วยแล้วให้แก่ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกให้เป็นผู้รับจ้าง โดยแบ่งออกเป็นรายงวด รวม 2 งวด หลังสิ้นสุดการบริการงานในแต่ละงวด ภายใน 30 วัน เมื่อผู้รับจ้างได้ให้บริการงานดังกล่าว และส่งมอบรายงาน**ในรูปแบบเอกสารสื่อสิ่งพิมพ์ และบันทึกลงบนสื่ออิเล็กทรอนิกส์หรือช่องทางที่ธนาคารกำหนด จำนวน 1 ชุด** ได้ถูกต้อง เรียบร้อยและครบถ้วนตามสัญญาจ้างหรือข้อตกลง และธนาคารได้ตรวจรับมอบงานจ้างเรียบร้อยแล้ว ดังรายละเอียดต่อไปนี้

งวดที่ 1 ชำระร้อยละ 40 เมื่อผู้ยื่นข้อเสนอได้ปฏิบัติงานตามรายละเอียดและขอบเขตงานตามข้อ 4.1 และข้อ 4.2 พร้อมส่งมอบเอกสาร ให้แล้วเสร็จภายใน 180 วัน นับถัดจากวันที่ลงนามสัญญา ดังต่อไปนี้

1) รายงานผลการตรวจสอบและวิเคราะห์ความเสี่ยงของช่องโหว่ด้านความมั่นคงปลอดภัย จำนวน 1 ชุด

2) หนังสือยืนยันสิทธิการใช้งาน License Tenable Nessus Professional 1 ปี + Nessus Fundamentals จำนวน 1 License

3) หนังสือยืนยันไม่มีโปรแกรมแอบแฝง จำนวน 1 ฉบับ

งวดที่ 2 (งวดสุดท้าย) ชำระร้อยละ 60 เมื่อผู้ยื่นข้อเสนอได้ปฏิบัติงานตามรายละเอียดและขอบเขตงาน ตามข้อ 4.3.1 - 4.3.5 จนแล้วเสร็จ ครบถ้วนตามขอบเขตงานที่กำหนด พร้อมส่งมอบรายงานผลการตรวจสอบทดสอบเจาะระบบ จำนวน 1 ชุด และบริการเพิ่มเติมตามข้อ 4.8 โดยคำนวณจากจำนวน Man day ที่ใช้ในการบริการตามจริงที่ได้ตกลงร่วมกับธนาคาร (ถ้ามี) ให้แล้วเสร็จภายใน 330 วัน นับถัดจากวันที่ลงนามสัญญา

8. อัตราค่าปรับ

8.1 กรณีที่ผู้รับจ้างนำงานที่รับจ้างไปจ้างช่วงให้ผู้อื่นทำอีกทอดหนึ่งโดยไม่ได้รับอนุญาตจากธนาคารจะกำหนดค่าปรับสำหรับการฝ่าฝืนดังกล่าวเป็นจำนวนร้อยละ 10 ของวงเงินของงานจ้างช่วงนั้น

8.2 กรณีที่ไม่สามารถส่งมอบตามงวดงานในข้อ 7. ผู้ยื่นข้อเสนอจะต้องยินยอมให้ธนาคารปรับเป็นรายวันในอัตราร้อยละ 0.1 (ศูนย์จุดหนึ่ง) ของมูลค่างานทั้งหมด (รวมภาษีมูลค่าเพิ่ม) นับถัดจากวันครบกำหนดการส่งมอบจนถึงวันที่ได้ส่งมอบงานถูกต้องครบถ้วน หรือวันที่ธนาคารบอกเลิกจ้าง

ทั้งนี้ หากธนาคารตรวจสอบแล้วพบว่างานดังกล่าวที่ส่งมอบไม่ตรงตามขอบเขตการดำเนินงานและข้อกำหนดด้านเทคนิคที่กำหนดในสัญญา ธนาคารสงวนสิทธิ์ที่จะไม่รับมอบงานจ้างทั้งหมด หรือเพียงบางส่วน หรือให้ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกดำเนินการเปลี่ยนแปลง และ/หรือปรับปรุงแก้ไขให้ถูกต้องตามคำชี้ขาดของธนาคารด้วยค่าใช้จ่ายของผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกเองทั้งสิ้น ทั้งนี้ ระยะเวลาที่เสียไปเพราะเหตุดังกล่าว ไม่เป็นเหตุให้ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกมีสิทธิขยายระยะเวลาการส่งมอบเกินกำหนดเวลาที่ระบุในสัญญา หรือข้อยกเว้น หรือลดค่าปรับได้