หอการค้าไทย
THE THAI CHAMBER OF COMMERCE
สภาหอการค้าแห่งประเทศไทย
BOARD OF TRADE OF THAILAND

ประกาศ

หอการค้าไทยและสภาหอการค้าแห่งประเทศไทย

ที่ ๐๓๑ /2569

เรื่อง ประกวดราคาการจัดจ้างงานบริการทดสอบระบบเทคโนโลยีสารสนเทศ

****

หอการค้าไทย มีความประสงค์จะประกวดราคาการจัดจ้างงานบริการทดสอบระบบเทคโนโลยีสารสนเทศ ของหอการค้าไทยและสภาหอการค้าแห่งประเทศไทย ดังรายละเอียดคุณลักษณะเงื่อนไขคุณสมบัติและขอบเขตของงาน (TOR) ตามเอกสารแนบท้ายนี้

1. เป็นนิติบุคคล ที่ดำเนินธุรกิจให้บริการด้านการทดสอบ ประเมิน และให้คำแนะนำ ที่สอดคล้องกับโครงการไม่น้อยกว่า 5 ปี และมีมาตรฐานการทดสอบเป็นที่ยอมรับ เช่น OWASP TOP 10, NIST และได้รับการตรวจสอบตามมาตรฐานในระดับสากลที่สอดคล้องกับโครงการ และมีใบรับรองที่ยังมีผลบังคับใช้ เช่น ISO9001:2015, ISO/IEC27001, ISOIEC27701 เป็นต้น
2. ทีมบุคลากรมีความเชี่ยวชาญเฉพาะ ตามหลักมาตรฐานความมั่นคงปลอดภัยสากล มีวุฒิบัตรที่เกี่ยวข้องกับโครงการอย่างน้อย 1 รายการและยังมีผลบังคับใช้ เช่น OSCP, CEH, CISSP, GPEN เป็นต้น
3. ไม่ประกอบธุรกิจที่มีความเสี่ยง ที่เป็นสาเหตุของความเสียต่อสาธารณะ
4. ไม่เป็นผู้ที่ระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานของทางราชการและได้แจ้งเวียนชื่อแล้ว หรือไม่เป็นผู้ที่ได้รับผลของการสั่งให้นิติบุคคลหรือบุคคลอื่นเป็นผู้ทิ้งงานตามระเบียบของทางราชการ
5. ต้องแนบสำเนาหนังสือรับรองการจดทะเบียนหุ้นส่วนบริษัท พร้อมวัตถุประสงค์ของการประกอบกิจการ (ที่มีอายุไม่เกิน 6 เดือน) นับถึงวันที่ยื่นขอเสนองาน
6. ราคาที่เสนอประกวดราคาให้รวมภาษีมูลค่าเพิ่ม และผู้รับดำเนินการจะถูกหักภาษี ณ ที่จ่าย
7. สอบถามข้อมูลเพิ่มเติมได้ที่ หอการค้าไทย เลขที่ 150 ถนนราชบพิธ เขตพระนคร กรุงเทพฯ 10200 ส่วนงานจัดซื้อจัดจ้าง โทร 02-018-6888 ต่อ 3350,3360 ตั้งแต่วันที่ 28 เมษายน – 11 พฤษภาคม 2569 ระหว่างเวลา 08.30-16.30 น.(เว้นวันหยุดราชการ) หรือดูรายละเอียดเพิ่มเติมที่ www.thaichamber.org

กำหนดยื่นซองประกวดราคาภายในวันที่ 11 พฤษภาคม 2569 เวลา 08.30-16.30 น. ณ สถานที่ดังกล่าว

ประกาศ ณ วันที่ 28 เมษายน 2569

(นายธวัชชัย เศรษฐจินดา)
กรรมการเลขาธิการ

ขอบเขตของงาน (Terms of Reference: TOR)
โครงการจัดหาบริการทดสอบระบบเทคโนโลยีสารสนเทศ
หอการค้าไทย และ สภาหอการค้าแห่งประเทศไทย

1. หลักการและเหตุผล

หอการค้าไทยและสภาหอการค้าแห่งประเทศไทย จัดตั้งขึ้นตามพระราชบัญญัติหอการค้า พ.ศ. 2509 โดยมีสถานะเป็นองค์กรหลักในการส่งเสริมและสนับสนุนการประกอบธุรกิจทั้งด้านการค้าการบริการ อุตสาหกรรมเกษตรกรรมและการเงินมุ่งเน้นการเป็นศูนย์กลางในการเชื่อมโยงเครือข่ายความร่วมมือระหว่างภาครัฐเอกชนและภาคประชาชนทั้งในและต่างประเทศเพื่อขับเคลื่อนเศรษฐกิจไทยให้เติบโตอย่างยั่งยืนด้วยนวัตกรรมและมาตรฐานการดำเนินธุรกิจที่เป็นสากล

ในปัจจุบัน หอการค้าไทยและสภาหอการค้าแห่งประเทศไทยได้นำระบบเทคโนโลยีสารสนเทศมากกว่า 20 ระบบมาใช้เป็นกลไกสำคัญในการบริหารจัดการฐานข้อมูลสมาชิกและการให้บริการเครือข่ายทั่วประเทศ อย่างไรก็ตาม ท่ามกลางการเปลี่ยนแปลงทางเทคโนโลยีอย่างรวดเร็ว ความเสี่ยงจากภัยคุกคามทางไซเบอร์ (CyberThreats)มีแนวโน้มสูงขึ้นและซับซ้อนยิ่งขึ้นไม่ว่าจะเป็นภัยจากภายนอกหรือความเสี่ยงที่อาจเกิดขึ้นจากกระบวนการทำงานภายใน ซึ่งอาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบและข้อมูลสำคัญขององค์กร

หอการค้าไทยและสภาหอการค้าแห่งประเทศไทยจึงตระหนักถึงความสำคัญในการป้องกันและลดความเสี่ยงดังกล่าวเพื่อเสริมสร้างมาตรการป้องกันให้มีประสิทธิภาพสูงสุดตามมาตรฐานความปลอดภัยสารสนเทศสากล

2. วัตถุประสงค์

2.1 เพื่อสร้างความมั่นใจในกระบวนการพัฒนา การใช้งานระบบมีความมั่นคง ป้องกันความเสี่ยงตามมาตรฐาน ด้วยการทดสอบและประเมินช่องโหว่ (Vulnerability Assessment: VA) และทดสอบเจาะระบบ (Penetration Testing) ระบบเทคโนโลยีสารสนเทศสำคัญ

2.2 สร้างความเชื่อมั่นแก่เจ้าหน้าที่ สมาชิก ผู้ใช้บริการถึงปลอดภัยของระบบสารสนเทศและกระบวนการให้บริการขององค์กร

2.3 เพื่อปรับปรุงแก้ไขและปิดช่องโหว่ที่อาจถูกคุกคามโดยผู้ไม่ประสงค์ดีป้องกันการเข้าถึงข้อมูลโดยมิชอบหรือการกระทำที่ส่งผลกระทบต่อการทำงานของระบบอย่างมีประสิทธิภาพ

2.4 เพื่อยกระดับภาพลักษณ์ขององค์กรด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (Cybersecurity) โดยเน้นหลักการความลับ (Confidentiality), ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูล

2.5 เพื่อดำเนินการแก้ไขและปรับปรุงประเด็นข้อเสนอแนะที่ได้รับจากการตรวจสอบของหน่วยงานตรวจสอบระบบสารสนเทศภายนอก (External IT Auditor) ให้ครบถ้วนสมบูรณ์

3. คุณสมบัติผู้เสนอราคา

3.1 เป็นนิติบุคคลที่ไม่มีความสัมพันธ์ที่อาจก่อให้เกิดผลประโยชน์ทับซ้อนกับองค์กรหรือบริษัทที่องค์กรใช้บริการพัฒนาระบบงานต่างๆ

3.2 ไม่ประกอบธุรกิจที่มีความเสี่ยง ที่เป็นสาเหตุของความเสียหายต่อสาธารณะ

3.3 มีประสบการณ์ให้บริการแก่บริษัทหรือองค์กรที่มีลักษณะใกล้เคียงกับหอการค้าไทยและสภาหอการค้าแห่งประเทศไทย

3.4 มีประสบการณ์เป็นผู้ให้บริการด้านการทดสอบ ประเมิน และให้คำแนะนำ ที่สอดคล้องกับโครงการไม่น้อยกว่า 5 ปี และมีมาตรฐานการทดสอบเป็นที่ยอมรับ เช่น OWASP Top 10, NIST เป็นต้น

3.5 เป็นนิติบุคคลที่ได้รับการตรวจสอบตามมาตรฐานในระดับสากลที่สอดคล้องกับโครงการและมีใบรับรองที่ยังมีผลบังคับใช้ อาทิ เช่น ISO9001:2015, ISO/IEC27001, ISO/IEC27701 เป็นต้น

3.6 มีทีมบุคลากรมีความเชี่ยวชาญเฉพาะในการบริหารจัดการตามหลักมาตรฐานความมั่นคงปลอดภัยสากล มีวุฒิบัตรที่เกี่ยวข้องกับโครงการอย่างน้อย 1 รายการ และ ยังมีผลบังคับใช้เช่น OSCP (Offensive Security Certified Professional), CEH (Certified Ethical Hacker), CISSP (Certified Information Systems Security Professional), GPEN (GIAC Penetration Tester), CompTIA Pentest+, CPENT (Certified Penetration Testing Professional) เป็นต้น

3.7 ผู้เสนอราคาต้องจัดบุคลากรที่มีความรู้ เข้าใจ และเข้าถึงระบบ กระบวนการ และ เจ้าหน้าที่องค์กรเพื่ออธิบาย แนะนำ รายละเอียดโครงการได้อย่างมีประสิทธิภาพ

3.8 ต้องปฏิบัติตามมาตรการรักษาความลับของข้อมูล (NDA: Non- Disclosure Agreement) อย่างเคร่งครัด เนื่องจากต้องเข้าถึงข้อมูลสำคัญและระบบสำคัญขององค์กร

4. ขอบเขตการดำเนินงาน

ผู้เสนอราคาต้องดำเนินการทดสอบ ต้องครอบคลุม 7 ขั้นตอนตามมาตรฐาน PTES (Penetration Testing Execution Standard) ดังนี้

4.1 ศึกษา แลกเปลี่ยน และเก็บความต้องการลักษณะระบบใช้งาน กระบวนการทำงานขององค์กรและโครงสร้างภายในที่จำเป็น (Information Gathering)

4.2 วางแผนงาน และ กำหนดระยะเวลาในการทดสอบ จัดลำดับการขั้นตอน และ จัดทำรายงานตามขอบเขตการทดสอบและเจาะระบบ พร้อม รายงานเพื่อเริ่มต้นโครงการอย่างเป็นทางการ (Kick-Off)

4.3 แจ้งรายละเอียด ถึงสถานการณ์การทดสอบ วิธีที่ใช้ในการทดสอบ หลักเกณฑ์การให้คะแนน ทีมงานที่เกี่ยวข้อง รวมถึงผลกระทบอย่างชัดเจนเพื่อประสานงานและเตรียมความพร้อมก่อนการทดสอบและเจาะระบบ เป็นระยะ

4.4 ทดสอบและเจาะระบบ ตามแผนงานที่วางไว้

4.4.1 วิเคราะห์ช่องโหว่ (Vulnerability Analysis)

4.4.2 การโจมตีจำลอง (Exploitation)

4.4.3 การวิเคราะห์ผลกระทบ (Post-Exploitation)

4.5 จัดทำรายงานภาษาไทยอย่างละเอียด และชัดเจน

- รายงานมี 2 เอกสารหลัก
  - Vulnerability Testing
    - ผลตรวจครั้งแรก (Pre-Testing Report)
    - ผลตรวจสุดท้าย (Post-Testing Report)
  - Penetration Testing
    - ผลตรวจครั้งแรก (Pre-Testing Report)
    - ผลตรวจสุดท้าย (Post-Testing Report)
- หลักเกณฑ์การประเมินตามมาตรฐาน เช่น CVSS
- ระบุสถานการณ์ที่ทดสอบ (Scenario Testing)
- ปัญหา/ช่องโหว่ที่พบ พร้อมรูปภาพ Log Timestamp (หากมี) และระดับความเสี่ยง/ความรุนแรง/อันตรายของปัญหา
- รายละเอียดพร้อมแนวทางแก้ไขและคำแนะนำที่เข้าใจ ปฏิบัติตามได้จริง
- วิเคราะห์ผลกระทบในเชิงเทคนิคและธุรกิจ
- เอกสารอยู่ในรูปแบบ Soft Copy และ Hard Copy อย่างเป็นทางการ

4.6 กำกับ ดูแลและให้คำปรึกษา เพื่อสร้างความเข้าใจ และปรับปรุง แก้ไขในทางที่เหมาะสม จนกว่าจะดำเนินการครบตามข้อตกลง

4.7 จัดประชุมรายงานกระบวนการแกทีมทำงาน ผู้บริหาร และ คณะกรรมการ ถึงความคืบหน้า สรุปปัญหาความเสี่ยง และข้อเสนอแนะในการยกระดับความปลอดภัยสารสนเทศในภาพรวมขององค์กร

5. ความต้องการการทดสอบช่องโหว่และเจาะระบบ

5.1 รองรับการทดสอบและเจาะระบบสำคัญ ภายใต้การใช้งานขององค์กรหอการค้าไทยและสภาหอการค้าแห่งประเทศไทย

5.2 ดำเนินการทดสอบช่องโหว่ (Vulnerability Assessment: VA) และ ทดสอบเจาะระบบ (Penetration Testing) ต้องอ้างอิงตามแนวทาง OWASP Web Security Testing Guide (WSTG) เวอร์ชันล่าสุด โดยครอบคลุมช่องโหว่พื้นฐานตาม OWASP Top 10 เป็นอย่างน้อย

5.3 เครื่องมือที่ใช้ทดสอบต้องได้รับลิขสิทธิ์อย่างถูกต้อง (Licensed Software) และอัปเดตฐานข้อมูล (Signatures/Payloads)ให้เป็นปัจจุบันที่สุด ณ เวลาที่ตรวจสอบ เพื่อให้รองรับการตรวจจับภัยคุกคามใหม่ๆ

5.3 การทดสอบที่ผสมผสานจำลองการโจมตีโดยผู้เชี่ยวชาญที่ได้รับสิทธิ์การเข้าถึงข้อมูลบางส่วน (เช่น ข้อมูลโครงสร้างเครือข่าย หรือบัญชีผู้ใช้ทั่วไป) เพื่อจำลองสถานการณ์ที่สมจริงทั้งจากมุมมองคนภายนอกที่ต้องการเจาะระบบ และเจ้าหน้าที่ภายในที่อาจใช้สิทธิ์มิชอบ ในรูปแบบ Gray Box

5.4 ขอบเขตที่ต้องการให้ทดสอบมี 7 ระบบสำคัญ

5.4.1 เครือข่ายอินเทอร์เน็ตมีสาย (LAN) และ ไร้สาย (WiFi) ต้องอ้างอิงตามมาตรฐาน NIST SP 800-115 หรือ OSSTMM เพื่อประเมินความปลอดภัยในระดับโครงสร้างพื้นฐาน

5.4.2 ระบบสื่อสารประชาสัมพันธ์เว็บไซต์องค์กร (Thaichamber Website)

5.4.3 ระบบการจัดการสมาชิก (Member Registration) และบริการสิทธิประโยชน์ (Line OA: TCC Connect)

5.4.4 ระบบออกใบรับรองแหล่งกำเนิดสินค้าเพื่อการส่งออก (CO)

5.4.5 งานจัดแสดงสินค้า THAIFEX-Anuga เพื่อผู้ประกอบการ

5.4.6 งานจัดแสดงสินค้า THAIFEX-HOREC เพื่อผู้ประกอบการ

5.4.7 ระบบการรับชำระเงินขององค์กร (e-FMS)

5.5 การทดสอบต้องไม่ส่งผลกระทบต่อการให้บริการขององค์กร

5.6 ดำเนินการทดสอบแบบ Online และ/หรือ Onsite ตามความเหมาะสม

5.7 แจ้งผล วิเคราะห์ และแนะนำช่องโหว่ที่พบพร้อมจัดลำดับอย่างชัดเจน

5.8 มีการ Revisit Testing (Post-Testing) หลังจากปรับปรุงแก้ไขเป็นที่แล้วเสร็จ พร้อมจัดทำรายงาน

6. หน้าที่และความรับผิดชอบของผู้เสนอราคา

6.1 ผู้เสนอราคาจะต้องดำเนินการตามขอบเขตการดำเนินงานที่กำหนดภายใต้ข้อ 4 และ ข้อ 5

6.2 ผู้เสนอราคาจะต้องเริ่มดำเนินงานตามแผนงานโครงการทันทีที่ทำสัญญาร่วมกับหอการค้าไทยและสภาหอการค้าแห่งประเทศไทย หรือเริ่มในวันเวลาที่เหมาะสมเพื่อให้สอดคล้องและบรรลุตามเป้าหมายแผนงาน

6.3 ผู้เสนอราคาจะต้องอนุญาตให้เจ้าหน้าที่องค์กรที่เกี่ยวข้อง เครือข่ายองค์กร มีส่วนร่วมในกิจกรรมขั้นตอนการทำงานจริง ตั้งแต่การการติดตั้ง การตั้งค่า (Configuration) ไปจนถึงการทดสอบระบบ (Testing) รวมถึงการสรุปผลรายงาน (Reporting) เพื่อให้เกิดการถ่ายทอดเทคโนโลยีและองค์ความรู้ ที่จะสามารถใช้ในการดูแลระบบงานต่อไปในอนาคต

6.4 ผู้ชนะการประกวดราคาต้องจัดหาบุคลากรอย่างเพียงพอสำหรับควบคุม ติดตามแผนงานการทดสอบ รายงาน และคำแนะนำ

6.4.1 บุคลากรที่มีความเชี่ยวชาญมาตรการ รักษาความมั่นคงปลอดภัยของระบบไม่น้อยกว่าจำนวน 1 คน

6.4.2 บุคลากรด้านประเมินมาตรการการรักษาความมั่นคงปลอดภัยของระบบไม่น้อยกว่าจำนวน 2 คน

6.4.3 บุคลากรด้านการทดสอบเจาะระบบไม่น้อยกว่าจำนวน 3 คน

6.4.4 ผู้ประสานงานโครงการไม่น้อยกว่าจำนวน 1 คน

6.4.5 โดยบุคคลากรที่เสนอใน โครงการ 1 คน รับผิดชอบงานได้ 1 ตำแหน่งเท่านั้น

6.5 การประเมินความเสี่ยง หรือทดสอบเจาะระบบ ผู้เสนอราคาจะต้องดำเนินการโดยใช้เครื่องมือโปรแกรมหรือซอฟท์แวร์ที่น่าเชื่อถือ(อ้างอิงตามความต้องการที่ระบุในข้อ 5.3) และเป็นเจ้าของสิทธิ์หรือได้รับอนุญาต ให้ใช้งานอย่างถูกต้องตามกฎหมาย เพื่อการใช้งานซอฟต์แวร์ในการทำซ้ำ ดัดแปลง หรือเผยแพร่ สัญญาอนุญาต (License)

6.6 กรณีที่องค์กรไม่สามารถปิดช่องโหว่ตามคำแนะนำมาตรฐานได้ ผู้เสนอราคา มีหน้าที่รับผิดชอบในการวิเคราะห์ เสนอแนว และให้คำปรึกษาหาทางแก้ไขทดแทน (Compensating Controls) เพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ และให้ระบบใช้งานได้ต่อโดยปลอดภัย

6.7 ในกรณีที่ผู้ชนะประกวดราคาละเลยไม่ปฏิบัติ หรือมีการปฏิบัติงาน และก่อให้เกิดความเสียหาย อุบัติเหตุ ภยันตราย ต่อการใช้งานหรือไม่เป็นตามมาตรฐาน ผู้ชนะการประกวดราคาจะต้องรับผิดชอบค่าใช้จ่ายต่างๆในการดำเนินการแก้ไข โดยไม่สามารถเรียกร้องค่าใช้จ่ายใด ๆที่เกิดขึ้นจากหอการค้าไทยและสภาหอการค้าแห่งประเทศไทยและไม่สามารถนำเป็นข้ออ้างในการขอขยายระยะเวลาการดำเนินโครงการระบบสารสนเทศ

6.8 ผู้เสนอราคาจะต้องไม่ว่าจ้างช่วง (Subcontract) มอบหมายงาน ถ่ายโอนงาน หรือละทิ้งให้คนอื่นทำงานแทนไม่ว่าจะเป็นทั้งหมด หรือบางส่วนของโครงการ ยกเว้นได้รับอนุญาตเป็นหนังสือยิมยอมจากผู้ว่าจ้างตามกฎหมาย

7. ระยะเวลาในการดำเนินโครงการ

ระยะเวลาในการดำเนินการทดสอบภายใน 90 วัน (เก้าสิบวัน) (หรือตามที่ผู้เสนอราคาประเมินแผนงานตามความเหมาะสม)

8. งบประมาณของโครงการ

งบประมาณในการจัดหาและจัดจ้างสำหรับโครงการนี้ เป็นจำนวนเงิน 800,000 บาท (แปดแสนบาทถ้วน) ไม่รวมภาษีมูลค่าเพิ่ม ทั้งนี้ การแบ่งงวดงานและรายละเอียดเงื่อนไขการชำระเงินจะถูกกำหนดในเอกสารสัญญาต่อไป

9. สอบถามข้อมูลเพิ่มเติม

ฝ่ายเทคโนโลยีสารสนเทศ
นางสาว วัชรินทร์ วัชรศิริสุข
โทรศัพท์ 02-0186888 ต่อ 2400
อีเมล it@thaichamber.org
เลขที่ 150 ถ.ราชบพิธ แขวงวัดราชบพิธ เขตพระนคร กทม. 10200