คุณลักษณะเฉพาะ
โครงการตรวจสอบหาช่องโหว่ ประเมิน และหาจุดอ่อนของ
ระบบเทคโนโลยีสารสนเทศของสำนักงาน ป.ป.ช

โดย

สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติ
(สำนักงาน ป.ป.ช.)

๑. โครงการ

โครงการตรวจสอบหาช่องโหว่ ประเมิน และหาจุดอ่อนของระบบเทคโนโลยีสารสนเทศของสำนักงาน ป.ป.ช

๒. หลักการและเหตุผล

ปัจจุบันการโจมตีหรือภัยคุกคามทางคอมพิวเตอร์จากผู้ไม่ประสงค์ดีซึ่งได้มีเพิ่มขึ้นอย่างรวดเร็วและมีการพัฒนาอย่างต่อเนื่องในรูปแบบต่าง ๆ ที่มีการใช้เทคโนโลยีและเครื่องมือที่มีความทันสมัยมากขึ้น สำนักงาน ป.ป.ช. ได้ตระหนักถึงภัยคุกคามทางคอมพิวเตอร์ดังกล่าว และได้มีการพัฒนาและปรับปรุงระบบการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมาอย่างต่อเนื่องเพื่อควบคุมและป้องกันภัยคุกคามทางคอมพิวเตอร์ที่อาจเกิดขึ้นอย่างต่อเนื่อง เพื่อธำรงไว้ซึ่งคุณสมบัติความมั่นคงปลอดภัยด้านสารสนเทศตามมาตรฐานสากล ได้แก่ การรักษาความลับของข้อมูล (Confidentiality) การรักษาความครบถ้วนของข้อมูล (Integrity) และการที่ระบบสามารถพร้อมให้บริการอยู่เสมอ (Availability)

ดังนั้น เพื่อเพิ่มประสิทธิภาพการบริหารการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน ป.ป.ช. และลดความเสี่ยงจากภัยคุกคามคอมพิวเตอร์ที่อาจจะเกิดขึ้น จึงจำเป็นต้องดำเนินโครงการตรวจสอบหาช่องโหว่ ประเมิน และหาจุดอ่อนของระบบเทคโนโลยีสารสนเทศของสำนักงาน ป.ป.ช. เพื่อจัดจ้างผู้ที่มีความรู้ความเชี่ยวชาญในการตรวจสอบช่องโหว่ของระบบเทคโนโลยีสารสนเทศ

๓. วัตถุประสงค์

๓.๑ เพื่อตรวจสอบหาช่องโหว่ ประเมิน และหาจุดอ่อนของระบบเทคโนโลยีสารสนเทศของสำนักงาน ป.ป.ช.

๓.๒ เพื่อลดความเสี่ยงจากภัยคุกคามคอมพิวเตอร์จากผู้ไม่ประสงค์ดีซึ่งได้มีเพิ่มขึ้นอย่างรวดเร็วและมีการพัฒนาอย่างต่อเนื่องในรูปแบบต่าง ๆ ต่อระบบเทคโนโลยีสารสนเทศ สำนักงาน ป.ป.ช.

๓.๓ เพื่อเพิ่มประสิทธิภาพการบริหารการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน ป.ป.ช. ธำรงไว้ซึ่งคุณสมบัติความมั่นคงปลอดภัยตามมาตรฐานสากล ได้แก่ การรักษาความลับของข้อมูล (Confidentiality) การรักษาความครบถ้วนของข้อมูล (Integrity) และการที่ระบบสามารถพร้อมให้บริการอยู่เสมอ (Availability)

๓.๔ เพื่อพัฒนาศักยภาพด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของเจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ หรือผู้ที่เกี่ยวข้อง

๔. ประโยชน์ที่คาดว่าจะได้รับ

๔.๑ การบริหารการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักงาน ป.ป.ช. มีประสิทธิภาพเพิ่มขึ้นเป็นไปตามมาตรฐานสากล

๔.๒ ความเสี่ยงจากภัยคุกคามคอมพิวเตอร์จากผู้ไม่ประสงค์ดีที่อาจจะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศ สำนักงาน ป.ป.ช. ลดลง

๔.๓ เจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศมีศักยภาพ ความรู้ ความสามารถด้านการบริหารการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำนักงาน ป.ป.ช. เพิ่มขึ้น

/๕. กลุ่มเป้าหมาย...

๕. กลุ่มเป้าหมาย

สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติ

๖. คุณสมบัติของผู้เสนอราคา

๖.๑ คุณสมบัติของผู้เสนอราคา

๖.๑.๑ มีความสามารถตามกฎหมาย

๖.๑.๒ ไม่เป็นบุคคลล้มละลาย

๖.๑.๓ ไม่อยู่ระหว่างเลิกกิจการ

๖.๑.๔ ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราวตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

๖.๑.๕ ไม่เป็นผู้ที่ถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานของทางราชการและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐแล้ว

๖.๑.๖ มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนด

๖.๑.๗ เป็นบุคคลธรรมดาหรือนิติบุคคลที่ประกอบอาชีพรับจ้างดังกล่าว

๖.๑.๘ ไม่เป็นผู้มีผลประโยชน์ร่วมกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติ

๖.๑.๙ ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกันซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย

๖.๑.๑๐ ผู้เสนอราคาต้องลงทะเบียนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement : e-GP) ของกรมบัญชีกลาง

๖.๑.๑๑ ผู้เสนอราคาต้องมีผลงานการทดสอบเจาะระบบสารสนเทศให้แก่สถาบันการเงิน หน่วยงานภาครัฐ รัฐวิสาหกิจ หรือเอกชนอย่างน้อย ๑ โครงการ ในวงเงินไม่น้อยกว่า ๕ แสนบาท โดยเป็นสัญญาที่ทำมาไม่เกิน ๕ ปี นับถึงวันยื่นเสนอทางระบบอิเล็กทรอนิกส์ โดยผู้เสนอราคาต้องส่งหนังสือรับรองผลงานของหน่วยงานนั้น ๆ โดยต้องมีหัวหน้าหน่วยงาน หรือผู้ทำการแทนหน่วยงานนั้นทำการรับรอง และส่งมอบสำเนาสัญญาจ้าง และขอบเขตการดำเนินงาน ซึ่งแสดงถึงการทดสอบเจาะระบบสารสนเทศแล้วเสร็จ ทั้งนี้ สำนักงาน ป.ป.ช. สงวนสิทธิ์ที่จะตรวจสอบวินิจฉัยข้อเท็จจริง โดยตรงจากผู้รับรองที่เสนอมานั้น

๖.๑.๑๒ ผู้เสนอราคาต้องมีบุคลากรหลักในโครงการ ดังต่อไปนี้

(๑) หัวหน้าโครงการ

<u>คุณสมบัติ</u>:

- สำเร็จการศึกษาระดับปริญญาโท
- มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยระบบเครือข่ายสื่อสารและความปลอดภัยคอมพิวเตอร์อย่างน้อย ๓ ปี
- มีประสบการณ์ในการบริหารโครงการตรวจสอบช่องโหว่ ประเมินและหาจุดอ่อนของระบบเทคโนโลยีสารสนเทศของสถาบันการเงิน หน่วยงานภาครัฐ รัฐวิสาหกิจ หรือเอกชน
- ได้รับใบรับรอง (Certificate) และยังไม่หมดอายุ อย่างน้อย ๑ รายการ ดังต่อไปนี้
  - CISSP (Certified Information Systems Security Professional) หรือ
  - CISA (Certified Information Systems Auditor) หรือ
  - CISM (Certified Information Security Manager) หรือ

/➢ ใบรับรอง...

- ใบรับรองด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) ที่ได้รับการยอมรับในระดับสากล

(๒) บุคลากร/ทีมงานโครงการ (ผู้เชี่ยวชาญเพื่อทดสอบเจาะระบบสารสนเทศ) อย่างน้อย ๒ คน

<u>คุณสมบัติ</u>

- สำเร็จการศึกษาระดับปริญญาตรี
- มีประสบการณ์ในการตรวจสอบช่องโหว่ ประเมินและหาจุดอ่อนของระบบเทคโนโลยีสารสนเทศของสถาบันการเงิน หน่วยงานภาครัฐ รัฐวิสาหกิจ หรือเอกชน
- ได้รับใบรับรอง (Certificate) ระดับผู้เชี่ยวชาญ และยังไม่หมดอายุอย่างน้อย ๑ รายการ ดังต่อไปนี้
  - EC-Council LPT (License Penetration Tester) Master หรือ EC – Council Certified Security Analyst (ECSA) หรือ
  - Infosec Institute Certified Expert Penetration Tester (CEPT) หรือ
  - Offensive Security Certified Professional (OSCP) หรือ Evasion Techniques and Breaching Defense (OSEP) หรี Offensive Security Web Expert (OSWE) หรือ
  - Global Information Assurance Certification (GIAC) ประกอบด้วย Penetration Tester (GPEN) และ Web Application Penetration Tester (GWAPT) หรือ
  - CREST ประกอบด้วย Certified Simulated Attack (CCSAS) หรือ Certified Web Application Tester (CCT Web App) หรือ CREST Registered Penetration Tester (CRT) หรือ
  - eLearnSecurity Certified Professional Penetration Tester (eCPPT) หรือ eLearnSecurity Web application Penetration Tester (eWPT)
  - Certificate Red Team Professional (CRTP)

(๓) ผู้ประสานงานโครงการ อย่างน้อยจำนวน ๑ คน

<u>คุณสมบัติ</u>

- สำเร็จการศึกษาระดับปริญญาตรี
- มีประสบการณ์ในการทำงานในการประสานงานโครงการอย่างน้อย ๑ ปี

๗. ระยะเวลาดำเนินโครงการ

ระยะเวลาดำเนินการ ๒๗๐ วัน นับถัดจากวันลงนามในสัญญา

๘. ขอบเขตการดำเนินงาน

ผู้เสนอราคาต้องดำเนินการตามเงื่อนไขและขอบเขตการดำเนินงานของ สำนักงาน ป.ป.ช. อย่างน้อย ดังนี้

๘.๑ จัดทำแผนบริหารโครงการ (Project Plan) ประกอบด้วยอย่างน้อย ดังนี้

๘.๑.๑ แผนการดำเนินงานตามขอบเขตการดำเนินงานที่กำหนด

๘.๑.๒ แนวทางการดำเนินงาน ขั้นตอนการปฏิบัติงาน ความเสี่ยงและการบริหารความเสี่ยง เทคนิค ข้อมูลผู้ดำเนินงาน และข้อมูลอื่น ๆ ที่เกี่ยวข้องในการดำเนินงานตามขอบเขตการดำเนินงาน

/๘.๒ ดำเนินการ...

๘.๒ ดำเนินการตรวจสอบหาช่องโหว่ ประเมิน และหาจุดอ่อนของระบบแบบ White Box โดยจะต้องดำเนินการค้นหาช่องโหว่ในทุก ๆ หน้า ทุก ๆ ฟังก์ชัน ทุก ๆ Module ที่ใช้งาน และชุดคำสั่ง (Source Code) ของระบบเป้าหมาย และจะต้องค้นหาช่องโหว่ทั้งด้านเทคนิคและช่องโหว่ด้าน Business Logic และดำเนินการทดสอบเจาะระบบในรูปแบบผสมผสาน โดยการทดสอบด้วยการใช้เครื่องมือเจาะระบบแบบอัตโนมัติ (Automate Tool) ทั้งแบบ Commercial Tool และแบบ Open-source Tool ผสมผสานกับความเชี่ยวชาญของบุคลากร (Human Skill) พร้อมเก็บหลักฐานจากการทดสอบ (ผู้รับจ้างจะต้องใช้การทดสอบและวิเคราะห์ด้วยตัวบุคคลเองด้วย (Manual Test) มิให้ใช้เครื่องมืออัตโนมัติ (Automatic Test Tool) เพียงอย่างเดียว) เจาะจาก Internal ผ่าน Security Device และไม่ผ่าน Security Device ได้แก่ ทดสอบเจาะระบบ (Penetration Testing) และทดสอบเจาะระบบซ้ำ (Revisit Pentest) จำนวนระบบเป้าหมาย ๕ ระบบ จำนวน ๑๐ IP ได้แก่

๑) ระบบการประเมินและคุณธรรมและความโปร่งใส จำนวน ๒ หมายเลขไอพี

๒) ระบบขอรับการสนับสนุนเงินจากกองทุน ป.ป.ช. จำนวน ๒ หมายเลขไอพี

๓) ระบบบริหารทรัพยากรบุคคลและระบบประเมินบุคลากร (HRMAS) จำนวน ๔ หมายเลขไอพี

๔) ระบบรายงานและติดตามประเมินผลการดำเนินงานตามแผนปฏิบัติการป้องกันการทุจริตขององค์กรปกครองส่วนท้องถิ่น (e-PlanNACC) จำนวน ๑ หมายเลขไอพี

๕) ระบบรายงานและติดตามประเมินผลการดำเนินงานตามแผนปฏิบัติการป้องกันการทุจริตของรัฐวิสาหกิจ (SE-PlanNACC) จำนวน ๑ หมายเลขไอพี

โดยมีขอบเขตการดำเนินงาน ดังนี้

๘.๒.๑ ดำเนินการตรวจสอบหาช่องโหว่ ประเมิน และหาจุดอ่อนของระบบเป้าหมายแบบ White Box โดยจะต้องดำเนินการค้นหาช่องโหว่ในทุก ๆ หน้า ทุก ๆ ฟังก์ชัน ทุก ๆ Module ที่ใช้งานตาม Open Web Application Security Project (OWASP) Testing guide

๘.๒.๒ ดำเนินการตรวจสอบหาช่องโหว่ ประเมิน และหาจุดอ่อนแบบ White Box ชุดคำสั่ง (Source Code) ของระบบเป้าหมายไม่รวม Library ตาม OWASP Secure Coding Practices Quick Reference Guide ประกอบด้วยหัวข้อต่าง ๆ ดังนี้

(๑) ตรวจสอบการนำเข้าข้อมูลทั้งหมด (Input Validation)

(๒) ตรวจสอบการแสดงหรือส่งออกข้อมูลทั้งหมด (Output Validation)

(๓) ตรวจสอบกลไกการยืนยันตัวตนและการจัดการรหัสผ่าน (Authentication and Password Management)

(๔) ตรวจสอบการจัดการเซสชันของผู้ใช้งานหลังการยืนยันตัวตน (Session Management)

(๕) ตรวจสอบการควบคุมการเข้าถึงระบบ (Access Control)

(๖) ตรวจสอบการใช้งานการเข้ารหัสลับข้อมูล (Cryptographic Practices)

(๗) ตรวจสอบการจัดการความผิดพลาดและการบันทึกล็อก (Error Handling and Logging)

(๘) ตรวจสอบการรักษาความมั่นคงปลอดภัยข้อมูล (Data Protection)

(๙) ตรวจสอบการรักษาความมั่นคงปลอดภัยของการสื่อสารข้อมูล (Communication Security)

(๑๐) ตรวจสอบการตั้งค่าเครื่องแม่ข่าย (Server Configuration)

(๑๑) ตรวจสอบการรักษาความมั่นคงปลอดภัยระบบฐานข้อมูล (Database Security)

(๑๒) ตรวจสอบการจัดการไฟล์ของแอปพลิเคชัน (File Management)

/(๑๓) ตรวจสอบ...

(๑๓) ตรวจสอบการจัดการหน่วยความจำของแอปพลิเคชัน (Memory Management)

๘.๒.๓ ดำเนินการทดสอบเจาะระบบเครื่องแม่ข่าย ระบบเครือข่ายคอมพิวเตอร์ และระบบโครงสร้างพื้นฐานสารสนเทศ

ประเมินความมั่นคงปลอดภัยระบบเครื่องแม่ข่าย ระบบเครือข่ายคอมพิวเตอร์ และระบบโครงสร้างพื้นฐานสารสนเทศ เพื่อค้นหาจุดอ่อนหรือตรวจสอบช่องโหว่ของระบบที่อาจถูกใช้เป็นช่องทางในการเจาะระบบเพื่อเข้าถึงข้อมูลสำคัญของหน่วยงาน

๘.๒.๔ ต้องอนุญาตให้เจ้าหน้าที่ผู้ที่เกี่ยวข้อง เข้าร่วมสังเกตการทดสอบเจาะระบบเพื่อสร้างความตระหนักรู้ด้านภัยคุกคามที่อาจจะเกิดขึ้น

๘.๒.๕ จัดประชุมนำเสนอผลการตรวจสอบหาช่องโหว่ ประเมิน และหาจุดอ่อนของระบบเทคโนโลยีสารสนเทศของสำนักงาน ป.ป.ช. ตามข้อ ๘.๒.๑ ข้อ ๘.๒.๒ และข้อ ๘.๒.๓ และจัดทำรายงานผลการประชุม

๘.๒.๖ จัดทำรายงานผลการวิเคราะห์และผลการทดสอบเจาะระบบสารสนเทศกลุ่มเป้าหมาย ตามข้อ ๘.๒.๑ ข้อ ๘.๒.๒ และข้อ ๘.๒.๓ พร้อมประเมินความเสี่ยง โดยมีเนื้อหาครอบคลุมถึงวิธีการทดสอบ ผลการประเมิน พร้อมผลการวิเคราะห์ผลกระทบความเสี่ยง และข้อแนะนำเพื่อใช้ในการแก้ปัญหา และต้องมีหัวข้อแสดงข้อมูลเหล่านี้เป็นอย่างน้อย ดังนี้

(๑) บทสรุปสำหรับผู้บริหาร
(๒) ระบบที่ทำการทดสอบ
(๓) วิธีการ และรายละเอียดในการทดสอบ
(๔) ประเภทของช่องโหว่ที่ดำเนินการทดสอบ
(๕) ผลการทดสอบเจาะระบบ (ช่องโหว่ที่ตรวจพบ)
(๖) ระดับความเสี่ยงช่องโหว่และผลกระทบที่อาจจะเกิดขึ้น
(๗) ช่วงวันเวลาที่ดำเนินการทดสอบ
(๘) แสดงภาพของการทดสอบระบบ (Screen Capture)
(๙) แนวทางและวิธีการแก้ไขจากผลการดำเนินการทดสอบ
(๑๐) แนวทางและวิธีการเพื่อเพิ่มประสิทธิภาพในการรักษาความปลอดภัยระบบสารสนเทศ
(๑๑) ประเมินค่าใช้จ่ายในการดำเนินการแก้ไข (ถ้ามี)

๘.๓ ดำเนินการทดสอบเจาะระบบซ้ำ (Revisit Penetration Testing) ตามข้อ ๘.๒ และจัดประชุมเพื่อนำเสนอผลทดสอบเจาะระบบซ้ำ และจัดทำรายงานผลการวิเคราะห์ฯ โดยมีเนื้อหาครอบคลุมตามข้อ ๘.๒.๖

๘.๔ เข้าร่วมประชุมเพื่อรายงานผลการดำเนินงานต่อคณะกรรมการ/คณะอนุกรรมการที่เกี่ยวข้อง

๘.๕ จัดอบรมเพื่อถ่ายทอดความรู้เกี่ยวกับการทดสอบเจาะระบบ (Penetration Testing) และการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศให้กับเจ้าหน้าที่สำนักงาน ป.ป.ช. ดังนี้

๘.๕.๑ หลักสูตรการทดสอบเจาะระบบ (Penetration Testing) บนระบบจำลอง จำนวน ๑ ระบบ โดยมีวัตถุประสงค์เพื่อให้เจ้าหน้าที่ของสำนักงานทราบถึงกระบวนการทดสอบเจาะระบบตั้งแต่เริ่มต้นจนถึงกระบวนการสุดท้าย และได้ลงมือปฏิบัติจริงบนระบบที่ได้จำลองขึ้นมา จำนวนผู้เข้าร่วมอย่างน้อย ๒๐ คน จำนวน ๑ หลักสูตร ระยะเวลาการอบรมวันละไม่น้อยกว่า ๖ ชั่วโมง อย่างน้อย ๓๐ ชั่วโมง

๘.๕.๒ หลักสูตรความรู้ด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศสำหรับผู้ดูแลระบบ ผู้รับผิดชอบ หรือผู้เกี่ยวข้องกับระบบสารสนเทศ จำนวนผู้เข้าร่วมอบรมไม่น้อยกว่า ๓๐ คน จำนวน ๑ หลักสูตร ระยะเวลาการอบรมวันละไม่น้อยกว่า ๖ ชั่วโมง อย่างน้อย ๑๘ ชั่วโมง

/ทั้งนี้...

ทั้งนี้ ผู้เสนอราคาจะต้องดำเนินการจัดการบันทึกการอบรม และจัดทำเป็นไฟล์วีดีโอ สำหรับเผยแพร่ บันทึกลงสื่อจัดเก็บข้อมูล จำนวน ๓ ชุด โดยที่ผู้ที่เสนอราคารับผิดชอบค่าใช้จ่ายในเรื่องวิทยากร สถานที่ ค่าอาหารว่าง อาหารกลางวัน เครื่องดื่ม และค่าเอกสารประกอบการฝึกอบรม

๘.๖ ผู้เสนอราคาต้องแจ้งเจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศ สำนักงาน ป.ป.ช. ให้ทราบทุกครั้งก่อนเข้าดำเนินงานในแต่ละขั้นตอน

๘.๗ การดำเนินงานต้องไม่ส่งผลกระทบหรือสร้างความเสียหายต่อระบบงาน หากเกิดความเสียหาย ผู้เสนอราคาต้องรับผิดชอบในการทำให้ระบบงานนั้นใช้งานได้เป็นปกติดังเดิม โดยไม่คิดค่าใช้จ่ายใด ๆ เพิ่มเติม

๘.๘ ผู้เสนอราคาต้องรับทราบและปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักงาน ป.ป.ช. ที่เกี่ยวข้องอย่างเคร่งครัด

๘.๙ ผู้เสนอราคาจะต้องปฏิบัติตามนโยบาย มาตรการ ระเบียบวิธีปฏิบัติ และคู่มือการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO ๒๗๐๐๑ ของสำนักเทคโนโลยีสารสนเทศ สำนักงาน ป.ป.ช. และกฎหมายอื่น ๆ ที่เกี่ยวข้อง

๙. ข้อกำหนดในการตรวจรับงานและการส่งมอบงาน

ผู้เสนอราคา จะต้องส่งมอบเอกสารตามรายการทั้งหมดให้ถูกต้องและครบถ้วนตามที่กำหนด พร้อมบันทึกลงสื่อจัดเก็บข้อมูล อย่างน้อยจำนวน ๓ ชุด ตามงวดงาน ดังต่อไปนี้

<u>งวดที่ ๑</u> ส่งมอบงาน ข้อ ๘.๑ ภายใน ๓๐ วัน นับถัดจากวันลงนามในสัญญาจัดซื้อจัดจ้าง

<u>งวดที่ ๒</u> ส่งมอบงาน ภายใน ๑๕๐ วัน นับถัดจากวันลงนามในสัญญาจัดซื้อจัดจ้าง ตามขอบเขตการดำเนินงานตามหัวข้อต่าง ๆ ดังนี้

- ข้อ ๘.๒

<u>งวดที่ ๓</u> ส่งมอบงาน ภายใน ๒๗๐ วัน นับถัดจากวันลงนามในสัญญาจัดซื้อจัดจ้าง ตามขอบเขตการดำเนินงานตามหัวข้อต่าง ๆ ดังนี้

- ข้อ ๘.๓
- ข้อ ๘.๕

๑๐. เงื่อนไขการจ่ายเงิน

การชำระเงินตามจำนวนในสัญญาแบ่งเป็น ๒ งวด ภายหลังจากที่คณะกรรมการตรวจการจ้างได้ตรวจรับรายงานต่าง ๆ ที่ต้องส่งมอบถูกต้องเรียบร้อยแล้ว ดังนี้

<u>งวดที่ ๑</u> ชำระค่าจ้างจำนวนร้อยละ ๔๐ ของวงเงินตามสัญญาจ้าง เมื่อสำนักงาน ป.ป.ช. ได้ตรวจรับงานงวดที่ ๑ และงานงวดที่ ๒ เรียบร้อยแล้ว

<u>งวดที่ ๒</u> ชำระค่าจ้างจำนวนร้อยละ ๖๐ ของวงเงินตามสัญญาจ้าง เมื่อสำนักงาน ป.ป.ช. ได้ตรวจรับงานงวดที่ ๓ เรียบร้อยแล้ว

/๑๑. การรักษาข้อมูล...

๑๑. การรักษาข้อมูล

ผู้เสนอราคาต้องเก็บรักษาข้อมูลสำนักงาน ป.ป.ช. และข้อมูลส่วนบุคคลไว้เป็นความลับ และไม่เปิดเผยให้บุคคลภายนอกทราบ ทั้งนี้ หากมีการฝ่าฝืนผู้เสนอราคาจะต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นและตามที่กฎหมายกำหนดและต้องลงนาม "สัญญาที่จะไม่เปิดเผยข้อมูล (Non-Disclosure Agreement) และข้อตกลงในการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement) และการปฏิบัติตามนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ" ทั้งนี้ร่างสัญญาดังกล่าวมีรายละเอียดตามภาคผนวกที่แนบท้ายร่างขอบเขตของงาน (Terms of Reference : TOR) ฉบับนี้

๑๒. เกณฑ์การพิจารณา

๑๒.๑ ในการเสนอราคาครั้งนี้ สำนักงาน ป.ป.ช. จะพิจารณาตัดสินโดยใช้หลักเกณฑ์การประเมินค่าประสิทธิภาพต่อราคา (Price Performance)

๑๒.๒ สำนักงาน ป.ป.ช. จะพิจารณาให้คะแนนการประเมินค่าประสิทธิภาพต่อราคา (Price Performance) โดยพิจารณาให้คะแนนตามปัจจัยหลักและน้ำหนักที่กำหนด คือ

(๑) ราคาที่เสนอราคา (Price) เป็นตัวแปรหลักบังคับ น้ำหนักร้อยละ ๓๐

(๒) คุณภาพและคุณสมบัติที่เป็นประโยชน์ต่อทางสำนักงาน ป.ป.ช. น้ำหนักร้อยละ ๗๐

โดยกำหนดให้มีน้ำหนักรวมทั้งหมดเท่ากับร้อยละ ๑๐๐

๑๓. รายละเอียดเอกสารประกอบการพิจารณาการเข้าเสนอราคา

๑๓.๑ ผู้เสนอราคาต้องจัดเตรียมเอกสารทางด้านเทคนิคเพื่อแสดงคุณลักษณะเฉพาะตามที่ได้กำหนดไว้ ดังนี้

(๑) หนังสือรับรองผลงานของหน่วยงาน โดยต้องมีหัวหน้าหน่วยงาน หรือผู้ทำการแทนหน่วยงานนั้นทำการรับรอง และส่งมอบสำเนาสัญญาจ้าง และขอบเขตการดำเนินงาน ซึ่งแสดงถึงการทดสอบเจาะระบบสารสนเทศแล้วเสร็จ ทั้งนี้ สำนักงาน ป.ป.ช. สงวนสิทธิ์ที่จะตรวจสอบวินิจฉัยข้อเท็จจริง โดยตรงจากผู้รับรองที่เสนอมานั้น ๆ

(๒) รายชื่อของหัวหน้าโครงการ บุคลากร/ทีมงานโครงการ (ผู้เชี่ยวชาญเพื่อทดสอบเจาะระบบสารสนเทศ) และผู้ประสานงานโครงการ พร้อมสำเนาเอกสารหลักฐานคุณวุฒิ ปริญญาบัตร/ประกาศนียบัตรความเชี่ยวชาญ ประวัติการทำงาน ใบรับรอง (Certificate)

(๓) แผนการดำเนินงาน ขั้นตอนการดำเนินงาน และขั้นตอนการประเมินความเสี่ยง เช่น การจำแนกความเสี่ยง คำอธิบายความเสี่ยง และรูปแบบรายงานผลการวิเคราะห์และผลการทดสอบเจาะระบบสารสนเทศ (5)5.1.

(๔) Methodology กระบวนการ หรือวิธีการที่ใช้ในการประเมินความมั่นคงปลอดภัยและตรวจสอบค้นหาช่องโหว่ของระบบสารสนเทศ และชุดคำสั่ง (Source Code) และแนวทางการบริหารการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศเพื่อลดความเสี่ยงจากภัยคุกคามคอมพิวเตอร์ที่อาจจะเกิดขึ้น (5)5.2

(๕) เครื่องมือ และเทคนิคที่ใช้ในการประเมินความมั่นคงปลอดภัยและตรวจสอบค้นหาช่องโหว่ในชุดคำสั่ง (Source Code) 5.3

ทั้งนี้ ไม่อนุญาตให้มีการขอส่งเอกสารเพิ่มเติมในภายหลังไม่ว่ากรณีใด ๆ เอกสารทั้งหมดผู้เสนอราคาจะต้องยื่นผ่านระบบจัดซื้อจัดจ้างฯ (e-GP)

๑๓.๒ ผู้เสนอราคาต้องจัดทำตารางการเปรียบเทียบรายละเอียดคุณลักษณะเฉพาะตามข้อกำหนดของสำนักงาน ป.ป.ช. กับที่เสนอเป็นข้อๆ ในแต่ละรายการอย่างละเอียดโดยพิมพ์เป็นเอกสารประกอบการนำเสนอพร้อมทั้งบ่งชี้ในแต่ละรายการอย่างครบถ้วนและชัดเจน

/๑๔. วงเงิน...

๑๔. วงเงินในการจัดหา (เงินงบประมาณ)

๓,๕๐๐,๐๐๐.๐๐ บาท (สามล้านห้าแสนบาทถ้วน)

๑๕. หน่วยงานที่รับผิดชอบและสถานที่ติดต่อ

สำนักเทคโนโลยีสารสนเทศ สำนักงาน ป.ป.ช.

สถานที่ติดต่อเพื่อขอทราบข้อมูลเพิ่มเติมหรือเสนอแนะวิจารณ์ หรือแสดงความคิดเห็นโดยเปิดเผยตัวได้ที่

๑) ทางไปรษณีย์

ส่งถึง เลขาธิการคณะกรรมการ ป.ป.ช.

สำนักงาน ป.ป.ช. เลขที่ ๓๖๑ ถ. นนทบุรี ต. ท่าทราย อ. เมืองนนทบุรี

จ. นนทบุรี ๑๑๐๐๐

๒) โทรศัพท์ ๐-๒๕๒๘-๔๘๐๐ ต่อ ๓๐๓๑

๓) โทรสาร ๐-๒๕๒๘-๔๙๘๒

๔) อีเมล egp23_nac@nacc.go.th

ภาคผนวก ๑

หลักเกณฑ์การพิจารณาข้อเสนอด้านเทคนิค

โครงการตรวจสอบหาช่องโหว่ ประเมิน และหาจุดอ่อนของระบบเทคโนโลยีสารสนเทศของสำนักงาน ป.ป.ช.

๑. สำนักงาน ป.ป.ช. จะพิจารณาคุณสมบัติของผู้เสนอราคา หากคุณสมบัติไม่เป็นไปตามหลักเกณฑ์ที่กำหนดไว้ สำนักงาน ป.ป.ช. จะไม่พิจารณาข้อเสนอทางเทคนิค

๒. ในการเสนอราคาครั้งนี้ สำนักงาน ป.ป.ช. จะพิจารณาตัดสินโดยใช้หลักเกณฑ์การประเมินค่าประสิทธิภาพต่อราคา (Price Performance)

๓. สำนักงาน ป.ป.ช. จะพิจารณาให้คะแนนการประเมินค่าประสิทธิภาพต่อราคา (Price Performance) โดยพิจารณาให้คะแนนตามปัจจัยหลักและน้ำหนักที่กำหนด คือ

(๑) ราคาที่เสนอราคา (Price) เป็นตัวแปรหลักบังคับ น้ำหนักร้อยละ ๓๐

(๒) คุณภาพและคุณสมบัติที่เป็นประโยชน์ต่อทางสำนักงาน ป.ป.ช. น้ำหนักร้อยละ ๗๐

โดยกำหนดให้มีน้ำหนักรวมทั้งหมด เท่ากับ ร้อยละ ๑๐๐

๔. สำนักงาน ป.ป.ช. จะพิจารณาจากผู้เสนอราคาที่ได้รับคะแนนข้อเสนอด้านเทคนิคหรือข้อเสนออื่น ๆ สูงสุดและเรียงลำดับคะแนนต่อไปเป็นอันดับที่ ๒ ๓ ตามลำดับ และขอสงวนสิทธิคัดเลือกผู้เสนอราคาที่มีคะแนนข้อเสนอด้านเทคนิคหรือข้อเสนออื่น ๆ และเสนอราคาภายในวงเงินที่กำหนด หากผู้เสนอราคามีคะแนนข้อเสนอด้านเทคนิคหรือข้อเสนออื่น ๆ เท่ากันจะพิจารณาจากข้อเสนอด้านราคาเป็นลำดับถัดไป

๕. เกณฑ์การพิจารณาข้อเสนอด้านเทคนิคหรือข้อเสนออื่น ๆ (คะแนนเต็ม ๑๐๐ คะแนน)

สำนักงาน ป.ป.ช. จะพิจารณาข้อเสนอด้านเทคนิคหรือข้อเสนออื่น ๆ ของผู้เสนอราคาเฉพาะที่มีคุณสมบัติและหลักฐานเอกสารถูกต้อง โดยมีเกณฑ์การพิจารณา ดังนี้

หลักเกณฑ์การให้คะแนน	คะแนน
(๑) ผลงานที่ผ่านมา	๑๐ คะแนน
(๒) บุคลากร/ทีมงาน	๒๐ คะแนน
(๓) ข้อเสนอในการดำเนินการตรวจสอบช่องโหว่ ประเมิน และหาจุดอ่อนของระบบ e-learning ต้านทุจริตการศึกษา แบบ White Box ตามรายละเอียดขอบเขตการดำเนินงานข้อ ๘.๒ และ ๘.๓	๒๕ คะแนน
(๔) ข้อเสนอในการดำเนินการตรวจสอบหาช่องโหว่ ประเมิน และหาจุดอ่อนแบบ White Box ชุดคำสั่ง (Source Code) ของระบบเป้าหมายรวมทั้ง Library	๓๐ คะแนน
(๕) ข้อเสนอโครงการ	๑๕ คะแนน
รวม	**๑๐๐ คะแนน**

หมายเหตุ : สำนักงาน ป.ป.ช. จะนำคะแนนทั้ง ๒ ตัวแปรหลักมาคำนวณเป็นร้อยละ เพื่อพิจารณาผลต่อไป

/โดยมี...

โดยมีรายละเอียดหลักเกณฑ์การให้คะแนน ดังต่อไปนี้

(๑) ผลงานที่ผ่านมา ๑๐ คะแนน

การพิจารณาในส่วนนี้พิจารณาจากจำนวนโครงการที่มีลักษณะที่เกี่ยวข้องกับการทดสอบเจาะระบบสารสนเทศ และได้รับการยอมรับด้านคุณภาพงาน โดยสำนักงาน ป.ป.ช. พิจารณาจากหนังสือรับรองผลงานของหน่วยงาน โดยต้องมีหัวหน้าหน่วยงาน หรือผู้ทำการแทนหน่วยงานนั้นทำการรับรอง และส่งมอบสำเนาสัญญาจ้าง และขอบเขตการดำเนินงาน ซึ่งแสดงถึงการทดสอบเจาะระบบสารสนเทศแล้วเสร็จ ทั้งนี้สำนักงาน ป.ป.ช. สงวนสิทธิ์ที่จะตรวจสอบวินิจฉัยข้อเท็จจริง โดยตรงจากผู้รับรอง

หลักเกณฑ์การให้คะแนน	สูตรการคำนวณ	คะแนน
ผลงานการทดสอบเจาะระบบสารสนเทศให้แก่สถาบันการเงินภายในประเทศ ในวงเงินไม่น้อยกว่า ๕ แสนบาท โดยเป็นสัญญาที่ทำมาไม่เกิน ๕ ปี นับถึงวันยื่นซองเสนอราคา (จำนวนโครงการ)	จำนวนโครงการ x ๒	ไม่เกิน ๑๐ คะแนน
รวม		**๑๐ คะแนน**

(๒) บุคลากร/ทีมงาน ๒๐ คะแนน

การพิจารณาในส่วนนี้ประกอบด้วยหัวข้อการประเมิน ดังนี้

(๒.๑) คุณสมบัติและประสบการณ์ของหัวหน้าโครงการ (๑๐ คะแนน)

หลักเกณฑ์การให้คะแนน	สูตรการคำนวณ	คะแนน
มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยระบบเครือข่ายสื่อสารและความปลอดภัยคอมพิวเตอร์อย่างน้อย ๓ ปี	จำนวนปีประสบการณ์ ตั้งแต่ ๕ ปีขึ้นไป ๕ คะแนน ตั้งแต่ ๔ ปีขึ้นไป ๓ คะแนน ตั้งแต่ ๓ ปีขึ้นไป ๑ คะแนน	ไม่เกิน ๕ คะแนน
มีประสบการณ์ในการบริหารโครงการตรวจสอบช่องโหว่ ประเมินและหาจุดอ่อนของระบบเทคโนโลยีสารสนเทศของสถาบันการเงิน หน่วยงานภาครัฐ รัฐวิสาหกิจ หรือเอกชน	<u>จำนวนโครงการ</u> ๑ โครงการ ๑ คะแนน ๒ โครงการ ๓ คะแนน ตั้งแต่ ๓ โครงการขึ้นไป ๕ คะแนน กรณีมีโครงการของสถาบันการเงินจะได้รับคะแนนเพิ่ม ๓ คะแนน	ไม่เกิน ๕ คะแนน
รวม		**๑๐ คะแนน**

/(๒.๒) คุณสมบัติ...

(๒.๒) คุณสมบัติและประสบการณ์ของทีมงาน (ผู้เชี่ยวชาญเพื่อทดสอบเจาะระบบสารสนเทศ) (๑๐ คะแนน)

คะแนน: คำนวณจากคะแนนเฉลี่ยของบุคลากร/ทีมงานทั้งหมด

หลักเกณฑ์การให้คะแนน	สูตรการคำนวณ	คะแนน
มีประสบการณ์ในการตรวจสอบช่องโหว่ ประเมิน และหาจุดอ่อนระบบเทคโนโลยีสารสนเทศของหน่วยงานภาครัฐ รัฐวิสาหกิจ เอกชน หรือหน่วยงานที่น่าเชื่อถือไม่เกิน ๓ ปีที่ผ่านมา	<u>จำนวนโครงการ</u> ๑ โครงการ ๑ คะแนน ๒ โครงการ ๓ คะแนน ตั้งแต่ ๓ โครงการขึ้นไป ๕ คะแนน กรณีมีโครงการของสถาบันการเงินจะได้รับคะแนนเพิ่ม ๓ คะแนน	ไม่เกิน ๕ คะแนน
ใบรับรอง (Certificate) ตามที่กำหนด	จำนวนใบรับรอง (Certificate) X ๒.๕	ไม่เกิน ๕ คะแนน
รวม		**๑๐ คะแนน**

(๓) ข้อเสนอในการดำเนินการตรวจสอบหาช่องโหว่ ประเมิน และหาจุดอ่อนของ ระบบ e-learning ด้านทุจริตการศึกษา แบบ White Box ตามรายละเอียดขอบเขตการดำเนินงาน ข้อ ๘.๒ และข้อ ๘.๓ (๒๕ คะแนน)

- <u>เสนอ</u> ดำเนินการตรวจสอบหาช่องโหว่ฯ ระบบ e-learning ด้านทุจริตการศึกษา ได้ ๒๕ คะแนน
- <u>ไม่เสนอ</u> ดำเนินการตรวจสอบหาช่องโหว่ฯ ระบบ e-learning ด้านทุจริตการศึกษา ได้ ๐ คะแนน

(๔) ข้อเสนอในการดำเนินการตรวจสอบหาช่องโหว่ ประเมิน และหาจุดอ่อนแบบ White Box ชุดคำสั่ง (Source Code) ของระบบเป้าหมายรวมทั้ง Library (๓๐ คะแนน)

- <u>เสนอ</u> ดำเนินการตรวจสอบหาช่องโหว่ฯ แบบ White Box ชุดคำสั่ง (Source Code) ของระบบเป้าหมายรวมทั้ง Library ได้ ๓๐ คะแนน
- <u>ไม่เสนอ</u> ดำเนินการตรวจสอบหาช่องโหว่ ฯ แบบ White Box ชุดคำสั่ง (Source Code) ของระบบเป้าหมายรวมทั้ง Library ได้ ๐ คะแนน

(๕) ข้อเสนอโครงการ ๑๕ คะแนน

๕.๑ แผนการดำเนินงาน ขั้นตอนการดำเนินงาน และขั้นตอนการประเมินความเสี่ยง เช่น การจำแนกความเสี่ยง คำอธิบายความเสี่ยง และรูปแบบรายงานผลการวิเคราะห์และผลการทดสอบเจาะระบบสารสนเทศ (๕ คะแนน)

๕.๒ Methodology กระบวนการ หรือวิธีการที่ใช้ในการประเมินความมั่นคงปลอดภัยและตรวจสอบค้นหาช่องโหว่ของระบบสารสนเทศ และชุดคำสั่ง (Source Code) และแนวทางการบริหารการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศเพื่อลดความเสี่ยงจากภัยคุกคามคอมพิวเตอร์ที่อาจจะเกิดขึ้น (๕ คะแนน)

/๕.๓ เครื่องมือ ...

๕.๓ เครื่องมือ และเทคนิคที่ใช้ในการประเมินความมั่นคงปลอดภัยและตรวจสอบค้นหาช่องโหว่ในชุดคำสั่ง (Source Code) (๕ คะแนน)

ปัญหาขัดแย้งหรือการตีความ

ในกรณีที่มีความจำเป็นต้องตีความข้อใด หรือมีข้อความใดที่ขัดแย้งในการประกาศเสนอราคา หรือเอกสารเสนอราคา หรือในเอกสารอื่นใดก็ตาม ซึ่งมีความจำเป็นต้องวินิจฉัยเพื่อให้การเสนอราคาครั้งนี้เป็นไปด้วยความเรียบร้อยบรรลุวัตถุประสงค์ของสำนักงาน ป.ป.ช. สำนักงาน ป.ป.ช. สงวนสิทธิ์ที่จะเป็นผู้ตีความและวินิจฉัยข้อขัดแย้ง คำวินิจฉัยนี้ให้ถือเป็นอันเด็ดขาดและถึงที่สุด