ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและราคากลาง (ราคาอ้างอิง)

ในการจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง

1. ชื่อโครงการ **การจ้างผู้ให้บริการประเมินช่องโหว่ของระบบเครือข่ายการสื่อสารและระบบคอมพิวเตอร์ (Vulnerability Assessment) และทดสอบเจาะระบบ (Penetration Test) สำหรับระบบ EXIM Supply Chain Finance Platform**

   /หน่วยงานเจ้าของโครงการ **ฝ่ายพัฒนากระบวนการและนวัตกรรม**

2. วงเงินงบประมาณที่ได้รับจัดสรร **1,000,000.- บาท (หนึ่งล้านบาทถ้วน)**

3. วันที่กำหนดราคากลาง (ราคาอ้างอิง) - 1 ธ.ค. 2563
   เป็นเงิน 797,150.- บาท (เจ็ดแสนเก้าหมื่นเจ็ดพันหนึ่งร้อยห้าสิบบาทถ้วน)

4. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)
   สืบราคาจาก บริษัท ดีลอยท์ ทู้ช โธมัทสุ ไชยยศ ที่ปรึกษา จำกัด

5. รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง) ทุกคน

5.1 นายธรรมณิช	ศรีจันทรา	ผู้ช่วยผู้บริหารฝ่ายกลุ่มอุตสาหกรรม 1
5.2 นางสาวณัฏฐิณี	อังควาณิชย์สุข	ผู้ช่วยผู้บริหารฝ่ายพันธมิตรและสำนักงานผู้แทน
5.3 นางสาวดลณภา	รัศมีเทศ	ผู้บริหารส่วนผลิตภัณฑ์และการค้าระหว่างประเทศ ฝ่ายพัฒนาผลิตภัณฑ์

ผนวก 1

ขอบเขตการดำเนินงาน

การจ้างผู้ให้บริการประเมินช่องโหว่ของระบบเครือข่ายการสื่อสารและระบบคอมพิวเตอร์ (Vulnerability Assessment) และทดสอบเจาะระบบ (Penetration Test) สำหรับระบบ EXIM Supply Chain Finance Platform

---

1. **ขอบเขตการดำเนินงาน (Scope of Work)**

ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกต้องดำเนินการตามเงื่อนไขและขอบเขตความต้องการของธนาคาร อย่างน้อยดังนี้

1.1 จัดทำแผนดำเนินงานอย่างละเอียด โดยต้องเสนอแผนดำเนินงานดังกล่าวให้ธนาคาร เห็นชอบก่อนดำเนินงาน

1.2 ระบบงานเป้าหมายคือ

ระบบคอมพิวเตอร์แม่ข่าย (Server) และอุปกรณ์ในระบบเครือข่าย (Network Equipment) ที่ให้บริการระบบ "EXIM SCF"

1.3 ดำเนินการตรวจสอบ ประเมินหาจุดอ่อน วิเคราะห์ความเสี่ยงและผลกระทบของช่องโหว่ด้านความมั่นคงปลอดภัย (Vulnerability Assessment) เพื่อสำรวจสถานภาพด้านความปลอดภัยของเครื่องคอมพิวเตอร์แม่ข่าย (Server) หรืออุปกรณ์ในระบบเครือข่าย (Network Equipment) หรืออุปกรณ์ในระบบรักษาความปลอดภัยสารสนเทศ (Security Device) ของระบบงานเป้าหมายจำนวนไม่น้อยกว่า 15 อุปกรณ์ หรือ 15 IP Address จำนวน 2 ครั้ง (1st Scan และ Re-visit) เพื่อเปรียบเทียบผลการปิดช่องโหว่ พร้อมทั้งจัดทำข้อเสนอแนะ รายงานผลการตรวจสอบและวิเคราะห์ความเสี่ยงของช่องโหว่ด้านความมั่นคงปลอดภัยทั้ง 2 ครั้ง เพื่อเป็นแนวทางแก้ไขระบบสารสนเทศและระบบที่เกี่ยวข้อง โดยครอบคลุมระบบงานเป้าหมายในข้อ 1.2

1.4 ในการตรวจสอบช่องโหว่ ประเมินหาจุดอ่อน วิเคราะห์ความเสี่ยงและผลกระทบ (Vulnerability Assessment) ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกต้องดำเนินการโดยใช้โปรแกรมหรือซอฟท์แวร์ทั้งที่เป็นแบบ Commercial และ Noncommercial ที่มีความน่าเชื่อถือไม่น้อยกว่า 2 โปรแกรม และเป็นโปรแกรมที่ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกมีลิขสิทธิ์ถูกต้อง

1.5 ในการดำเนินการตรวจสอบช่องโหว่ ประเมินหาจุดอ่อน วิเคราะห์ความเสี่ยงและผลกระทบ (Vulnerability Assessment) ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกต้องดำเนินการโดยยึดตามมาตรฐานไม่ต่ำกว่า Common Vulnerability Scoring System (CVSS) version 3 หรือ SANS Critical Security Controls Top 20 Version 7 (www.sans.org/top20) โดยครอบคลุมในระดับต่างๆ ดังนี้

1.5.1 แอปพลิเคชันซอร์ฟแวร์ที่ใช้งาน (Application Software) (Website)

1.5.2 ระบบปฏิบัติการของเครื่องคอมพิวเตอร์แม่ข่าย (Server Operating Systems)

1.5.3 อุปกรณ์เครือข่ายสื่อสาร (Network Equipment)

1.5.4 อุปกรณ์ในระบบรักษาความปลอดภัยสารสนเทศ (Security Equipment)

1.6 ดำเนินการทดสอบเจาะระบบ EXIM SCF (Web Application) จำนวน 1 URL ตามระยะเวลาการ Go live ของเว็บแอพพลิเคชั่น โดยดำเนินการทดสอบ จำนวน 2 ครั้ง เพื่อเปรียบเทียบผลการดำเนินการปิดช่องโหว่ ดังนี้

1.6.1 ดำเนินการทดสอบเจาะระบบในรูปแบบ Grey-Box Penetration Testing โดยธนาคารจะจัดเตรียม USERNAME และ PASSWORD ในการเข้าถึง พร้อมจัดเตรียมชุดข้อมูลในการทดสอบ ผู้ยื่นข้อเสนอที่ได้รับคัดเลือกต้องดำเนินการค้นหาช่องโหว่ในทุกๆ หน้า ทุกๆ ฟังก์ชันของ EXIM SCF web application โดยจะต้องค้นหาช่องโหว่ทั้งทางด้านเทคนิค เช่น OWASP Top 10 application risk และ ช่องโหว่ทาง business logic

1.6.2 ดำเนินการทดสอบเจาะระบบจากเครือข่ายภายนอกธนาคาร External Penetration Testing (Black-Box) เพื่อนำเอาข้อมูลสำคัญ เช่น บัญชีผู้ดูแลระบบพร้อมทั้งรหัสผ่าน หรือบัญชีผู้ใช้พร้อมรหัสผ่าน หรือ ข้อมูลอื่นๆ ที่มีความสำคัญ รวมถึงการกระทำใดๆ ที่อาจทำให้ธนาคาร ได้ทราบถึงความเสี่ยงจากการถูกเจาะระบบ ในการทดสอบจะดำเนินการเหมือนกับการเจาะระบบโดยไวรัสหรือแฮกเกอร์ที่ปฏิบัติการจริง โดยดำเนินการการทดสอบเพื่อหาช่องทางในการเข้าถึงระบบ (Exploit) เป็นการเข้าถึงระบบโดยผ่านช่องโหว่ต่างๆ เพื่อมุ่งเจาะระบบแม่ข่ายและเครือข่าย โดยครอบคลุมระบบงานเป้าหมายตามข้อ 1.2

1.6.3 ในการทดสอบ Grey-Box Penetration Testing ต้องครอบคลุม Open Web Application Security Project (OWASP) TOP 10 ปี 2017 หรือใหม่กว่า

1.6.4 ดำเนินการทดสอบการเจาะระบบจากเครือข่ายภายนอกธนาคาร External Penetration Testing (Black-Box) นี้ จะต้องใช้วิธีการที่เป็นไปตามมาตรฐานดังต่อไปนี้เป็นอย่างน้อย 1 ข้อ (Version ล่าสุดที่มีการประกาศในการใช้งาน ณ วันที่ลงนามในสัญญา)

1.6.4.1 Open Source Security Testing Methodology (OSSTM)

1.6.4.2 NIST SP800-115 Guideline on Network Security Testing

1.6.5 ดำเนินการทดสอบเจาะระบบในรูปแบบการแบบผสมผสาน คือการทดสอบโดยใช้โปรแกรมเจาะระบบแบบอัตโนมัติ (Automate Tool) ทั้งที่เป็น Commercial Tool และที่เป็น Open Source Tool ผสมผสานกับความเชี่ยวชาญของบุคลากร (Human Skill) พร้อมเก็บหลักฐานจากการทดสอบ (ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกต้องใช้การทดสอบและวิเคราะห์ด้วยตัวบุคคลเองด้วย (Manual Test) มิให้ใช้เครื่องมืออัตโนมัติ (Automatic Test Tool) เพียงอย่างเดียว)

1.7 จัดทำรายงานผลการทดสอบการเจาะระบบแต่ละระยะ และนำเสนอเอกสารการประเมินและวิเคราะห์ความปลอดภัย ผลการประเมิน จุดอ่อน ระดับความเสี่ยง และคำแนะนำการปรับปรุงแก้ไขข้อบกพร่อง รวมถึงผลกระทบที่อาจเกิดขึ้นอย่างละเอียดพร้อมแนวทางการแก้ไข รวมถึง เวลาโดยประมาณในการแก้ไขต่อธนาคาร ดังนี้

1.7.1 จัดทำรายงานอย่างละเอียด โดยมีเนื้อหา ครอบคลุมถึง วิธีการทดสอบ ผลการ ประเมินต่างๆ (ตามข้อ 1.3 และ 1.6) พร้อมผลการวิเคราะห์ผลกระทบจากความเสี่ยง และคำแนะนำในการแก้ไขปัญหาที่ค้นพบเพื่อปรับปรุงความมั่นคง ปลอดภัย

1.7.2 จัดทำรายงานสรุปผลการประเมิน และคำแนะนำสำหรับผู้บริหาร (Executive Summary) ความยาวไม่เกิน 2 หน้า

1.7.3 นำเสนอผลการประเมินต่างๆ (ตามข้อ 1.3 และ 1.6) พร้อมคำแนะนำและ วิธีดำเนินการในการแก้ปัญหาเพื่อปรับปรุงความมั่นคงปลอดภัยให้แก่ธนาคาร หลังจากนั้น ธนาคารจะดำเนินการปรับปรุงระบบ โดยมีระยะเวลาไม่เกิน 1 เดือน นับจากผู้ยื่นข้อเสนอส่งมอบข้อ 1.7.3 และแจ้งให้ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกดำเนินการต่อในข้อ 1.7.4

1.7.4 ประเมินความเสี่ยงเพื่อหาช่องโหว่ และการทดสอบเจาะระบบ (Penetration Testing) ซ้ำและจัดทำรายงานการทดสอบ

1.8 รวบรวมและจัดทำรายงานการดำเนินการ แผนการดำเนินการ ขั้นตอนการดำเนินการ ผลการทดสอบทั้งหมด บทวิเคราะห์ คำแนะนำ การแก้ไข การตรวจสอบหลังการแก้ไข และบทสรุปผู้บริหารทั้งหมด โดยจัดทำเป็นเอกสารพร้อมส่งทั้งแบบ Hardcopy และ Softcopy ในรูปแบบ Portable Document Format (PDF) เพื่อนำเสนอผู้บริหารของธนาคาร จำนวน 2 ชุด

1.9 แจ้งให้ธนาคารทราบทุกครั้งก่อนเข้าดำเนินงานในแต่ละขั้นตอน ถึงแผนการเข้าดำเนินงาน รายละเอียดการดำเนินการ เครื่องมือที่ใช้ โปรแกรมที่เกี่ยวข้อง และเทคนิคที่ใช้ในการเจาะระบบ รวมถึงการประเมินผลกระทบที่อาจมีขึ้น เพื่อป้องกันไม่ให้เกิดความเสียหายต่อระบบที่ทดสอบนั้น ทั้งนี้ จะต้องแจ้งให้ธนาคารทราบล่วงหน้าอย่างน้อย 3 วันทำการและจะดำเนินการได้หลังจากที่ได้รับความเห็นชอบทุกครั้ง

1.10 รับผิดชอบในการแนะนำแนวทางการปิดช่องโหว่ให้กับผู้ดูแลและผู้พัฒนาระบบของธนาคารที่อาจส่งผลกระทบต่อระดับความปลอดภัยของระบบเทคโนโลยีสารสนเทศของธนาคาร ภายหลังจากการทดสอบการเจาะระบบและการประเมินความเสี่ยง รวมถึงการปรับปรุงความมั่นคงปลอดภัยของระบบ EXIM SCF ให้เป็นไปอย่างเหมาะสม หรือตามที่ธนาคารกำหนด

1.11 ผู้ดูแลและผู้พัฒนาระบบของธนาคารจะเป็นผู้ดำเนินการปิดช่องโหว่ที่พบ ตามคำแนะนำและวิธีการที่ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกได้นำเสนอ โดยมีผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกให้คำปรึกษาจนดำเนินการแล้วเสร็จ

1.12 หลังจากที่ผู้ดูแลและผู้พัฒนาระบบของธนาคารดำเนินการปิดช่องโหว่ตามข้อ 1.10 แล้ว ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกต้องดำเนินการตรวจสอบผลการปิดช่องโหว่หรือจุดอ่อน เพื่อยืนยันช่องโหว่ที่พบว่าได้รับการแก้ไขแล้ว และหาช่องโหว่ที่อาจยังเหลืออยู่ (Re-visit)

1.13 หากในข้อ 1.12 ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกตรวจสอบพบจุดอ่อนหรือช่องโหว่เดิมที่ได้รายงานและแก้ไขไปแล้วในข้อ 1.10 ให้ถือเป็นความรับผิดชอบของผู้ดูแลและผู้พัฒนาระบบของธนาคารในการดำเนินการแก้ไข โดยมีผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกให้คำปรึกษาจนดำเนินการแล้วเสร็จ และระหว่างดำเนินการแก้ไขผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกสามารถระงับการทดสอบชั่วคราว จนกว่าผู้ดูแลและผู้พัฒนาระบบของธนาคารจะดำเนินการแก้ไขเสร็จสิ้น จึงดำเนินการตรวจสอบเพื่อยืนยันผลการแก้ไขให้กับทางธนาคารได้รับทราบต่อไป

1.14 ปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศของธนาคาร

1.15 แต่งตั้งผู้แทนอย่างน้อยหนึ่งคนเพื่อรับผิดชอบและควบคุมการดำเนินงาน รวมทั้งเป็นผู้ติดต่อประสานงานกับธนาคาร

1.16 จัดทำผังโครงสร้างทีมงาน (Project Organization) และกำหนดบทบาทหน้าที่ของบุคลากร โดยบุคลากรต้องรับผิดชอบต่อการดำเนินงานตลอดงานจ้าง โดยต้องมาทำงานที่ธนาคาร เมื่อธนาคารต้องการ

1.17 ดำเนินการให้บุคลากรตามข้อ 1.16 ยินยอมให้ธนาคารมีสิทธิที่จะตรวจสอบประวัติของบุคคล

1.18 การเปลี่ยนแปลงตัวบุคลากรที่รับผิดชอบดังกล่าวข้างต้นในภายหลัง จะทำได้ก็ต่อเมื่อได้แจ้งให้ธนาคารทราบเป็นหนังสือ และได้รับความเห็นชอบจากธนาคารแล้ว โดยผู้เข้ามาแทนที่จะต้องมีคุณสมบัติไม่น้อยกว่าผู้ที่ตนจะเข้ามาแทนที่ด้วย

1.19 จัดให้มีการประชุมเพื่อรายงานการดำเนินการและความคืบหน้าของโครงการ ต่อธนาคาร เป็นระยะเวลาที่ชัดเจนอย่างต่อเนื่อง จนกระทั่งสิ้นสุดงานจ้าง

1.20 ยินยอมให้ธนาคารมีสิทธิในการเข้าตรวจสอบการทำงานจนกระทั่งสิ้นสุดงานจ้าง

1.21 การดำเนินงานของผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกต้องไม่ส่งผลกระทบหรือสร้างความเสียหายต่อระบบงานของธนาคาร หากมีความเสียหายใดๆ อันเกิดจากการดำเนินการของผู้ยื่นข้อเสนอที่ได้รับการคัดเลือก จะต้องรายงานให้ธนาคาร ได้ทราบทันที และจะต้องเป็นผู้รับผิดชอบต่อความเสียหายนั้น รวมถึงจะต้องทำให้ระบบงานที่เสียหาย หรือได้รับผลกระทบนั้น กลับมาใช้งานได้เป็นปกติดังเดิมภายในระยะอันรวดเร็ว โดยไม่มีค่าใช้จ่ายใดๆ ทั้งสิ้น

1.22 ทำหนังสือรับรองเพื่อยืนยันต่อธนาคารว่า ซอฟต์แวร์ทุกประเภทที่นำมาใช้กับงานของธนาคารในครั้งนี้ ไม่มีโปรแกรมแอบแฝงหรือโปรแกรมมุ่งร้าย และผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกจะต้องเป็นผู้รับผิดชอบต่อความเสียหายที่อาจเกิดขึ้นจากการนำเอาโปรแกรมเหล่านั้นมาใช้ในงานดังกล่าว

1.23 ใช้เอกสารข้อมูล เครื่องมือ ฮาร์ดแวร์และซอฟท์แวร์ต่างๆในการดำเนินการ อย่างถูกต้อง ตามกฎหมาย ไม่ละเมิดลิขสิทธิ์หรือสิทธิบัตรของผู้อื่น ในกรณีเอกสาร ข้อมูล เครื่องมือฮาร์ดแวร์ และ ซอฟท์แวร์ต่างๆ ที่ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกนำมาใช้ในการดำเนินการเป็นการละเมิดลิขสิทธิ์หรือสิทธิบัตรของผู้อื่น ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกต้องเป็นผู้ชำระค่าเสียหายและค่าใช้จ่ายที่เกี่ยวกับหรือเกี่ยวเนื่องกับกรณีดังกล่าวทั้งสิ้นให้แก่ธนาคารและ/หรือบุคคลภายนอกผู้ถูกละเมิดนั้น

1.24 ดำเนินการให้ธนาคารได้สิทธิโดยชอบ ในการใช้ซอฟต์แวร์ที่มีผู้อื่นเป็นเจ้าของลิขสิทธิ์ หรือสิทธิบัตร หรือทรัพย์สินทางปัญญาอื่นๆ สำหรับข้อมูลที่เกิดขึ้นหรือซอฟต์แวร์ที่พัฒนาขึ้น (Source Code) และรับผิดชอบในกรณีที่มีการกล่าวหาฟ้องร้อง หรือเรียกค่าเสียหายใดๆ จากเจ้าของลิขสิทธิ์ หรือ สิทธิบัตร หรือทรัพย์สินทางปัญญานั้นๆ

1.25 จัดทำสัญญาไม่เปิดเผยข้อมูลพร้อมลงนามให้แก่ธนาคาร และธนาคารขอสงวนสิทธิในข้อมูลทั้งหมดของโครงการนี้ทั้งระบบงาน และเอกสารทั้งหมดที่จัดทำขึ้นถือเป็นลิขสิทธิ์ของธนาคาร โดยผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกจะไม่นำเอกสาร และข้อมูลใดๆ ที่ได้รับ หรือจัดทำขึ้นเกี่ยวกับระบบนี้ไปทำการเปิดเผยหรือ เผยแพร่ โดยไม่ได้รับความเห็นชอบอย่างเป็นทางการจากธนาคาร อีกทั้งมีหน้าที่ในการเก็บรักษาข้อมูลที่ได้รับจากธนาคาร และข้อมูลที่เกี่ยวข้องกับธนาคาร ตลอดจนรายงานผลการดำเนินงานไว้เป็นความลับ ทั้งในระหว่างระยะเวลาสัญญารับจ้าง และสิ้นสุดการรับจ้าง

1.26 จัดหาสื่อเก็บข้อมูลที่เหมาะสมและปลอดภัย หากจำเป็นที่จะต้องนำข้อมูลออกจากธนาคาร กรณีการดำเนินการภายในธนาคาร

1.27 ไม่นำอุปกรณ์ประมวลผลที่ไม่ใช่ของธนาคารมาต่อเข้าระบบเครือข่ายภายในของธนาคาร เว้นแต่ได้รับอนุญาตจากหน่วยงานของธนาคารที่ควบคุมดูแลการทำงาน

1.28 หากส่วนหนึ่งส่วนใดที่มิได้ระบุไว้ในเอกสารนี้แต่มิความจำเป็นต้องจัดทำ หรือจัดหาเพื่อให้งานแล้วเสร็จ ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกต้องจัดทำ หรือจัดหามาให้เพียงพอต่อการใช้งานของธนาคาร และต้องส่งมอบให้เป็นกรรมสิทธิ์ หรือสิทธิ หรือลิขสิทธิ์ของธนาคารทั้งหมด โดยไม่คิดค่าใช้จ่ายใดๆ เพิ่มเติม