ขอบเขตของงาน (Terms of Reference : TOR)

จ้างทดสอบเจาะระบบแพลตฟอร์มข้อมูล

1. ความเป็นมา

สถาบันข้อมูลขนาดใหญ่ (สขญ.) ได้จัดทำพัฒนาแพลตฟอร์มเชื่อมโยงและวิเคราะห์ข้อมูล หรือ ดีทู เพื่อขับเคลื่อนการพัฒนาการบริหารจัดการและวิเคราะห์ข้อมูลขนาดใหญ่ โดยมีแผนงานดำเนินโครงการในด้านวางรากฐานระบบข้อมูลเปิด ข้อมูลภาครัฐ ภาคเอกชน รวมไปถึงกลไกการเชื่อมต่อข้อมูล กลไกการรักษาความปลอดภัย สนับสนุนทรัพยากรในการประมวลผล สร้างชุดข้อมูลเปิดสาธารณะ สร้างรายงานแดชบอร์ดหรือโมเดลทางคณิตศาสตร์ และการเปิดเผยข้อมูลที่ลดความเป็นข้อมูลส่วนบุคคลเพื่อสนับสนุนให้เกิดการใช้ประโยชน์ข้อมูลร่วมกัน ทั้งนี้โครงสร้างของแพลตฟอร์ม ดีทู จะแบ่งออกเป็น 2 ส่วน หลักๆ คือ แพลตฟอร์มกลาง (Central) และ แพลตฟอร์มข้อมูลรายสาขา (Sectorial)

เพื่อให้การดำเนินงานเป็นไปอย่างต่อเนื่อง มั่นคงปลอดภัย ทั้งนี้เนื่องจากแนวโน้มของการโจมตีทางไซเบอร์ผ่านระบบสารสนเทศนั้นมีอัตราเพิ่มขึ้นอย่างมีนัยยะสำคัญ รวมถึงการที่แฟลตฟอร์ม ดีทู ต้องมีการตรวจสอบความมั่นคงปลอดภัยทางไซเบอร์อย่างสม่ำเสมอ สขญ. จึงมีความประสงค์จ้างผู้เชี่ยวชาญภายนอกที่มีความสามารถและประสบการณ์ด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ เข้าประเมินความมั่นคงปลอดภัยของระบบงานแพลตฟอร์ม ดีทู ทั้ง 2 ส่วนอันได้แก่ แพลตฟอร์มกลาง (Central) และ แพลตฟอร์มข้อมูลรายสาขา (Sectorial) รวมถึงระบบเครือข่ายสื่อสาร ระบบคอมพิวเตอร์ และระบบวิเคราะห์ข้อมูลเพื่อให้การบริหารจัดการและควบคุมระบบเทคโนโลยีสารสนเทศ โครงการแพลตฟอร์ม ดีทู มีความปลอดภัยมากยิ่งขึ้น

2. วัตถุประสงค์

ในการดำเนินงานบริหารและจัดการข้อมูล และวิเคราะห์ข้อมูลบนแฟลตฟอร์ม ดีทู (Central, Sectorial) จำเป็นต้องมีผู้เชี่ยวชาญเข้ามาทำการ ประเมินความเสี่ยง ตรวจสอบความมั่นคงปลอดภัยทางไซเบอร์ รวมทั้งปิดช่องโหว่ที่ตรวจพบ เพื่อให้แฟลตฟอร์ม ดีทู ดำเนินการได้อย่างมั่นคงปลอดภัย และสามารถ comply ได้กับมาตรฐานสากล เช่น ISO 27001 เป็นต้น โดยกำหนดระยะเวลาดำเนินการเป็น 90 วัน (3 เดือน) โดยมีวัตถุประสงค์ดังต่อไปนี้

2.1 เพื่อประเมินความเสี่ยง อันอาจเกิดขึ้นได้กับ แพลตฟอร์มกลาง (Central) และ แพลตฟอร์มข้อมูลรายสาขา (Sectorial) แพลตฟอร์มใดแพลตฟอร์มหนึ่ง หรือ ทั้ง 2 แพลตฟอร์ม พร้อมๆ กัน อันอาจจะเกิดขึ้นได้ในอนาคต

2.2 เพื่อระบุความเสี่ยง หรือช่องโหว่ อันอาจเกิดขึ้นได้กับ แพลตฟอร์มกลาง (Central) และ แพลตฟอร์มข้อมูลรายสาขา (Sectorial) แพลตฟอร์มใดแพลตฟอร์มหนึ่ง หรือ ทั้ง 2 แพลตฟอร์ม พร้อมๆ กัน อันอาจจะเกิดขึ้นได้ในอนาคต

2.3 เพื่อวิเคราะห์ความเสี่ยง อันอาจเกิดขึ้นได้กับ แพลตฟอร์มกลาง (Central) และ แพลตฟอร์มข้อมูลรายสาขา (Sectorial) แพลตฟอร์มใดแพลตฟอร์มหนึ่ง หรือ ทั้ง 2 แพลตฟอร์ม พร้อมๆ กัน อันอาจจะเกิดขึ้นได้ในอนาคต

2.4 เพื่อจัดการความเสี่ยง อันอาจเกิดขึ้นได้กับ แพลตฟอร์มกลาง (Central) และ แพลตฟอร์มข้อมูลรายสาขา (Sectorial) แพลตฟอร์มใดแพลตฟอร์มหนึ่ง หรือ ทั้ง 2 แพลตฟอร์ม พร้อมๆ กัน อันอาจจะเกิดขึ้นได้ในอนาคต

2.5 เพื่อทราบความเสี่ยง อันอาจเกิดขึ้นได้กับ แพลตฟอร์มกลาง (Central) และ แพลตฟอร์มข้อมูลรายสาขา (Sectorial) แพลตฟอร์มใดแพลตฟอร์มหนึ่ง หรือ ทั้ง 2 แพลตฟอร์ม พร้อมๆ กัน อันอาจจะเกิดขึ้นได้ในอนาคต

2.6 เพื่อจัดทำแผนการจัดการ และแนวทางการจัดการความเสี่ยงและช่องโหว่ อันอาจเกิดขึ้นได้กับ แพลตฟอร์มกลาง (Central) และ แพลตฟอร์มข้อมูลรายสาขา (Sectorial) แพลตฟอร์มใดแพลตฟอร์มหนึ่ง หรือ ทั้ง 2 แพลตฟอร์ม พร้อมๆ กัน อันอาจจะเกิดขึ้นได้ในอนาคต

2.7 เพื่อให้มี การประเมินช่องโหว่ (VA) และการทดสอบเจาะระบบเพื่อค้นหาช่องโหว่และจุดอ่อน

2.8 เพื่อจัดทำรายงานสำหรับการรับเข้าการประเมินตามมาตรฐาน ISO 27001 (2022)

2.9 เพื่อพัฒนา และจัดการข้อมูลและระบบต่างๆ บนแพลตฟอร์ม ดีทู ทั้ง 2 ส่วน (Central, Sectorial)

3. คุณสมบัติของผู้เสนอราคา

มีความสามารถตามกฎหมาย

3.1 ไม่เป็นบุคคลล้มละลาย

3.2 ไม่อยู่ระหว่างเลิกกิจการ

3.3 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราวเนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.4 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.5 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.6 เป็นบุคคลธรรมดาหรือนิติบุคคลผู้มีอาชีพตามที่ประกาศ

3.7 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่น หรือกระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรม

3.8 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกันซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

3.9 ผู้ยื่นข้อเสนอต้องลงทะเบียนที่มีข้อมูลถูกต้องครบถ้วนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement : e-GP) ของกรมบัญชีกลาง

3.10 ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ ดังนี้

1. กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยหรือต่างประเทศ ซึ่งได้จดทะเบียนเกินกว่า 1 ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก 1 ปีสุดท้ายก่อนวันยื่นข้อเสนอ งบแสดงฐานะการเงิน 1 ปีสุดท้ายก่อนวันยื่นข้อเสนอ หมายถึง งบแสดงฐานะการเงินย้อนไปก่อนวันที่หน่วยงานของรัฐกำหนดให้เป็นวันยื่นข้อเสนอ 1 ปีปฏิทิน เว้นแต่กรณีนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย หากวันยื่นข้อเสนอเป็นช่วงระยะเวลาที่กรมพัฒนาธุรกิจการค้ากำหนดให้นิติบุคคลยื่นงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ซึ่งจะอยู่ในช่วงเดือนมกราคม - เดือนพฤษภาคม ของทุกปี โดยนิติบุคคลที่เป็นผู้ยื่นข้อเสนอนั้นยังอยู่ในช่วงของการยื่นงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า คือ ช่วงเดือนมกราคม - เดือนพฤษภาคม กรณีนี้ให้สามารถยื่นงบแสดงฐานะการเงินย้อนไปอีก 1 ปี ได้

2. กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า หรือกรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงิน ให้พิจารณาการกำหนดมูลค่าของทุนจดทะเบียน โดยผู้ยื่นข้อเสนอจะต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอ ไม่ต่ำกว่า 8 ล้านบาท

3. สำหรับการจัดซื้อจัดจ้างครั้งหนึ่งที่มีวงเงินเกิน 500,000 บาทขึ้นไป กรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดา ให้พิจารณาจากหนังสือรับรองบัญชีเงินฝากไม่เกิน 90 วัน ก่อนวันยื่นข้อเสนอ โดยต้องมีเงินฝากคงเหลือในบัญชีธนาคารเป็นมูลค่า 1 ใน 4 ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอ ในแต่ละครั้ง และหากเป็นผู้ชนะการจัดซื้อจัดจ้างหรือเป็นผู้ได้รับการคัดเลือกจะต้องแสดงหนังสือรับรองบัญชีเงินฝากที่มีมูลค่าดังกล่าวอีกครั้งหนึ่งในวันลงนามในสัญญา

4. กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ สามารถดำเนินการได้ดังนี้

(1) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย หรือบุคคลธรรมดาที่ถือสัญชาติไทย ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ 1 ใน 4 ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง จะเป็นสินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรอง หรือที่สำนักงานสาขารับรอง

(2) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศ หรือบุคคลธรรมดาที่มิได้ถือสัญชาติไทย ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ 1 ใน 4 ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง จะเป็นสินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์ และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคาร แห่งประเทศไทยแจ้งเวียนให้ทราบ หรือเป็นสินเชื่อที่ธนาคารต่างประเทศหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารกลางต่างประเทศนั้น ตามรายชื่อบริษัทที่ธนาคารกลางต่างประเทศนั้นแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรอง หรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ

นับถึงวันยื่นข้อเสนอไม่เกิน 90 วัน

5. กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศ หรือบุคคลธรรมดาที่มิได้ถือสัญชาติไทย ตามข้อ 2 ข้อ 3 และข้อ 4 (2) มูลค่าจะต้องเป็นไปตามอัตราแลกเปลี่ยนเงินตรา
ตามประกาศที่ธนาคารแห่งประเทศไทยกำหนด ในช่วงระหว่างวันที่เผยแพร่ประกาศและเอกสารประกวดราคาในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (e - GP) จนถึงวันเสนอราคา

ทั้งนี้ ผู้ยื่นข้อเสนอจะต้องยื่นเอกสารที่แสดงให้เห็นถึงข้อมูลเกี่ยวกับมูลค่าสุทธิของกิจการแล้วแต่กรณี ประกอบกับเอกสารดังกล่าวจะต้องผ่านการรับรองตามระเบียบกระทรวงการต่างประเทศว่าด้วยการรับรองเอกสาร พ.ศ. 2539 และที่แก้ไขเพิ่มเติมกำหนด โดยจะต้องยื่นเอกสารดังกล่าวในวันยื่นข้อเสนอ หากผู้ยื่นข้อเสนอมิได้มีการยื่นเอกสารดังกล่าวมาพร้อมกับการยื่นข้อเสนอให้ถือว่าผู้ยื่นข้อเสนอรายนั้นยื่นเอกสารไม่ครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารประกวดราคา

6. กรณีตาม ข้อ 1 - ข้อ 5 ไม่ใช้บังคับกรณีดังต่อไปนี้

(6.1) กรณีที่ผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐภายในประเทศ

(6.2) นิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการตามพระราชบัญญัติล้มละลาย พ.ศ. 2483 และที่แก้ไขเพิ่มเติม

(6.3) งานจ้างก่อสร้างที่กรมบัญชีกลางได้ขึ้นทะเบียนผู้ประกอบการงานก่อสร้างแล้ว และงานจ้างก่อสร้างที่หน่วยงานของรัฐที่ได้มีการจัดทำบัญชีผู้ประกอบการงานก่อสร้างที่มีคุณสมบัติเบื้องต้นไว้แล้วก่อนวันที่พระราชบัญญัติการจัดซื้อจัดจ้างฯ มีผลใช้บังคับ

(6.4) การจัดซื้อจัดจ้างตามมาตรา 56 วรรคหนึ่ง (2) (ข) และ (ค) แห่งพระราชบัญญัติการจัดซื้อจัดจ้างฯ

(6.5) การซื้ออสังหาริมทรัพย์และการเช่าอสังหาริมทรัพย์

(6.6) กรณีงานจ้างบริการหรืองานจ้างเหมาบริการกับบุคคลธรรมดา เช่น จ้างพนักงานขับรถ ครูชาวต่างชาติ พนักงานเก็บขยะ พนักงานบันทึกข้อมูล เป็นต้น

3.11 ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ "กิจการร่วมค้า" ต้องมีคุณสมบัติ ดังนี้

3.11.1 การกำหนดสัดส่วนในการเข้าร่วมค้าของคู่สัญญา

กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลักข้อตกลงฯ จะต้องมีการกำหนดสัดส่วนหน้าที่ และความรับผิดชอบในปริมาณงาน สิ่งของ หรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

3.11.2 งานซื้อหรือจ้าง และงานก่อสร้าง

กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลักกิจการร่วมค้านั้นต้องใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

สำหรับข้อตกลงฯ ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมค้าหลัก ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในหนังสือเชิญชวน

3.11.3 การยื่นข้อเสนอของกิจการร่วมค้า

(1) กรณีที่ข้อตกลงฯ กำหนดให้มีการมอบหมายผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า การยื่นข้อเสนอดังกล่าวไม่ต้องมีหนังสือมอบอำนาจ

สำหรับข้อตกลงฯ ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้ยื่นข้อเสนอผู้เข้าร่วมค้าทุกรายจะต้องลงลายมือชื่อในหนังสือมอบอำนาจให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า

(2) การยื่นข้อเสนอด้วยวิธีคัดเลือก

หากผู้เข้าร่วมค้ารายใดได้รับหนังสือเชิญชวนจากหน่วยงานของรัฐแล้วให้ผู้เข้าร่วมค้าที่ได้รับมอบหมายหรือมอบอำนาจตามข้อ (1) สามารถดำเนินการยื่นข้อเสนอในนามกิจการร่วมค้า

4. ขอบเขตของงาน

ผู้รับจ้างตรวจประเมินช่องโหว่และทดสอบเจาะระบบ แฟลตฟอร์ม ดีทู ครอบคลุม Central/ Sectorial/ Agent nodes โดยต้องดำเนินงานตามรายละเอียดขอบเขตในการดำเนินงาน เนื้อหาอย่างน้อยดังนี้

4.1 ต้องจัดทำแผนการดำเนินงาน โดยต้องเสนอแผนดำเนินงานดังกล่าวให้ สขญ. และดำเนินการจัดประชุมเพื่อนำเสนอแผนการดำเนินงานเมื่อเริ่มต้นโครงการ (Kick off) เพื่อสื่อความกับผู้เกี่ยวข้องก่อนเข้าดำเนินการประเมินช่องโหว่และทดสอบเจาะระบบ ดังนี้

(1) แผนการดำเนินงาน

(2) ขอบเขตการดำเนินการ

(3) วิธีการทดสอบ

(4) เกณฑ์การประเมินความเสี่ยงของช่องโหว่

(5) ผังโครงสร้างทีมงาน (Project Organization) และกำหนดบทบาทหน้าที่ของบุคลากร ดังนี้

- ผู้จัดการโครงการ (Project Manager)
- ผู้ควบคุมคุณภาพโครงการ (Quality Assurance)
- ผู้ทดสอบเจาะระบบ (Tester)

4.2 ดำเนินการประเมินช่องโหว่ (Vulnerability Assessment) โดยให้ครอบคลุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) ระบบคลาวด์ (Cloud) อุปกรณ์ในระบบเครือข่าย (Network Equipment) และอุปกรณ์ในระบบรักษาความปลอดภัยสารสนเทศ (Security Device) ของระบบเครือข่ายภายใน (Internal Network) สขญ. ตามที่ สขญ. กำหนด จำนวนไม่น้อยกว่า 22 อุปกรณ์ หรือ 22 IP Addresses โดยการใช้โปรแกรมคอมพิวเตอร์ที่มีลิขสิทธิ์ที่เป็นที่ยอมรับในระดับสากลในด้านการค้นหาช่องโหว่และประเมินความเสี่ยง ผลประเมินความเสี่ยงของช่องโหว่ ต้องอิงตามมาตรฐาน Common Vulnerability Scoring System (CVSS) version 3 ซึ่งระบุค่า CVSS Base Score สำหรับแต่ละรายการ พร้อมทั้งจัดลำดับความสำคัญของการแก้ไขโดยพิจารณาระดับการเปิดรับความเสี่ยง (Exposure Level) เช่น การเปิดเผยให้เข้าถึงจากภายนอก, การต้องผ่านการพิสูจน์ตัวตนก่อนเข้าถึง, ความสามารถในการยกระดับสิทธิการเข้าถึง, และการเข้าถึงระบบหรือข้อมูลภายใน

4.2.1 จัดทำรายงานการประเมินช่องโหว่ และการทดสอบอย่างละเอียด โดยมีเนื้อหาครอบคลุมถึง วิธีการทดสอบ ผลการประเมิน พร้อมผลการวิเคราะห์ผลกระทบจากความเสี่ยง และข้อแนะนำเพื่อใช้ในการแก้ไขปัญหา

4.2.2 ดำเนินการจัดประชุมเพื่อชี้แจงรายละเอียดของช่องโหว่ที่พบ และให้คำปรึกษาในการปิดช่องโหว่แก่ผู้ดูแลระบบ และผู้พัฒนาระบบงาน เพื่อให้ผู้ดูแลระบบและผู้พัฒนาระบบงานสามารถปิดช่องโหว่ได้อย่างถูกต้อง

4.3 ดำเนินการทดสอบเจาะระบบ แบบ Black Box Penetration Testing โดยต้องดำเนินการตามแนวทางมาตรฐานสากล Open Source Security Testing Methodology Manual (OSSTMM) หรือ NIST Special Publication 800-115 หรือ มาตรฐานสากลอื่นที่เทียบเท่าในส่วนที่เกี่ยวข้องกับการทดสอบเจาะระบบ ทั้งนี้การทดสอบต้องครอบคลุมความเสี่ยงตาม OWASP Top 10 สำหรับ Web Application เวอร์ชันล่าสุด และ OWASP API Security Top 10 เวอร์ชันล่าสุด (ในกรณีที่ระบบมีส่วนติดต่อแบบ API) สำหรับการทดสอบเจาะเว็บแอปพลิเคชันต้องครอบคลุมอย่างน้อย ดังต่อไปนี้

- เว็บแอปพลิเคชัน data catalog
- เว็บแอปพลิเคชัน data pipeline
- เว็บแอปพลิเคชัน data visualization

- เว็บแอปพลิเคชัน jupyter notebook
- เว็บแอปพลิเคชัน object storage
- เว็บแอปพลิเคชัน data gov tools
- เว็บแอปพลิเคชัน data warehouse

4.3.1 จัดทำรายงานการทดสอบเจาะระบบ และการทดสอบอย่างละเอียด โดยมีเนื้อหาครอบคลุมถึง วิธีการทดสอบ ผลการประเมิน พร้อมผลการวิเคราะห์ผลกระทบจากความเสี่ยง และข้อแนะนำเพื่อใช้ในการแก้ไขปัญหา

4.3.2 ดำเนินการจัดประชุมเพื่อชี้แจงรายละเอียดของช่องโหว่ที่พบ และให้คำปรึกษาในการปิดช่องโหว่แก่ผู้ดูแลระบบ และผู้พัฒนาระบบงาน เพื่อให้ผู้ดูแลระบบและผู้พัฒนาระบบงานสามารถปิดช่องโหว่ได้อย่างถูกต้อง

4.4 ดำเนินการทดสอบจุดเชื่อมต่อและกลไกการสื่อสาร โดยต้องครอบคลุมการสื่อสารข้อมูลระหว่าง Central/ Sectorial/ Agent node ซึ่งอาจสื่อสารในรูปแบบ การเชื่อมต่อผ่าน API (REST / SOAP / GraphQL หรืออื่น ๆ) การแลกเปลี่ยนข้อมูลผ่าน Message Queue / Webhook / File Transfer การสื่อสารผ่าน Network หรือ Internet (TLS/HTTPS/VPN) ทั้งนี้ผู้รับจ้างต้องดำเนินการทดสอบการควบคุมการแบ่งแยกเครือข่าย (Network Segmentation Control) และการเคลื่อนย้ายภายในระบบ (Lateral Movement) โดยจำลองสถานการณ์การถูกบุกรุกจากระบบหนึ่ง และประเมินความสามารถในการเข้าถึงระบบอื่นระหว่าง Central/ Sectorial/ Agent node เพื่อยืนยันว่ากลไกการควบคุมการเข้าถึงเป็นไปตามการออกแบบด้านความมั่นคงปลอดภัย และไม่สามารถข้ามขอบเขตความเชื่อถือ (Trust Boundary) ได้

4.4.1 จัดทำรายงานการประเมินช่องโหว่และจุดอ่อน และการทดสอบอย่างละเอียด โดยมีเนื้อหาครอบคลุมถึง วิธีการทดสอบ ผลการประเมิน พร้อมผลการวิเคราะห์ผลกระทบจากช่องโหว่และจุดอ่อน และข้อแนะนำเพื่อใช้ในการแก้ไขปัญหา

4.4.2 ดำเนินการจัดประชุมเพื่อชี้แจงรายละเอียดของช่องโหว่และจุดอ่อนที่พบ และให้คำปรึกษาในการปิดช่องโหว่แก่ผู้ดูแลระบบ และผู้พัฒนาระบบงาน เพื่อให้ผู้ดูแลระบบและผู้พัฒนาระบบงานสามารถปิดช่องโหว่ได้อย่างถูกต้อง

4.5 ดำเนินการประเมินช่องโหว่และทดสอบเจาะระบบ ทดสอบเจาะระบบซ้ำ (Revisit) ตามข้อที่ 4.2-4.4 จำนวน 1 ครั้ง หลังจากที่ สขญ. ได้ดำเนินการแก้ไขช่องโหว่แล้ว (รวมขอบเขตในโครงการ เท่ากับ 2 ครั้ง) พร้อมทั้งจัดทำรายงานผลและข้อเสนอแนะการแก้ไข

4.6 ผู้ให้บริการต้องดำเนินการทดสอบเฉพาะขอบเขตที่ได้รับอนุญาตเท่านั้น ได้แก่ IP Address, URL, Domain, ระบบหรือบัญชีผู้ใช้งานที่องค์กรกำหนดเป็นลายลักษณ์อักษร และต้องไม่ดำเนินการทดสอบที่อาจก่อให้เกิดผลกระทบต่อความพร้อมใช้งานของระบบ เช่น การทดสอบแบบ Denial of Service (DoS), การทดสอบแบบ Stress Test หรือการกระทำใดที่อาจทำให้ระบบหยุดชะงัก เว้นแต่จะได้รับอนุมัติเป็นกรณีเฉพาะ ทั้งนี้การทดสอบต้องดำเนินการภายในช่วงเวลาที่องค์กรกำหนดเท่านั้น

4.7 รายงานผลการประเมินช่องโหว่และการทดสอบเจาะระบบ ต้องมีการเชื่อมโยง (Mapping) ระหว่างช่องโหว่และความเสี่ยงที่ตรวจพบกับมาตรฐาน ISO/IEC 27001:2022 ในส่วนของ Annex A Controls ที่เกี่ยวข้อง โดยจัดทำตารางสรุปการเชื่อมโยง (Mapping Table) พร้อมข้อเสนอแนะเพื่อใช้ในการทำ Risk treatment plan ต่อไปได้

5. กำหนดระยะเวลาส่งมอบงาน

ผู้รับจ้างจะต้องส่งมอบงานทั้งหมดภายในระยะเวลา 90 วัน นับถัดจากวันลงนามในสัญญา

6. สถานที่ส่งมอบงาน

ผู้รับจ้างจะต้องส่งมอบงานจัดจ้าง “ทดสอบเจาะระบบแพลตฟอร์มข้อมูล” ณ สถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน)

7. ระยะเวลาส่งมอบงานและเงื่อนไขการชำระเงิน

สขญ. จะชำระเงินเต็มจำนวน เมื่อผู้รับจ้างได้ส่งมอบงานทั้งหมด และคณะกรรมการได้ตรวจรับเรียบร้อยแล้ว

8. หลักเกณฑ์ในการพิจารณาคัดเลือกข้อเสนอ

เกณฑ์ราคา

8.1 หากผู้ยื่นข้อเสนอซึ่งเป็นผู้ประกอบการ SMEs เสนอราคาสูงกว่าราคาต่ำสุดของผู้ยื่นข้อเสนอรายอื่นที่ไม่เกินร้อยละ 10 ให้หน่วยงานของรัฐจัดซื้อจัดจ้างกับผู้ประกอบการ SMEs ดังกล่าว โดยจัดเรียงลำดับผู้ยื่นข้อเสนอซึ่งเป็นผู้ประกอบการ SMEs ซึ่งเสนอราคาสูงกว่าราคาต่ำสุดของผู้ยื่นข้อเสนอรายอื่นไม่เกินร้อยละ 10 ที่จะเรียกมาทำสัญญาไม่เกิน 3 ราย

ผู้ยื่นข้อเสนอที่เป็นกิจการร่วมค้าที่จะได้สิทธิตามวรรคหนึ่ง ผู้เข้าร่วมค้าทุกรายจะต้องเป็นผู้ประกอบการ SMEs

ทั้งนี้ ผู้ประกอบการ SMEs ที่จะได้แต้มต่อด้านราคาตามวรรคหนึ่ง จะต้องมีวงเงินสัญญาสะสมตามปีปฏิทินรวมกับราคาที่เสนอในครั้งนี้แล้ว มีมูลค่ารวมกันไม่เกินมูลค่าของรายได้ตามขนาดที่ขึ้นทะเบียนไว้กับ สสว.

8.2 หากผู้ยื่นข้อเสนอได้เสนอพัสดุที่ได้รับการรับรองและออกเครื่องหมายการค้าที่ผลิตภายในประเทศไทย (Made In Thailand) จากสภาอุตสาหกรรมแห่งประเทศไทย เสนอราคาสูงกว่าราคาต่ำสุด ของผู้เสนอราคารายอื่นไม่เกินร้อยละ 5 ให้จัดซื้อจัดจ้างจากผู้ยื่นข้อเสนอที่ได้รับการรับรองและออกเครื่องหมายสินค้าที่ผลิตภายในประเทศ (Made In Thailand) จากสภาอุตสาหกรรมแห่งประเทศไทย

อนึ่ง หากในการเสนอราคาครั้งนั้น ผู้ยื่นข้อเสนอรายใดมีคุณสมบัติทั้งข้อ 6.1 และข้อ 6.2 ให้ผู้ยื่นข้อเสนอรายนั้นได้แต้มต่อในการเสนอราคาสูงกว่าผู้ยื่นข้อเสนอรายอื่นไม่เกินร้อยละ 15

8.3 หากผู้ยื่นข้อเสนอซึ่งมิใช่ผู้ประกอบการ SMEs แต่เป็นบุคคลธรรมดาที่ถือสัญชาติไทยหรือนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยเสนอราคาสูงกว่าราคาต่ำสุดของผู้ยื่นข้อเสนอซึ่งเป็นบุคคลธรรมดาที่มิได้ถือสัญชาติไทยหรือนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายของต่างประเทศไม่เกินร้อยละ 3 ให้จัดซื้อจัดจ้างกับบุคคลธรรมดาที่ถือสัญชาติไทยหรือนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยดังกล่าว

ผู้ยื่นข้อเสนอที่เป็นกิจการร่วมค้าที่จะได้สิทธิตามวรรคหนึ่ง ผู้เข้าร่วมค้าทุกรายจะต้องเป็นบุคคลธรรมดาที่ถือสัญชาติไทยหรือนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย

9. วงเงินงบประมาณ

งบประมาณประจำปี 2569 เป็นเงินจำนวน 1,500,000 บาท (หนึ่งล้านห้าแสนบาทถ้วน) ซึ่งได้รวมภาษีมูลค่าเพิ่มไว้แล้ว

10. อัตราค่าปรับ

หากผู้รับจ้างไม่สามารถส่งมอบงานได้ตามเวลาที่กำหนดไว้ในสัญญา ผู้รับจ้างจะต้องชำระค่าปรับ ให้แก่ สขญ. เป็นรายวัน ในอัตราร้อยละ 0.10 (ศูนย์จุดหนึ่งศูนย์) ของมูลค่าสัญญาจ้าง แต่จะต้องไม่ต่ำกว่าวันละ 100 บาท

11. สถานที่ติดต่อขอรับทราบข้อมูลเพิ่มเติม

สถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน)
เลขที่ 234/432 ซอยลาดพร้าว 12 ถนนลาดพร้าว
แขวงจอมพล เขตจตุจักร กรุงเทพมหานคร 10900
ไปรษณีย์อิเล็กทรอนิกส์ chayasin.sa@bdi.or.th

คณะกรรมการจัดทำรายละเอียดขอบเขตของงาน

ลงชื่อ..... ประธานกรรมการ
(นางสาวฐิติรัตน์ บุญช่วยชู)

ลงชื่อ.....กรรมการ
(นายรัฐพล ชูเกาะทวด)

ลงชื่อ.....กรรมการและเลขานุการ
(นายชยสิน แซ่เตีย)