ขอบเขตความต้องการ (TOR)

โครงการ NDID Member Qualification Assessment Framework (MQA)

1. ความเป็นมา

บริษัทเฮงลิสซิ่งแอนด์แคปปิตอลจำกัด (มหาชน) ได้จัดทำ “โครงการพัฒนาระบบการพิสูจน์และยืนยันตัวตนทางดิจิตอล (Digital ID)” เพื่อยกระดับการให้บริการดิจิทัลอย่างมีประสิทธิภาพ มีความมั่นคงปลอดภัย และเพื่อสร้างความมั่นใจในการทำธุรกรรมออนไลน์กับทางบริษัทได้สะดวกยิ่งขึ้น จึงมีความประสงค์จัดจ้างผู้เชี่ยวชาญตรวจสอบความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศจากภายนอก เพื่อประเมินสถานะความมั่นคงปลอดภัยด้านสารสนเทศ ตรวจสอบ วิเคราะห์ และให้คำแนะนำในการปรับปรุงด้านระบบรักษาความปลอดภัยของระบบเครือข่ายและระบบคอมพิวเตอร์ของระบบพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital ID) ของบริษัท

2. วัตถุประสงค์

2.1. เพื่อให้ได้รับรองเป็นสมาชิกที่ได้รับอนุญาตให้เชื่อมต่อระบบ กับระบบ NDID Platform

2.2. เพื่อให้เกิดการปรับปรุงให้มีความมั่นคงปลอดภัยที่สูงขึ้น

2.3. เพื่อให้ระบบเกิดความน่าเชื่อถือและมีความมั่นคงปลอดภัยที่เพียงพอ ต่อการรับมือกับภัยคุกคามด้านไซเบอร์

3. คุณสมบัติของผู้ยื่นข้อเสนอ

3.1. ผู้ยื่นข้อเสนอต้องเป็นนิติบุคคลตามกฎหมายที่ได้จดทะเบียนในประเทศไทย หรือ เป็นกลุ่มร่วมทำงาน (Consortium) หรือ กิจการร่วมค้า (Joint Venture)

3.2. ผู้ยื่นข้อเสนอต้องไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้เสนอรายอื่นที่เข้าเสนอราคา หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรมในการเสนอราคาครั้งนี้

3.3. ผู้ยื่นข้อเสนอต้องไม่เป็นผู้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นเสนอราคาได้มีคำสั่งให้สละสิทธิ์ความคุ้มกันเช่นว่านั้น

3.4. ผู้ยื่นข้อเสนอยินยอมรับข้อกำหนด เงื่อนไขและรายละเอียดที่ระบุในขอบเขตของงานฉบับนี้ทั้งหมดโดยไม่มีเงื่อนไขใดๆ ทั้งสิ้น

3.5. บุคลากรด้านผู้ทำการประเมินมาตรการรักษาความมั่นคงปลอดภัยของระบบต้อง ได้รับการรับรองหรือได้รับประกาศนียบัตรรับรองความรู้จากหน่วยงานในระดับสากลตามที่ระบุในเอกสาร NDID Member Qualification Assessment Framework (MQA) สำหรับสมาชิกที่ขอเชื่อมต่อ ดังนี้

3.5.1. ประกาศนียบัตร Certified Information System Auditor (CISA) หรือ

3.5.2. ประกาศนียบัตร Certified Information Security Manager (CISM) หรือ

3.5.3. ประกาศนียบัตร Certified Information System Security Professional (CISSP) หรือ

3.5.4. ประกาศนียบัตร ISO 27001 Information Security Management Systems Lead Auditor

3.6. บุคลากรด้านการทดสอบเจาะระบบต้อง ได้รับการรับรองหรือได้รับประกาศนียบัตรรับรองความรู้ความสามารถทางด้านความมั่นคงปลอดภัยไซเบอร์ จากหน่วยงานในระดับสากลตามที่ระบุในเอกสาร NDID Member Qualification Assessment Framework (MQA) สำหรับสมาชิกที่ขอเชื่อมต่อ ดังนี้

3.6.1. ประกาศนียบัตร GIAC Penetration Tester (GPEN) หรือ

3.6.2. ประกาศนียบัตร EC-Council - Computer Hacking Forensic Investigator (CHFI) หรือ

3.6.3. ประกาศนียบัตร Offensive Security Certified Professional (OSCP) หรือ

3.6.4. ประกาศนียบัตร Certified Ethical Hacker (CEH)

ทั้งนี้ บุคลากรดำเนินงานที่เสนอในโครงการทุกตำแหน่ง ต้องแนบแนบเอกสารหลักฐานเกี่ยวกับวุฒิการศึกษา ใบประกาศนียบัตรที่ยังไม่หมดอายุ และรายละเอียดลำดับขั้นของประกาศนียบัตร (Certificate Career Path) ที่ได้รับ ประสบการณ์ทำงานและความเชี่ยวชาญ มาในวันที่เสนอราคาด้วย

3.7. มีความสามารถตามกฎหมาย

3.8. ไม่เป็นบุคคลล้มละลาย

3.9. ไม่อยู่ระหว่างเลิกกิจการ

4. ขอบเขตของงานที่ต้องการ

ผู้รับจ้างต้องดำเนินการตรวจสอบ วิเคราะห์ และให้คำแนะนำในการปรับปรุงด้านระบบการรักษาความปลอดภัยของระบบเครือข่ายและระบบคอมพิวเตอร์ของระบบพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital ID) ของทางบริษัท โดยจะต้องครอบคลุมขอบเขตการดำเนินงาน ดังนี้

4.1 ทำการตรวจสอบความมั่นคงปลอดภัยของระบบพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital ID) ของบริษัท ให้รองรับการเชื่อมต่อกับบริการยืนยันตัวตนรูปแบบดิจิทัล (National Digital ID - NDID) โดยการตรวจสอบ วิเคราะห์ และประเมินมาตรการรักษาความมั่นคงปลอดภัยของระบบตามเอกสาร NDID Member Qualification Assessment Framework (MQA) สำหรับสมาชิกที่ขอเชื่อมต่อ และทำการทดสอบเจาะระบบผ่านเครือข่ายภายในและเครือข่ายภายนอกบริษัท พร้อมให้คำแนะนำการปิดช่องโหว่ที่พบ

4.2 บุคลากรที่เสนอให้ดำเนินโครงการ ตั้งแต่ช่วงเสนอราคาจนกระทั่งสิ้นสุดโครงการ จะต้องเป็นบุคคลเดียวกัน แต่หากมีความจำเป็นต้องเปลี่ยนแปลง ต้องมีการแจ้งเป็นหนังสืออย่างเป็น

ทางการแก่บริษัท เพื่อให้ทราบเป็นลายลักษณ์อักษรและพิจารณาถึงความเปลี่ยนแปลงนั้น อีกทั้ง บุคลากรที่เสนอเข้ามาใหม่ จะต้องมีคุณสมบัติไม่น้อยกว่าบุคลากรเดิม

4.3 ผู้รับจ้างมีสิทธิในการเสนอบุคลากรในโครงการเพิ่มเติมได้ โดยต้องมีคุณสมบัติตามข้อกำหนด โดยต้องแจ้งให้แก่บริษัททราบเป็นลายลักษณ์อักษรและพิจารณาถึงการเพิ่มบุคลากรในโครงการนั้น โดยไม่มีค่าใช้จ่ายเพิ่มเติม

4.4 ผู้รับจ้างต้องจัดทำแผนดำเนินงาน โดยต้องเสนอแผนดำเนินงานดังกล่าวให้บริษัทเห็นชอบก่อน

4.5 ผู้รับจ้างต้องแจ้งพนักงาน ให้บริษัททราบทุกครั้งก่อนเข้าดำเนินการต่าง ๆ ถึงแผนการเข้าดำเนินงาน เครื่องมือที่ใช้ หรือเทคนิคที่ใช้ในการเจาะระบบ รวมถึงการประเมินผลกระทบที่อาจเกิดขึ้นระหว่างดำเนินงาน ทั้งนี้รับจ้างจะต้องแจ้ง บริษัททราบล่วงหน้าอย่างน้อย 1 วันทำการ และจะดำเนินการได้หลังจากที่ได้รับความเห็นชอบทุกครั้ง

4.6 ผู้รับจ้างต้องดำเนินการประเมินมาตรการการรักษาความมั่นคงปลอดภัยของระบบตามแบบประเมินตนเองสำหรับสมาชิกที่จะทำหน้าที่เป็น Relying Party (RP) และ Identity Provider (IdP) (สมาชิกระดับ 1) ตามเอกสาร NDID Member Qualification Assessment Framework (MQA) สำหรับสมาชิกที่ขอเชื่อมต่อกับบริการยืนยันตัวตนรูปแบบดิจิทัล (National Digital ID - NDID) หรือแบบประเมินอื่นตามที่ผู้ว่าจ้างกำหนด

4.7 ผู้รับจ้างต้องทำการศึกษาระบบ Digital ID ของบริษัท ซึ่งครอบคลุมถึงระบบย่อยต่าง ๆ อย่างน้อย ดังนี้

- 4.7.1 ระบบ Digital ID ของบริษัท ซึ่งรองรับการพิสูจน์ และยืนยันตัวตนสำหรับประชาชนทั่วไป
- 4.7.2 ระบบ Digital ID ของบริษัท ซึ่งรองรับบริหารจัดการผู้ใช้งานโดยเจ้าหน้าที่ที่ได้รับมอบหมาย (User Management)
- 4.7.3 ระบบ Digital ID ของบริษัท ที่รองรับการเชื่อมต่อกับหน่วยงานภายนอกเพื่อการยืนยันตัวตน โดยใช้ OpenID Protocol
- 4.7.4 ระบบ Digital ID ของบริษัท ที่รองรับการเชื่อมต่อกับระบบงานอื่น ๆ ของบริษัท (API) เพื่อรองรับการพิสูจน์ และออกบัญชีผู้ใช้ให้ประชาชน (e-KYC)
- 4.7.5 ระบบ Digital ID ของบริษัท ที่เชื่อมต่อกับระบบพิสูจน์และยืนยันตัวตนตามมาตรฐานที่ NDID กำหนด

หมายเหตุ: โดยมีรายละเอียดผังโครงสร้างของระบบที่เกี่ยวข้องตามภาคผนวก ก. และรายละเอียด API ข้อ 4.7.4 ตามภาคผนวก ข.

4.8 ผู้รับจ้างต้องดำเนินการค้นหาช่องโหว่ ประเมินหาจุดอ่อน ประเมินความเสี่ยง และผลกระทบ (Vulnerability Assessment) ในระบบเครือข่าย (Network) จากเครือข่ายภายนอกในรูปแบบที่เรียกว่า External VA โดยครอบคลุมระบบ Digital ID ของบริษัท ตามข้อ 4.7 พร้อมจัดทำข้อเสนอแนะ สำหรับแนวทางแก้ไขระบบสารสนเทศและระบบที่เกี่ยวข้อง

4.9 ผู้รับจ้างต้องดำเนินการทดสอบเจาะระบบ (Penetration Testing) ตามมาตรฐาน OWAPS Top 10 Web Application Security Risks หรือCWE/SANS TOP 25 Most Dangerous Software Errors เป็นอย่างน้อย จากเครือข่ายภายนอกในรูปแบบที่เรียกว่า External Penetration Testing ทั้งแบบ Gray-Box และ Black-Box ที่ระบบ Digital ID ของบริษัท ตามข้อ 4.7 พร้อมจัดทำรายงาน ข้อเสนอแนะ สำหรับแนวทางแก้ไขระบบสารสนเทศระบบที่เกี่ยวข้อง และ Certificate ที่เกี่ยวข้องกับการทดสอบเจาะระบบของผู้ทดสอบเจาะระบบ

4.10 ผู้รับจ้างต้องให้คำแนะนำกระบวนการสำรองข้อมูล (Backup) ก่อนทำการทดสอบเจาะระบบ (Penetration Testing) และกู้ข้อมูลคืน (Rollback) หลังจากดำเนินการเสร็จสิ้นแล้วทุกครั้ง เพื่อให้ระบบกลับคืนสู่สภาพเดิมเสมอ

4.11 จัดให้มีบุคลากรที่มีความรู้ความเชี่ยวชาญเข้าร่วมประชุมเพื่อนำเสนอผลการทดสอบเจาะระบบ (Penetration Testing) และประเมินความเสี่ยงเพื่อหาช่องโหว่ (Vulnerability Assessment) พร้อมทั้งแนะนำการปิดช่องโหว่ที่พบ

4.12 ผู้รับจ้างต้องดำเนินการทดสอบเจาะระบบซ้ำ (Revisit) นับถัดจากวันที่บริษัท มีหนังสือแจ้งให้ผู้รับจ้างดำเนินการ พร้อมจัดทำรายงานผลการทดสอบทั้งหมด บทวิเคราะห์ คำแนะนำ การแก้ไข การตรวจสอบหลังการแก้ไข และบทสรุปผู้บริหาร หลังจากที่บริษัทได้ดำเนินการแก้ไขช่องโหว่แล้ว และกรณีที่บริษัท ไม่สามารถดำเนินการปิดช่องโหว่เดิม ตามคำแนะนำการปิดช่องโหว่ ผู้รับจ้างจะต้องวิเคราะห์และหาแนวทางการแก้ไขอื่น ๆ และนำเสนอผลการทดสอบเจาะระบบซ้ำ (Revisit) ต่อที่ประชุมตามที่บริษัท กำหนด

4.13 ผู้รับจ้างต้องใช้เอกสารข้อมูล เครื่องมือ ฮาร์ดแวร์และซอฟต์แวร์ต่าง ๆ ในการดำเนินการอย่างถูกต้องตามกฎหมาย ไม่ละเมิดลิขสิทธิ์หรือสิทธิบัตรของผู้อื่น

4.14 หากมีส่วนหนึ่งส่วนใดที่มิได้ระบุไว้ในเอกสารนี้ แต่มีความจำเป็นต้องจัดทำหรือ ผู้รับจ้างต้องจัดหาให้เพียงพอต่อการใช้งานของบริษัท โดยไม่คิดค่าใช้จ่ายเพิ่มเติม

4.15 ผู้รับจ้างต้องจัดทำสัญญาไม่เปิดเผยข้อมูลพร้อมลงนามให้แก่บริษัท โดยข้อมูล และเอกสารทั้งหมดของโครงการนี้ที่จัดทำขึ้นถือเป็นลิขสิทธิ์ของบริษัท ผู้รับจ้างจะไม่นำเอกสารและข้อมูลใด ๆ ที่ได้รับไปทำการเปิดเผย หรือเผยแพร่ โดยไม่ได้รับความเห็นชอบจากบริษัทเป็นลายลักษณ์อักษร

1. ระยะเวลาการดำเนินการและการส่งมอบงาน

ผู้เสนอนำเสนอแผนการดำเนินการให้บริษัท ฯ พิจารณา

2. หลักฐานการยื่นข้อเสนอ

6.1 คุณสมบัติของผู้เสนอราคา

6.2 รายละเอียดข้อเสนอ ตามขอบเขตของงานและการบริการ

6.3 เงื่อนไขการจ่ายเงิน ระยะเวลาเครดิต

6.4 ค่าใช้จ่ายหรือส่วนลด และรายละเอียดอื่นที่เป็นประโยชน์ต่อการพิจารณา

7. หลักเกณฑ์ในการพิจารณา

บริษัทจะพิจารณาคัดเลือกผู้ยื่นข้อเสนอที่ผ่านเกณฑ์ด้านคุณภาพ (ข้อเสนอด้านเทคนิค) และเกณฑ์ราคา โดยมีสัดส่วนน้ำหนักของเกณฑ์คุณภาพ (ข้อเสนอด้านเทคนิค) น้ำหนักร้อยละ 80 และเกณฑ์ราคา น้ำหนักร้อยละ 20 โดยบริษัทจะดำเนินการตามลำดับ ดังนี้

7.1 ตรวจสอบการมีผลประโยชน์ร่วมกัน และความครบถ้วนถูกต้องของเอกสารหลักฐานต่าง ๆ แล้วพิจารณาคัดเลือกรายที่ไม่มีผลประโยชน์ร่วมกัน มีคุณสมบัติและเอกสารหลักฐานต่าง ๆ ครบถ้วนถูกต้อง และพิจารณาข้อเสนอด้านเทคนิคต่อไป สำหรับรายที่มีผลประโยชน์ร่วมกัน หรือมีคุณสมบัติหรือยื่นเอกสารหลักฐานต่าง ๆ ไม่ครบถ้วนถูกต้อง บริษัทจะไม่ทำการประเมินค่าประสิทธิภาพต่อราคาตามหลักเกณฑ์ที่กำหนด

7.2 พิจารณาข้อเสนอด้านเทคนิคของผู้รับจ้างทุกราย หากผู้ประสงค์จะเสนอราคาใดมีคุณสมบัติไม่ถูกต้องหรือยื่นหลักฐานการยื่นข้อเสนอไม่ถูกต้อง หรือไม่ครบถ้วน บริษัทจะไม่รับพิจารณาข้อเสนอของผู้ประสงค์จะเสนอราคารายนั้น เว้นแต่เป็นข้อผิดพลาดหรือผิดหลงเพียงเล็กน้อยหรือผิดแผกในส่วนที่มิใช่สาระสำคัญเฉพาะในกรณีที่พิจารณาเห็นว่าจะเป็นประโยชน์ต่อบริษัทเท่านั้น

ทั้งนี้บริษัท จะเชิญให้ผู้ยื่นข้อเสนอทุกรายที่มีคุณสมบัติและยื่นเอกสารครบถ้วนถูกต้องตามข้อ 7.1 นำเสนอด้านเทคนิค โดยจะพิจารณาประเมินค่าประสิทธิภาพตามหลักเกณฑ์ ดังนี้

เกณฑ์การพิจารณา	กำหนดน้ำหนักเท่ากับร้อยละ
1. คุณสมบัติและคุณภาพของบุคลากรในโครงการ	**50**
1.1 คุณสมบัติของบุคลากรโครงการ ในด้านความเชี่ยวชาญมาตรการรักษาความมั่นคงปลอดภัย	10
1.2 คุณสมบัติและจำนวนบุคลากรของโครงการ ในด้านการประเมินมาตรการรักษาความมั่นคงปลอดภัย	20
1.3 คุณสมบัติและจำนวนบุคลากรของโครงการ ในด้านการเจาะระบบ	20
2. ผลงานและประสบการณ์ของผู้เสนอราคา	**20**
3. การนำเสนอ ความรู้ความเข้าใจในโครงการ แผนการดำเนินงาน ประสบการณ์ และการตอบคำถาม	**30**
3.1 จัดทำเอกสารแผนการดำเนินงานครอบคลุมทุกด้านของโครงการ โดยยื่นเข้ามาพร้อมในวันเสนอราคา	10

เกณฑ์การพิจารณา	กำหนดน้ำหนัก เท่ากับร้อยละ
3.2 การนำเสนอ ตามข้อเสนอที่ยื่นในวันเสนอราคา ชัดเจนครบถ้วน และความเข้าใจในโครงการ	10
3.3 การตอบคำถาม	10
รวมคะแนน	**100**

ทั้งนี้ ข้อเสนอด้านเทคนิคที่ผ่านเกณฑ์การพิจารณา ต้องได้รับคะแนนการประเมินด้านคุณภาพ (Performance) ไม่น้อยกว่าร้อยละ 70 ตามภาคผนวก ค. (รายละเอียด หลักเกณฑ์การพิจารณาข้อเสนอด้านคุณภาพ)

7.3 ข้อเสนอด้านเทคนิคที่ผ่านเกณฑ์การพิจารณาตามข้อ 2.2 จะได้รับการประเมินค่าประสิทธิภาพต่อราคาตามสัดส่วนข้อเสนอด้านเทคนิคและข้อเสนอด้านราคาที่กำหนดและจัดลำดับเรียงตามคะแนนข้อเสนอที่ได้รับคะแนนประเมินสูงสุดจะได้รับการคัดเลือก และบริษัท จะพิจารณาเจรจาต่อรองราคาตามที่เห็นสมควรเพื่อประโยชน์บริษัท ต่อไป

7.4 ผู้รับจ้างจะพิจารณาเกณฑ์คุณภาพและคุณสมบัติที่เป็นประโยชน์ โดยเชิญผู้เสนอราคาที่ผ่านคุณสมบัติเบื้องต้น เข้ามานำเสนอข้อมูล ภายหลังจากที่คณะกรรมการพิจารณาผล พิจารณาผู้เสนอราคาที่ผ่านคุณสมบัติเบื้องต้นแล้วเท่านั้น

7.5 กรณีผู้ได้รับการคัดเลือกไม่ไปทำสัญญาภายในวันเวลาที่กำหนดบริษัท จะพิจารณาเรียกรายลำดับถัดไปเพื่อเจรจาต่อรองและ/หรือทำสัญญาต่อไป หรืออาจพิจารณายกเลิกการประกาศเชิญชวนเพื่อดำเนินการใหม่ตามวิธีหรือขั้นตอนตามระเบียบที่เกี่ยวข้องต่อไป

อนุมัติโดย

.....

จุลวุธ เกษตรสุวรรณ
ผู้ช่วยกรรมการผู้จัดการใหญ่
ฝ่ายเทคโนโลยีสารสนเทศ