

ขอบเขตงาน (Term of Reference)
การจ้างที่ปรึกษาเพื่อตรวจติดตามรอบที่ ๑ สำหรับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
ตามมาตรฐาน ISO/IEC ๒๗๐๐๑ และการจ้างทดสอบเจาะระบบ
(ISO/IEC ๒๗๐๐๑ Surveillance, Vulnerability Assessment
and Penetration Testing)

๑. หลักการและเหตุผล

สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (สำนักงาน กสทช.) โดยสำนักเทคโนโลยีสารสนเทศ มีการจัดทำกระบวนการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC ๒๗๐๐๑:๒๐๑๓ และกระบวนการบริหารจัดการความมั่นคงปลอดภัยข้อมูลส่วนบุคคลตามมาตรฐาน ISO/IEC ๒๗๗๐๑:๒๐๑๓ จนได้รับการรับรองตามมาตรฐานตั้งแต่ปี พ.ศ. ๒๕๖๕ แล้วนั้น เพื่อให้การดำเนินการในกระบวนการดังกล่าวมีความต่อเนื่องและได้รับการตรวจติดตามจากผู้ตรวจประเมินภายนอก (Certification Body) อย่างสม่ำเสมอ สำนักเทคโนโลยีสารสนเทศ จึงมีความจำเป็นที่จะต้องจัดให้มีที่ปรึกษาเพื่อกำหนดแผนการพัฒนาระบบ ปรับปรุง สนับสนุน และกำกับให้การดำเนินงานของสำนักเทคโนโลยีสารสนเทศ สอดคล้องกับมาตรฐานทั้งสองดังกล่าว รวมถึงต้องมีการจัดจ้างผู้ตรวจประเมินภายนอกเข้ามาดำเนินการตรวจสอบตามมาตรฐานทั้งสองด้วย ทั้งนี้ การจัดให้สำนักเทคโนโลยีสารสนเทศ สำนักงาน กสทช. ได้ดำเนินการสอดคล้องกับมาตรฐานทั้งสองนั้นมีความจำเป็นเพื่อให้สอดคล้องกับพระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์ภาคีรัฐ พ.ศ. ๒๕๕๔ และที่แก้ไขเพิ่มเติม พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาคีรัฐ พ.ศ. ๒๕๕๔ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ซึ่งมีการกำหนดมาตรการด้านความมั่นคงปลอดภัยเพื่อดูแลรักษาข้อมูลธุรกรรมอิเล็กทรอนิกส์ภาคีรัฐ ดูแลปกป้องข้อมูลส่วนบุคคลที่สำนักงาน กสทช. มีการประมวลผล และรักษาความมั่นคงปลอดภัยทางไซเบอร์ รวมถึงเพื่อดำเนินการในกิจกรรมด้านการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยและภัยคุกคามทางไซเบอร์ ซึ่งเป็นหนึ่งในกระบวนการสำคัญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้สอดคล้องกับมาตรฐาน ISO/IEC ๒๗๐๓๕ (Information Security Incident Management) เพื่อให้สำนักเทคโนโลยีสารสนเทศ มีกระบวนการบริหารจัดการเพื่อตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยและภัยคุกคามทางไซเบอร์ได้อย่างเป็นมาตรฐานสากลเพิ่มเติมไปจากเดิม ดังนั้น สำนักเทคโนโลยีสารสนเทศได้ตระหนักและเล็งเห็นความสำคัญในการดำเนินการให้สอดคล้องกับกฎหมาย ระเบียบ และข้อบังคับดังที่กล่าวมาข้างต้น รวมถึงดำเนินการให้สอดคล้องกับมาตรฐานสากล ซึ่งเป็นหนึ่งในกลยุทธ์ด้านเทคโนโลยีสารสนเทศของสำนักงาน กสทช.

นอกจากนี้ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (สกมช.) ได้มีประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ ข้อ ๒๑.๓ การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing) โดยกำหนดให้พิจารณาดำเนินการประเมินช่องโหว่และทดสอบเจาะระบบอย่างน้อยปีละ ๑ ครั้ง และหากได้รับการร้องขอจากคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กม.) หรือ สกมช. โดยสำนักงาน กสทช. ต้องส่งสำเนารายงานสรุปผลการทดสอบเจาะระบบ เพื่อประโยชน์ในการประเมินระดับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ไปยังหน่วยงานดังกล่าว ในการนี้สำนักงาน กสทช. จำเป็นต้องเพิ่มระดับการตรวจสอบความมั่นคงปลอดภัยของสำนักงาน กสทช. โดยทำการประเมินช่องโหว่และทดสอบการเจาะระบบ (Vulnerability Assessment and Penetration Testing) ให้สอดคล้องกับสถานการณ์ปัจจุบัน และสอดคล้องกับข้อกำหนดตามประมวลฯ เพื่อให้ระบบสารสนเทศของสำนักงาน กสทช. เกิดความมั่นคงปลอดภัย สร้างความเชื่อมั่นในการดำเนินกิจการและสร้างภาพลักษณ์ที่ดีในการให้บริการสารสนเทศของสำนักงาน กสทช.

ดังนั้น เพื่อให้สำนักเทคโนโลยีสารสนเทศ สำนักงาน กสทช. ปฏิบัติตามเป้าหมายดังกล่าวได้ครบถ้วน จึงมีความจำเป็นต้องจัดจ้างที่ปรึกษาเพื่อเข้ามาดำเนินการพัฒนา ปรับปรุง กระบวนการด้านการรักษา ความมั่นคงปลอดภัย การประเมินช่องโหว่และทดสอบการเจาะระบบ (Vulnerability Assessment and Penetration Testing) และตรวจติดตามกระบวนการต่าง ๆ ให้สอดคล้องกับมาตรฐานการบริหารจัดการ ความมั่นคงปลอดภัยสารสนเทศ ISO/IEC ๒๗๐๐๑:๒๐๑๓ มาตรฐานการบริหารจัดการความมั่นคงปลอดภัยข้อมูล ส่วนบุคคลตามมาตรฐาน ISO/IEC ๒๗๗๐๑:๒๐๑๙ ตลอดจนพัฒนากระบวนการด้านการตอบสนองต่อเหตุการณ์ ด้านความมั่นคงปลอดภัยให้สอดคล้องกับมาตรฐาน ISO/IEC ๒๗๐๓๕ เพื่อให้เกิดประสิทธิภาพและประสิทธิผล สูงสุดในการดำเนินการของสำนักงาน กสทช. ด้านความมั่นคงปลอดภัยสารสนเทศ การคุ้มครองข้อมูลส่วนบุคคล และการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย รวมถึงเป็นการธำรงไว้ซึ่งชื่อเสียง ภาพลักษณ์ และเป็นการปฏิบัติให้สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับที่เกี่ยวข้อง

๒. วัตถุประสงค์

จ้างที่ปรึกษาเพื่อพัฒนาระบบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและระบบบริหารจัดการความมั่นคงปลอดภัยข้อมูลส่วนบุคคลของสำนักเทคโนโลยีสารสนเทศ สำนักงาน กสทช. ให้เป็นไปตาม ข้อกำหนดมาตรฐานสากล ISO/IEC ๒๗๐๐๑:๒๐๑๓ มาตรฐานสากล ISO/IEC ๒๗๗๐๑:๒๐๑๙ และมาตรฐาน ISO/IEC ๒๗๐๓๕ เพื่อให้การปฏิบัติเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศข้อมูลส่วนบุคคล และการตอบสนอง ต่อเหตุการณ์ด้านความมั่นคงปลอดภัยมีความสอดคล้องเหมาะสมและเป็นไปตามกฎหมายและระเบียบ ข้อบังคับที่เกี่ยวข้อง และเป็นการสร้างความเชื่อมั่นและภาพลักษณ์ที่ดีแก่สำนักงาน กสทช. จากการได้รับ ใบรับรองตามมาตรฐานสากลที่เป็นที่ยอมรับ

๓. คุณสมบัติของที่ปรึกษา

ผู้ยื่นข้อเสนอต้องมีคุณสมบัติพื้นฐานที่กำหนด ตามพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุ ภาครัฐ พ.ศ. ๒๕๖๐ และระบบการจัดซื้อจัดจ้างภาครัฐ (Electronic Government Procurement : e-GP) ตามที่แนบในภาคผนวก ๑

๔. ขอบเขตของงานจ้างที่ปรึกษา

ขอบเขตของการดำเนินงานของที่ปรึกษาต้องประกอบด้วยงาน ดังต่อไปนี้

๔.๑ ศึกษา วิเคราะห์ และจัดทำรายงานผลการศึกษาเบื้องต้น (Inception Report) โดยมีเนื้อหา ประกอบด้วย

๔.๑.๑ การวิเคราะห์ความสอดคล้องของสภานภาพการดำเนินงานในปัจจุบันของสำนัก เทคโนโลยีสารสนเทศกับข้อกำหนดของมาตรฐาน ISO/IEC ๒๗๐๐๑ (Information Security Management System; ISMS) และข้อกำหนดมาตรฐาน ISO/IEC ๒๗๗๐๑ (Privacy Information Management System) เพื่อวางแผนทาง ปรับปรุงแก้ไขให้สอดคล้องและผ่านการตรวจติดตาม และวิเคราะห์ช่องว่าง (Gap Analysis) กับข้อกำหนดมาตรฐาน ISO/IEC ๒๗๐๓๕

๔.๑.๒ กำหนดวิธีการ รูปแบบ และเครื่องมือที่เหมาะสมสำหรับจะนำมาใช้ในการประเมิน ช่องโหว่ การทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing) และการจำลองการโจมตีเสมือนจริง เพื่อกำหนดแนวทางการดำเนินงานโครงการ

๔.๒ ดำเนินการร่วมกับบุคลากรของสำนักเทคโนโลยีสารสนเทศ ในลักษณะการทำงานร่วมกับที่ปรึกษา (Co-Sourcing) เพื่อพัฒนา แก้ไข ปรับปรุง กระบวนการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) กระบวนการบริหารจัดการข้อมูลส่วนบุคคล (PIMS) และจัดทำและพัฒนากระบวนการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยให้สอดคล้องกับมาตรฐาน ISO/IEC ๒๗๐๓๕ ตามลำดับ โดยมีขอบเขตการดำเนินงานดังนี้

- ๔.๒.๑ ปรับปรุงแก้ไขบริบทขององค์กรทั้งภายในและภายนอก รวมถึงความคาดหวังและความต้องการจากผู้มีส่วนได้ส่วนเสีย สำหรับขอบเขตในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) การบริหารจัดการข้อมูลส่วนบุคคล (PIMS) และการบริหารจัดการเพื่อตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัย (ISO/IEC ๒๗๐๓๕) พร้อมทั้งนำเสนอคณะกรรมการที่เกี่ยวข้องเพื่อพิจารณาอนุมัติ
- ๔.๒.๒ ปรับปรุงแก้ไขระเบียบวิธีในการประเมินความเสี่ยงความมั่นคงปลอดภัยสารสนเทศ ความมั่นคงปลอดภัยข้อมูลส่วนบุคคล การกำหนดเกณฑ์เพื่อใช้ในการประเมินความเสี่ยงและกลยุทธ์ในการจัดการกับความเสี่ยงในระดับต่าง ๆ ให้สอดคล้องกับข้อกำหนดของมาตรฐาน ISMS, PIMS และการบริหารจัดการเพื่อตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัย (ISO/IEC ๒๗๐๓๕)
- ๔.๒.๓ ดำเนินการประเมินความเสี่ยงทรัพย์สินสารสนเทศและข้อมูลส่วนบุคคล ตามขอบเขตและจัดทำเป็นรายงานผลการประเมินความเสี่ยงที่สอดคล้องกับข้อกำหนดของมาตรฐาน ISMS, PIMS และมาตรฐาน ISO/IEC ๒๗๐๓๕
- ๔.๒.๔ ปรับปรุง แก้ไข เอกสารแสดงมาตรการที่เลือกใช้มาตรการรักษาความมั่นคงปลอดภัยในระบบบริหารจัดการรักษาความมั่นคงปลอดภัยสารสนเทศ (Statement of Application: SoA) โดยอ้างอิงตามภาคผนวกของมาตรฐาน ISMS, PIMS และมาตรฐาน ISO/IEC ๒๗๐๓๕ และมีความสอดคล้องกับผลการประเมินความเสี่ยง
- ๔.๒.๕ จัดทำ หรือปรับปรุง นโยบายและขั้นตอนปฏิบัติต่าง ๆ (Policies & Procedures) แนวปฏิบัติที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล รายการเอกสารต่าง ๆ ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลให้สอดคล้องตาม และขั้นตอนกระบวนการที่เกี่ยวข้องกับการรับมือกับเหตุการณ์ด้านความมั่นคงปลอดภัย (Plan and Prepare, Detection and Reporting, Assessment and Decision, Response, Lessons Learnt) ตามข้อกำหนดมาตรฐาน ISMS, PIMS และมาตรฐาน ISO/IEC ๒๗๐๓๕ ตามลำดับ
- ๔.๒.๖ เสนอแผนการปรับปรุงการดำเนินการด้านการรักษาความมั่นคงปลอดภัยให้สอดคล้องมาตรการ ข้อ ๗ Additional ISO/IEC ๒๗๐๐๒ guidance for PII controllers และ/หรือ ข้อ ๘ Additional ISO/IEC ๒๗๐๐๒ guidance for PII processors ของมาตรฐาน PIMS ตามลักษณะของการควบคุมข้อมูลส่วนบุคคลซึ่งสอดคล้องตามขอบเขตที่กำหนด
- ๔.๒.๗ จัดทำ หรือปรับปรุง แก้ไข แผนและตัวชี้วัดเพื่อเป็นการวัดประสิทธิผลของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Effectiveness Measurement) ให้สอดคล้องกับข้อกำหนดของมาตรฐาน ISMS, PIMS และมาตรฐาน ISO/IEC ๒๗๐๓๕ ตามลำดับ
- ๔.๒.๘ ปรับปรุง แก้ไข และร่วมดำเนินการทดสอบแผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan) ให้กับระบบสารสนเทศตามขอบเขตของกระบวนการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) และขอบเขตของกระบวนการบริหารจัดการข้อมูลส่วนบุคคล (PIMS) ให้สอดคล้องกับข้อกำหนดมาตรฐาน ISMS, PIMS และมาตรฐาน ISO/IEC ๒๗๐๓๕ ตามลำดับ

- ๔.๒.๙ ดำเนินการจัดทำแผน และทดสอบ กระบวนการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ และแผนการรับมือกับภัยคุกคามทางไซเบอร์ และนำผลที่ได้มาปรับปรุงแผนดังกล่าว อย่างน้อย ๑ สถานการณ์จำลอง ให้สอดคล้องกับมาตรฐาน ISMS, PIMS และมาตรฐาน ISO/IEC ๒๗๐๓๕ ตามลำดับ
- ๔.๒.๑๐ ดำเนินการบริหารจัดการเอกสารสารสนเทศ (Documented Information) เพื่อใช้ในการอ้างอิงและดำเนินการระบบบริหารจัดการความมั่นคงปลอดภัยให้สอดคล้องกับข้อกำหนดของมาตรฐาน ISMS, PIMS และมาตรฐาน ISO/IEC ๒๗๐๓๕ ตามลำดับ รวมทั้ง เหมาะสมกับระบบบริหารจัดการเอกสาร (Document Management System) ที่สำนักเทคโนโลยีสารสนเทศมีการใช้งาน
- ๔.๒.๑๑ จัดทำแผนการตรวจสอบ ตลอดจนให้คำปรึกษาและคำแนะนำแก่ทีมผู้ตรวจสอบภายในของสำนักเทคโนโลยีสารสนเทศ (ISMS Internal Auditor) ในการดำเนินการตรวจสอบภายในและจัดทำรายงานผลการตรวจสอบตามแผนการตรวจสอบ ซึ่งต้องสอดคล้องตามข้อกำหนดของมาตรฐาน ISMS, PIMS และมาตรฐาน ISO/IEC ๒๗๐๓๕ ตามลำดับ
- ๔.๒.๑๒ ให้คำปรึกษา และคำแนะนำ ในการติดตามการแก้ไขข้อบกพร่องที่ตรวจพบจากการตรวจสอบภายใน (Corrective and Preventive Actions) ของทั้งกระบวนการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) การบริหารจัดการข้อมูลส่วนบุคคล (PIMS) และการรับมือกับเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ
- ๔.๒.๑๓ ให้คำปรึกษา และดำเนินการเตรียมการในส่วนความรับผิดชอบของผู้บริหาร (Management Review) เพื่อทบทวนการพัฒนาและการดำเนินงานการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) การบริหารจัดการข้อมูลส่วนบุคคล (PIMS) และการรับมือกับเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ
- ๔.๒.๑๔ ให้คำปรึกษา และคำแนะนำ รวมทั้งรับผิดชอบค่าใช้จ่ายทั้งหมดในการจัดหา Certification Body เพื่อการตรวจติดตามในการขอการรับรองการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) การบริหารจัดการความมั่นคงปลอดภัยข้อมูลส่วนบุคคล (PIMS) และการรับมือกับเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ ให้สอดคล้องกับตามมาตรฐานสากล ISO/IEC ๒๗๐๐๑ มาตรฐาน ISO/IEC ๒๗๗๐๑ และมาตรฐาน ISO/IEC ๒๗๐๓๕ ตามลำดับจนได้รับการรับรองตามขอบเขตที่กำหนด (Scope of Work)
- ๔.๒.๑๕ ให้คำปรึกษา และคำแนะนำในการแก้ไข Non Conformity (NC) (ถ้ามี) ที่ได้รับการตรวจประเมินของ Certification Body และจัดทำแผนการดำเนินการเพื่อแก้ไข และตอบ NC ให้กับ Certification Body ภายในระยะเวลาที่กำหนด
- ๔.๒.๑๖ ดำเนินการจัดรายงานผลการประเมินความสอดคล้องการปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และกฎหมายลำดับรองที่เกี่ยวข้อง
- ๔.๓ ดำเนินการค้นหา สืบหา และวิเคราะห์ข้อมูลที่เกี่ยวข้องกับองค์กรผ่าน Open Source Intelligence (OSINT) จากแหล่งข้อมูลเปิดทั่วไปที่สามารถเข้าถึงได้ ดังนี้
- ๔.๓.๑ ทำการหาเครื่องเซิร์ฟเวอร์เปิดให้เข้าถึงผ่านเครือข่ายอินเทอร์เน็ต อาทิเช่น การหาข้อมูลด้วย Shodan, การหาข้อมูลด้วย Zoomeye, การหาข้อมูลด้วย Google เป็นต้น
- ๔.๓.๒ ทำการหาข้อมูลที่อยู่ในอินเทอร์เน็ต หรือ Darkweb อาทิเช่น การหาข้อมูลด้วย Github, การหาข้อมูลด้วย Dehashed, การหาข้อมูลด้วย Bing เป็นต้น
- ๔.๓.๓ หาแอปพลิเคชันที่ผู้ใช้งานทั่วไปใช้งานในปัจจุบัน อาทิเช่น การหาข้อมูลด้วย Google, การหาข้อมูลด้วย Play Store, การหาข้อมูลด้วย Apple Store เป็นต้น

๔.๓.๔ ค้นหาอีเมลที่ใช้ภายในสำนักงาน กสทช. อาทิเช่น การหาข้อมูลด้วย Google, การหาข้อมูลด้วย Bing, การหาข้อมูลด้วย DuckDuckGo เป็นต้น

๔.๔ ดำเนินการทดสอบเจาะระบบและประเมินช่องโหว่ จากเครือข่ายภายนอกของสำนักงาน กสทช. (External Penetration Testing and Vulnerabilities Assessment) มีรายละเอียดดังนี้

๔.๔.๑ ตรวจสอบการเข้าถึงจากเครือข่ายภายนอก (External Network Reconnaissance) ด้วยวิธี Black Box

๔.๔.๒ ตรวจสอบช่องโหว่จากเครือข่ายภายนอกจะต้องครอบคลุมในระดับระบบปฏิบัติการของเครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์ในระบบเครือข่าย (Network Equipment) และอุปกรณ์ในระบบรักษาความปลอดภัยสารสนเทศ (Security Device) ของสำนักงาน กสทช. จำนวนไม่น้อยกว่า ๒๕๔ หมายเลขไอพี (External Vulnerability Assessment) โดยครอบคลุมอย่างน้อยดังนี้

(๑) External non-intrusive scanning of the selected hosts

(๒) Execute vulnerability and port scanning assessments

(๓) Open ports

(๔) Configuration details

(๕) The presence of known vulnerabilities and/or system weaknesses

๔.๔.๓ ดำเนินการทดสอบเจาะระบบด้วยวิธีการที่เป็นไปตามมาตรฐานและใช้ Version ล่าสุดที่มีการประกาศในการใช้งาน อย่างน้อย ๑ มาตรฐาน ดังต่อไปนี้

(๑) Opensource Security Testing Methodology (OSSTM)

(๒) NIST SP๘๐๐-๑๑๕ Guideline on Network Security Testing

๔.๔.๔ ดำเนินการทดสอบหาช่องทางในการบุกรุกเข้าถึงเครือข่ายเทคโนโลยีสารสนเทศของสำนักงาน กสทช. (External Penetration Testing) โดยครอบคลุมอย่างน้อยดังนี้

(๑) Port scanning

(๒) Vulnerability scanning

(๓) Exploitation frameworks (where appropriate)

(๔) Unauthenticated web application testing

(๕) Trojan horse (Remote Access Trojan)

๔.๔.๕ ดำเนินการทดสอบเจาะระบบในรูปแบบผสมผสาน โดยการทดสอบด้วยการใช้เครื่องมือเจาะระบบแบบอัตโนมัติ (Automate Tool) ทั้งแบบ Commercial Tool และแบบ Open-source Tool ผสมผสานกับความเชี่ยวชาญของบุคลากร (Human Skill) พร้อมเก็บหลักฐานจากการทดสอบ (ผู้รับจ้างจะต้องใช้การทดสอบและวิเคราะห์ด้วยตัวบุคคลเองด้วย (Manual Test))

๔.๔.๖ ดำเนินการทดสอบเจาะระบบไม่ให้เกิดกระทบกับการใช้งานระบบเทคโนโลยีสารสนเทศสำนักงาน กสทช. โดยระหว่างการทดสอบเจาะระบบหากเกิดความผิดปกติของระบบที่ทำการทดสอบ จะต้องรีบแก้ไขและแจ้งให้เจ้าหน้าที่ของสำนักงาน กสทช. ให้ทราบทันที

๔.๔.๗ จัดทำรายงานสรุปผลการทดสอบเจาะระบบและการวิเคราะห์ช่องโหว่รวมถึงข้อค้นพบอย่างละเอียด โดยรายงานจะต้องมีเนื้อหาสาระประกอบไปด้วยอย่างน้อย ดังนี้

(๑) บทสรุปผู้บริหาร

(๒) วิธีการและขั้นตอนการทดสอบ

(๓) รายละเอียดช่องโหว่ พร้อมประเมินความรุนแรงของช่องโหว่

(๔) คำแนะนำในการปิดช่องโหว่

๔.๔.๘ จัดประชุมเพื่อนำเสนอผลการทดสอบเจาะระบบและการวิเคราะห์ช่องโหว่รวมถึงข้อค้นพบต่อสำนักงาน กสทช. พร้อมข้อเสนอแนะและแนวทางการแก้ไขโดยละเอียด

๔.๕ ดำเนินการประเมินช่องโหว่ เครือข่ายภายในของสำนักงาน กสทช. (Internal Penetration Testing and Vulnerabilities Assessment) ด้วยวิธี Black Box โดยมีรายละเอียด ดังนี้

๔.๕.๑ ตรวจสอบการเข้าถึงเครือข่ายภายใน (Internal Network Reconnaissance) อย่างน้อยดังนี้

- (๑) Administrator Desktops
- (๒) Active Directory Services
- (๓) Routing Infrastructure
- (๔) Key Internal Websites
- (๕) การเดาสุ่ม Username Password

๔.๕.๒ ตรวจสอบช่องโหว่ของเครือข่ายภายในจะต้องครอบคลุมในระดับระบบปฏิบัติการของเครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์ในระบบเครือข่าย (Network Equipment) และอุปกรณ์ในระบบรักษาความปลอดภัยสารสนเทศ (Security Device) ของ สำนักงาน กสทช. จำนวนไม่น้อยกว่า ๑,๕๒๔ หมายเลขไอพี (Internal Vulnerability Assessment) โดยครอบคลุมอย่างน้อยดังนี้

- (๑) External non-intrusive scanning of the selected hosts
- (๒) Execute vulnerability and port scanning assessments
- (๓) Exploitation frameworks (where appropriate)
- (๔) Open ports
- (๕) Configuration details
- (๖) The presence of known vulnerabilities and/or system weaknesses

๔.๕.๓ ดำเนินการทดสอบเจาะระบบจากเครือข่ายภายในสำนักงาน กสทช. แบบ Grey-box Test ให้ดำเนินการโดยอ้างอิงตามมาตรฐาน NIST SP๘๐๐-๑๑๕ และใช้ Version ล่าสุดที่มีการประกาศในการใช้งาน ซึ่ง สำนักงาน กสทช. จะเตรียมข้อมูลให้บางส่วนในการเข้าถึง

๔.๕.๔ ดำเนินการทดสอบหาช่องทางในการเจาะเข้าถึงเครือข่ายเทคโนโลยีสารสนเทศของสำนักงาน กสทช. (Internal Penetration Testing) อย่างน้อยดังนี้

- (๑) Port scanning
- (๒) Vulnerability scanning
- (๓) Exploitation frameworks (where appropriate)
- (๔) Unauthenticated web application testing
- (๕) Trojan horse (Remote Access Trojan)

๔.๕.๕ ดำเนินการทดสอบเจาะระบบในรูปแบบผสมผสาน โดยการทดสอบด้วยการใช้เครื่องมือเจาะระบบแบบอัตโนมัติ (Automate Tool) ทั้งแบบ Commercial Tool และแบบ Open-source Tool ผสมผสานกับความเชี่ยวชาญของบุคลากร (Human Skill) พร้อมเก็บหลักฐานจากการทดสอบ (ผู้รับจ้างจะต้องใช้การทดสอบและวิเคราะห์ด้วยตัวบุคคลเองด้วย (Manual Test)

๔.๕.๖ ดำเนินการทดสอบเจาะระบบไม่ให้เกิดกระทบกับการใช้งานระบบเทคโนโลยีสารสนเทศสำนักงาน กสทช. โดยระหว่างการทดสอบเจาะระบบหากเกิดความผิดปกติของระบบที่ทำการทดสอบ จะต้องรีบแก้ไขและแจ้งให้เจ้าหน้าที่ของสำนักงาน กสทช. ให้ทราบทันที

๔.๕.๗ จัดทำรายงานสรุปผลการทดสอบเจาะระบบและการวิเคราะห์ช่องโหว่รวมถึงข้อค้นพบอย่างละเอียด โดยรายงานจะต้องมีเนื้อหาสาระประกอบไปด้วยอย่างน้อย ดังนี้

- (๑) บทสรุปผู้บริหาร
- (๒) วิธีการและขั้นตอนการทดสอบ
- (๓) รายละเอียดช่องโหว่ พร้อมประเมินความรุนแรงของช่องโหว่
- (๔) คำแนะนำในการปิดช่องโหว่

๔.๕.๘ จัดประชุมเพื่อนำเสนอผลการทดสอบเจาะระบบและการวิเคราะห์ช่องโหว่รวมถึงข้อค้นพบต่อสำนักงาน กสทช. พร้อมข้อเสนอแนะและแนวทางการแก้ไขโดยละเอียด

๔.๖ ดำเนินการทดสอบหาช่องทางการเจาะเข้าถึงระบบเทคโนโลยีสารสนเทศของสำนักงาน กสทช. (Application Penetration test) ๘ Web Application โดยตรวจสอบความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (Web Application Security Assessment) ตามมิติของ CIA Triad โดยครอบคลุมอย่างน้อยดังนี้

๔.๖.๑ ทดสอบเจาะระบบเว็บแอปพลิเคชันทั้งแบบ Black-box Test ให้ดำเนินการโดยอ้างอิงตาม Open Web Application Security Project (OWASP) Testing guide และใช้ Version ล่าสุดที่มีการประกาศในการใช้งาน

๔.๖.๒ ดำเนินการทดสอบเจาะระบบเว็บแอปพลิเคชันแบบ Black-box Test ในการทดสอบจะดำเนินการเหมือนกับการเจาะระบบโดยไวรัสหรือแฮกเกอร์ที่ปฏิบัติการจริงตามมิติของ CIA Triad และทดสอบหาช่องทางการเข้าถึงระบบ (Exploit) ผ่านช่องโหว่ต่าง ๆ โดยครอบคลุมรายละเอียดดังนี้

(๑) External assessment (identification of application security issues via Internet presented applications; or through simulated-external applications as applicable)

(๒) Testing from the perspective of an unregistered user – ‘Black Box’ testing

(๓) Review of the ability to withstand attacks from injected or manipulated code

(๔) Assess scenarios through which a non-load-based denial of service condition can be introduced

(๕) Assess user access controls, user segregation and authentication

(๖) Attempt to gain unauthorized access to data, to modify data without authority, or to otherwise compromise the security model implemented by the system

๔.๖.๓ ดำเนินการทดสอบเจาะระบบในรูปแบบผสมผสาน โดยการทดสอบด้วยการใช้เครื่องมือเจาะระบบแบบอัตโนมัติ (Automate Tool) ทั้งแบบ Commercial Tool และแบบ Open-source Tool ผสมผสานกับความเชี่ยวชาญของบุคลากร (Human Skill) พร้อมเก็บหลักฐานจากการทดสอบ (ผู้รับจ้างจะต้องใช้การทดสอบและวิเคราะห์ด้วยตัวบุคคลเองด้วย (Manual Test)

๔.๖.๔ ดำเนินการทดสอบเจาะระบบไม่ให้เกิดกระทบกับการใช้งานระบบเทคโนโลยีสารสนเทศสำนักงาน กสทช. โดยระหว่างการทดสอบเจาะระบบหากเกิดความผิดปกติของระบบที่ทำการทดสอบ จะต้องรีบแก้ไขและแจ้งให้เจ้าหน้าที่ของสำนักงาน กสทช. ให้ทราบทันที

๔.๖.๕ จัดทำรายงานสรุปผลการทดสอบเจาะระบบและการวิเคราะห์ช่องโหว่รวมถึงข้อค้นพบ

๔.๖.๖ อย่างละเอียด โดยรายงานจะต้องมีเนื้อหาสาระประกอบไปด้วยอย่างน้อย ดังนี้

- (๑) บทสรุปผู้บริหาร
- (๒) วิธีการและขั้นตอนการทดสอบ
- (๓) รายละเอียดช่องโหว่ พร้อมประเมินความรุนแรงของช่องโหว่
- (๔) คำแนะนำในการปิดช่องโหว่

๔.๖.๗ จัดประชุมเพื่อนำเสนอผลการทดสอบเจาะระบบและการวิเคราะห์ช่องโหว่รวมถึงข้อค้นพบต่อสำนักงาน กสทช. พร้อมข้อเสนอแนะและแนวทางการแก้ไขโดยละเอียด

๔.๗ จำลองการโจมตีเสมือนจริงจากผู้โจมตีภายนอกที่จะโจมตีสำนักงาน กสทช. โดยจำลองการโจมตีจากสถานการณ์จำลองที่ใกล้เคียงกับกลุ่มผู้โจมตีมืออาชีพบนอินเทอร์เน็ต (APT actor) ตามข้อมูลเผยแพร่ของ ThaiCert หรือหน่วยงานด้านความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้อง จำนวน ๑ สถานการณ์ เพื่อประเมินความสามารถในการตอบสนองต่อภัยคุกคามทางไซเบอร์ของ สำนักงาน กสทช. ตามมาตรฐาน MITRE framework

๔.๗.๑ มีการใช้ข้อมูล Threat Intelligence กำหนดสถานการณ์จำลอง โดยสถานการณ์จำลองที่กำหนดจะสอดคล้องกับความเสี่ยงที่หน่วยงานภาครัฐในไทยเผชิญ และรูปแบบภัยคุกคามทางไซเบอร์ในปัจจุบันเพื่อให้การทดสอบใกล้เคียงสถานการณ์จริงมากที่สุด

๔.๗.๒ ทดสอบบนระบบในสภาพแวดล้อมจริง (Production) โดยไม่มีผลกระทบต่อ Production แต่อย่างใด

๔.๗.๓ พยายามเข้าถึงเครือข่าย/ระบบภายใน ของสำนักงาน กสทช.หรือเข้าถึงข้อมูลสำคัญที่เกี่ยวข้องกับสำนักงาน กสทช.

๔.๗.๔ ต้องจัดทำรายงานและให้คำปรึกษาพร้อม

๔.๗.๕ จัดประชุมเพื่อนำเสนอผลการทดสอบเจาะระบบและการวิเคราะห์ช่องโหว่รวมถึงข้อค้นพบต่อสำนักงาน กสทช. พร้อมข้อเสนอแนะและแนวทางการแก้ไขโดยละเอียด

๔.๘ จัดทำข้อเสนอแนะดำเนินการจัดทำแนวทางในการปรับปรุงแก้ไขระบบเครือข่าย และระบบเทคโนโลยีสารสนเทศของ สำนักงาน กสทช. ให้มีความมั่นคงปลอดภัยสอดคล้องตามมาตรฐานสากล โดยอ้างอิงจากรายงานผลการประเมินความเสี่ยงที่เกิดจากช่องโหว่และการเจาะเข้าถึงเครือข่ายและระบบเทคโนโลยีสารสนเทศของ สำนักงาน กสทช. และดำเนินการตรวจสอบซ้ำและให้คำแนะนำในการปิดช่องโหว่ในข้อ ๔.๔ - ๔.๖ ต่อเนื่องอีก ๙๐ วัน หลังจากนำเสนอผลการทดสอบ

๔.๙ การดำเนินการจัดการประชุมและฝึกอบรม อย่างน้อยตามหลักสูตรต่อไปนี้

๔.๙.๑ หลักสูตรข้อกำหนดตามมาตรฐาน ISO/IEC ๒๗๐๐๑ มาตรฐาน ISO/IEC ๒๗๗๐๑ และมาตรฐาน ISO/IEC ๒๗๐๓๕ โดยมีระยะเวลาในการอบรมไม่น้อยกว่า ๖ ชั่วโมง จำนวนผู้เข้าร่วมอบรมไม่น้อยกว่า ๑๒ คน

๔.๙.๒ หลักสูตรสร้างความเข้าใจในนโยบาย ขั้นตอนปฏิบัติ และแนวปฏิบัติต่าง ๆ ตามมาตรฐาน ISO/IEC ๒๗๐๐๑ มาตรฐาน ISO/IEC ๒๗๗๐๑ และมาตรฐาน ISO/IEC ๒๗๐๓๕ ระยะเวลาในการอบรมไม่น้อยกว่า ๑๒ ชั่วโมง จำนวนผู้เข้าร่วมอบรมไม่น้อยกว่า ๑๒ คน

๔.๙.๓ หลักสูตรการตรวจสอบมาตรการด้านความมั่นคงปลอดภัยเพื่อให้สอดคล้องตามมาตรฐาน ISO/IEC ๒๗๐๐๑ และมาตรฐาน ISO/IEC ๒๗๗๐๑ ระยะเวลาในการอบรมไม่น้อยกว่า ๑๒ ชั่วโมง จำนวนผู้เข้าร่วมอบรมไม่น้อยกว่า ๑๒ คน

๔.๙.๔ หลักสูตรอบรมให้ความรู้และพัฒนาทักษะ Blue Team ของสำนักงาน กสทช. เพื่อหาแนวทางป้องกันในการจำลองการโจมตีเสมือนจริงระยะเวลาในการอบรมไม่น้อยกว่า ๒๔ ชั่วโมง จำนวนผู้เข้าร่วมอบรมไม่น้อยกว่า ๑๐ คน

๔.๙.๕ หลักสูตรการจัดการฝึกซ้อมเพื่อจำลองการโจมตีเสมือนจริงตามข้อ ๔.๗ ระยะเวลาในการฝึกซ้อมไม่น้อยกว่า ๑๒ ชั่วโมง จำนวนผู้เข้าร่วมฝึกซ้อมไม่น้อยกว่า ๑๐ คน

- ๔.๙.๖ จัดประชุมชี้แจงแนวทางการปรับปรุงแก้ไขระบบสารสนเทศและการปิดช่องโหว่ (Patch Management) แก่บุคลากรที่ดูแลระบบสารสนเทศและผู้รับจ้างดูแลระบบสารสนเทศของสำนักงาน กสทช. มีระยะเวลาการประชุมไม่น้อยกว่า ๑๒ ชั่วโมง จำนวนผู้เข้าร่วมประชุมไม่น้อยกว่า ๒๐ คน
- ๔.๙.๗ หลักสูตรเพื่อสร้างความตระหนักเกี่ยวกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.๒๕๕๓ ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เนื้อหาด้าน Information Security Awareness และเนื้อหาด้านการสร้างความตระหนักในการแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ เป็นระยะเวลาไม่น้อยกว่า ๓ ชั่วโมง โดยมีผู้เข้าอบรมอย่างน้อย ๗๐ คน

๕. บุคลากรของที่ปรึกษา

ที่ปรึกษาจะต้องจัดให้มีบุคลากรที่มีความรู้ความชำนาญเพื่อดำเนินงานตามขอบเขตงาน โดยมีคุณสมบัติ ประสบการณ์ และจำนวนอย่างน้อย ดังนี้

๕.๑ หัวหน้าโครงการ จำนวน ๑ คน

๕.๑.๑ จบการศึกษาน้อยในระดับปริญญาเอกในสาขาที่เกี่ยวข้องกับคอมพิวเตอร์ สาขาวิศวกรรมศาสตร์ หรือการจัดการเทคโนโลยีสารสนเทศ และมีประสบการณ์ด้านการบริหารโครงการที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ เป็นระยะเวลาไม่น้อยกว่า ๑๕ ปี โดยต้องมีระยะเวลาดำเนินงานไม่น้อยกว่า ๒ man-month

๕.๑.๒ ได้รับประกาศนียบัตรอย่างน้อย ดังนี้ ISO/IEC ๒๗๐๐๑ Information Security Management System Lead Auditor

๕.๒ ที่ปรึกษาโครงการด้าน ISO จำนวน ๑ คน

๕.๒.๑ ที่ปรึกษาด้าน ISO ๒๗๐๐๑ ISO ๒๗๗๐๑ และ ISO ๒๗๐๓๕ จบการศึกษาน้อยในระดับปริญญาเอก และมีประสบการณ์ด้านการกำกับดูแลด้านเทคโนโลยีสารสนเทศหรือการรักษาความมั่นคงปลอดภัยสารสนเทศ หรือ การตรวจสอบด้านสารสนเทศ เป็นระยะเวลาไม่น้อยกว่า ๑๕ ปี โดยต้องมีระยะเวลาดำเนินงานไม่น้อยกว่า ๒ man-month ต้องได้รับประกาศนียบัตรที่เกี่ยวข้องอย่างน้อย ดังนี้

- ISO/IEC ๒๗๐๐๑ Lead Auditor หรือ
- ISO/IEC ๒๗๗๐๑ Lead Auditor หรือ
- COBIT Foundation (Control Objectives for Information and Related Technology)

๕.๓ ที่ปรึกษาโครงการด้านการเจาะระบบ จำนวน ๑ คน

๕.๓.๑ ที่ปรึกษาด้านการเจาะระบบวุฒิการศึกษาไม่ต่ำกว่า ปริญญาโท สาขาวิศวกรรมศาสตร์ หรือ สาขาเทคโนโลยีสารสนเทศ หรือวิทยาศาสตร์ ที่มีประสบการณ์อย่างน้อย ๑๕ ปี และมีประสบการณ์ในการบริหารโครงการที่เกี่ยวข้องการจัดจ้างในครั้งนี้ จำนวน ๑ คน โดยมีระยะเวลาดำเนินงานไม่น้อยกว่า ๑๑ man-month และได้รับประกาศนียบัตรอย่างน้อย ดังนี้

- CompTIA Security+ หรือ
- CEH (Certified Ethical Hacker) หรือ
- CompTIA Cybersecurity Analyst (CySA+)

๕.๔ หัวหน้าทีมที่ปรึกษา ISO จำนวน ๑ คน

- ๕.๔.๑ จบการศึกษอย่างน้อยในระดับปริญญาตรี และมีประสบการณ์ด้านการกำกับดูแลด้านเทคโนโลยีสารสนเทศหรือ การรักษาความมั่นคงปลอดภัยสารสนเทศ หรือ การตรวจสอบด้านสารสนเทศ เป็นระยะเวลาไม่น้อยกว่า ๑๕ ปี โดยต้องมีระยะเวลาดำเนินงานไม่น้อยกว่า ๘ man-month
- ๕.๔.๒ ได้รับประกาศนียบัตร Certified ISMS Auditor รับรองโดยสถาบัน International Register of Certificated Auditors (IRCA) ในระดับหลักสูตรไม่ต่ำกว่า ISO/IEC ๒๗๐๐๑ Lead Auditor และ ISO/IEC ๒๗๗๐๑ Implementation หรือ ISO/IEC ๒๗๐๓๕ Implementation

๕.๕ ทีมที่ปรึกษา ISO จำนวน ๑ คน

- ๕.๕.๑ จบการศึกษอย่างน้อยในระดับปริญญาตรี และมีประสบการณ์ด้านการกำกับดูแลด้านเทคโนโลยีสารสนเทศหรือ การรักษาความมั่นคงปลอดภัยสารสนเทศ หรือ การตรวจสอบด้านสารสนเทศ เป็นระยะเวลาไม่น้อยกว่า ๕ ปี โดยต้องมีระยะเวลาดำเนินงานไม่น้อยกว่า ๘ man-month
- ๕.๕.๒ ได้รับประกาศนียบัตร ISO/IEC ๒๗๐๐๑ Lead Auditor หรือ ISO/IEC ๒๗๗๐๑ Implementation หรือ ISO/IEC ๒๗๐๓๕ Implementation

๕.๖ หัวหน้าทีมที่ปรึกษาด้านเทคนิค จำนวน ๑ คน

- ๕.๖.๑ จบการศึกษอย่างน้อยในระดับปริญญาโท และมีประสบการณ์ด้านการกำกับดูแลด้านเทคโนโลยีสารสนเทศหรือ การรักษาความมั่นคงปลอดภัยสารสนเทศ หรือ การตรวจสอบด้านสารสนเทศ เป็นระยะเวลาไม่น้อยกว่า ๕ ปี โดยต้องมีระยะเวลาดำเนินงานไม่น้อยกว่า ๒ man-month
- ๕.๖.๒ ได้รับประกาศนียบัตรอย่างน้อย ดังนี้
- CompTIA Security+ หรือ
 - CEH (Certified Ethical Hacker) หรือ
 - CompTIA Cybersecurity Analyst (CySA+) และ
 - ISO/IEC ๒๗๐๐๑ หรือ ISO/IEC ๒๗๗๐๑ หรือ ISO/IEC ๒๗๐๓๕ Implementation

๕.๗ ทีมที่ปรึกษาด้านเทคนิค จำนวน ๒ คน

- ๕.๖.๑ นักเทคนิคจบการศึกษอย่างน้อยในระดับปริญญาตรี และมีประสบการณ์ด้านการกำกับดูแลด้านเทคโนโลยีสารสนเทศหรือ การรักษาความมั่นคงปลอดภัยสารสนเทศ หรือ การตรวจสอบด้านสารสนเทศ เป็นระยะเวลาไม่น้อยกว่า ๕ ปี จำนวน ๒ คน โดยต้องมีระยะเวลาดำเนินงานไม่น้อยกว่า ๔ man-month และได้รับประกาศนียบัตร อย่างน้อย ดังนี้
- CompTIA Security+ หรือ
 - CEH (Certified Ethical Hacker) หรือ
 - ISO/IEC ๒๗๐๐๑ หรือ ISO/IEC ๒๗๗๐๑ หรือ ISO/IEC ๒๗๐๓๕ Implementation

๕.๘ ทีมที่ปรึกษาด้านเทคนิค (นักเจาะระบบ) จำนวน ๓ คน

- ๕.๘.๑ นักเจาะระบบ วุฒิการศึกษาไม่ต่ำกว่า ปริญญาตรี สาขาวิศวกรรมศาสตร์ หรือ สาขาเทคโนโลยีสารสนเทศ หรือวิทยาศาสตร์ ที่มีประสบการณ์อย่างน้อย ๕ ปี จำนวน ๓ คน โดยมีระยะเวลาการทำงานไม่น้อยกว่าคนละ ๑๐ man-month และได้รับประกาศนียบัตรอย่างน้อย ดังนี้
- GIAC Penetration Tester (GPEN) หรือ

- CompTIA Pentest+ หรือ
- Offensive Security Certified Professional (OSCP) หรือ
- Pentest+ หรือ
- CEH (Certified Ethical Hacker)

๕.๙ ทีมที่ปรึกษาด้านเทคนิค (ผู้ช่วยนักเจาะระบบ) จำนวน ๒ คน

๕.๙.๑ ผู้ช่วยนักเจาะระบบ วุฒิการศึกษาไม่ต่ำกว่า ปริญญาตรี สาขาวิศวกรรมศาสตร์ หรือสาขาเทคโนโลยีสารสนเทศ หรือวิทยาศาสตร์ ที่มีประสบการณ์อย่างน้อย ๕ ปี จำนวน ๒ คน โดยมีระยะเวลาการทำงานไม่น้อยกว่าคนละ ๙.๕ man-month

๖. ระยะเวลาดำเนินการ

ภายใน ๓๖๐ วัน นับถัดจากวันลงนามในสัญญา

๗. ระยะเวลาการส่งมอบงาน

ที่ปรึกษาต้องส่งมอบงานพร้อม Data Files ที่จัดเก็บในสื่อบันทึกข้อมูลชนิด Flash Drive และในรูปแบบเอกสารจำนวน ๕ ชุด โดยแบ่งออกเป็นงวดงานดังนี้

งวดที่ ๑ ส่งมอบงาน ข้อ ๔.๑ ภายใน ๖๐ วัน นับถัดจากวัน ลงนามในสัญญา

งวดที่ ๒ ส่งมอบงาน ข้อ ๔.๒.๑, ๔.๒.๒, ๔.๒.๓, ๔.๒.๔ , ๔.๓, ๔.๔, ๔.๕, ๔.๙.๔ และข้อ ๔.๙.๕ ภายใน ๙๐ วันนับถัดจากวันลงนามในสัญญา

งวดที่ ๓ ส่งมอบงาน ข้อ ๔.๒.๕, ๔.๒.๖, ๔.๒.๗, ๔.๒.๘, ๔.๒.๑๖, ๔.๖, ๔.๗, ๔.๙.๑, ๔.๙.๒, ๔.๙.๓ และข้อ ๔.๙.๖ ภายใน ๒๑๐ วัน นับถัดจากวันลงนามในสัญญา

งวดที่ ๔ ส่งมอบงาน ข้อ ๔.๒.๙, ๔.๒.๑๐, ๔.๒.๑๑, ๔.๒.๑๒, ๔.๒.๑๓, ๔.๒.๑๔, ๔.๒.๑๕ และข้อ ๔.๙.๗ ภายใน ๓๖๐ วัน นับถัดจากวันลงนามในสัญญา

๘. วงเงินที่ใช้ในการจัดหา

วงเงินรวมทั้งสิ้น ๙,๕๙๑,๐๐๐.- บาท (เก้าล้านห้าแสนเก้าหมื่นหนึ่งพันบาทถ้วน) ซึ่งเป็นราคาที่รวมภาษีมูลค่าเพิ่มและค่าใช้จ่ายทั้งปวงไว้ด้วยแล้ว โดยเบิกจ่ายจากงบประมาณ ปี ๒๕๖๖ จำนวนเงิน ๔,๗๙๕,๕๐๐.- บาท (สี่ล้านเจ็ดแสนเก้าหมื่นห้าพันห้าร้อยบาทถ้วน) และผูกพันงบประมาณปี ๒๕๖๗ จำนวนเงิน ๔,๗๙๕,๕๐๐.- บาท (สี่ล้านเจ็ดแสนเก้าหมื่นห้าพันห้าร้อยบาทถ้วน) รายการอื่น ค่าจ้างที่ปรึกษาเพื่อศึกษาวิจัย ประเมินผล หรือพัฒนาระบบต่าง ๆ

๙. เงื่อนไขการชำระเงิน

สำนักงาน กสทช. จะชำระเงินตามจำนวนในสัญญาจ้างหลังจากที่ได้ตรวจรับถูกต้องเรียบร้อยแล้ว และที่ปรึกษาปฏิบัติถูกต้องครบถ้วนตามที่สำนักงาน กสทช. กำหนด โดยจะชำระเงินตามเงื่อนไขและกำหนดเวลาการชำระเงินดังนี้

งวดที่ ๑ เบิกจ่ายเงินเป็นจำนวน ร้อยละ ๑๐ ของวงเงินตามสัญญาของการดำเนินงานโครงการ หลังจากที่ได้รับมอบงานในงวดงานที่ ๑ แล้วเสร็จและผ่านการตรวจรับจากคณะกรรมการตรวจรับพัสดุในงานจ้างที่ปรึกษา เรียบร้อยแล้ว

งวดที่ ๒ เบิกจ่ายเงินเป็นจำนวน ร้อยละ ๔๐ ของวงเงินตามสัญญาของการดำเนินงานโครงการ หลังจากที่ได้รับมอบงานในงวดงานที่ ๒ แล้วเสร็จและผ่านการตรวจรับจากคณะกรรมการตรวจรับพัสดุในงานจ้างที่ปรึกษา เรียบร้อยแล้ว

งวดที่ ๓ เบิกจ่ายเงินเป็นจำนวน ร้อยละ ๓๐ ของวงเงินตามสัญญาของการดำเนินงานโครงการ หลังจากที่ได้รับมอบงานในงวดงานที่ ๓ แล้วเสร็จและผ่านการตรวจรับจาก คณะกรรมการตรวจรับพัสดุในงานจ้างที่ปรึกษา เรียบร้อยแล้ว

งวดที่ ๔ เบิกจ่ายเงินเป็นจำนวน ร้อยละ ๒๐ ของวงเงินตามสัญญาของการดำเนินงานโครงการ หลังจากที่ได้รับมอบงานในงวดงานที่ ๔ แล้วเสร็จและผ่านการตรวจรับจาก คณะกรรมการตรวจรับพัสดุในงานจ้างที่ปรึกษา เรียบร้อยแล้ว

๑๐. การจัดทำข้อเสนอของที่ปรึกษา

ที่ปรึกษาจะต้องทำข้อเสนอโครงการเป็นภาษาไทย ประกอบด้วย เอกสารและหลักฐาน ข้อเสนอทางเทคนิค และข้อเสนอทางการเงิน โดยมีรายละเอียดข้อเสนอ ดังนี้

๑๐.๑. เอกสารและหลักฐานเกี่ยวกับผู้ยื่นข้อเสนอ ประกอบด้วย

๑๐.๑.๑ หลักฐานการจดทะเบียนเป็นนิติบุคคลที่จัดตั้งตามกฎหมายไทย ต้องมีสำเนาหรือภาพถ่ายหนังสือการรับรองการจดทะเบียนเป็นนิติบุคคลของสำนักงานทะเบียนหุ้นส่วนบริษัทกลาง หรือสำนักงานทะเบียนหุ้นส่วนบริษัทจังหวัด กรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์ ที่แสดงว่าได้จดทะเบียนเป็นผู้มีอำนาจทำนิติกรรมแทนนิติบุคคลทุนจดทะเบียน และวัตถุประสงค์ของนิติบุคคลฉบับที่จดทะเบียนล่าสุด ซึ่งรับรองสำเนาถูกต้องโดยผู้มีอำนาจทำนิติกรรมแทนนิติบุคคลพร้อมทั้งประทับตราสำคัญของนิติบุคคลโดยหนังสือรับรองการจดทะเบียนดังกล่าวต้องออกให้ไม่เกิน ๓ เดือน นับจากวันที่ยื่นเสนอ

๑๐.๑.๒ หลักฐานของกรรมการผู้จัดการ หรือหุ้นส่วนผู้จัดการ ต้องมีสำเนาหรือภาพถ่ายทะเบียนบ้านระบุสัญชาติของกรรมการผู้จัดการหรือหุ้นส่วนผู้จัดการซึ่งรับรองสำเนาถูกต้องโดยผู้มีอำนาจทำนิติกรรมแทนนิติบุคคล

๑๐.๑.๓ ในกรณีที่ปรึกษาเป็นหน่วยงานราชการ/ สถาบันการศึกษา ให้ยื่นหนังสือมอบอำนาจของหัวหน้าส่วนราชการ/ สถาบันการศึกษา ที่ให้ผูใดเป็นผู้ดำเนินการ รวมทั้งหลักฐานสำเนาบัตรประชาชน บัตรราชการ พร้อมรับรองสำเนาถูกต้อง พร้อมทั้งต้องมีสำเนาภาพถ่ายหนังสือจัดตั้งหน่วยงาน รวมทั้งอำนาจหน้าที่ของหน่วยงานซึ่งรับรองสำเนาถูกต้องโดยผู้มีอำนาจลงนามของหน่วยงาน

๑๐.๑.๔ หนังสือมอบอำนาจซึ่งปิดอากรแสตมป์ตามกฎหมายในกรณีที่ปรึกษามอบอำนาจให้บุคคลอื่นลงนามในเอกสารข้อเสนอแทน

๑๐.๒. ข้อเสนอทางเทคนิค

ที่ปรึกษาจะต้องจัดทำข้อเสนอด้านเทคนิคที่ประกอบด้วย

๑๐.๒.๑ ผลงานและประสบการณ์ของที่ปรึกษา ประกอบด้วย ผลงานที่ทางหน่วยงานเคยทำมาก่อน โดยเฉพาะส่วนที่เกี่ยวข้องกับการศึกษาในด้านที่เกี่ยวข้องหรือการศึกษาที่คล้ายคลึงกับลักษณะของงานหรือภารกิจตามขอบเขตของงานนี้ ทั้งนี้ ในส่วนผลงานให้แนบหนังสือรับรองผลงาน และ/หรือ สำเนาเอกสารสัญญาที่ได้ดำเนินการแล้วเสร็จ และเป็นผลงานที่เป็นคู่สัญญาโดยตรงกับส่วนราชการ หน่วยงานของรัฐ หน่วยงานตามกฎหมายว่าด้วยระเบียบบริหารราชการส่วนท้องถิ่น หน่วยงานอื่นซึ่งมีกฎหมายบัญญัติให้มีฐานะเป็นราชการบริหารส่วนท้องถิ่น รัฐวิสาหกิจ หรือหน่วยงานเอกชนที่สำนักงาน กสทช. เชื่อถือ ตลอดจนหลักฐานอื่น ๆ เพื่อเพิ่มความเชื่อมั่น เช่น รางวัลและเอกสารอื่น ๆ ที่สามารถอ้างอิงได้ (ถ้ามี)

- ๑๐.๒.๒ วิธีการบริหารและวิธีการดำเนินงาน ตามที่กำหนดในขอบเขตของงานข้อ ๔ โดยผู้ยื่นข้อเสนอจะต้องนำเสนอแผนงาน แนวทางการบริหารและวิธีการดำเนินงานอย่างละเอียด ระยะเวลาการดำเนินงาน บุคลากรที่ดำเนินงาน นอกจากนี้ จะต้องนำเสนอเพื่อแสดงให้เห็นถึงความเข้าใจในโครงการและทักษะความสามารถในการดำเนินการโครงการได้ตามวัตถุประสงค์โครงการและขอบเขตของงาน หรือข้อเสนออื่น ๆ ที่เป็นประโยชน์ต่อการดำเนินงานและสอดคล้องกับขอบเขตของงาน
- ๑๐.๒.๓ คุณสมบัติ ประสบการณ์ และจำนวนของบุคลากรที่เข้าร่วมงาน โดยต้องประกอบด้วยรายละเอียดประวัติ คุณวุฒิ และประสบการณ์การทำงานของที่ปรึกษาที่ผ่านมาของบุคลากรที่ได้เสนอมาในโครงการ ซึ่งสอดคล้องตามข้อ ๕ บุคลากรของที่ปรึกษา

๑๐.๓. ข้อเสนอทางด้านราคา

- ๑๐.๓.๑ ราคาที่จะเสนอจะต้องรวมถึงค่าใช้จ่ายต่าง ๆ ซึ่งรวมถึงภาษีมูลค่าเพิ่มภาษีเงินได้ ค่าอากรแสตมป์ ฯลฯ โดยจะต้องแสดงรายละเอียดค่าใช้จ่ายต่าง ๆ ที่จะต้องใช้ในการดำเนินการตามขอบเขตของงานแต่ละรายการตามแผนปฏิบัติการ และเสนอสรุปเป็นราคาค่าบริการทั้งหมด
- ๑๐.๓.๒ รายละเอียดค่าจ้างบุคลากร โดยแสดงรายละเอียดจำนวนคน-เดือน และอัตราค่าจ้างเป็นรายบุคคล และแนบหลักฐานด้านการเงิน เช่น สลิปเงินเดือน หนังสือรับรองเงินเดือน หรือสำเนาหลักฐานการชำระภาษี (ภ.ง.ด. ๙๑)
- ๑๐.๓.๓ รายละเอียดค่าใช้จ่ายเพิ่มเติมต่าง ๆ เช่น ค่าใช้จ่ายในการจัดการประชุม การจัดฝึกอบรมเพื่อถ่ายทอดความรู้ การประชุมหารือกลุ่มย่อย ค่าพาหนะเดินทาง ค่าวัสดุอุปกรณ์ ค่าจัดทำรายงาน ค่าถ่ายเอกสาร และค่าใช้จ่ายที่เกี่ยวข้อง เป็นต้น

๑๐.๔. วิธีการยื่นข้อเสนอ ผู้ยื่นข้อเสนอต้องแยกซองในการยื่นข้อเสนอเป็น ๓ ซอง และให้ยื่นพร้อมกันโดยถือปฏิบัติ ดังนี้

- ๑๐.๔.๑ ซองที่ ๑ ให้บรรจุเอกสารและหลักฐานเกี่ยวกับผู้ยื่นข้อเสนอ จำนวน ๕ ชุด (ตัวจริง ๑ ชุด สำเนา ๔ ชุด)
- ๑๐.๔.๒ ซองที่ ๒ ให้บรรจุข้อเสนอด้านเทคนิค จำนวน ๕ ชุด (ตัวจริง ๑ ชุด สำเนา ๔ ชุด)
- ๑๐.๔.๓ ซองที่ ๓ ให้บรรจุข้อเสนอด้านราคา จำนวน ๑ ชุด

โดยเอกสารทั้ง ๓ ซอง จะต้องปิดผนึกให้เรียบร้อย และรับรองสำเนาถูกต้องโดยผู้มีอำนาจทำนิติกรรมแทนนิติบุคคล/ผู้มีอำนาจลงนามของหน่วยงาน/ผู้ได้รับมอบอำนาจถูกต้องตามกฎหมาย พร้อมทั้งประทับตรา

เจ้าหน้าที่ของถึงประธานกรรมการดำเนินงานจ้างที่ปรึกษา สำนักงานคณะกรรมการกฤษฎีกา กระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ เลขที่ ๘๗ ซอยพหลโยธิน ๘ แขวงสามเสนใน เขตพญาไท กรุงเทพฯ ๑๐๔๐๐ ภายในกำหนดตามหนังสือเชิญชวน

๑๑. หลักเกณฑ์ในการพิจารณาคัดเลือกข้อเสนอ

โดยที่งานจ้างที่ปรึกษารั้งนี้ เพื่อให้ดำเนินการตรวจสอบและติดตามการดำเนินงานของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Surveillance Audit) รอบที่ ๒ และมีการจัดจ้างผู้ตรวจรับรอง (Certificate Body) เข้ามาตรวจรับรองตามรอบการตรวจติดตามดังกล่าว ซึ่งเป็นงานต่อเนื่องที่ต้องดำเนินการต่อจากเดิมให้ครบวงจร เพื่อคงสถานะใบรับรองที่สำนักงาน กสทช. ได้รับไว้ให้ถูกต้อง นอกจากนี้ สำนักงานคณะกรรมการการกฤษฎีกาความมั่นคงปลอดภัยไซเบอร์ (สกมช.) ได้มีประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ ข้อ ๒๑.๓ การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing) โดยกำหนดให้พิจารณาดำเนินการประเมินช่องโหว่และ

ทดสอบเจาะระบบอย่างน้อยปีละ ๑ ครั้ง ข้อ ๑๔.๑ ต้องจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ข้อ ๒๔.๓ การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise) จึงจำเป็นต้องมีการขอการรับรองมาตรฐานในส่วนที่เกี่ยวข้องกับ ISO/IEC ๒๗๐๓๕ (Information Security Incident Management) เพื่อให้สำนักเทคโนโลยีสารสนเทศ มีกระบวนการบริหารจัดการเพื่อตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยและภัยคุกคามทางไซเบอร์ ได้อย่างเป็นมาตรฐานสากลเพิ่มเติมไปจากเดิม สำนักงาน กสทช. จะดำเนินการจัดจ้างโดยวิธีคัดเลือก ตามพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. ๒๕๖๐ มาตรา ๗๕ และมาตรา ๗๖ (๒) ประกอบกับระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. ๒๕๖๐ ข้อ ๑๒๖ (๒) ในสัดส่วนด้านคุณภาพ ๗๐ และด้านราคา ๓๐ โดยคณะกรรมการจ้างที่ปรึกษาตามวิธีที่กำหนด จะพิจารณาคัดเลือกข้อเสนอตามลำดับ ดังนี้

๑๑.๑ สำนักงาน กสทช. จะพิจารณาข้อเสนอของที่ปรึกษาทุกราย เว้นแต่ที่ปรึกษาที่ยื่นเอกสารหลักฐานไม่ครบถ้วนตามข้อ ๑๐.๑ ในส่วนที่เป็นสาระสำคัญ หรือครบถ้วนแต่ไม่ถูกต้อง จะไม่รับพิจารณาข้อเสนอของที่ปรึกษารายนั้น และในการพิจารณาคัดเลือกข้อเสนอจะคำนึงถึงความคุ้มค่าและวัตถุประสงค์ของงานจ้างที่ปรึกษาเป็นสำคัญ โดยพิจารณาเกณฑ์ด้านคุณภาพเป็นลำดับแรกก่อน คุณภาพด้านต่าง ๆ รวม ๓ หัวข้อ มีคะแนนน้ำหนักรวม ๑๐๐ และจำแนกสัดส่วนน้ำหนักแต่ละหัวข้อ ประกอบด้วย ดังนี้

- | | |
|--|------------------|
| (๑) ผลงานที่ผ่านมาของผู้ยื่นข้อเสนอ | น้ำหนักร้อยละ ๒๐ |
| (๑.๑) ผลงานของที่ปรึกษา | (ร้อยละ ๑๐) |
| (๑.๒) ประสบการณ์เฉพาะ | (ร้อยละ ๑๐) |
| (๒) วิธีบริหารและวิธีปฏิบัติงาน | น้ำหนักร้อยละ ๔๐ |
| (๒.๑) กรอบแนวคิดและแผนการดำเนินงานตาม ข้อ ๔ | (ร้อยละ ๕) |
| (๒.๒) ความเข้าใจในแนวทางการประเมินความเสี่ยงทั้งด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ การบริหารจัดการด้านข้อมูลส่วนบุคคล และการบริหารจัดการด้านการรับมือกับเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ | (ร้อยละ ๑๕) |
| (๒.๓) ทักษะในการประเมินหาความเสี่ยงที่เกิดจากช่องโหว่ที่ค้นพบของเครือข่ายและระบบเทคโนโลยีสารสนเทศ | (ร้อยละ ๑๕) |
| (๒.๔) ข้อเสนออื่น ๆ ที่เป็นประโยชน์ต่อการดำเนินงาน และสอดคล้องกับขอบเขตของงาน | (ร้อยละ ๕) |
| (๓) จำนวนและคุณลักษณะเฉพาะของบุคลากรที่ร่วมงาน | น้ำหนักร้อยละ ๔๐ |

ทั้งนี้ การประเมินคะแนนตามเกณฑ์ด้านคุณภาพแต่ละหัวข้อ มีรายละเอียดคะแนนหัวข้อย่อยและการให้คะแนนตามเอกสารแนบท้ายของงานในภาคผนวก ก และพิจารณาเปรียบเทียบคุณภาพระหว่างผู้ยื่นข้อเสนอด้วยกัน ซึ่งคะแนนที่ได้รับการประเมินแต่ละหัวข้อจะแปลงเป็นคะแนนน้ำหนักตามสัดส่วนของแต่ละหัวข้อที่กำหนด รวมคะแนนน้ำหนักเต็ม ๗๐ ข้อเสนอที่ผ่านเกณฑ์คุณภาพจะต้องได้คะแนนน้ำหนักไม่น้อยกว่าร้อยละ ๘๐ (๕๖)

๑๑.๒ ข้อเสนอของที่ปรึกษาด้านคุณภาพที่ได้รับการประเมินคะแนนและถ่วงน้ำหนักตามข้อ ๑๑.๑ แล้ว เพื่อนำไปรวมกับคะแนนตามสัดส่วนน้ำหนักของราคา (คะแนนเต็มร้อยละ ๓๐) โดยข้อเสนอด้านราคาที่ต่ำที่สุด (ต่ำสุด) จะได้คะแนนน้ำหนักเต็มตามสัดส่วนที่กำหนด และข้อกำหนดด้านราคาของรายลำดับถัดไปจะได้คะแนนลดลงตามสัดส่วนความแตกต่างของระหว่างข้อเสนอราคาของรายนั้นกับข้อเสนอด้านราคาของรายต่ำสุด

๑๑.๓ ข้อเสนอของที่ปรึกษาที่ได้รับการประเมินน้ำหนักตามสัดส่วนด้านคุณภาพและด้านราคาตามข้อ ๑๑.๒ มากที่สุดจะได้รับการคัดเลือกให้เป็นที่ปรึกษาในงานจ้างครั้งนี้ ทั้งนี้

คณะกรรมการจ้างที่ปรึกษาตามวิธีที่กำหนด จะพิจารณาความเหมาะสมของข้อเสนอด้านราคาของที่ปรึกษาที่ได้รับการคัดเลือก รวมทั้งเจรจาต่อรองอัตราค่าจ้างที่ปรึกษาและอื่น ๆ ตามความเหมาะสม และเป็นไปตามหลักเกณฑ์การคำนวณอัตราค่าจ้างที่ปรึกษาตามระเบียบและกฎหมายที่เกี่ยวข้องต่อไป

๑๒. เงื่อนไขอื่น ๆ

- ๑๒.๑ ที่ปรึกษาต้องเก็บรักษาข้อมูลของสำนักงาน กสทช. และข้อมูลที่ได้รับจากการดำเนินโครงการไว้เป็นความลับ จะเปิดเผยให้ผู้ใดทราบมิได้ และไม่นำไปใช้ในวัตถุประสงค์อื่นนอกเหนือจากการดำเนินการในโครงการนี้
- ๑๒.๒ ลิขสิทธิ์ในผลงานและเอกสาร รวมถึงไฟล์ดิจิทัลที่ได้รับจากผลการศึกษา ให้ตกเป็นของสำนักงาน กสทช. แต่เพียงผู้เดียว การเผยแพร่เอกสารหรือจัดทำสำเนาเพิ่มเติมจากที่จ้าง เป็นสิทธิชอบธรรมของสำนักงาน กสทช.
- ๑๒.๓ ที่ปรึกษามีหน้าที่จะต้องตรวจสอบบุคลากรที่เสนอเข้ามาในโครงการว่ามีบุคลากรที่ยังคงดำเนินการเป็นที่ปรึกษาให้กับสำนักงาน กสทช. อยู่ในโครงการใดหรือไม่ กรณีอยู่ในโครงการ จะต้องตรวจสอบรับรองระยะเวลาดำเนินงาน เพื่อมิให้เป็นการใช้ทรัพยากรซ้ำซ้อน ซึ่งจะส่งผลต่อความคุ้มค่าของการใช้เงินงบประมาณ ทั้งนี้บุคลากรหลักของที่ปรึกษา ต้องมีระยะเวลาปฏิบัติงานตามสัญญาไม่ซ้ำซ้อนกับงานในโครงการอื่น ๆ ของที่ปรึกษา ที่ดำเนินการในช่วงเวลาเดียวกัน หากผู้ว่าจ้างพบว่าบุคลากรหลักไม่ว่าคนหนึ่งคนใดหรือหลายคนปฏิบัติงานซ้ำซ้อนกับงานในโครงการอื่น ๆ ไม่ว่าจะพบในระหว่างปฏิบัติงานตามสัญญาหรือในภายหลัง ผู้ว่าจ้างมีสิทธิบอกเลิกสัญญา และ/หรือเรียกค่าเสียหายจากที่ปรึกษาหรือปรับค่าจ้างได้
- ๑๒.๔ ในกรณีที่ที่ปรึกษา มีเหตุจำเป็นต้องเปลี่ยนตัวบุคลากรดำเนินงานในโครงการนี้ ที่ปรึกษาฯ ต้องเสนอขอความเห็นชอบจากสำนักงาน กสทช. ก่อน โดยบุคลากรใหม่ต้องมีคุณสมบัติเทียบเท่าหรือดีกว่าบุคลากรเดิม ทั้งนี้สำนักงาน กสทช. สงวนสิทธิ์ในการพิจารณาปรับลดอัตราค่าจ้างบุคลากรที่ปรึกษาได้ตามความเหมาะสม
- ๑๒.๕ หากที่ปรึกษาไม่สามารถทำงานให้แล้วเสร็จตามเวลาที่กำหนดไว้ในสัญญา และผู้ว่าจ้างยังมิได้บอกเลิกสัญญา ที่ปรึกษาจะต้องชำระค่าปรับให้แก่ผู้ว่าจ้างในอัตรา ร้อยละ ๐.๑ ของวงเงินค่าจ้างฯ นับถัดจากวันที่กำหนดแล้วเสร็จตามสัญญา หรือวันที่ผู้ว่าจ้างได้ขยายระยะเวลาตามสัญญาจนถึงวันที่ทำงานแล้วเสร็จจริงนอกจากนี้ที่ปรึกษายอมให้ผู้ว่าจ้างเรียกค่าเสียหายอันเกิดจากการที่ปรึกษาทำงานล่าช้า เฉพาะส่วนที่เกินกว่าจำนวนค่าปรับ และค่าใช้จ่ายดังกล่าวได้อีกด้วย
- ๑๒.๖ ที่ปรึกษาที่ได้รับการคัดเลือกจะต้องทำสัญญากับสำนักงาน กสทช. ตามแบบสัญญาจ้างที่ที่ปรึกษาคณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดตามที่ประกาศในราชกิจจานุเบกษา และวางหลักประกันสัญญาเป็นอย่างใดอย่างหนึ่งที่กำหนด มูลค่าร้อยละ ๕ ของค่าจ้างที่ปรึกษา เว้นแต่กรณีที่ปรึกษาที่ได้รับการคัดเลือกเป็นหน่วยงานของรัฐ ไม่ต้องวางหลักประกันสัญญา
- ๑๒.๗ ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกให้เป็นผู้ชนะการเสนอราคา หรือชนะการประกวดราคา จะต้องทำแผนการทำงานที่แสดงถึงขั้นตอนต่าง ๆ ตามขอบเขตของงานฯ ให้สอดคล้องกับระยะเวลาดำเนินงาน หรือระยะเวลาการส่งมอบที่เสนอไว้ เพื่อให้คณะกรรมการตรวจรับพัสดุติดตามเร่งรัด และประเมินผลการดำเนินงานให้เป็นไปตามที่กำหนด โดยต้องจัดทำแผนการทำงานเสนอภายใน ๑๕ วัน นับถัดจากวันลงนามในสัญญา ทั้งนี้ แผนการทำงานดังกล่าว ให้ถือเป็นเอกสารส่วนหนึ่งของสัญญา



แบบหนังสือรับรองวงเงินสินเชื่อ

เลขที่.....

วันที่.....

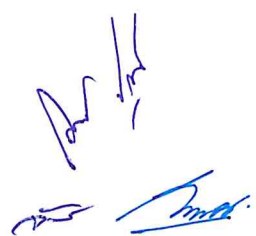
เรื่อง รับรองวงเงินสินเชื่อ

ตามที่.....(ชื่อผู้ประกอบการ นิติบุคคล/บุคคลธรรมดา).....เลขประจำตัว
 ผู้เสียภาษีอากร / เลขประจำตัวประชาชนเลขที่.....จะขอเข้ารับการขึ้นทะเบียน
 เป็นผู้ประกอบการงานก่อสร้าง ซึ่งตามหลักเกณฑ์และวิธีการคัดเลือกเป็นผู้ประกอบการงานก่อสร้าง
 กำหนดให้ผู้ยื่นคำขอต้องเสนอหนังสือรับรองวงเงินสินเชื่อ/จะเข้ายื่นข้อเสนอกับหน่วยงานของรัฐ
 ซึ่งเงื่อนไขการยื่นข้อเสนอกรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสิทธิของกิจการหรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอ
 ที่จะเข้ายื่นข้อเสนอ ผู้ยื่นข้อเสนอต้องขอวงเงินสินเชื่อจากธนาคาร โดยต้องมีวงเงินสินเชื่อ ๑ ใน ๔ ของมูลค่า
 งบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอใน แต่ละครั้ง จึงมีความประสงค์ให้ธนาคาร.....
 (ชื่อธนาคาร).....รับรองวงเงินสินเชื่อเพื่อประกอบการพิจารณาด้วย นั้น

.....(ชื่อธนาคาร).....ขอรับรองว่า.....(ชื่อผู้ประกอบการ นิติบุคคล/
 บุคคลธรรมดา).....มีวงเงินทุนหมุนเวียนในวงเงินไม่ต่ำกว่า.....บาท
 (.....จำนวนเงินเป็นอักษร.....) และยินดีให้วงเงินสินเชื่อภายในวงเงิน บาท
 (.....จำนวนเงินเป็นอักษร.....)

ขอแสดงความนับถือ

.....
(ชื่อผู้ลงนาม).....
(ชื่อธนาคาร).....



แบบหนังสือรับรองวงเงินสินเชื่ออิเล็กทรอนิกส์

เลขที่.....

วันที่.....

เรื่อง รับรองวงเงินสินเชื่อ

ตามที่.....(ชื่อผู้ประกอบการ นิติบุคคล/บุคคลธรรมดา).....เลขประจำตัว
ผู้เสียภาษีอากร/เลขประจำตัวประชาชน เลขที่.....จะขอเข้ารับการขึ้นทะเบียน
เป็นผู้ประกอบการงานก่อสร้าง ซึ่งตามหลักเกณฑ์และวิธีการคัดเลือกเป็นผู้ประกอบการงานก่อสร้าง
กำหนดให้ผู้ยื่นคำขอต้องเสนอหนังสือรับรองวงเงินสินเชื่อ/จะเข้ายื่นขอเสนอกับหน่วยงานของรัฐ
ซึ่งเงื่อนไขการยื่นข้อเสนอกรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสิทธิของกิจการหรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอ
ที่จะเข้ายื่นข้อเสนอ ผู้ยื่นข้อเสนอต้องขอวงเงินสินเชื่อจากธนาคาร โดยต้องมีวงเงินสินเชื่อ 1 ใน 4 ของมูลค่า
งบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอใน แต่ละครั้ง จึงมีความประสงค์ให้ธนาคาร.....
(ชื่อธนาคาร).....รับรองวงเงินสินเชื่อ เพื่อประกอบการพิจารณาด้วย นั้น

.....(ชื่อธนาคาร).....ขอรับรองว่า.....(ชื่อผู้ประกอบการนิติบุคคล/
บุคคลธรรมดา).....มีวงเงินทุนหมุนเวียนในวงเงินไม่ต่ำกว่า.....
บาท(.....จำนวนเงินเป็นอักษร.....) และยินดีให้วงเงินสินเชื่อภายในวงเงิน
บาท (.....จำนวนเงินเป็นอักษร.....)

ขอแสดงความนับถือ

..... (ชื่อธนาคาร).....

** เอกสารฉบับนี้จัดพิมพ์โดยระบบอิเล็กทรอนิกส์ **

คุณสมบัติของผู้ยื่นข้อเสนอ

๑. มีความสามารถตามกฎหมาย
๒. ไม่เป็นบุคคลล้มละลาย
๓. ไม่อยู่ระหว่างเลิกกิจการ
๔. ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง
๕. ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทำงานและได้แจ้งเวียนชื่อให้เป็นผู้ทำงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทำงานเป็นหุ้นส่วน ผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย
๖. มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา
๗. เป็นบุคคลธรรมดาหรือนิติบุคคลผู้มีอาชีพรับจ้างงานที่จ้างครั้งนี้
๘. ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่สำนักงาน กสทช. ณ วันที่ได้รับหนังสือเชิญชวนให้เข้ายื่นข้อเสนอ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการยื่นข้อเสนอครั้งนี้
๙. ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นนั้น
๑๐. ที่ปรึกษาที่จะเข้าร่วมการเสนองานกับหน่วยงานของรัฐ ต้องเป็นที่ปรึกษาที่ได้ขึ้นทะเบียนไว้กับ ศูนย์ข้อมูลที่เป็นที่ปรึกษา กระทรวงการคลัง สาขา ICT: เทคโนโลยีสารสนเทศและการสื่อสาร (Information and Communication Technology Sector) มา ต ร ร ฐ า น ค ุ ณ ภ า พ (QS) : Quality Standard Sector ความเชี่ยวชาญ Rod๒๐: มาตรฐานระบบรักษาความปลอดภัยของข้อมูลองค์กร (ISO ๒๗๐๐๑)
๑๑. ที่ปรึกษาผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ ดังนี้
 - (๑) กรณีเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยซึ่งได้จดทะเบียนเกินกว่า ๑ ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก ๑ ปีสุดท้ายก่อนวันที่ยื่นข้อเสนอ
 - (๒) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอไม่น้อยกว่า ๒,๐๐๐,๐๐๐ บาท
 - (๓) กรณีที่ปรึกษาผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอ ผู้ยื่นข้อเสนอต้องมีวงเงินสินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์ และประกอบธุรกิจค้าประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยมียอดเงินรวมของวงเงินสินเชื่อไม่น้อยกว่า ๒,๓๙๗,๗๕๐ บาท คิดเป็น ๑ ใน ๔ ของมูลค่าโครงการหรือรายการที่ยื่นเสนอในแต่ละครั้ง ซึ่งสำนักงานใหญ่รับรองหรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอไม่เกิน ๙๐ วัน

(๔) กรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดาจะต้องแสดงหนังสือรับรองบัญชีเงินฝากไม่เกิน ๙๐ วัน ก่อนวันยื่นข้อเสนอ โดยต้องมีเงินฝากคงเหลือในบัญชีธนาคารเป็นมูลค่าไม่น้อยกว่ากว่า ๒,๓๙๗,๗๕๐ บาท คิดเป็น ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง และหากเป็นผู้ชนะการจัดซื้อจัดจ้างหรือเป็นผู้ได้รับการคัดเลือกจะต้องแสดงหนังสือรับรองบัญชีเงินฝากที่มีมูลค่าดังกล่าวอีกครั้งหนึ่งในวันลงนามในสัญญา

คุณสมบัติในข้อนี้ ยกเว้นกรณีที่ยื่นข้อเสนอเป็นหน่วยงานของรัฐ หรือนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการตามพระราชบัญญัติล้มละลาย (ฉบับที่ ๑๐) พ.ศ. ๒๕๖๑

๑๒. ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ “กิจการร่วมค้า” ต้องมีคุณสมบัติดังนี้

กิจการร่วมค้าที่ยื่นข้อเสนอ ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน เว้นแต่ในกรณีกิจการร่วมค้าที่มีข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก กิจการร่วมค่านั้นสามารถใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียว เป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงดังกล่าวจะต้องมีการกำหนดสัดส่วนหน้าที่ และความรับผิดชอบในปริมาณงาน สิ่งของ หรือมูลค่าตามสัญญา มากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

ทั้งนี้ กิจการร่วมค้า หมายถึง “กิจการที่มีข้อตกลงระหว่างผู้เข้าร่วมค้าเป็นลายลักษณ์อักษรว่าจะดำเนินการร่วมกันเป็นทางการค้าหรือหากำไรระหว่างบริษัทกับบริษัท บริษัทกับห้างหุ้นส่วนนิติบุคคล ห้างหุ้นส่วนนิติบุคคลกับห้างหุ้นส่วนนิติบุคคล หรือระหว่างบริษัทและ/หรือห้างหุ้นส่วนนิติบุคคลกับบุคคลธรรมดา คณะบุคคลที่มีใช้นิติบุคคล ห้างหุ้นส่วนสามัญ นิติบุคคลอื่น หรือนิติบุคคลที่ตั้งขึ้นตามกฎหมายของต่างประเทศ โดยข้อตกลงนั้นอาจกำหนดให้มีผู้เข้าร่วมค้าหลักก็ได้”

การกำหนดเกณฑ์การพิจารณาคัดเลือกข้อเสนอ

๑. ผลงานที่ผ่านมาของผู้ยื่นข้อเสนอ (น้ำหนักร้อยละ ๒๐)

ในหัวข้อนี้ จะพิจารณาการให้คะแนนในเชิงคุณภาพและเชิงปริมาณ ดังนี้

- (๑) ผลงานของที่ปรึกษา : โดยพิจารณาจากลักษณะของผลงานที่มีขอบเขตและวิธีการนำเสนอที่สอดคล้องหรือใกล้เคียงกับลักษณะงานตามขอบเขตของงานและวัตถุประสงค์มากที่สุด
- (๒) ประสิทธิภาพเฉพาะ : โดยพิจารณาจากผลงาน จำนวนผลงาน และมูลค่าของผลงานที่มีลักษณะสอดคล้องหรือใกล้เคียงกับงานตามขอบเขตของงาน โดยเทียบสัดส่วนกับจำนวนผลงานของผู้ยื่นข้อเสนอด้วยกัน

เกณฑ์การพิจารณาที่ให้คะแนน	ระดับคะแนน
๑. ผลงานที่ผ่านมาของผู้ยื่นข้อเสนอ (๑๐๐ คะแนน) (น้ำหนักร้อยละ ๒๐) มีผลงานที่ผ่านมาจำนวนอย่างน้อย ๑ โครงการ/ชิ้นงาน ที่มีขอบเขตงานใกล้เคียงหรือเท่ากับเนื้อหาของโครงการนี้ เช่น เคยเป็นที่ปรึกษาให้กับหน่วยงานภาครัฐหรือเอกชนจนได้รับการรับรองตามมาตรฐาน ISO/IEC ๒๗๐๐๑:๒๐๑๓ หรือ ISO/IEC ๒๗๗๐๑:๒๐๑๙ และมีประวัติเคยเป็นที่ปรึกษาให้กับหน่วยงานที่ปฏิบัติหน้าที่กำกับดูแล หรือเคยดำเนินการพัฒนา ปรับปรุง กระบวนการด้านการรักษาความมั่นคงปลอดภัย การประเมินช่องโหว่และทดสอบการเจาะระบบ (Vulnerability Assessment and Penetration Testing)	
๑.๑ ผลงานของที่ปรึกษา : ผลงานที่ผ่านมาตามข้อ ๑๐.๒.๑ (๑๐๐ คะแนน) (น้ำหนักร้อยละ ๑๐)	
มีการนำเสนอผลงานที่ผ่านมา โดยในขอบเขตงานที่นำเสนอมีการให้คำปรึกษา หน่วยงานจนผ่านการรับรองตามมาตรฐาน ISO/IEC ๒๗๐๐๑:๒๐๑๓ และ ISO/IEC ๒๗๗๐๑:๒๐๑๙ และ มาตรฐานอื่น ๆ เช่น ISO/IEC ๒๗๐๓๕ หรือ ISO/IEC ๓๘๕๐๐ เป็นต้น	๑๐๐ คะแนน
มีการนำเสนอผลงานที่ผ่านมา โดยในขอบเขตงานที่นำเสนอมีการให้คำปรึกษา หน่วยงานจนผ่านการรับรองตามมาตรฐาน ISO/IEC ๒๗๐๐๑:๒๐๑๓ และ ISO/IEC ๒๗๗๐๑:๒๐๑๙	๙๐ คะแนน
มีการนำเสนอผลงานที่ผ่านมา โดยในขอบเขตงานที่นำเสนอมีการให้คำปรึกษา หน่วยงานจนผ่านการรับรองตามมาตรฐาน ISO/IEC ๒๗๐๐๑:๒๐๑๓ เพียงมาตรฐานเดียว	๘๐ คะแนน
๑.๒ ประสิทธิภาพเฉพาะ : จำนวนผลงานที่ผ่านมา (๑๐๐ คะแนน) (น้ำหนักร้อยละ ๑๐)	
มีผลงานที่มีขอบเขตและวิธีการนำเสนอใกล้เคียงกับลักษณะงานตามขอบเขตของงาน ไม่น้อยจำนวน ๓ ผลงาน	๑๐๐ คะแนน
มีผลงานที่มีขอบเขตและวิธีการนำเสนอใกล้เคียงกับลักษณะงานตามขอบเขตของงาน ไม่น้อยจำนวน ๒ ผลงาน	๙๐ คะแนน
มีผลงานที่มีขอบเขตและวิธีการนำเสนอใกล้เคียงกับลักษณะงานตามขอบเขตของงาน ไม่น้อยจำนวน ๑ ผลงาน	๘๐ คะแนน

๒. วิธีการบริหารและวิธีปฏิบัติงาน (น้ำหนักร้อยละ ๔๐)

ในหัวข้อนี้ จะพิจารณาการให้คะแนนจากข้อเสนอที่สามารถนำขอบเขตของงานที่กำหนดไว้มาจัดทำเป็นแผนและวิธีการดำเนินงาน การตรวจสอบ ที่สอดคล้องกับระยะเวลาดำเนินงานของสำนักงาน กสทช. ได้ชัดเจนและเป็นรูปธรรมมากที่สุด

รายละเอียดการให้คะแนน		ระดับคะแนน
๒. วิธีการบริหารและวิธีการดำเนินงาน (๑๐๐ คะแนน) (น้ำหนักร้อยละ ๔๐)		
๒.๑ กรอบแนวคิดและแผนการดำเนินงานตาม ข้อ ๔ (น้ำหนักร้อยละ ๕)		
เกณฑ์การพิจารณาที่ให้คะแนน	คะแนน	วิธีการประเมิน
มีกรอบแนวคิดและแผนการดำเนินงานตามวัตถุประสงค์และขอบเขตของงาน มีรายละเอียดอย่างชัดเจน มีกรอบระยะเวลาการดำเนินการและแจกแจงบุคคลากรที่รับผิดชอบตามแผนการดำเนินงาน และมีการนำเอากรอบมาตรฐานสากลหรือกรอบแนวคิดที่เป็นประโยชน์เข้ามาประยุกต์ใช้กับการดำเนินงานและสามารถตอบวัตถุประสงค์และขอบเขตของงาน และมีแผนงานที่สามารถนำไปปฏิบัติได้จริง	๑๐๐	ผู้ประเมินจะพิจารณาจากเอกสารที่ผู้ยื่นข้อเสนอยื่นมา โดยจัดทำเป็นรูปแบบเอกสาร ขนาดกระดาษ A๔ และผู้ประเมินจะให้ คะแนนตามรายการที่ผู้ยื่นข้อเสนอนำเอกสารยื่นมา
มีกรอบแนวคิดและแผนการดำเนินงานตามวัตถุประสงค์และขอบเขตของงาน มีรายละเอียดอย่างชัดเจน มีกรอบระยะเวลาการดำเนินการแต่ไม่แจกแจงบุคคลากรที่รับผิดชอบตามแผนการดำเนินงาน	๘๐	
๒.๒ ความเข้าใจในแนวทางการประเมินความเสี่ยงทั้งด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ การบริหารจัดการด้านข้อมูลส่วนบุคคล และการบริหารจัดการด้านการรับมือกับเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (น้ำหนักร้อยละ ๑๕)		
เกณฑ์การพิจารณาที่ให้คะแนน	คะแนน	วิธีการประเมิน
มีการนำเสนอแนวทางการประเมินความเสี่ยงและมีการนำเสนอเครื่องมืออำนวยความสะดวกหรือวิธีการบริหารจัดการเอกสารที่สอดคล้องกับมาตรฐาน ISO/IEC ๒๗๐๐๑, ISO/IEC ๒๗๗๐๑ และ ISO/IEC ๒๗๐๓๕ และนำมาประยุกต์ใช้กับระบบจัดการเอกสารที่สำนักเทคโนโลยีสารสนเทศมีการใช้งานในปัจจุบันได้	๑๐๐	ผู้ประเมินจะพิจารณาจากเอกสารที่ผู้ยื่นข้อเสนอยื่นมา โดยจัดทำเป็นรูปแบบเอกสาร ขนาดกระดาษ A๔ และผู้ประเมินจะให้ คะแนนตามรายการที่ผู้ยื่นข้อเสนอนำเอกสารยื่นมา
มีการนำเสนอแนวทางการประเมินความเสี่ยงที่สอดคล้องกับมาตรฐาน ISO/IEC ๒๗๐๐๑, ISO/IEC ๒๗๗๐๑ และ ISO/IEC ๒๗๐๓๕ และนำไปใช้กับแนวทางที่สำนักเทคโนโลยีสารสนเทศมีการใช้งานในปัจจุบันได้	๘๐	

๒.๓ ทักษะในการประเมินหาความเสี่ยงที่เกิดจากช่องโหว่ที่ค้นพบของเครือข่ายและระบบเทคโนโลยีสารสนเทศ (น้ำหนักร้อยละ ๑๕)		
เกณฑ์การพิจารณาที่ให้คะแนน	คะแนน	วิธีการประเมิน
มีทักษะในการประเมินหาความเสี่ยงที่เกิดจากช่องโหว่ที่ค้นพบของเครือข่ายและระบบเทคโนโลยีสารสนเทศ ทั้งช่องโหว่จากเครือข่ายภายนอกและภายใน ทักษะการเจาะระบบตามมาตรฐาน Open Web Application Security Project (OWASP) ทักษะการโจมตีระบบสารสนเทศ ทักษะการตรวจสอบค่าความเหมาะสมของเครื่องแม่ข่าย และทักษะการตรวจสอบการรั่วไหลของข้อมูลสำนักงาน กสทช. ใน Dark Web	๑๐๐	ผู้ประเมินจะพิจารณาจากเอกสารที่ผู้ยื่นข้อเสนออื่นมา โดยจัดทำเป็นรูปแบบเอกสาร ขนาดกระดาษ A๔ และผู้ประเมินจะให้ คะแนนตามรายการที่ผู้ยื่นข้อเสนอนำเอกสารอื่นมา
มีทักษะในการประเมินหาความเสี่ยงที่เกิดจากช่องโหว่ที่ค้นพบของเครือข่ายและระบบเทคโนโลยีสารสนเทศ ทั้งช่องโหว่จากเครือข่ายภายนอกและภายใน	๘๐	
๒.๔ ข้อเสนออื่น ๆ ที่เป็นประโยชน์ต่อการดำเนินงาน และสอดคล้องกับขอบเขตของงาน (น้ำหนักร้อยละ ๕)		
เกณฑ์การพิจารณาที่ให้คะแนน	คะแนน	วิธีการประเมิน
มีข้อเสนออื่น ๆ ที่เป็นประโยชน์ต่อการดำเนินงาน และสอดคล้องกับขอบเขตของงาน	๑๐๐	ผู้ประเมินจะพิจารณาจากเอกสารที่ผู้ยื่นข้อเสนออื่นมา โดยจัดทำเป็นรูปแบบเอกสาร ขนาดกระดาษ A๔ และผู้ประเมินจะให้ คะแนนตามรายการที่ผู้ยื่นข้อเสนอนำเอกสารอื่นมา
ไม่มีข้อเสนออื่น ๆ ที่เป็นประโยชน์ต่อการดำเนินงาน และสอดคล้องกับขอบเขตของงาน	๐	

รายละเอียดการให้คะแนน				ระดับคะแนน			
๓. จำนวนและคุณลักษณะเฉพาะของบุคลากรที่ร่วมงาน (น้ำหนักร้อยละ ๔๐)							
โดยที่ปรึกษาจะต้องแสดงรายละเอียดคุณวุฒิการศึกษา ความเชี่ยวชาญหรือประสบการณ์ของบุคลากรหลัก และประกาศนียบัตรตามขอบเขตงานข้อ ๕ (ถ้ามี) พร้อมเอกสารหลักฐานอ้างอิง โดยมีคะแนนรวมทั้งสิ้น ๑๐๐ คะแนน ซึ่งผู้ประเมินจะให้คะแนนแก่บุคลากรของผู้ยื่นข้อเสนอทั้ง ๑๓ คน ดังนี้							
๑. หัวหน้าโครงการ	คะแนนเต็ม ๑๐ คะแนน						
	ด้านประสบการณ์ (๔ คะแนน)			ด้านวุฒิการศึกษา (๓ คะแนน)		ด้านประกาศนียบัตร (๓ คะแนน)	
	มากกว่า ๒๐ ปี	มากกว่า ๑๕ ปี	๑๕ ปี	ปริญญาเอก	มากกว่า ๒ ปี	๒ ปี	๑ ปี
	๔ คะแนน	๓ คะแนน	๒ คะแนน	๓ คะแนน	๓ คะแนน	๒ คะแนน	๑ คะแนน
	คะแนนเต็ม ๗ คะแนน						
๒. ที่ปรึกษาโครงการด้าน ISO	ด้านประสบการณ์ (๓ คะแนน)			ด้านวุฒิการศึกษา (๒ คะแนน)		ด้านประกาศนียบัตร (๒ คะแนน)	
	มากกว่า ๒๐ ปี	มากกว่า ๑๕ ปี	๑๕ ปี	ปริญญาเอก	มากกว่า ๒ ปี	๒ ปี	๑ ปี
	๓ คะแนน	๒ คะแนน	๑ คะแนน	๒ คะแนน	๒ คะแนน	๑.๕ คะแนน	๑ คะแนน
	คะแนนเต็ม ๗ คะแนน						
	๓. ที่ปรึกษาโครงการด้านการจากระบบ	ด้านประสบการณ์ (๓ คะแนน)			ด้านวุฒิการศึกษา (๒ คะแนน)		ด้านประกาศนียบัตร (๒ คะแนน)
มากกว่า ๒๐ ปี		มากกว่า ๑๕ ปี	๑๕ ปี	ปริญญาเอก	มากกว่า ๒ ปี	๒ ปี	๑ ปี
๓ คะแนน		๒ คะแนน	๑ คะแนน	๒ คะแนน	๒ คะแนน	๑.๕ คะแนน	๑ คะแนน
คะแนนเต็ม ๗ คะแนน							
ที่ปรึกษาจะต้องมีประสบการณ์ทำงานและวุฒิการศึกษาซึ่งเป็นสาขาวิชาเดียวกันกับที่กำหนดตามข้อ ๕ (๕.๓)		ด้านประสบการณ์ (๓ คะแนน)			ด้านวุฒิการศึกษา (๒ คะแนน)		ด้านประกาศนียบัตร (๒ คะแนน)
	มากกว่า ๒๐ ปี	มากกว่า ๑๕ ปี	๑๕ ปี	ปริญญาโท	มากกว่า ๒ ปี	๒ ปี	๑ ปี
	๓ คะแนน	๒ คะแนน	๑ คะแนน	๑ คะแนน	๒ คะแนน	๑.๕ คะแนน	๑ คะแนน
	คะแนนเต็ม ๗ คะแนน						
	คะแนนเต็ม ๗ คะแนน						

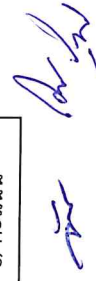



รายละเอียดการใช้คะแนน	ระดับคะแนน						
	คะแนนเต็ม ๑๐ คะแนน						
๔. หัวหน้าทีมที่ปรึกษา ISO หัวหน้าทีมที่ปรึกษาจะต้องมีประสบการณ์ ทำงานและวุฒิการศึกษาตรงกับที่กำหนด ตามข้อ ๕ (๕.๔)	ด้านประสบการณ์ (๔ คะแนน)		ด้านวุฒิการศึกษา (๓ คะแนน)		ด้านประกาศนียบัตร (๓ คะแนน)		
	มากกว่า ๒๐ ปี	มากกว่า ๑๕ ปี	๑๕ ปี	ปริญญาโท	ปริญญาตรี	มากกว่า ๓ ปี	๓ ปี
	๔ คะแนน	๓ คะแนน	๒ คะแนน	๓ คะแนน	๒ คะแนน	๓ คะแนน	๑ คะแนน
๕. ทีมที่ปรึกษา ISO ทีมที่ปรึกษาจะต้องมีประสบการณ์ทำงานและ วุฒิการศึกษาตรงกับที่กำหนดตามข้อ ๕ (๕.๕)	คะแนนเต็ม ๗ คะแนน						
	ด้านประสบการณ์ (๓ คะแนน)		ด้านวุฒิการศึกษา (๒ คะแนน)		ด้านประกาศนียบัตร (๒ คะแนน)		
	มากกว่า ๑๐ ปี	มากกว่า ๕ ปี	๕ ปี	ปริญญาโท	ปริญญาตรี	มากกว่า ๒ ปี	๒ ปี
	๓ คะแนน	๒ คะแนน	๑ คะแนน	๒ คะแนน	๑ คะแนน	๒ คะแนน	๑ คะแนน
๖. หัวหน้าทีมที่ปรึกษาด้านเทคนิค หัวหน้าทีมที่ปรึกษาด้านเทคนิคจะต้องมี ประสบการณ์ทำงานและวุฒิการศึกษาตรงกับ ที่กำหนดตามข้อ ๕ (๕.๖)	คะแนนเต็ม ๑๐ คะแนน						
	ด้านประสบการณ์ (๔ คะแนน)		ด้านวุฒิการศึกษา (๓ คะแนน)		ด้านประกาศนียบัตร (๓ คะแนน)		
	มากกว่า ๑๐ ปี	มากกว่า ๕ ปี	๕ ปี	ปริญญาโท	ปริญญาตรี	มากกว่า ๒ ปี	๒ ปี
	๔ คะแนน	๓ คะแนน	๒ คะแนน	๒ คะแนน	๑ คะแนน	๒ คะแนน	๑ คะแนน
๗. ทีมที่ปรึกษาด้านเทคนิค (คนที่ ๑) ทีมที่ปรึกษาด้านเทคนิคจะต้องมีประสบการณ์ ทำงานและวุฒิการศึกษาตรงกับที่กำหนดตาม ข้อ ๕ (๕.๗)	คะแนนเต็ม ๗ คะแนน						
	ด้านประสบการณ์ (๓ คะแนน)		ด้านวุฒิการศึกษา (๒ คะแนน)		ด้านประกาศนียบัตร (๒ คะแนน)		
	มากกว่า ๑๐ ปี	มากกว่า ๕ ปี	๕ ปี	ปริญญาเอก	ปริญญาโท	มากกว่า ๓ ปี	๓ ปี
	๔ คะแนน	๓ คะแนน	๒ คะแนน	๓ คะแนน	๒ คะแนน	๓ คะแนน	๑ คะแนน





รายละเอียดการให้คะแนน	ระดับคะแนน						
๘. ทีมที่ปรึกษาด้านเทคนิค (คนที่ ๒) ทีมที่ปรึกษาด้านเทคนิคจะต้องมีประสบการณ์ทำงานและวุฒิการศึกษาตรงกับที่กำหนดตามข้อ ๕ (๕.๓)	คะแนนเต็ม ๗ คะแนน						
	ด้านประสบการณ์ (๓ คะแนน)		ด้านวุฒิการศึกษา (๒ คะแนน)		ด้านประกาศนียบัตร (๒ คะแนน)		
	มากกว่า ๑๐ ปี	มากกว่า ๕ ปี	๕ ปี	ปริญญาโท	ปริญญาตรี	มากกว่า ๓ ปี	๓ ปี
	๓ คะแนน	๒ คะแนน	๑ คะแนน	๒ คะแนน	๑ คะแนน	๒ คะแนน	๑.๕ คะแนน
	คะแนนเต็ม ๗ คะแนน						
๙. ทีมที่ปรึกษาด้านเทคนิค (นักเจาะระบบคนที่ ๑) ทีมที่ปรึกษาจะต้องมีประสบการณ์ทำงานและวุฒิการศึกษาซึ่งเป็นสาขาวิชาเดียวกันกับที่กำหนดตามข้อ ๕ (๕.๔)	ด้านประสบการณ์ (๓ คะแนน)		ด้านวุฒิการศึกษา (๒ คะแนน)		ด้านประกาศนียบัตร (๒ คะแนน)		
	มากกว่า ๑๐ ปี	มากกว่า ๕ ปี	๕ ปี	ปริญญาโท	ปริญญาตรี	มากกว่า ๒ ปี	๒ ปี
	๓ คะแนน	๒ คะแนน	๑ คะแนน	๒ คะแนน	๑ คะแนน	๒ คะแนน	๑.๕ คะแนน
	คะแนนเต็ม ๗ คะแนน						
	คะแนนเต็ม ๗ คะแนน						
๑๐. ทีมที่ปรึกษาด้านเทคนิค (นักเจาะระบบคนที่ ๒) ทีมที่ปรึกษาจะต้องมีประสบการณ์ทำงานและวุฒิการศึกษาซึ่งเป็นสาขาวิชาเดียวกันกับที่กำหนดตามข้อ ๕ (๕.๔)	ด้านประสบการณ์ (๓ คะแนน)		ด้านวุฒิการศึกษา (๒ คะแนน)		ด้านประกาศนียบัตร (๒ คะแนน)		
	มากกว่า ๑๐ ปี	มากกว่า ๕ ปี	๕ ปี	ปริญญาโท	ปริญญาตรี	มากกว่า ๒ ปี	๒ ปี
	๓ คะแนน	๒ คะแนน	๑ คะแนน	๒ คะแนน	๑ คะแนน	๒ คะแนน	๑.๕ คะแนน
	คะแนนเต็ม ๗ คะแนน						
	คะแนนเต็ม ๗ คะแนน						
๑๑. ทีมที่ปรึกษาด้านเทคนิค (นักเจาะระบบคนที่ ๓) ทีมที่ปรึกษาจะต้องมีประสบการณ์ทำงานและวุฒิการศึกษาซึ่งเป็นสาขาวิชาเดียวกันกับที่กำหนดตามข้อ ๕ (๕.๔)	ด้านประสบการณ์ (๓ คะแนน)		ด้านวุฒิการศึกษา (๒ คะแนน)		ด้านประกาศนียบัตร (๒ คะแนน)		
	มากกว่า ๑๐ ปี	มากกว่า ๕ ปี	๕ ปี	ปริญญาโท	ปริญญาตรี	มากกว่า ๒ ปี	๒ ปี
	๓ คะแนน	๒ คะแนน	๑ คะแนน	๒ คะแนน	๑ คะแนน	๒ คะแนน	๑.๕ คะแนน
	คะแนนเต็ม ๗ คะแนน						
	คะแนนเต็ม ๗ คะแนน						
	ด้านประสบการณ์ (๓ คะแนน)		ด้านวุฒิการศึกษา (๒ คะแนน)		ด้านประกาศนียบัตร (๒ คะแนน)		
	มากกว่า ๑๐ ปี	มากกว่า ๕ ปี	๕ ปี	ปริญญาโท	ปริญญาตรี	มากกว่า ๒ ปี	๒ ปี
	๓ คะแนน	๒ คะแนน	๑ คะแนน	๒ คะแนน	๑ คะแนน	๒ คะแนน	๑.๕ คะแนน
	คะแนนเต็ม ๗ คะแนน						
	คะแนนเต็ม ๗ คะแนน						



รายละเอียดการให้คะแนน	ระดับคะแนน				
๑๒. ทีมที่ปรึกษาด้านเทคนิค (ผู้ช่วยนักเจาะระบบคนที่ ๑) ทีมที่ปรึกษาจะต้องมีประสบการณ์ทำงานและวุฒิการศึกษาซึ่งเป็นสาขาวิชาเดียวกันที่กำหนดตามข้อ ๕ (๕.๙)	คะแนนเต็ม ๗ คะแนน				
	ด้านประสบการณ์ (๔ คะแนน)		ด้านวุฒิการศึกษา (๓ คะแนน)		
	มากกว่า ๑๐ ปี	มากกว่า ๕ ปี	๕ ปี	ปริญญาโท	ปริญญาตรี
	๔ คะแนน	๓ คะแนน	๒ คะแนน	๓ คะแนน	๒ คะแนน
๑๓. ทีมที่ปรึกษาด้านเทคนิค (ผู้ช่วยนักเจาะระบบคนที่ ๒) ทีมที่ปรึกษาจะต้องมีประสบการณ์ทำงานและวุฒิการศึกษาซึ่งเป็นสาขาวิชาเดียวกันที่กำหนดตามข้อ ๕ (๕.๙)	คะแนนเต็ม ๗ คะแนน				
	ด้านประสบการณ์ (๔ คะแนน)		ด้านวุฒิการศึกษา (๓ คะแนน)		
	มากกว่า ๑๐ ปี	มากกว่า ๕ ปี	๕ ปี	ปริญญาโท	ปริญญาตรี
	๔ คะแนน	๓ คะแนน	๒ คะแนน	๓ คะแนน	๒ คะแนน
การให้คะแนนในหัวข้อนี้ จะขึ้นอยู่กับประสบการณ์ คุณวุฒิ และประวัติของบุคลากรหลักและบุคลากรสนับสนุนที่เสนอ เป็นไปตามที่กำหนดตามข้อ ๕ นอกจากนี้ จะพิจารณารายละเอียดและความครอบคลุมครบถ้วนดังกล่าวแล้ว จะพิจารณาเปรียบเทียบระหว่างข้อเสนอของผู้ยื่นข้อเสนอแต่ละราย ข้อเสนอที่ดีที่สุดจะได้คะแนนเต็มหรือได้มากที่สุด ข้อเสนอที่ดีรองลงไปจะได้คะแนนลดหลั่นตามความเหมาะสมในช่วงคะแนนของหัวข้อนั้น					



