ขอบเขตของงาน

โครงการยกระดับศักยภาพการดำเนินงานศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคการบิน (TA-CERT)

1. ความเป็นมา

สำนักงานการบินพลเรือนแห่งประเทศไทย (กพท.) ในฐานะหน่วยงานควบคุมหรือกำกับดูแล (Regulator) ด้านการขนส่งทางอากาศ ภายใต้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และประกาศที่เกี่ยวข้อง ได้จัดให้มีศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคการบิน (Thailand Aviation - Computer Emergency Response Team : TA-CERT) เพื่อทำหน้าที่และดำเนินภารกิจด้านการประสานงาน เฝ้าระวัง รับมือ และแก้ไขภัยคุกคามทางไซเบอร์ให้แก่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านการขนส่งทางอากาศ (หน่วยงาน CII)

การดำเนินภารกิจด้านการเฝ้าระวังภัยคุกคามทางไซเบอร์ของ TA-CERT ครอบคลุมการเฝ้าระวังความเสี่ยงและติดตามแนวโน้มของการเกิดภัยคุกคามทางไซเบอร์ การแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์หรือช่องโหว่ที่อาจถูกใช้เป็นช่องทางในการก่อภัยคุกคาม ตลอดจนการวิเคราะห์และตรวจสอบข่าวกรองเกี่ยวกับภัยคุกคามทางไซเบอร์ และการเผยแพร่ข้อมูลที่จำเป็นเพื่อสนับสนุนให้หน่วยงานที่อยู่ภายใต้การดูแลสามารถดำเนินมาตรการป้องกันหรือจัดการกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ได้อย่างเหมาะสม

เพื่อให้การดำเนินงานของ TA-CERT สามารถสนับสนุนภารกิจดังกล่าวได้อย่างต่อเนื่อง และเพิ่มขีดความสามารถในการรวบรวม ติดตาม วิเคราะห์ ตรวจสอบ และบริหารจัดการข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์ รวมถึงการแจ้งเตือน การเผยแพร่ และการแลกเปลี่ยนข้อมูลที่เกี่ยวข้องกับภาคการบิน ตลอดจนการพัฒนาศักยภาพบุคลากรและกระบวนการดำเนินงานที่เกี่ยวข้อง กพท. จึงมีความจำเป็นต้องดำเนิน โครงการยกระดับศักยภาพการดำเนินงานศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคการบิน (TA-CERT) เพื่อยกระดับการดำเนินงานของ TA-CERT ให้สามารถสนับสนุน กพท. และหน่วยงานสมาชิก TA-CERT ในการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพและต่อเนื่อง

2. วัตถุประสงค์

2.1 เพื่อยกระดับศักยภาพการดำเนินงานของ TA-CERT ในการเฝ้าระวัง ติดตาม วิเคราะห์ และแจ้งเตือนภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับภาคการบิน

2.2 เพื่อเพิ่มประสิทธิภาพในการรวบรวม บริหารจัดการ และแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ระหว่าง กพท. หน่วยงานสมาชิก TA-CERT และหน่วยงานที่เกี่ยวข้อง

2.3 เพื่อสนับสนุนการวิเคราะห์และเผยแพร่ข้อมูลข่าวกรองภัยคุกคาม ข่าวสาร การแจ้งเตือน และคำแนะนำด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นประโยชน์ต่อภาคการบิน

2.4 เพื่อพัฒนาศักยภาพบุคลากรของ กพท. และหน่วยงานสมาชิก TA-CERT ด้านความมั่นคงปลอดภัยไซเบอร์

3. คุณสมบัติของผู้ยื่นข้อเสนอ

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

(นายวีระ ระบายศรี)	(นางสาวอรรวรรณ ใจเอื้อ)	(นาวาอากาศเอก กรเอก ชิษณุชาบุญวิภัค)	(นายรักพิรุนห์ รุจิรวงษ์สกุล)	(นายจักรพรรณ มีนคร)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 เป็นบุคคลธรรมดาหรือนิติบุคคลผู้มีอาชีพรับจ้างงานที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่สำนักงาน ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกันซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

3.10 ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ “กิจการร่วมค้า” ต้องมีคุณสมบัติดังนี้

3.10.1 การกำหนดสัดส่วนในการเข้าร่วมค้าของคู่สัญญา

กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงฯ จะต้องมีการกำหนดสัดส่วนหน้าที่ และความรับผิดชอบในปริมาณงาน สิ่งของ หรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

3.10.2 งานซื้อหรือจ้าง และงานก่อสร้าง

กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก กิจการร่วมค้านั้นต้องใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

สำหรับข้อตกลงฯ ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมหลัก ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในหนังสือเชิญชวน

3.10.3 การยื่นข้อเสนอของกิจการร่วมค้า

(1) กรณีที่ข้อตกลงฯ กำหนดให้มีการมอบหมายผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า การยื่นข้อเสนอดังกล่าวไม่ต้องมีหนังสือมอบอำนาจ

สำหรับข้อตกลงฯ ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้ยื่นข้อเสนอ ผู้เข้าร่วมค้าทุกรายจะต้องลงลายมือชื่อในหนังสือมอบอำนาจให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า

(2) การยื่นข้อเสนอด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding) ให้ผู้เข้าร่วมค้าที่ได้รับมอบหมายหรือมอบอำนาจตามข้อ 3.10.3 (1) ดำเนินการซื้อและดาวน์โหลดเอกสารประกวดราคาอิเล็กทรอนิกส์ กรณีที่มีการจำหน่ายเอกสารจึงจะมีสิทธิในการเข้ายื่นข้อเสนอในนามกิจการร่วมค้าได้

3.11 ผู้ยื่นข้อเสนอต้องลงทะเบียนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement : e - GP) ของกรมบัญชีกลาง

3.12 ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ เป็นไปตามหนังสือคณะกรรมการวินิจฉัยปัญหาการจัดซื้อจัดจ้างและการบริการพัสดุภาครัฐ ด่วนที่สุด ที่ กค (กวจ) 0405.2/ว 124 ลงวันที่ 1 มีนาคม 2566 ดังนี้

(นายวีระ ระบายศรี)	(นางสาวอรรวรรณ ใจเอื้อ)	(นาวาอากาศเอก กรเอก ชิษณุชาบุญวิภัค)	(นายรักพิรุนห์ รุจิรวงษ์สกุล)	(นายจักรพรรณ มีนคร)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

3.12.1 กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยหรือต่างประเทศซึ่งได้จดทะเบียนเกินกว่า 1 ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก 1 ปีสุดท้ายก่อนวันยื่นข้อเสนอ งบแสดงฐานะการเงิน 1 ปีสุดท้ายก่อนวันยื่นข้อเสนอ หมายถึง งบแสดงฐานะการเงินย้อนไปก่อนวันที่หน่วยงานของรัฐกำหนดให้เป็นวันยื่นข้อเสนอ 1 ปีปฏิทิน เว้นแต่กรณีนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยหากวันยื่นข้อเสนอเป็นช่วงระยะเวลาที่กรมพัฒนาธุรกิจการค้ากำหนดให้นิติบุคคลยื่นงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ซึ่งจะอยู่ในช่วงเดือนมกราคม - เดือนพฤษภาคม ของทุกปี โดยนิติบุคคลที่เป็นผู้ยื่นข้อเสนอนั้นยังอยู่ในช่วงของการยื่นงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า คือ ช่วงเดือนมกราคม - เดือนพฤษภาคม ของทุกปี กรณีนี้ให้สามารถยื่นงบแสดงฐานะการเงินย้อนไปอีก 1 ปี ได้

3.12.2 กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า หรือกรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงิน ให้พิจารณาการกำหนดมูลค่าของทุนจดทะเบียน โดยผู้ยื่นข้อเสนอจะต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอ ต้องมีทุนจดทะเบียนไม่ต่ำกว่า 8 ล้านบาท

3.12.3 สำหรับการจัดซื้อจัดจ้างครั้งหนึ่งที่มีวงเงินเกิน 500,000 บาทขึ้นไป กรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดา ให้พิจารณาจากหนังสือรับรองบัญชีเงินฝากไม่เกิน 90 วัน ก่อนวันยื่นข้อเสนอ โดยต้องมีเงินฝากคงเหลือในบัญชีธนาคารเป็นมูลค่า 1 ใน 4 ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง และหากเป็นผู้ชนะการจัดซื้อจัดจ้าง หรือเป็นผู้ได้รับการคัดเลือกจะต้องแสดงหนังสือรับรองบัญชีเงินฝากที่มีมูลค่าดังกล่าวอีกครั้งหนึ่งในวันลงนามในสัญญา

3.12.4 กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการ หรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ สามารถดำเนินการได้ดังนี้

(1) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย หรือบุคคลธรรมดาที่ถือสัญชาติไทย ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ 1 ใน 4 ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง จะเป็นสินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรองหรือ ที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอ ไม่เกิน 90 วัน

(2) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศ หรือบุคคลธรรมดาที่มิได้ถือสัญชาติไทย ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ 1 ใน 4 ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง จะเป็นสินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุน เพื่อการพาณิชย์และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ หรือเป็นสินเชื่อที่ธนาคารต่างประเทศ หรือบริษัทเงินทุนหลักทรัพย์ ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์ และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารกลางต่างประเทศนั้น ตามรายชื่อบริษัทที่ธนาคารกลางต่างประเทศนั้นแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวม

(นายวีระ ระบายศรี)	(นางสาวอรรวรรณ ใจเอื้อ)	(นาวาอากาศเอก กรเอก ชิษณุชาบุญวิภัค)	(นายรักพิรุนห์ รุจิรวงษ์สกุล)	(นายจักรพรรณ มีนคร)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

ของวงเงินสินเชื่อที่สำนักงานใหญ่รับรอง หรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอไม่เกิน 90 วัน)

3.12.5 กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศ หรือบุคคลธรรมดาที่มิได้ถือสัญชาติไทยตามข้อ 3.12.2, 3.12.3 และ 3.12.4 (2) มูลค่าจะต้องเป็นไปตามอัตราแลกเปลี่ยนเงินตราตามประกาศที่ธนาคารแห่งประเทศไทยกำหนด ในช่วงระหว่างวันที่เผยแพร่ประกาศและเอกสารประกวดราคาในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (e - GP) จนถึงวันเสนอราคา

ทั้งนี้ ผู้ยื่นข้อเสนอจะต้องยื่นเอกสารที่แสดงให้เห็นถึงข้อมูลเกี่ยวกับมูลค่าสุทธิของกิจการแล้วแต่กรณี ประกอบกับเอกสารดังกล่าวจะต้องผ่านการรับรองตามระเบียบกระทรวงการต่างประเทศว่าด้วยการรับรองเอกสาร พ.ศ. 2539 และที่แก้ไขเพิ่มเติมกำหนด โดยจะต้องยื่นเอกสารดังกล่าวในวันยื่นข้อเสนอ หากผู้ยื่นข้อเสนอมิได้มีการยื่นเอกสารดังกล่าวมาพร้อมกับการยื่นข้อเสนอให้ถือว่าผู้ยื่นข้อเสนอรายนั้นยื่นเอกสารไม่ครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารประกวดราคา

3.13 กรณีตามข้อ 3.12.1 – 3.12.5 ไม่ใช้ข้อบังคับกับกรณีดังต่อไปนี้

3.13.1 กรณีที่ผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐภายในประเทศ

3.13.2 นิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการ ตามพระราชบัญญัติล้มละลาย พ.ศ. 2483 และที่แก้ไขเพิ่มเติม

3.13.3 งานจ้างก่อสร้างที่กรมบัญชีกลางได้ขึ้นทะเบียนผู้ประกอบการงานก่อสร้างแล้ว และงานจ้างก่อสร้างที่หน่วยงานของรัฐที่ได้มีการจัดทำบัญชีผู้ประกอบการงานก่อสร้าง ที่มีคุณสมบัติเบื้องต้นไว้แล้วก่อนวันที่พระราชบัญญัติการจัดซื้อจัดจ้างฯ มีผลใช้บังคับ

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

3.13.5 การซื้ออสังหาริมทรัพย์และการเช่าอสังหาริมทรัพย์

3.13.6 กรณีงานจ้างบริการหรืองานจ้างเหมาบริการกับบุคคลธรรมดา เช่น จ้างพนักงานขับรถ ครูชาวต่างชาติ พนักงานเก็บขยะ พนักงานบันทึกข้อมูล เป็นต้น

3.14 ผู้ยื่นข้อเสนอจะต้องมีผลงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์หรือการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (Cybersecurity or IT Security) หรือด้านการแลกเปลี่ยนข่าวกรองภัยคุกคาม (Threat Intelligence) หรือการจัดตั้ง/ให้บริการศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยสารสนเทศ (SOC / CERT / CSIRT) หรือการพัฒนาระบบแลกเปลี่ยนข้อมูลสารสนเทศ (Web Portal / Threat Intelligence Platform) ระยะเวลาของสัญญาอย่างน้อย 1 ปี ที่มีมูลค่าสัญญาเดียวไม่น้อยกว่า 10,000,000.00 บาท โดยเป็นผลงานที่แล้วเสร็จไม่เกินกว่า 5 ปี นับถึงวันที่ยื่นเสนอราคา และเป็นผลงานที่เป็นคู่สัญญาโดยตรงกับหน่วยงานของรัฐ หรือหน่วยงานเอกชนที่สำนักงานเชื่อถือ

3.14.1 หากเป็นผลงานกับหน่วยงานของรัฐ จะต้องแนบหนังสือรับรองผลงาน และสำเนาสัญญาจ้างพร้อมรับรองสำเนาถูกต้องมาพร้อมกันในวันยื่นข้อเสนอ

3.14.2 หากเป็นผลงานกับหน่วยงานของเอกชน จะต้องแนบหนังสือรับรองผลงาน สำเนาสัญญาจ้างและใบกำกับภาษี หรือเอกสารหลักฐานการชำระเงิน พร้อมรับรองสำเนาถูกต้องมาพร้อมกันในวันยื่นข้อเสนอ

3.15 ผู้ยื่นข้อเสนอจะต้องได้รับการแต่งตั้งเป็นตัวแทนจำหน่ายจากผู้ผลิต ระบบหรือโมดูลสำหรับบริหารจัดการแหล่งข้อมูลภัยคุกคาม (Threat Intelligence) หรือตัวแทนจำหน่ายในประเทศไทย โดยให้ยื่นพร้อมการเสนอราคา

(นายวีระ ระบายศรี) ประธานกรรมการ (นางสาวอรรวรรณ ใจเอื้อ) กรรมการ (นาวาอากาศเอก กรเอก ชิษณุชาบุญวิภัค) กรรมการ (นายรักพิรุนห์ รุจิรวงษ์สกุล) กรรมการ (นายจักรพรรณ มีนคร) กรรมการ

4. ขอบเขตของงาน

ผู้ยื่นข้อเสนอต้องดำเนินงานเพื่อยกระดับศักยภาพการดำเนินงานของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคการบิน (TA-CERT) ให้สามารถสนับสนุนการดำเนินภารกิจของ กพท. และการให้บริการแก่หน่วยงานสมาชิก TA-CERT ได้อย่างต่อเนื่องตลอดระยะเวลาสัญญา โดยมีขอบเขตการดำเนินงาน ดังต่อไปนี้

4.1 ระบบบริหารจัดการและแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์

4.1.1 ผู้ยื่นข้อเสนอต้องจัดให้มีระบบสำหรับบริหารจัดการและแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์เพื่อสนับสนุนการรับ รวบรวม จัดเก็บ บริหารจัดการ และแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ รวมถึง Indicators of Compromise (IOC) โดยมีคุณสมบัติและความสามารถไม่น้อยกว่าที่กำหนดใน **ภาคผนวก 1**

4.1.2 ผู้ยื่นข้อเสนอต้องจัดให้มีสิทธิการใช้งาน การติดตั้ง การกำหนดค่า การดูแลระบบ การแก้ไขข้อขัดข้อง และการสนับสนุนการใช้งานระบบตามข้อ 4.1.1 เพื่อให้ระบบสามารถให้บริการได้ตามข้อกำหนดตลอดระยะเวลาสัญญา

4.1.3 ผู้ยื่นข้อเสนอต้องดำเนินการเชื่อมต่อระบบตามข้อ 4.1.1 กับ MISP Node ของ กพท. ที่มีอยู่เดิม เพื่อให้สามารถรับและแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ระหว่างระบบได้ โดยการดำเนินการดังกล่าวต้องไม่ส่งผลกระทบต่อการเชื่อมต่อและการแลกเปลี่ยนข้อมูลระหว่าง MISP Node ของ กพท. กับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ที่มีอยู่เดิม

4.1.4 ผู้ยื่นข้อเสนอต้องจัดให้ระบบสามารถรองรับการแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์กับระบบของหน่วยงานสมาชิก TA-CERT ตามที่ กพท. กำหนด

4.1.5 ผู้ยื่นข้อเสนอต้องกำหนดค่าและควบคุมการแลกเปลี่ยนข้อมูลให้เป็นไปตามระดับการเปิดเผยข้อมูล สิทธิการเข้าถึง และหลักเกณฑ์การแบ่งปันข้อมูลที่ กพท. กำหนด

4.1.6 ก่อนดำเนินการเชื่อมต่อหรือปรับเปลี่ยนการตั้งค่าที่เกี่ยวข้องกับ MISP Node ของ กพท. ที่มีอยู่เดิม ผู้ยื่นข้อเสนอต้องจัดทำแผนการดำเนินงาน สำรองค่าการตั้งค่าที่เกี่ยวข้อง และจัดเตรียมแนวทางการกู้คืนหรือย้อนกลับการเปลี่ยนแปลง (Rollback) เพื่อให้สามารถคืนค่าระบบได้ในกรณีที่การดำเนินการส่งผลกระทบต่อระบบเดิม

4.1.7 ผู้ยื่นข้อเสนอต้องดำเนินการทดสอบการทำงาน การเชื่อมต่อ และการแลกเปลี่ยนข้อมูลของระบบรวมถึงแก้ไขข้อบกพร่องที่ตรวจพบให้แล้วเสร็จก่อนเปิดใช้งานจริง (Go-Live)

4.1.8 การจัดทำและส่งมอบคู่มือและเอกสารประกอบระบบ

ผู้ยื่นข้อเสนอต้องจัดทำและส่งมอบคู่มือและเอกสารประกอบระบบบริหารจัดการและแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ให้สอดคล้องกับระบบและรูปแบบการให้บริการที่นำมาใช้จริง และมีรายละเอียดเพียงพอสำหรับการใช้งาน การบริหารจัดการ การกำหนดค่า และการดูแลระบบ โดยอย่างน้อยประกอบด้วย

(1) เอกสารแสดงสถาปัตยกรรมและการเชื่อมต่อของระบบที่นำมาใช้ในโครงการ โดยแสดงองค์ประกอบที่เกี่ยวข้องกับการให้บริการ การเชื่อมต่อกับ MISP Node ของ กพท. ที่มีอยู่เดิม การเชื่อมต่อกับระบบของหน่วยงานสมาชิก TA-CERT และการเชื่อมต่อกับระบบอื่นที่เกี่ยวข้อง

(2) เอกสารการติดตั้งและการกำหนดค่าระบบ ตามรูปแบบการติดตั้งและการให้บริการที่นำมาใช้จริง โดยครอบคลุมการกำหนดค่าที่จำเป็นต่อการทำงาน การเชื่อมต่อ และการแลกเปลี่ยนข้อมูลของระบบ

(3) คู่มือผู้ดูแลระบบ (Administrator Manual) ฉบับภาษาไทย โดยครอบคลุมการบริหารจัดการผู้ใช้งานและสิทธิ การกำหนดค่าระบบ การบริหารจัดการข้อมูลภัยคุกคามทางไซเบอร์ การนำเข้าและแลกเปลี่ยนข้อมูล การกำหนดระดับการเปิดเผยข้อมูล การตรวจสอบสถานะการทำงาน และการแก้ไขปัญหาเบื้องต้น

(4) คู่มือการใช้งานระบบ (User Manual) ฉบับภาษาไทย โดยครอบคลุมการใช้งานฟังก์ชันสำหรับการรับ รวบรวม ค้นหา บริหารจัดการ และแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์

ผู้ยื่นข้อเสนอต้องปรับปรุงคู่มือและเอกสารตามข้อนี้ให้เป็นปัจจุบันและสอดคล้องกับระบบที่ใช้งานจริงตลอดระยะเวลาสัญญา

4.2 ระบบหรือโมดูลด้านข่าวกรองภัยคุกคามทางไซเบอร์ (Threat Intelligence)

4.2.1 ผู้ยื่นข้อเสนอต้องจัดให้มีระบบหรือโมดูลด้านข่าวกรองภัยคุกคาม (Threat Intelligence) สำหรับสนับสนุนการดำเนินงานของ TA-CERT ในการรวบรวม สืบค้น ติดตาม วิเคราะห์ และเชื่อมโยงข้อมูลภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับ กพท. หน่วยงานสมาชิก TA-CERT และภาคการบิน โดยมีคุณสมบัติและความสามารถไม่น้อยกว่าที่กำหนดใน **ภาคผนวก 2**

4.2.2 ผู้ยื่นข้อเสนอต้องจัดให้มีสิทธิการใช้งาน สิทธิการเข้าถึงข้อมูล และสิทธิอื่นที่จำเป็นต่อการใช้งานระบบหรือโมดูลตามข้อ 4.2.1 ตลอดระยะเวลาสัญญา

4.2.3 ผู้ยื่นข้อเสนอต้องกำหนดค่าระบบหรือโมดูลให้สามารถติดตาม Domain ของ กพท. และหน่วยงานสมาชิก TA-CERT ตามรายชื่อและขอบเขตที่ กพท. กำหนด เพื่อใช้ในการค้นหา ติดตาม และวิเคราะห์ข้อมูลภัยคุกคามทางไซเบอร์ที่เกี่ยวข้อง

4.2.4 ระบบหรือโมดูลต้องสามารถค้นหาและติดตามทรัพย์สินดิจิทัลภายนอก (External Digital Assets) ที่สัมพันธ์กับ Domain ตามข้อ 4.2.3 เช่น Domain, Subdomain และ IP Address รวมถึงทรัพย์สินดิจิทัลภายนอกประเภทอื่นตามรายละเอียดที่กำหนดในภาคผนวก 2

4.2.5 ระบบหรือโมดูลต้องสามารถค้นหา ติดตาม และแจ้งเตือนข้อมูลภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับ กพท. และหน่วยงานสมาชิก TA-CERT ตามประเภทข้อมูลและเงื่อนไขที่กำหนดในภาคผนวก 2

4.2.6 ระบบหรือโมดูลต้องสามารถสืบค้นข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์เพื่อใช้ประกอบการตรวจสอบและวิเคราะห์ภัยคุกคาม เช่น Indicators of Compromise (IOC) ข้อมูลช่องโหว่ ข้อมูลมัลแวร์ เทคนิคและวิธีการของผู้ก่อภัยคุกคาม ตลอดจนข้อมูลความสัมพันธ์ที่เกี่ยวข้อง ตามรายละเอียดที่กำหนดใน **ภาคผนวก 2**

4.2.7 ผู้ยื่นข้อเสนอต้องดำเนินการติดตั้งหรือกำหนดค่า ทดสอบ และจัดเตรียมระบบหรือโมดูลให้พร้อมใช้งาน รวมถึงดำเนินการเชื่อมโยงหรือแลกเปลี่ยนข้อมูลกับระบบตามข้อ 4.1 ในส่วนที่จำเป็นต่อการดำเนินงานของ TA-CERT

4.2.8 การจัดทำและส่งมอบคู่มือและเอกสารประกอบระบบ

ผู้ยื่นข้อเสนอต้องจัดทำและส่งมอบคู่มือและเอกสารประกอบระบบหรือโมดูลด้านข่าวกรองภัยคุกคามทางไซเบอร์ (Threat Intelligence) ให้สอดคล้องกับระบบหรือโมดูลที่นำมาใช้จริง โดยอย่างน้อยประกอบด้วย

(1) เอกสารรายละเอียดระบบหรือโมดูล ซึ่งแสดงภาพรวมการทำงาน องค์ประกอบที่เกี่ยวข้อง และการเชื่อมต่อหรือแลกเปลี่ยนข้อมูลกับระบบอื่นที่เกี่ยวข้อง

(2) เอกสารทางเทคนิคที่จำเป็นสำหรับการนำระบบหรือโมดูลมาใช้งาน การกำหนดค่า และการดูแลระบบ ตามรูปแบบการให้บริการที่นำมาใช้

(3) คู่มือผู้ดูแลระบบ (Administrator Manual) ฉบับภาษาไทย โดยมีรายละเอียดครอบคลุมการบริหารจัดการผู้ใช้งาน การกำหนดสิทธิ การกำหนดค่า และการบริหารจัดการระบบหรือโมดูลในส่วนที่ผู้ดูแลระบบสามารถดำเนินการได้

(4) คู่มือผู้ใช้งาน (User Manual) ฉบับภาษาไทย โดยมีรายละเอียดครอบคลุมฟังก์ชันและความสามารถของระบบหรือโมดูลที่จัดให้ใช้งานตามขอบเขตของงานนี้

4.3 การดำเนินงานด้านข่าวกรองภัยคุกคามทางไซเบอร์ (Threat Intelligence Operations)

4.3.1 ผู้ยื่นข้อเสนอต้องดำเนินการรวบรวม ติดตาม และตรวจสอบข้อมูลภัยคุกคามทางไซเบอร์จากแหล่งข้อมูลที่น่าเชื่อถือทั้งในประเทศและต่างประเทศ ครอบคลุมข้อมูลภัยคุกคาม ช่องโหว่ แคมเปญการโจมตี ข้อมูลตัวบ่งชี้การบุกรุก (Indicators of Compromise: IOCs) และข้อมูลอื่นที่เกี่ยวข้องกับ กพท. หน่วยงานสมาชิก TA-CERT และภาคการบิน

4.3.2 ผู้ยื่นข้อเสนอต้องวิเคราะห์ข้อมูลตามข้อ 4.3.1 เพื่อวิเคราะห์แนวโน้มของภัยคุกคาม (Trend Analysis) ความเชื่อมโยงของภัยคุกคามที่เกี่ยวข้องกับ กพท. หน่วยงานสมาชิก TA-CERT หรือภาคการบิน รวมถึงวิเคราะห์ช่องโหว่และเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่สำคัญ พร้อมจัดทำข้อเสนอแนะหรือแนวทางในการป้องกันและลดผลกระทบ

4.3.3 ผู้ยื่นข้อเสนอต้องจัดเก็บผลการรวบรวม ติดตาม ตรวจสอบ และวิเคราะห์ข้อมูลตามข้อ 4.3.1 และข้อ 4.3.2 โดยต้องสามารถเรียกดูข้อมูลดังกล่าวได้ตลอดระยะเวลาสัญญา ทั้งนี้ ผู้ยื่นข้อเสนอต้องจัดให้มีทรัพยากรที่จำเป็นและเพียงพอสำหรับการจัดเก็บและเรียกดูข้อมูลดังกล่าว

4.3.4 เมื่อพบภัยคุกคามทางไซเบอร์ที่มีระดับความรุนแรงสูงและอาจส่งผลกระทบต่อ กพท. หน่วยงานสมาชิก TA-CERT หรือภาคการบิน ผู้ยื่นข้อเสนอต้องจัดทำการแจ้งเตือนเร่งด่วน (Ad-hoc Critical Alert) และแจ้งเตือนผ่านจดหมายอิเล็กทรอนิกส์ (E-mail) หรือช่องทางอื่นที่ กพท. กำหนด โดยอย่างน้อยต้องมีรายละเอียดของภัยคุกคาม ผลกระทบที่อาจเกิดขึ้น ข้อมูลทางเทคนิคที่เกี่ยวข้อง และข้อเสนอแนะเบื้องต้นในการป้องกันหรือลดผลกระทบ

4.3.5 ผู้ยื่นข้อเสนอต้องจัดทำข่าวสารด้านความมั่นคงปลอดภัยไซเบอร์รายสัปดาห์ (Weekly Cybersecurity News) ไม่น้อยกว่าสัปดาห์ละ 1 ครั้ง ในรูปแบบบทความ Infographic หรือรูปแบบอื่นที่ กพท. เห็นชอบ และเผยแพร่ผ่านจดหมายอิเล็กทรอนิกส์ (E-mail) หรือช่องทางอื่นที่ กพท. กำหนด รวมถึงนำเข้าสู่ TA-CERT Web Application

4.3.6 ผู้ยื่นข้อเสนอต้องจัดทำและแจ้งข่าวสารที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ผ่านจดหมายอิเล็กทรอนิกส์ (E-mail) หรือช่องทางอื่นที่ กพท. กำหนด โดยจำแนกข่าวสารอย่างน้อย ดังนี้

(1) ข่าวกรองภัยคุกคามทางไซเบอร์ (Threat Intelligence) โดยให้มีรายละเอียดตามลักษณะของภัยคุกคามและข้อมูลที่สามารถตรวจสอบได้ อย่างน้อยประกอบด้วย

(1.1) ชื่อหรือประเภทของภัยคุกคามหรือมัลแวร์

(1.2) คำอธิบายและภาพรวมของภัยคุกคาม

(1.3) หมายเลข CVE และค่า CVSS ในกรณีที่เกี่ยวข้อง

(1.4) รายละเอียดของภัยคุกคาม ผลกระทบ และระบบหรือผลิตภัณฑ์ที่ได้รับผลกระทบ

(1.5) แนวทางการแก้ไข ป้องกัน หรือลดผลกระทบ

(1.6) ข้อมูลตัวบ่งชี้การบุกรุก (Indicators of Compromise: IOCs) ในกรณีที่มีข้อมูลดังกล่าว

(1.7) แหล่งที่มาหรือแหล่งอ้างอิงของข้อมูล

กรณีผลการวิเคราะห์พบว่าภัยคุกคามดังกล่าวอาจส่งผลกระทบต่อ กพท. หน่วยงานสมาชิก TA-CERT หรือภาคการบิน ผู้ยื่นข้อเสนอต้องวิเคราะห์ผลกระทบและดำเนินการแจ้งเตือนตามกระบวนการที่ กพท. กำหนด เพื่อสนับสนุนการดำเนินมาตรการป้องกันหรือลดผลกระทบได้อย่างทันท่วงที

(2) ข่าวสารด้านภัยคุกคามทางไซเบอร์ (Cybersecurity News) เช่น แนวโน้มการโจมตี ช่องโหว่ที่ตรวจพบใหม่ เทคนิคหรือเครื่องมือที่ใช้ในการโจมตี และสถานการณ์ด้านภัยคุกคามทางไซเบอร์ที่ควรเฝ้าระวัง

4.3.7 ผู้ยื่นข้อเสนอต้องนำข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์ที่ผ่านการตรวจสอบและวิเคราะห์แล้วเข้าสู่ระบบบริหารจัดการและแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ตามข้อ 4.1 เพื่อสนับสนุนการจัดเก็บ การบริหารจัดการ และการแลกเปลี่ยนข้อมูลระหว่าง กพท. หน่วยงานสมาชิก TA-CERT และหน่วยงานที่เกี่ยวข้อง ตามสิทธิและขอบเขตการเปิดเผยข้อมูลที่ กพท. กำหนด

4.3.8 ผู้ยื่นข้อเสนอต้องจัดให้มีการนำเข้าหรือปรับปรุงข้อมูลตัวบ่งชี้การบุกรุก (Indicators of Compromise: IOCs) และข้อมูลทางเทคนิคที่เกี่ยวข้องในระบบตามข้อ 4.1 ไม่น้อยกว่าสัปดาห์ละ 3 ครั้ง โดยสามารถดำเนินการแบบอัตโนมัติหรือโดยผู้ปฏิบัติงาน ทั้งนี้ ก่อนเผยแพร่หรือแลกเปลี่ยนข้อมูลกับหน่วยงานที่เกี่ยวข้อง ผู้ยื่นข้อเสนอต้องตรวจสอบแหล่งที่มา ความน่าเชื่อถือ และความเกี่ยวข้องของข้อมูล รวมทั้งกำหนดระดับการเปิดเผยข้อมูลตามหลักเกณฑ์ที่ กพท. กำหนด

กรณีตรวจพบภัยคุกคามที่มีระดับความรุนแรงสูงหรืออาจส่งผลกระทบต่อ กพท. หน่วยงานสมาชิก TA-CERT หรือภาคการบิน ผู้ยื่นข้อเสนอต้องนำเข้าหรือปรับปรุงข้อมูลที่เกี่ยวข้องในระบบ และดำเนินการแจ้งเตือนตามกระบวนการที่ กพท. กำหนดโดยไม่ชักช้า โดยไม่ต้องรอรอบการดำเนินการตามปกติ

4.4 การพัฒนา TA-CERT Web Application

4.4.1 ผู้ยื่นข้อเสนอต้องดำเนินการวิเคราะห์ ออกแบบ พัฒนา ติดตั้ง กำหนดค่า ทดสอบ และเปิดใช้งานเว็บแอปพลิเคชันของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคการบิน (TA-CERT Web Application) เพื่อสนับสนุนการบริหารจัดการข้อมูลและการดำเนินงานของ TA-CERT รวมถึงใช้เป็นช่องทางในการเผยแพร่และแลกเปลี่ยนข้อมูลที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยระบบต้องมีคุณสมบัติและความสามารถไม่น้อยกว่าที่กำหนดใน **ภาคผนวก 3**

4.4.2 การวิเคราะห์ความต้องการและออกแบบระบบ

ผู้ยื่นข้อเสนอต้องรวบรวมและวิเคราะห์ความต้องการร่วมกับ กพท. และจัดทำรายละเอียดการออกแบบ TA-CERT Web Application เพื่อเสนอให้ กพท. พิจารณาให้ความเห็นชอบก่อนนำผลการออกแบบดังกล่าวไปใช้ในการพัฒนาระบบ โดยอย่างน้อยต้องครอบคลุม ดังนี้

(1) ความต้องการ ขอบเขต และกระบวนการทำงานของระบบ

(2) สถาปัตยกรรมระบบ (System Architecture) และองค์ประกอบที่เกี่ยวข้อง

(3) โครงสร้างและความสัมพันธ์ของข้อมูล รวมถึงโครงสร้างฐานข้อมูลที่จำเป็นต่อการทำงานของระบบ

(4) กระบวนการบริหารจัดการข้อมูล และการกำหนดสิทธิการเข้าถึงและใช้งานระบบตามบทบาทของผู้ใช้งาน

(5) ข้อกำหนดและแนวทางด้านความมั่นคงปลอดภัยของระบบและข้อมูล

(6) การออกแบบส่วนติดต่อผู้ใช้งาน (User Interface: UI) โดยคำนึงถึงอัตลักษณ์ของ กพท. และให้รูปแบบการนำเสนอได้รับความเห็นชอบจาก กพท.

4.4.3 การจัดทำรูปจำลองระบบ (System Mock-up)

ผู้ยื่นข้อเสนอต้องจัดทำรูปจำลอง TA-CERT Web Application (System Mock-up) ตามผลการวิเคราะห์และออกแบบตามข้อ 4.4.2 โดยแสดงรูปแบบหน้าจอ โครงสร้างเมนู และกระบวนการทำงานที่สำคัญของระบบและนำเสนอต่อ กพท. เพื่อพิจารณา ทั้งนี้ ผู้ยื่นข้อเสนอต้องปรับปรุง System Mock-up ตามข้อเสนอแนะของ กพท. และนำเสนอให้ กพท. พิจารณาให้ความเห็นชอบก่อนนำไปใช้ในการพัฒนาระบบ

4.4.4 การพัฒนา ติดตั้ง และเปิดใช้งานระบบ

ผู้ยื่นข้อเสนอต้องดำเนินการพัฒนา ติดตั้ง กำหนดค่า และเปิดใช้งาน TA-CERT Web Application ตามผลการวิเคราะห์และออกแบบที่ กพท. ให้ความเห็นชอบ โดยอย่างน้อยต้องดำเนินการ ดังนี้

(1) พัฒนาระบบให้มีคุณสมบัติและความสามารถครบถ้วนตามที่กำหนดใน ภาคผนวก 3

(2) พัฒนาระบบตามหลักการพัฒนาซอฟต์แวร์อย่างมั่นคงปลอดภัย (Secure Software Development) และข้อกำหนดด้านความมั่นคงปลอดภัยที่กำหนดในขอบเขตของงานนี้

(3) ระบบต้องรองรับการบริหารจัดการและนำเสนอข้อมูลที่เกี่ยวข้องกับการดำเนินงานของ TA-CERT ตามสิทธิของผู้ใช้งานที่กำหนด

(4) ระบบต้องรองรับการใช้งานและการแสดงผลทั้งภาษาไทยและภาษาอังกฤษตามฟังก์ชันที่กำหนด และเปิดให้บริการภายใต้ชื่อโดเมนหรือ Subdomain ที่ กพท. กำหนด

(5) ผู้ยื่นข้อเสนอต้องจัดให้มีทรัพยากรและสภาพแวดล้อมที่จำเป็นสำหรับการพัฒนา ทดสอบ และให้บริการ TA-CERT Web Application อย่างเพียงพอตลอดระยะเวลาสัญญา โดยผู้ยื่นข้อเสนอเป็นผู้รับผิดชอบค่าใช้จ่ายที่เกี่ยวข้องกับการดำเนินงานตามขอบเขตของงานนี้ทั้งหมด

4.4.5 การทดสอบระบบ

ก่อนเปิดใช้งานจริง (Go-Live) ผู้ยื่นข้อเสนอต้องจัดทำแผนและดำเนินการทดสอบ TA-CERT Web Application เพื่อยืนยันว่าระบบมีคุณสมบัติและสามารถทำงานได้ตามข้อกำหนด โดยอย่างน้อยต้องดำเนินการ ดังนี้

(1) จัดทำแผนและกรณีทดสอบระบบ (Test Plan/Test Case) โดยระบุรายการทดสอบ ขั้นตอนการทดสอบ ผลที่คาดหวัง และเกณฑ์การผ่านของแต่ละกรณีทดสอบ ให้ครอบคลุมการทดสอบระบบโดยรวม พร้อมบันทึกผลการทดสอบ หากพบข้อผิดพลาดหรือข้อบกพร่อง ผู้ยื่นข้อเสนอต้องดำเนินการแก้ไขและทดสอบซ้ำ ในส่วนที่มีการแก้ไขให้แล้วเสร็จ พร้อมจัดทำรายงานผลการทดสอบเสนอ กพท.

(นายวีระ ระบายศรี)	(นางสาวอรรวรรณ ใจเอื้อ)	(นาวาอากาศเอก กรเอก ชิษณุชาบุญวิภัค)	(นายรักพิรุนห์ รุจิรวงษ์สกุล)	(นายจักรพรรณ มีนคร)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

(2) ผู้ยื่นข้อเสนอต้องดำเนินการทดสอบ UAT (User Acceptance Testing) ร่วมกับ กพท. เป็นระยะเวลาไม่น้อยกว่า 2 วันทำการ และดำเนินการแก้ไขข้อบกพร่องที่มีผลกระทบต่อการทำงานตามข้อกำหนดให้แล้วเสร็จก่อนเปิดใช้งานจริง (Go-Live)

(3) ผู้ยื่นข้อเสนอต้องดำเนินการประเมินช่องโหว่ด้านความมั่นคงปลอดภัย (Vulnerability Assessment: VA) ของ TA-CERT Web Application โดยครอบคลุมการทดสอบในลักษณะที่มีสิทธิผู้ใช้งาน (Authenticated/Credentialed Testing) และใช้เครื่องมือสำหรับตรวจสอบช่องโหว่อย่างน้อย 1 เครื่องมือ

(4) ผู้ยื่นข้อเสนอต้องดำเนินการทดสอบเจาะระบบเว็บแอปพลิเคชัน (Web Application Penetration Testing) ในรูปแบบ Grey-box ให้ครอบคลุม TA-CERT Web Application ที่จะเปิดให้บริการจริง โดยอ้างอิง OWASP Web Security Testing Guide (WSTG) หรือมาตรฐานหรือแนวทางการทดสอบด้านความมั่นคงปลอดภัยของเว็บแอปพลิเคชันอื่นที่เป็นที่ยอมรับในระดับสากล

(5) ผู้ยื่นข้อเสนอต้องดำเนินการแก้ไขช่องโหว่ระดับ Critical, High, Medium และ Low ที่ตรวจพบจากการดำเนินการตาม (4) และ (5) และดำเนินการทดสอบยืนยันผลการแก้ไข (Retest) ให้แล้วเสร็จก่อนเปิดใช้งานจริง (Go-Live) เว้นแต่กรณีที่ช่องโหว่ดังกล่าวไม่สามารถแก้ไขได้โดยตรงเนื่องจากข้อจำกัดทางเทคนิค ผู้ยื่นข้อเสนอต้องจัดทำเหตุผล ผลกระทบ การประเมินความเสี่ยง และมาตรการลดความเสี่ยงทดแทน (Compensating Controls) เสนอ กพท. พิจารณาให้ความเห็นชอบก่อนเปิดใช้งานจริง (Go-Live)

(6) ผู้ยื่นข้อเสนอต้องจัดทำรายงานผลการประเมินช่องโหว่และการทดสอบเจาะระบบ โดยอย่างน้อยต้องระบุขอบเขตการทดสอบ วิธีการทดสอบ เครื่องมือที่ใช้ รายการช่องโหว่หรือข้อตรวจพบ ตำแหน่งหรือส่วนของระบบที่ตรวจพบ ระดับความรุนแรง ผลกระทบ แนวทางการแก้ไข และผลการทดสอบยืนยันภายหลังการแก้ไข

4.4.6 การจัดทำและส่งมอบคู่มือและเอกสารประกอบระบบ

ผู้ยื่นข้อเสนอต้องจัดทำและส่งมอบคู่มือและเอกสารประกอบ TA-CERT Web Application ให้สอดคล้องกับระบบที่เปิดใช้งานจริง และมีรายละเอียดเพียงพอสำหรับการใช้งาน การดูแล และการติดตั้งระบบ โดยอย่างน้อยประกอบด้วย

(1) เอกสารผลการวิเคราะห์ความต้องการและออกแบบระบบ

(2) เอกสารสถาปัตยกรรมระบบ (System Architecture Document)

(3) เอกสารการติดตั้งและกำหนดค่าระบบ (Installation and Configuration Document)

(4) คู่มือผู้ดูแลระบบ (Administrator Manual) ฉบับภาษาไทย

(5) คู่มือผู้ใช้งาน (User Manual) ฉบับภาษาไทย

ผู้ยื่นข้อเสนอต้องปรับปรุงคู่มือและเอกสารตามข้อนี้ให้เป็นปัจจุบันและสอดคล้องกับระบบที่ใช้งานจริงตลอดระยะเวลาสัญญา

4.4.7 การส่งมอบ Source Code

ผู้ยื่นข้อเสนอต้องส่งมอบ Source Code ของ TA-CERT Web Application ในส่วนที่พัฒนาขึ้นภายใต้โครงการนี้ โดย Source Code และองค์ประกอบที่ส่งมอบต้องเป็นปัจจุบัน สอดคล้องกับระบบที่เปิดใช้งานจริง และสามารถนำระบบขึ้นใช้งาน (Deploy) โดยอย่างน้อยต้องดำเนินการ ดังนี้

(1) เมื่อเปิดใช้งานระบบจริง (Go-Live) ผู้ยื่นข้อเสนอต้องส่งมอบ Source Code เวอร์ชันที่ตรงกับระบบที่เปิดใช้งานจริง พร้อมไฟล์การกำหนดค่า (Configuration Files) โครงสร้างฐานข้อมูล ไฟล์หรือสคริปต์

ที่เกี่ยวข้องกับฐานข้อมูล รายการและไฟล์ที่ใช้ในการบริหารจัดการ Dependencies ตลอดจนไฟล์ สคริปต์ และองค์ประกอบอื่นที่จำเป็นสำหรับการ Build และ Deploy ระบบ

(2) ภายหลังการเปิดใช้งานจริง หากมีการแก้ไข ปรับปรุง หรือเพิ่มเติม TA-CERT Web Application ผู้ยื่นข้อเสนอต้องปรับปรุง Source Code ไฟล์การกำหนดค่า โครงสร้างฐานข้อมูล ไฟล์หรือสคริปต์ที่เกี่ยวข้อง และเอกสารประกอบที่ได้รับผลกระทบจากการเปลี่ยนแปลงให้เป็นปัจจุบันและสอดคล้องกับระบบที่ใช้งานจริง พร้อมจัดทำบันทึกรายการเปลี่ยนแปลง (Change Log) ตลอดระยะเวลาสัญญา

(3) ผู้ยื่นข้อเสนอต้องจัดทำรายการซอฟต์แวร์รหัสเปิด (Open-source Software) ไลบรารี และส่วนประกอบของบุคคลภายนอก (Third-party Components) ที่นำมาใช้ในการพัฒนา TA-CERT Web Application โดยระบุชื่อ เวอร์ชัน และประเภทสิทธิการใช้งานของแต่ละรายการ

(4) Source Code ไฟล์การกำหนดค่า และองค์ประกอบอื่นที่ส่งมอบต้องไม่มีรหัสผ่าน กุญแจเข้ารหัส (Cryptographic Key) Token, API Key หรือข้อมูลลับอื่นฝังอยู่ เว้นแต่ข้อมูลที่จำเป็นต่อการใช้งานระบบซึ่งต้องส่งมอบให้ กพท. ให้ผู้ยื่นข้อเสนอดำเนินการส่งมอบด้วยวิธีการที่มีความมั่นคงปลอดภัยและแยกออกจาก Source Code

(5) เมื่อสิ้นสุดการดำเนินงานตามสัญญา ผู้ยื่นข้อเสนอต้องส่งมอบ Source Code ฉบับสมบูรณ์ล่าสุด (Latest Complete Source Code) พร้อมไฟล์การกำหนดค่า โครงสร้างฐานข้อมูล ไฟล์หรือสคริปต์ที่เกี่ยวข้องกับฐานข้อมูล ไฟล์สำหรับบริหารจัดการ Dependencies และไฟล์หรือองค์ประกอบอื่นที่จำเป็นสำหรับการ Build และ Deploy ระบบ รวมถึงบันทึกรายการเปลี่ยนแปลง คู่มือ และเอกสารที่เกี่ยวข้องฉบับล่าสุด โดยสิ่งที่ส่งมอบทั้งหมดต้องสอดคล้องกับระบบที่ใช้งานจริง ณ วันที่ส่งมอบ

(6) ในการส่งมอบ Source Code ฉบับสมบูรณ์ล่าสุด ผู้ยื่นข้อเสนอต้องสาธิตการ Build และ Deploy TA-CERT Web Application จาก Source Code และไฟล์ที่ส่งมอบร่วมกับเจ้าหน้าที่ของ กพท. เพื่อยืนยันว่าสามารถนำ Source Code ที่ส่งมอบไปประกอบขึ้นระบบและติดตั้งใช้งานได้จริง

4.5 การพัฒนาศักยภาพและการเสริมสร้างความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์

4.5.1 การฝึกอบรมเพื่อพัฒนาศักยภาพด้านความมั่นคงปลอดภัยไซเบอร์

ผู้ยื่นข้อเสนอต้องจัดการฝึกอบรมเชิงปฏิบัติการ (Workshop) เพื่อพัฒนาความรู้และทักษะด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่เจ้าหน้าที่ของ กพท. และผู้แทนหน่วยงานสมาชิก TA-CERT จำนวนไม่น้อยกว่า 2 หลักสูตร โดยมีรายละเอียด ดังนี้

(1) หลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์ระดับผู้เชี่ยวชาญ
   (1.1) ผู้เข้ารับการฝึกอบรมจำนวนไม่น้อยกว่า 20 คน
   (1.2) ระยะเวลาการฝึกอบรมไม่น้อยกว่า 3 วัน
   (1.3) เนื้อหาการฝึกอบรมอย่างน้อยต้องครอบคลุมเรื่องดังต่อไปนี้
   - บทบาทด้านความปลอดภัยไซเบอร์ มาตรการควบคุม และการประเมินความมั่นคงปลอดภัย
   - การวิเคราะห์ภัยคุกคาม การโจมตี และการตอบสนองต่อเหตุการณ์
   - การออกแบบและใช้งานสถาปัตยกรรมความมั่นคงปลอดภัย
   - การบริหารจัดการตัวตน การพิสูจน์ตัวตน และโครงสร้างพื้นฐานกุญแจสาธารณะ
   - ความมั่นคงปลอดภัยคลาวด์ ความเป็นส่วนตัว และการป้องกันข้อมูล

(2) หลักสูตรผู้เชี่ยวชาญเฉพาะด้านการวิเคราะห์ความมั่นคงปลอดภัยทางไซเบอร์
   (2.1) ผู้เข้ารับการฝึกอบรมจำนวนไม่น้อยกว่า 20 คน
   (2.2) ระยะเวลาการฝึกอบรมไม่น้อยกว่า 3 วัน

(2.3) เนื้อหาการฝึกอบรมอย่างน้อยต้องครอบคลุมเรื่องดังต่อไปนี้

- การบริหารจัดการและวิเคราะห์ช่องโหว่
- ข่าวกรองภัยคุกคามและการติดตามภัยคุกคาม
- การเฝ้าระวัง วิเคราะห์ และตรวจจับกิจกรรมที่เป็นอันตราย
- การตอบสนองต่อเหตุการณ์และการสื่อสารในภาวะวิกฤต
- ความมั่นคงปลอดภัยแอปพลิเคชันและการบรรเทาการโจมตี

ผู้ยื่นข้อเสนอต้องจัดทำรายละเอียดหลักสูตรและกำหนดการฝึกอบรมเสนอ กพท. เพื่อพิจารณาให้ความเห็นชอบก่อนดำเนินการฝึกอบรม

ทั้งนี้ ผู้ยื่นข้อเสนอต้องรับผิดชอบค่าใช้จ่ายในการจัดฝึกอบรมทั้งหมด ซึ่งรวมถึงค่าสถานที่ ค่าวิทยากร ค่าอาหารและเครื่องดื่ม ค่าเอกสาร อุปกรณ์ และสื่อประกอบการฝึกอบรม ตลอดจนค่าใช้จ่ายอื่นที่เกี่ยวข้องการฝึกอบรมการใช้งานระบบและเครื่องมือสนับสนุนการปฏิบัติงาน

4.5.2 การฝึกอบรมการใช้งานและบริหารจัดการระบบ

ผู้ยื่นข้อเสนอต้องจัดการฝึกอบรมเชิงปฏิบัติการ (Workshop) สำหรับการใช้งานและบริหารจัดการระบบที่จัดให้มีภายใต้โครงการ โดยมีรายละเอียด ดังนี้

(1) ระบบบริหารจัดการและแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์

(1.1) การฝึกอบรมสำหรับผู้ใช้งาน (User Training)

จัดให้แก่เจ้าหน้าที่ของ กพท. และผู้แทนหน่วยงานสมาชิก TA-CERT รวมจำนวนไม่น้อยกว่า 20 คน ระยะเวลาไม่น้อยกว่า 1 วัน โดยครอบคลุมการใช้งานระบบตามสิทธิและบทบาทของผู้ใช้งาน

(1.2) การฝึกอบรมสำหรับผู้ดูแลระบบ (Administrator Training)

จัดให้แก่เจ้าหน้าที่ของ กพท. จำนวนไม่น้อยกว่า 3 คน ระยะเวลาไม่น้อยกว่า 1 วัน โดยครอบคลุมการกำหนดค่า การบริหารจัดการ และการดูแลระบบในส่วนที่เกี่ยวข้องกับผู้ดูแลระบบ

(2) ระบบหรือโมดูลด้านข่าวกรองภัยคุกคามทางไซเบอร์ (Threat Intelligence)

(2.1) การฝึกอบรมสำหรับผู้ดูแลระบบ (Administrator Training)

จัดให้แก่เจ้าหน้าที่ของ กพท. จำนวนไม่น้อยกว่า 3 คน ระยะเวลาไม่น้อยกว่า 1 วัน โดยครอบคลุมการใช้งานและบริหารจัดการระบบหรือโมดูลตามสิทธิและความสามารถที่ กพท. ได้รับ

(3) TA-CERT Web Application

(3.1) การฝึกอบรมสำหรับผู้ใช้งาน (User Training)

จัดให้แก่เจ้าหน้าที่ของ กพท. และผู้แทนหน่วยงานสมาชิก TA-CERT รวมจำนวนไม่น้อยกว่า 20 คน ระยะเวลาไม่น้อยกว่า 1 วัน โดยครอบคลุมการใช้งานระบบตามสิทธิและบทบาทของผู้ใช้งาน

(3.2) การฝึกอบรมสำหรับผู้ดูแลระบบ (Administrator Training)

จัดให้แก่เจ้าหน้าที่ของ กพท. จำนวนไม่น้อยกว่า 3 คน ระยะเวลาไม่น้อยกว่า 1 วัน โดยครอบคลุมการกำหนดค่า การบริหารจัดการ และการดูแลระบบในส่วนที่เกี่ยวข้องกับผู้ดูแลระบบ

ผู้ยื่นข้อเสนอต้องจัดทำรายละเอียดหลักสูตรและกำหนดการฝึกอบรมเสนอ กพท. เพื่อพิจารณาให้ความเห็นชอบก่อนดำเนินการฝึกอบรม

ทั้งนี้ ผู้ยื่นข้อเสนอต้องรับผิดชอบค่าใช้จ่ายในการจัดฝึกอบรมทั้งหมด ซึ่งรวมถึงค่าสถานที่ ค่าวิทยากร ค่าอาหารและเครื่องดื่ม ค่าเอกสาร อุปกรณ์ และสื่อประกอบการฝึกอบรม ตลอดจนค่าใช้จ่ายอื่นที่เกี่ยวข้องการฝึกอบรมการใช้งานระบบและเครื่องมือสนับสนุนการปฏิบัติงาน

(นายวีระ ระบายศรี)	(นางสาวอรรวรรณ ใจเอื้อ)	(นาวาอากาศเอก กรเอก ชิษณุชาบุญวิภัค)	(นายรักพิรุนห์ รุจิรวงษ์สกุล)	(นายจักรพรรณ มีนคร)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

4.5.3 การสนับสนุนการจัดทำและพัฒนากรอบการสื่อสารในภาวะวิกฤตด้านความมั่นคงปลอดภัยไซเบอร์ของ TA-CERT

ผู้ยื่นข้อเสนอต้องสนับสนุนและให้คำปรึกษาแก่ TA-CERT ในการจัดทำ พัฒนา และทดสอบกรอบการสื่อสารในภาวะวิกฤตด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อใช้เป็นแนวทางในการประสานงานและสื่อสารเมื่อเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อ กพท. หน่วยงานสมาชิก TA-CERT หรือภาคการบิน โดยต้องดำเนินการอย่างน้อย ดังนี้

(1) การศึกษาและวิเคราะห์ข้อมูล

ศึกษาและวิเคราะห์บริบทการดำเนินงานของ TA-CERT บทบาทของ กพท. หน่วยงานสมาชิก TA-CERT และหน่วยงานที่เกี่ยวข้อง รวมถึงประเภทและระดับความรุนแรงของเหตุการณ์ภัยคุกคามทางไซเบอร์ เพื่อกำหนดเกณฑ์การยกระดับเหตุการณ์ (Trigger Criteria) สำหรับการสื่อสารในภาวะวิกฤต

(2) การจัดทำกรอบการสื่อสารในภาวะวิกฤต

จัดทำกรอบการสื่อสารในภาวะวิกฤตด้านความมั่นคงปลอดภัยไซเบอร์ของ TA-CERT โดยอย่างน้อยต้องครอบคลุม

- โครงสร้าง บทบาท หน้าที่ และความรับผิดชอบของผู้เกี่ยวข้อง
- ขั้นตอนการประสานงานและกระบวนการตัดสินใจด้านการสื่อสาร
- ขั้นตอนการพิจารณาและอนุมัติข้อความก่อนเผยแพร่
- แนวทางการสื่อสารภายในและภายนอกองค์กร รวมถึงการประสานงานกับหน่วยงานที่เกี่ยวข้องและสื่อมวลชน
- แนวทางการจัดการข้อความสื่อสาร เพื่อให้ข้อมูลที่เผยแพร่มีความถูกต้องและสอดคล้องกัน

(3) การจัดทำเอกสารสนับสนุนการสื่อสาร

จัดทำแม่แบบข้อความและเอกสารสนับสนุนการสื่อสารที่สามารถนำไปปรับใช้เมื่อเกิดเหตุการณ์ ได้แก่ ข้อความแจ้งเตือนเร่งด่วน ตัวอย่างถ้อยแถลง คำถามและคำตอบสำหรับประเด็นที่อาจได้รับความสนใจ และแนวทางการสื่อสารกับสื่อมวลชน โดยครอบคลุมสถานการณ์ที่ส่งผลกระทบต่อหน่วยงานเดียว หลายหน่วยงาน หรือภาคการบินในวงกว้าง

(4) การรับฟังความคิดเห็นและปรับปรุงกรอบการสื่อสาร

จัดประชุมเชิงปฏิบัติการหรือรับฟังความคิดเห็นจากเจ้าหน้าที่ของ กพท. และผู้แทนหน่วยงานที่เกี่ยวข้อง เพื่อนำข้อเสนอแนะมาปรับปรุงกรอบการสื่อสารและเอกสารประกอบ ก่อนเสนอ กพท. พิจารณาให้ความเห็นชอบ

(5) การฝึกซ้อมและทดสอบกรอบการสื่อสาร

ผู้ยื่นข้อเสนอต้องจัดการฝึกซ้อมการสื่อสารในภาวะวิกฤตด้านความมั่นคงปลอดภัยไซเบอร์ไม่น้อยกว่า 2 ครั้งตลอดระยะเวลาสัญญา โดยใช้สถานการณ์จำลองที่สอดคล้องกับบริบทและความเสี่ยงของภาคการบิน เช่น Tabletop Exercise, Simulation Exercise หรือรูปแบบอื่นที่เหมาะสมกับวัตถุประสงค์ของการฝึกซ้อม เพื่อทดสอบบทบาท หน้าที่ ขั้นตอนการประสานงาน การตัดสินใจ และกระบวนการสื่อสารตามกรอบที่กำหนด โดยรูปแบบและสถานการณ์ที่ใช้ในการฝึกซ้อมต้องเสนอ กพท. เพื่อพิจารณาให้ความเห็นชอบก่อนดำเนินการ

(6) การสรุปผลและปรับปรุงกรอบการสื่อสาร

(นายวีระ ระบายศรี)	(นางสาวอรรวรรณ ใจเอื้อ)	(นาวาอากาศเอก กรเอก ชิษณุชาบุญวิภัค)	(นายรักพิรุนห์ รุจิรวงษ์สกุล)	(นายจักรพรรณ มีนคร)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

ผู้ยื่นข้อเสนอต้องจัดทำรายงานสรุปผลการฝึกซ้อมแต่ละครั้ง โดยระบุผลการทดสอบ ข้อค้นพบ ปัญหาและอุปสรรค จุดที่ควรปรับปรุง และข้อเสนอแนะ พร้อมนำผลที่ได้จากการฝึกซ้อมมาปรับปรุงกรอบการสื่อสารและเอกสารประกอบที่เกี่ยวข้อง

เมื่อดำเนินการฝึกซ้อมและปรับปรุงแล้วเสร็จ ผู้ยื่นข้อเสนอต้องจัดทำ กรอบการสื่อสารในภาวะวิกฤตด้านความมั่นคงปลอดภัยไซเบอร์ของ TA-CERT ฉบับสมบูรณ์ พร้อมเอกสารประกอบ เสนอ กพท. เพื่อพิจารณาให้ความเห็นชอบ

ทั้งนี้ ผู้ยื่นข้อเสนอต้องรับผิดชอบค่าใช้จ่ายทั้งหมดที่เกี่ยวข้องกับการดำเนินกิจกรรมตามข้อนี้ รวมถึงการจัดประชุมและการฝึกซ้อม ตลอดจนค่าเอกสาร อุปกรณ์ และสื่อประกอบกิจกรรม

4.5.4 การจัดให้มีบุคลากรสนับสนุนการดำเนินงานของ TA-CERT

ผู้ยื่นข้อเสนอต้องจัดให้มีบุคลากรเพื่อสนับสนุนการดำเนินงานของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคการบิน (TA-CERT) โดยมีคุณสมบัติและหน้าที่อย่างน้อย ดังนี้

(1) ผู้จัดการโครงการ (Project Manager)

ผู้ยื่นข้อเสนอต้องจัดให้มีผู้จัดการโครงการหรือผู้อำนวยการโครงการ (Project Manager or Project Director) จำนวนไม่น้อยกว่า 1 คน โดยต้องมีประสบการณ์ด้านการบริหารโครงการเทคโนโลยีสารสนเทศหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์ไม่น้อยกว่า 5 ปี และมีหน้าที่อย่างน้อย ดังนี้

(1.1) บริหารโครงการให้เป็นไปตามขอบเขตของงาน แผนการดำเนินงาน และข้อกำหนดของโครงการ รวมถึงกำกับดูแลการส่งมอบงานในแต่ละงวดให้ครบถ้วนและเป็นไปตามกำหนดเวลา

(1.2) บริหารความเสี่ยงของโครงการ โดยจัดทำและปรับปรุงทะเบียนความเสี่ยง (Risk Register) พร้อมกำหนดมาตรการรองรับ และรายงานต่อ กพท. เมื่อพบความเสี่ยงที่อาจส่งผลกระทบต่อการดำเนินโครงการ

(1.3) เป็นผู้ประสานงานหลักในการแก้ไขปัญหาหรือข้อขัดข้องที่เกิดขึ้นระหว่างการดำเนินโครงการ รวมถึงประสานบุคลากร ผู้เชี่ยวชาญ หรือทรัพยากรเพิ่มเติมที่จำเป็นต่อการแก้ไขปัญหา

(1.4) ให้คำปรึกษาและข้อเสนอแนะแก่ กพท. ในการพัฒนาและยกระดับการดำเนินงานของ TA-CERT ให้สอดคล้องกับภารกิจและขอบเขตของโครงการ

ผู้ยื่นข้อเสนอต้องยื่นหนังสือรับรองการทำงานของบุคลากรที่เสนอ เพื่อแสดงประสบการณ์ตามที่กำหนด พร้อมการยื่นข้อเสนอ

(2) บุคลากรระดับปฏิบัติการ (Operation Team)

ผู้ยื่นข้อเสนอต้องจัดให้มีบุคลากรระดับปฏิบัติการ (Operation Team) จำนวนไม่น้อยกว่า 1 คน โดยต้องมีประสบการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ไม่น้อยกว่า 2 ปี และต้องมีประกาศนียบัตรระดับสากลด้านความมั่นคงปลอดภัยไซเบอร์ (Certification) อย่างน้อย 1 รายการ ได้แก่

- CompTIA Security+
- CompTIA Cybersecurity Analyst (CySA+)
- GIAC Information Security Fundamentals (GISF)
- GIAC Security Essentials (GSEC)
- Certified Ethical Hacker (CEH)

(นายวีระ ระบายศรี)	(นางสาวอรรวรรณ ใจเอื้อ)	(นาวาอากาศเอก กรเอก ชิษณุชาบุญวิภัค)	(นายรักพิรุนห์ รุจิรวงษ์สกุล)	(นายจักรพรรณ มีนคร)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

หรือประกาศนียบัตรระดับสากลด้านความมั่นคงปลอดภัยไซเบอร์อื่นที่มีระดับและขอบเขตความรู้หรือทักษะเทียบเท่า

(2.1) บุคลากรระดับปฏิบัติการ (Operation Team) ต้องปฏิบัติงานประจำ ณ สถานที่ปฏิบัติงานของ TA-CERT ในวันและเวลาทำการของ กพท. และในกรณีที่ กพท. กำหนดให้ปฏิบัติงานนอกสถานที่หรือในรูปแบบอื่น ให้ปฏิบัติงานตามที่ กพท. กำหนด

(2.2) บุคลากรระดับปฏิบัติการ (Operation Team) ต้องสนับสนุนการดำเนินงานของ TA-CERT อย่างน้อยในด้านการเฝ้าระวังเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ การรวบรวมและบันทึกข้อมูลเหตุการณ์ การวิเคราะห์เหตุการณ์เบื้องต้น การประสานงานกับหน่วยงานที่เกี่ยวข้อง การจัดทำรายงาน และการสนับสนุนการดำเนินงานอื่นที่เกี่ยวข้องตามที่ กพท. มอบหมาย

ผู้ยื่นข้อเสนอต้องยื่นหนังสือรับรองการทำงาน และสำเนาประกาศนียบัตรระดับสากลด้านความมั่นคงปลอดภัยไซเบอร์ที่ยังมีผลใช้ได้ ณ วันที่ยื่นข้อเสนอ ของบุคลากรที่เสนอ

(3) บุคลากรระดับผู้เชี่ยวชาญ (Specialist Team)

ผู้ยื่นข้อเสนอต้องจัดให้มีบุคลากรระดับผู้เชี่ยวชาญ (Specialist Team) จำนวนไม่น้อยกว่า 1 คน โดยต้องมีประสบการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ไม่น้อยกว่า 5 ปี และต้องมี ประกาศนียบัตรระดับสากลด้านความมั่นคงปลอดภัยไซเบอร์ (Certification) อย่างน้อย 1 รายการ ได้แก่

- Certified Information Systems Security Professional (CISSP)
- GIAC Certified Incident Handler (GCIH)
- GIAC Certified Intrusion Analyst (GCIA)
- EC-Council Certified Incident Handler (ECIH)
- Certified Threat Intelligence Analyst (CTIA)
- Computer Hacking Forensic Investigator (CHFI)

หรือประกาศนียบัตรระดับสากลด้านความมั่นคงปลอดภัยไซเบอร์อื่นที่มีระดับและขอบเขตความรู้หรือทักษะเทียบเท่า

(3.1) บุคลากรระดับผู้เชี่ยวชาญ (Specialist Team) ต้องมีความเชี่ยวชาญด้านการวิเคราะห์ภัยคุกคาม (Threat Analysis) การตอบสนองต่อเหตุการณ์ (Incident Response) การวิเคราะห์การบุกรุก หรือการวิเคราะห์เชิงลึกด้านเทคนิค และสามารถปฏิบัติงานในรูปแบบระยะไกล (Remote/Online) เพื่อสนับสนุนและให้คำปรึกษาแก่ TA-CERT เมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ รวมถึงการวิเคราะห์ภัยคุกคามเชิงลึก การประเมินผลกระทบ การให้ข้อเสนอแนะทางเทคนิค และการสนับสนุนการแก้ไขปัญหาเมื่อได้รับการร้องขอจาก กพท.

ผู้ยื่นข้อเสนอต้องยื่นหนังสือรับรองการทำงาน และสำเนาประกาศนียบัตรระดับสากลด้านความมั่นคงปลอดภัยไซเบอร์ที่ยังมีผลใช้ได้ ณ วันที่ยื่นข้อเสนอ ของบุคลากรที่เสนอ

(4) ผู้ยื่นข้อเสนอต้องกำหนดช่องทางการติดต่อประสานงานกับบุคลากรระดับปฏิบัติการ (Operation Team) บุคลากรระดับผู้เชี่ยวชาญ (Specialist Team) และผู้จัดการโครงการ (Project Manager) ที่สนับสนุนการดำเนินงานของ TA-CERT และแจ้งให้ กพท. ทราบก่อนเริ่มดำเนินงาน โดยต้องปรับปรุงข้อมูลการติดต่อให้เป็นปัจจุบันตลอดระยะเวลาการดำเนินโครงการ

(นายวีระ ระบายศรี)	(นางสาวอรรวรรณ ใจเอื้อ)	(นาวาอากาศเอก กรเอก ชิษณุชาบุญวิภัค)	(นายรักพิรุนห์ รุจิรวงษ์สกุล)	(นายจักรพรรณ มีนคร)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

4.5.5 การประเมินและยกระดับศักยภาพการดำเนินงานของ TA-CERT (Maturity Assessment)

ผู้ยื่นข้อเสนอต้องดำเนินการประเมินและยกระดับศักยภาพการดำเนินงานของ TA-CERT โดยอ้างอิงกรอบหรือเครื่องมือการประเมินที่เป็นมาตรฐานสากล เพื่อประเมินระดับศักยภาพ (Maturity Level) และวิเคราะห์ช่องว่างของการดำเนินงาน (Gap Analysis) โดยอย่างน้อยต้องครอบคลุมด้านการบริหารจัดการ การบริหารความเสี่ยง การปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ การตอบสนองต่อเหตุการณ์ การบริหารข่าวกรองภัยคุกคาม การกำกับดูแล และการพัฒนาบุคลากร โดยแบ่งการดำเนินงานออกเป็น 2 รอบ ดังนี้

(1) การประเมินรอบที่ 1 (Baseline Assessment)

(1.1) ประเมินระดับศักยภาพ (Maturity Level) ปัจจุบันของ TA-CERT และวิเคราะห์ช่องว่างของการดำเนินงาน (Gap Analysis) เทียบกับกรอบหรือเครื่องมือการประเมินที่ใช้อ้างอิง

(1.2) จัดทำรายงานผลการประเมินรอบที่ 1 โดยแสดงผลการประเมินระดับศักยภาพ ช่องว่างที่ตรวจพบ และข้อเสนอแนะสำหรับการพัฒนาและยกระดับการดำเนินงานของ TA-CERT

(1.3) กำหนดเป้าหมายระดับศักยภาพ (Target Maturity Level) เพื่อใช้เป็นกรอบในการวางแผนและติดตามการพัฒนาศักยภาพการดำเนินงานของ TA-CERT ตลอดระยะเวลาโครงการ และเสนอ กพท. เพื่อพิจารณาให้ความเห็นชอบ

(1.4) จัดทำแผนการยกระดับศักยภาพ (Improvement Plan) โดยระบุกิจกรรม แนวทางดำเนินการ ผู้รับผิดชอบ และกรอบระยะเวลา ให้สอดคล้องกับผลการประเมิน ช่องว่างที่ตรวจพบ และเป้าหมายระดับศักยภาพที่ กพท. ให้ความเห็นชอบ

(1.5) สนับสนุนการดำเนินงานตามแผนการยกระดับศักยภาพ (Improvement Plan) ตลอดระยะเวลาโครงการ และรายงานความคืบหน้าของการดำเนินงานในรายงานสรุปประจำงวดงาน

(2) การประเมินรอบที่ 2 (Final Assessment)

(2.1) ประเมินระดับศักยภาพ (Maturity Level) ของ TA-CERT เมื่อสิ้นสุดช่วงการดำเนินงานที่กำหนด และเปรียบเทียบผลกับการประเมินรอบที่ 1 รวมถึงเป้าหมายระดับศักยภาพที่ กพท. ให้ความเห็นชอบ เพื่อแสดงให้เห็นถึงการเปลี่ยนแปลงของระดับศักยภาพในแต่ละด้าน

(2.2) วิเคราะห์ช่องว่างของการดำเนินงาน (Gap Analysis) ที่ยังคงเหลืออยู่ รวมถึงประเด็นที่ควรได้รับการพัฒนาหรือปรับปรุงเพิ่มเติม เพื่อใช้ประกอบการกำหนดทิศทางการพัฒนา TA-CERT ในระยะถัดไป

(2.3) จัดทำรายงานผลการประเมินรอบที่ 2 โดยแสดงผลการประเมิน การเปรียบเทียบกับผลการประเมินรอบที่ 1 ช่องว่างที่ยังคงเหลืออยู่ และข้อเสนอแนะสำหรับการพัฒนาและยกระดับการดำเนินงานของ TA-CERT

(2.4) จัดทำแผนพัฒนาศักยภาพของ TA-CERT (TA-CERT Roadmap) ระยะเวลาไม่น้อยกว่า 3 ปี โดยกำหนดแนวทางและกิจกรรมสำหรับการพัฒนาศักยภาพการดำเนินงานของ TA-CERT ให้สอดคล้องกับผลการประเมินและช่องว่างที่ตรวจพบ

(2.5) จัดทำ Dashboard สำหรับผู้บริหารเพื่อสรุปผลการประเมินระดับศักยภาพ ช่องว่างที่ตรวจพบ และแผนพัฒนาศักยภาพของ TA-CERT พร้อมนำเสนอผลการประเมินและแผนพัฒนาศักยภาพต่อ กพท.

(นายวีระ ระบายศรี)	(นางสาวอรรวรรณ ใจเอื้อ)	(นาวาอากาศเอก กรเอก ชิษณุชาบุญวิภัค)	(นายรักพิรุนห์ รุจิรวงษ์สกุล)	(นายจักรพรรณ มีนคร)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

4.6 การสื่อสารประชาสัมพันธ์และการสร้างการมีส่วนร่วมของ TA-CERT

4.6.1 การจัดทำกรอบการดำเนินงานและทิศทางการสื่อสารของ TA-CERT

ผู้ยื่นข้อเสนอต้องศึกษาและวิเคราะห์บทบาท ภารกิจ อำนาจหน้าที่ และการดำเนินงานของ TA-CERT เพื่อจัดทำกรอบการดำเนินงานและทิศทางการสื่อสารของ TA-CERT โดยมีรายละเอียดอย่างน้อย ดังนี้

(1) จัดทำร่างวิสัยทัศน์ (Vision) และพันธกิจ (Mission) ของ TA-CERT ให้สอดคล้องกับบทบาท ภารกิจ อำนาจหน้าที่ และทิศทางการดำเนินงานของ TA-CERT

(2) จัดทำกรอบบทบาทและขอบเขตการดำเนินงานของ TA-CERT โดยระบุกลุ่มหน่วยงานที่ TA-CERT ให้การประสานและสนับสนุน (Constituency) ขอบเขตการให้บริการ (Service Scope) และแนวทางการประสานงานกับหน่วยงานที่เกี่ยวข้อง

(3) จัดทำสารสำคัญสำหรับการสื่อสาร (Key Messages) เพื่อใช้เป็นแนวทางในการสื่อสารเกี่ยวกับบทบาท ภารกิจ และการดำเนินงานของ TA-CERT ผ่านเว็บไซต์ สื่อประชาสัมพันธ์ กิจกรรม และช่องทางการสื่อสารที่เกี่ยวข้อง

(4) นำเสนอร่างวิสัยทัศน์ พันธกิจ กรอบบทบาทและขอบเขตการดำเนินงาน และสารสำคัญสำหรับการสื่อสารต่อ กพท. เพื่อพิจารณาให้ความเห็นชอบ และปรับปรุงตามข้อเสนอแนะของ กพท. ก่อนจัดทำเป็นฉบับสมบูรณ์

ทั้งนี้ การจัดทำกรอบการดำเนินงานและทิศทางการสื่อสารของ TA-CERT ต้องสอดคล้องกับกฎหมาย ประกาศ นโยบาย และข้อกำหนดที่เกี่ยวข้อง รวมถึงบทบาท ภารกิจ และอำนาจหน้าที่ของ กพท. และ TA-CERT

4.6.2 การออกแบบและพัฒนาอัตลักษณ์และสื่อประชาสัมพันธ์ของ TA-CERT (Brand Identity)

ผู้ยื่นข้อเสนอต้องดำเนินการออกแบบและพัฒนาอัตลักษณ์ของ TA-CERT (Brand Identity) และจัดทำสื่อประชาสัมพันธ์ให้สอดคล้องกับบทบาท ภารกิจ และทิศทางการสื่อสารของ TA-CERT โดยมีรายละเอียดอย่างน้อย ดังนี้

(1) ออกแบบและจัดทำเครื่องหมาย (Logo) ของ TA-CERT พร้อมกำหนดองค์ประกอบอัตลักษณ์ ได้แก่ โทนสี รูปแบบตัวอักษร และองค์ประกอบกราฟิกที่ใช้ในการสื่อสารและประชาสัมพันธ์

(2) จัดทำแนวทางการใช้อัตลักษณ์ของ TA-CERT (Brand Guidelines) เพื่อกำหนดรูปแบบการนำอัตลักษณ์ไปใช้กับสื่อและช่องทางการสื่อสารต่าง ๆ

(3) ออกแบบและจัดทำสื่อประชาสัมพันธ์ในรูปแบบดิจิทัล เช่น Infographic, Banner หรือสื่อดิจิทัลอื่น เพื่อใช้เผยแพร่ข้อมูล บทบาท ภารกิจ กิจกรรม และการดำเนินงานของ TA-CERT ผ่านช่องทางที่ กพท. กำหนด

(4) นำเสนอแนวคิด รูปแบบอัตลักษณ์ และสื่อประชาสัมพันธ์ต่อ กพท. เพื่อพิจารณาให้ความเห็นชอบ พร้อมส่งมอบไฟล์ต้นฉบับที่สามารถนำไปใช้งานและแก้ไขได้

4.6.3 การจัดประชุมประจำปี TA-CERT (TA-CERT Annual Conference)

ผู้ยื่นข้อเสนอต้องดำเนินการจัดประชุมประจำปี TA-CERT (TA-CERT Annual Conference) ไม่น้อยกว่า 2 ครั้งตลอดระยะเวลาสัญญา โดยแต่ละครั้งมีผู้เข้าร่วมไม่น้อยกว่า 20 คน และมีระยะเวลาไม่น้อยกว่า

(นายวีระ ระบายศรี)	(นางสาวอรรวรรณ ใจเอื้อ)	(นาวาอากาศเอก กรเอก ชิษณุชาบุญวิภัค)	(นายรักพิรุนห์ รุจิรวงษ์สกุล)	(นายจักรพรรณ มีนคร)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

1 วัน เพื่อส่งเสริมการแลกเปลี่ยนความรู้และข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์ รวมถึงสร้างความร่วมมือระหว่าง กพท. หน่วยงานสมาชิก TA-CERT และหน่วยงานที่เกี่ยวข้อง โดยมีรายละเอียดอย่างน้อย ดังนี้

(1) จัดทำหัวข้อ เนื้อหา รูปแบบ กำหนดการ และรายชื่อวิทยากร เสนอ กพท. เพื่อพิจารณาให้ความเห็นชอบก่อนดำเนินการจัดประชุมแต่ละครั้ง โดยเนื้อหาต้องครอบคลุมผลการดำเนินงานของ TA-CERT สถานการณ์และแนวโน้มภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับภาคการบิน และการส่งเสริมความร่วมมือระหว่างหน่วยงานสมาชิก TA-CERT

(2) จัดให้มีวิทยากรหรือผู้เชี่ยวชาญที่มีความรู้และประสบการณ์สอดคล้องกับหัวข้อการประชุม เพื่อบรรยาย อภิปราย หรือแลกเปลี่ยนประสบการณ์ พร้อมจัดให้มีกิจกรรมแลกเปลี่ยนความคิดเห็นและรับฟังข้อเสนอแนะจากผู้เข้าร่วมประชุม

(3) ดำเนินการจัดประชุมและจัดให้มีผู้ประสานงานตลอดระยะเวลาการจัดกิจกรรม รวมถึงจัดเตรียมสถานที่ อาหารและเครื่องดื่ม เอกสาร อุปกรณ์ และสื่อประกอบการประชุม

(4) จัดทำรายงานสรุปผลการจัดประชุมแต่ละครั้ง โดยครอบคลุมสาระสำคัญของการประชุม ข้อคิดเห็นและข้อเสนอแนะจากผู้เข้าร่วม พร้อมเอกสารประกอบการประชุมและภาพกิจกรรม เสนอ กพท. ภายหลังการจัดประชุมแล้วเสร็จ

ทั้งนี้ ผู้ยื่นข้อเสนอต้องรับผิดชอบค่าใช้จ่ายในการจัดประชุมทั้งหมด ซึ่งรวมถึงค่าสถานที่ ค่าวิทยากร ค่าอาหารและเครื่องดื่ม ค่าเอกสาร อุปกรณ์ และสื่อประกอบการประชุม ตลอดจนค่าใช้จ่ายอื่นที่เกี่ยวข้อง

4.7 ในกรณีที่ กพท. มีการย้ายสถานที่ทำการในช่วงระหว่างระยะเวลาของสัญญา ผู้ยื่นข้อเสนอต้องดำเนินการให้ระบบสามารถใช้งานได้ตามปกติ และสนับสนุนการแก้ไขปัญหาการใช้งานเป็นระยะเวลาอย่างน้อย 1 เดือนนับจากวันที่ย้ายสถานที่แล้วเสร็จ โดยไม่มีค่าใช้จ่ายเพิ่มเติม

4.8 ระดับการให้บริการ (Service Level Agreement: SLA) โดยจำแนกตามระดับความรุนแรงของเหตุการณ์ (Severity Level) ดังนี้

ระดับความรุนแรง / ความเสี่ยง	คำนิยามและผลกระทบ	การดำเนินการตอบรับปัญหา	การดำเนินการแก้ไขสำเร็จ
สูงมาก (Very High)	ระบบหลักหยุดทำงานทั้งหมด กระทบผู้ใช้งานทั้งหมด	ตอบรับปัญหาภายใน 15 นาที	แก้ไขให้ระบบกลับมาใช้งานได้ภายใน 2 ชั่วโมง
สูง (High)	ระบบทำงานได้บางส่วน ประสิทธิภาพลดลงอย่างรุนแรง กระทบผู้ใช้งานวงกว้าง	ตอบรับปัญหาภายใน 30 นาที	แก้ไขให้ระบบกลับมาใช้งานได้ภายใน 4 ชั่วโมง
ปานกลาง (Medium)	ฟังก์ชันการทำงานบางส่วนมีปัญหา แต่ยังมีระบบสำรอง หรือกระทบผู้ใช้งานกลุ่มน้อย	ตอบรับปัญหาภายใน 2 ชั่วโมง	แก้ไขให้ระบบกลับมาใช้งานได้ภายใน 12 ชั่วโมง
ต่ำ (Low)	สอบถามข้อมูลทั่วไป การขอเปลี่ยนแปลงการกำหนดค่า (Change Request) หรือปัญหารูปลักษณ์	ตอบรับปัญหาภายใน 4 ชั่วโมง	แก้ไขให้ระบบกลับมาใช้งานได้ภายใน 24 ชั่วโมง

(นายวีระ ระบายศรี) ประธานกรรมการ (นางสาวอรรวรรณ ใจเอื้อ) กรรมการ (นาวาอากาศเอก กรเอก ชิษณุชาบุญวิภัค) กรรมการ (นายรักพิรุนห์ รุจิรวงษ์สกุล) กรรมการ (นายจักรพรรณ มีนคร) กรรมการ

5. กำหนดเวลาส่งมอบพัสดุ

ผู้รับจ้างจะต้องส่งมอบระบบงานตามขอบเขตของงานข้อ 4.1 และข้อ 4.2 แบบพร้อมใช้งาน และจัดส่งรายงานเอกสารที่เกี่ยวข้องกับการส่งมอบระบบฯ ภายใน 60 วัน นับถัดจากวันลงนามในสัญญา และคณะกรรมการตรวจรับพัสดุได้ทำการตรวจรับเรียบร้อยแล้ว โดยกำหนดระยะเวลาการดำเนินงาน 28 เดือน เริ่มนับตั้งแต่วันที่ 1 แห่งเดือนตามปฏิทิน

6. หลักเกณฑ์ในการพิจารณาคัดเลือกข้อเสนอ

ในการพิจารณาผลการยื่นข้อเสนอการประกวดราคาอิเล็กทรอนิกส์นี้ กพท. จะพิจารณาตัดสินโดยใช้เกณฑ์ราคาประกอบเกณฑ์อื่น กำหนดคะแนนรวมทั้งสิ้น 100 คะแนน แบ่งเป็นเกณฑ์ด้านราคา น้ำหนักร้อยละ 20 และเกณฑ์ด้านคุณภาพ น้ำหนักร้อยละ 80 โดยมีรายละเอียดดังนี้

6.1 เกณฑ์ด้านราคา กำหนดน้ำหนักเท่ากับร้อยละ 20

6.2 เกณฑ์ด้านคุณภาพ กำหนดน้ำหนักเท่ากับร้อยละ 80

ผู้ยื่นข้อเสนอต้องได้รับคะแนนด้านคุณภาพรวม ไม่น้อยกว่า 60 คะแนน จากคะแนนเต็ม 80 คะแนน จึงจะผ่านเกณฑ์ด้านคุณภาพ ทั้งนี้ คณะกรรมการฯ จะพิจารณาข้อเสนอด้านราคาเฉพาะผู้ยื่นข้อเสนอที่ผ่านเกณฑ์คะแนนขั้นต่ำด้านคุณภาพดังกล่าวเท่านั้น

สำหรับการทดสอบและสาธิตความสามารถของระบบ (Proof of Concept: POC) กพท.จะนัดหมายให้ผู้ยื่นข้อเสนอเข้าดำเนินการทดสอบและสาธิตความสามารถของระบบ ภายใน 5 วันทำการนับถัดจากวันเสนอราคา

คณะกรรมการฯ จะพิจารณาให้คะแนนด้านคุณภาพตามหลักเกณฑ์และรายละเอียดการประเมินที่กำหนด ดังนี้

6.2.1 แผนการดำเนินงาน (10 คะแนน)

ผู้ยื่นข้อเสนอต้องนำเสนอแผนการดำเนินงานที่จัดทำขึ้นและยื่นมาพร้อมข้อเสนอ โดยมีรายละเอียดสอดคล้องกับขอบเขตการดำเนินงานและระยะเวลาที่กำหนด

การให้คะแนนจะพิจารณาแยกตามรายการประเมินที่กำหนด ผู้ยื่นข้อเสนอต้องนำเสนอแผนการดำเนินงานที่มีรายละเอียดครบถ้วนตามรายการที่กำหนด จึงจะได้รับคะแนนเต็มของรายการนั้น หากไม่สามารถนำเสนอแผนการดำเนินงานได้ครบถ้วนตามรายการที่กำหนด ให้ 0 คะแนนในรายการนั้น โดยมีรายละเอียดและเกณฑ์การให้คะแนนดังนี้

รายการประเมิน	คะแนนเต็ม
1. แผนการจัดหา ติดตั้ง พัฒนา เชื่อมโยงระบบ และนำระบบขึ้นใช้งานจริง	4
2. แผนการให้บริการข่าวกรองภัยคุกคาม การเผยแพร่ข้อมูล และการสนับสนุนการดำเนินงาน TA-CERT	3
3. แผนการทดสอบระบบ การฝึกอบรม การส่งมอบงาน และการบริหารจัดการความเสี่ยงของโครงการ	3
รวม	**10**

6.2.2 ผลงานของผู้ยื่นข้อเสนอ (10 คะแนน)

พิจารณาจากจำนวนผลงานที่มีคุณสมบัติครบถ้วนตามข้อ 3.14 ของ TOR ดังนี้

จำนวนผลงาน	คะแนน
ตั้งแต่ 3 โครงการขึ้นไป	10
2 โครงการ	7
1 โครงการ	5

(นายวีระ ระบายศรี) ประธานกรรมการ (นางสาวอรรวรรณ ใจเอื้อ) กรรมการ (นาวาอากาศเอก กรเอก ชิษณุชาบุญวิภัค) กรรมการ (นายรักพิรุนห์ รุจิรวงษ์สกุล) กรรมการ (นายจักรพรรณ มีนคร) กรรมการ

6.2.4 การทดสอบและสาธิตความสามารถของระบบ (Proof of Concept: POC) (50 คะแนน)

ผู้ยื่นข้อเสนอต้องทดสอบและสาธิตความสามารถของระบบตามขั้นตอนและเงื่อนไขที่ กพท. กำหนด โดยแบ่งการประเมินออกเป็น 5 กิจกรรม กิจกรรมละ 10 คะแนน รวม 50 คะแนน

(1) การนำเสนอรูปจำลองการบริหารจัดการแหล่งข้อมูลภัยคุกคาม (Threat Intelligence) (10 คะแนน)

ผู้ยื่นข้อเสนอต้องสาธิตการทำงานของระบบบริหารจัดการแหล่งข้อมูลภัยคุกคาม โดยมีรายละเอียดและเกณฑ์การให้คะแนนดังนี้

โดยการให้คะแนนจะพิจารณาแยกตามรายการทดสอบที่กำหนด ผู้ยื่นข้อเสนอต้องสาธิตการทำงานได้ครบถ้วนตามรายการที่กำหนด จึงจะได้รับคะแนนเต็มของรายการนั้น หากไม่สามารถสาธิตได้ครบถ้วนตามรายการที่กำหนด ให้ 0 คะแนนในรายการนั้น

รายการที่ต้องสาธิต	คะแนน
1.1 แสดงภาพรวมคะแนนความมั่นคงปลอดภัยและรายละเอียดความเสี่ยงรายหน่วยงาน แสดงการแจ้งเตือนพร้อมจัดเรียงและคัดกรองตามระดับความรุนแรง และค้นหาสินทรัพย์ดิจิทัลพร้อมแสดงความเสี่ยงที่ตรวจพบ	5
1.2 ค้นหาข้อมูลจากฐานข้อมูล Threat Intelligence พร้อมคัดกรองตามเงื่อนไข แสดงข้อมูลการตรวจจับการละเมิดข้อมูลและเครื่องมือโจมตี และสร้างหรือส่งออกรายงานการแจ้งเตือนความเสี่ยงในรูปแบบ PDF และ CSV	5
รวม	**10**

(2) การสาธิตกระบวนการนำเข้าและแบ่งปันข้อมูลภัยคุกคาม (IOC) (10 คะแนน)

ผู้ยื่นข้อเสนอต้องสาธิตการนำเข้า บริหารจัดการ และแบ่งปัน IOC โดยสามารถควบคุมการแสดงข้อมูลตามสิทธิของผู้ใช้งานและปกปิดข้อมูลอ่อนไหวก่อนแบ่งปันให้หน่วยงานสมาชิกอื่น ทั้งนี้ สามารถใช้ข้อมูลทดสอบแทนข้อมูลจริงได้

โดยการให้คะแนนจะพิจารณาแยกตามรายการทดสอบที่กำหนด ผู้ยื่นข้อเสนอต้องสาธิตการทำงานได้ครบถ้วนตามรายการที่กำหนด จึงจะได้รับคะแนนเต็มของรายการนั้น หากไม่สามารถสาธิตได้ครบถ้วนตามรายการที่กำหนด ให้ 0 คะแนนในรายการนั้น

รายการที่ต้องสาธิต	คะแนน
2.1 ผู้ยื่นข้อเสนอต้องสาธิตการทำงานดังต่อไปนี้ (1) นำเข้าข้อมูล IOC เช่น IP Address, Domain, URL หรือ File Hash (2) แสดงข้อมูลต้นฉบับและข้อมูลอ่อนไหว และ (3) เลือกแบ่งปัน IOC ดังกล่าวเข้าสู่ระบบบริหารจัดการและแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์	5
2.2 ผู้ยื่นข้อเสนอต้องสาธิตการทำงานดังต่อไปนี้ (1) แสดงการแจ้งเตือนหรือรายการ IOC ที่หน่วยงานสมาชิกได้รับ (2) แสดงมุมมองของหน่วยงานสมาชิก โดยต้องปกปิดข้อมูลอ่อนไหวของผู้ส่ง และ (3) แสดงมุมมองของ TA-CERT โดยสามารถแสดงข้อมูลต้นฉบับได้ครบถ้วน	5
รวม	**10**

(3) การสาธิตความสามารถในการเชื่อมโยง (Correlate) ข้อมูลภัยคุกคาม (10 คะแนน)

ผู้ยื่นข้อเสนอต้องสาธิตการตรวจสอบและเชื่อมโยง IOC กับรายงานภัยคุกคามหรือแหล่งข้อมูล Threat Intelligence เพื่อประเมินความน่าเชื่อถือ ขอบเขต และผลกระทบของภัยคุกคาม โดยสามารถใช้ข้อมูลและแหล่งข้อมูลในระบบทดสอบหรือสภาพแวดล้อมจำลองได้

โดยการให้คะแนนจะพิจารณาแยกตามรายการทดสอบที่กำหนด ผู้ยื่นข้อเสนอต้องสาธิตการทำงานได้ครบถ้วนตามรายการที่กำหนด จึงจะได้รับคะแนนเต็มของรายการนั้น หากไม่สามารถสาธิตได้ครบถ้วนตามรายการที่กำหนด ให้ 0 คะแนนในรายการนั้น

(นายวีระ ระบายศรี)	(นางสาวอรรวรรณ ใจเอื้อ)	(นาวาอากาศเอก กรเอก ชิษณุชาบุญวิภัค)	(นายรักพิรุนห์ รุจิรวงษ์สกุล)	(นายจักรพรรณ มีนคร)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

รายการที่ต้องสาธิต	คะแนน
3.1 ผู้ยื่นข้อเสนอต้องสาธิตการทำงานดังต่อไปนี้ (1) เลือกหรือนำเข้าข้อมูล IOC ที่ต้องการทดสอบ (2) เชื่อมโยงข้อมูล IOC กับรายงานภัยคุกคามหรือแหล่งข้อมูล Threat Intelligence และ (3) แสดงแหล่งที่มาของข้อมูลพร้อมข้อมูลที่มีความสัมพันธ์กับ IOC	5
3.2 ผู้ยื่นข้อเสนอต้องสาธิตการทำงานดังต่อไปนี้ (1) แสดงผลว่า IOC เคยถูกตรวจพบหรือได้รับการยืนยันว่าเป็นภัยคุกคามหรือไม่ (2) แสดงประเภท ระดับความรุนแรง ขอบเขตหรือผลกระทบของภัยคุกคาม และ (3) นำผลการวิเคราะห์ไปจัดทำประกาศแจ้งเตือนหน่วยงานสมาชิก	5
รวม	**10**

(4) การสาธิตการแบ่งปัน IOC (10 คะแนน)

ผู้ยื่นข้อเสนอต้องสาธิตการรับ บริหารจัดการ คัดเลือก และส่งต่อ IOC ที่ได้รับการยืนยันแล้วไปยังระบบปลายทางที่กำหนด โดยสามารถใช้ระบบทดสอบหรือระบบจำลองแทนการเชื่อมต่อกับระบบจริงของหน่วยงานสมาชิกหรือ CERT อื่นได้

โดยการให้คะแนนจะพิจารณาแยกตามรายการทดสอบที่กำหนด ผู้ยื่นข้อเสนอต้องสาธิตการทำงานได้ครบถ้วนตามรายการที่กำหนด จึงจะได้รับคะแนนเต็มของรายการนั้น หากไม่สามารถสาธิตได้ครบถ้วนตามรายการที่กำหนด ให้ 0 คะแนนในรายการนั้น

รายการที่ต้องสาธิต	คะแนน
4.1 ผู้ยื่นข้อเสนอต้องสาธิตการทำงานดังต่อไปนี้ (1) รับหรือนำเข้าข้อมูล IOC ที่ได้รับการยืนยันแล้วเข้าสู่ระบบ (2) แสดงรายละเอียดของ IOC เช่น ประเภทข้อมูล แหล่งที่มา และสถานะการยืนยัน และ (3) ตรวจสอบหรือคัดเลือก IOC ที่ต้องการส่งต่อ	5
4.2 ผู้ยื่นข้อเสนอต้องสาธิตการทำงานดังต่อไปนี้ (1) การส่งต่อข้อมูล IOC ไปยังอุปกรณ์ความมั่นคงปลอดภัย(Security Device) ที่กำหนด และ (2) การแสดงผลการส่งต่อข้อมูล โดยต้องระบุสถานะการส่ง (สำเร็จ/ไม่สำเร็จ) วัน เวลา	5
รวม	**10**

(5) การนำเสนอรูปแบบและการใช้งานเว็บแอปพลิเคชัน TA-CERT (10 คะแนน)

ผู้ยื่นข้อเสนอต้องนำเสนอรูปแบบและการใช้งานเว็บแอปพลิเคชัน TA-CERT ในรูปแบบ Mockup หรือ Interactive Model เพื่อแสดงแนวทางการออกแบบ โครงสร้างเว็บไซต์ การนำเสนอข้อมูล และรูปแบบการใช้งาน โดยสามารถใช้ข้อมูลจำลองในการนำเสนอได้

โดยการให้คะแนนจะพิจารณาแยกตามรายการทดสอบที่กำหนด ผู้ยื่นข้อเสนอต้องสาธิตการทำงานได้ครบถ้วนตามรายการที่กำหนด จึงจะได้รับคะแนนเต็มของรายการนั้น หากไม่สามารถสาธิตได้ครบถ้วนตามรายการที่กำหนด ให้ 0 คะแนนในรายการนั้น

รายการที่ต้องสาธิต	คะแนนเต็ม
5.1 ผู้ยื่นข้อเสนอต้องนำเสนอดังต่อไปนี้ (1) หน้าหลักและโครงสร้างเมนูของเว็บไซต์ (2) ข้อมูลเกี่ยวกับ TA-CERT หน่วยงานสมาชิก ข่าวสาร ผลการดำเนินงาน และช่องทางติดต่อ	5
5.2 ผู้ยื่นข้อเสนอต้องนำเสนอดังต่อไปนี้ (1) Dashboard สถิติภัยคุกคามไซเบอร์ภาคการบินในรูปแบบกราฟหรือแผนภูมิ (2) แสดงการคัดกรองข้อมูลตามประเภทภัยคุกคาม ระดับความรุนแรง และช่วงเวลา (3) หน้าลงทะเบียนเข้าสู่ระบบ และ (4) แสดงรูปแบบหน้าจอสำหรับคอมพิวเตอร์และมือถือ	5
รวม	**10**

(นายวีระ ระบายศรี) ประธานกรรมการ | (นางสาวอรรวรรณ ใจเอื้อ) กรรมการ | (นาวาอากาศเอก กรเอก ชิษณุชาบุญวิภัค) กรรมการ | (นายรักพิรุนห์ รุจิรวงษ์สกุล) กรรมการ | (นายจักรพรรณ มีนคร) กรรมการ

6.2.4 ข้อเสนออื่น ๆ (10 คะแนน)

ผู้ยื่นข้อเสนอสามารถเสนอการจัดทำคู่มือแนวทางการรับมือเหตุการณ์ภัยคุกคามไซเบอร์ (Cybersecurity Incident Response Playbook) สำหรับหน่วยงานสมาชิก TA-CERT เพิ่มเติมจากขอบเขตงานที่กำหนด โดยไม่มีค่าใช้จ่ายเพิ่มเติม ซึ่งแต่ละฉบับต้องเป็นสถานการณ์ภัยคุกคามไซเบอร์ที่แตกต่างกัน

ผู้ยื่นข้อเสนอต้องระบุชื่อสถานการณ์ภัยคุกคามไซเบอร์ที่จะจัดทำคู่มือ พร้อมเสนอรายละเอียดอย่างน้อย ได้แก่ (1) ลักษณะของเหตุการณ์และผลกระทบที่อาจเกิดขึ้น (2) แนวทางการตรวจสอบและประเมินความรุนแรงของเหตุการณ์ (3) ขั้นตอนการรับมือ ควบคุมเหตุการณ์ และฟื้นฟูระบบ และ (4) รูปแบบและองค์ประกอบของคู่มือ โดยต้องประกอบด้วยขั้นตอนการรับมือเหตุการณ์ แผนผังลำดับขั้นตอนการดำเนินงาน (Workflow) และรายการตรวจสอบ (Checklist) เพื่อใช้ประกอบการดำเนินงานในแต่ละขั้นตอน โดยมีหลักเกณฑ์การให้คะแนนดังนี้

รายการประเมิน	คะแนน
1. เสนอจัดทำ Cybersecurity Incident Response Playbook เพิ่มเติมอย่างน้อย 2 ฉบับ โดยมีรายละเอียดครบถ้วนตามที่กำหนด	5
2. เสนอจัดทำ Cybersecurity Incident Response Playbook เพิ่มเติมอย่างน้อย 4 ฉบับ โดยมีรายละเอียดครบถ้วนตามที่กำหนด	10

7. วงเงินงบประมาณ

งบประมาณ จำนวน 35,000,000.00 บาท (สามสิบห้าล้านบาทถ้วน) ซึ่งได้รวมภาษีมูลค่าเพิ่ม และค่าใช้จ่ายอื่นทั้งปวงไว้ด้วยแล้ว งบประมาณผูกพันข้ามปีงบประมาณ พ.ศ. 2569 – 2571 วงเงินรวมทั้งสิ้น 35,000,000.00 บาท (สามสิบห้าล้านบาทถ้วน) โดยมีรายละเอียดการจัดสรรงบประมาณในแต่ละปี ดังนี้

1) ปีงบประมาณ พ.ศ. 2569 จำนวน 5,250,000.00 บาท
2) ปีงบประมาณ พ.ศ. 2570 จำนวน 15,750,000.00 บาท
3) ปีงบประมาณ พ.ศ. 2571 จำนวน 14,000,000.00 บาท

8. งวดงานและการจ่ายเงิน

สำนักงานการบินพลเรือนแห่งประเทศไทยจะจ่ายเงินค่าจ้างให้แก่ผู้รับจ้าง เมื่อผู้รับจ้างได้ส่งมอบระบบตามขอบเขตของงาน ข้อ 5 เรียบร้อยแล้ว โดยแบ่งออกเป็น 9 งวด ดังนี้

งวดที่ 1 เป็นจำนวนเงินในอัตราร้อยละ 15 ของวงเงินตามสัญญาทั้งหมด เมื่อผู้รับจ้างได้ปฏิบัติงานในเดือนที่ 1 - 3 โดยมีรายละเอียดดังต่อไปนี้

- ผู้รับจ้างจะต้องจัดการฝึกอบรมการใช้งานและบริหารจัดการระบบ พร้อมทั้งจัดทำรายงานผลการอบรม รายละเอียดตามขอบเขตของงานข้อ 4.5.2 (1) - (2)
- รายงานผลการวิเคราะห์ความต้องการ โครงสร้างสถาปัตยกรรมเว็บแอปพลิเคชัน พร้อมผลการออกแบบเชิงแนวคิด (Conceptual Design) และภาพจำลองหน้าจอ (Mock-up) ของการพัฒนา TA-CERT Web Application (ตามข้อกำหนดในข้อ 4.4 และภาคผนวก 3)
- รายงานผลดำเนินการพัฒนา TA-CERT Web Application (รายละเอียดตามข้อ 4.4 และภาคผนวก 3)
- ร่างกรอบการดำเนินงานและทิศทางการสื่อสารของ TA-CERT ตามข้อ 4.6.1
- ร่างอัตลักษณ์ของ TA-CERT (Brand Identity) ตามข้อ 4.6.2
- จัดทำรายงานผลการดำเนินงานรายเดือน และรายงานสรุปประจำงวดงาน (รายละเอียดตามข้อ 4.3)

(นายวีระ ระบายศรี)	(นางสาวอรรวรรณ ใจเอื้อ)	(นาวาอากาศเอก กรเอก ชิษณุชาบุญวิภัค)	(นายรักพิรุนห์ รุจิรวงษ์สกุล)	(นายจักรพรรณ มีนคร)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

- รายงานผลนำเข้าข้อมูล Indicators of Compromise (IOC) เข้าสู่แพลตฟอร์มบริหารจัดการ สำหรับการจัดเก็บ รวบรวม วิเคราะห์ และแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ (รายละเอียดตามข้อ 4.3.8)

- จัดทำรายงานผลการปฏิบัติงานของบุคลากร (Operation และ Specialist Team) (รายละเอียดตามข้อ 4.5.4 (2))

โดยผู้รับจ้างจะต้องส่งมอบให้แก่ กพท. ในรูปแบบเอกสารและไฟล์เอกสาร (USB Drive) จำนวน 1 ชุด และคณะกรรมการตรวจรับได้ทำการตรวจรับงานจ้างเรียบร้อยแล้ว

งวดที่ 2 เป็นจำนวนเงินในอัตราร้อยละ 15 ของวงเงินตามสัญญาทั้งหมด เมื่อผู้รับจ้างได้ปฏิบัติงานในเดือนที่ 4 – 7 โดยมีรายละเอียดดังต่อไปนี้

- รายงานผลการ ทดสอบ และปรับปรุง TA-CERT Web Application ให้แล้วเสร็จครบถ้วน (รายละเอียดตามข้อ 4.4 และ ภาคผนวก 3)

- ส่งมอบ TA-CERT Web Application อย่างเป็นทางการ พร้อมเอกสารประกอบระบบ (รายละเอียดตามข้อ 4.4 และ ภาคผนวก 3) นับถัดจากวันลงนามในสัญญา

- ส่งมอบซอร์สโค้ดของเว็บแอปพลิเคชันของ TA-CERT ครั้งที่ 1 พร้อมโครงสร้างฐานข้อมูลและเอกสารประกอบการติดตั้ง (รายละเอียดตามข้อ 4.4.7 (1))

- ผู้รับจ้างจะต้องจัดการฝึกอบรมการใช้งาน TA-CERT Web Application พร้อมทั้งจัดทำรายงานผลการอบรม (รายละเอียดตามข้อ 4.5.2 (3))

- กรอบการดำเนินงานและทิศทางการสื่อสารของ TA-CERT ฉบับสมบูรณ์ ตามข้อ 4.6.1

- อัตลักษณ์ของ TA-CERT (Brand Identity) และสื่อประชาสัมพันธ์ดิจิทัลฉบับสมบูรณ์ ตามข้อ 4.6.2 พร้อมไฟล์ต้นฉบับที่สามารถแก้ไขได้

- จัดทำรายงานผลการดำเนินงานรายเดือน และรายงานสรุปประจำงวดงาน (รายละเอียดตามข้อ 4.3)

- จัดทำและเผยแพร่ข่าวสารด้านความมั่นคงปลอดภัยไซเบอร์ (รายละเอียดตามข้อ 4.3.5)

- รายงานผลนำเข้าข้อมูล Indicators of Compromise (IOC) เข้าสู่แพลตฟอร์มบริหารจัดการ สำหรับการจัดเก็บ รวบรวม วิเคราะห์ และแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ (รายละเอียดตามข้อ 4.3.8)

- จัดทำรายงานผลการปฏิบัติงานของบุคลากร (Operation และ Specialist Team) (รายละเอียดตามข้อ 4.5.4 (2))

- รายงานผลการประเมินระดับศักยภาพ (Maturity Assessment) รอบที่ 1 พร้อมผลการวิเคราะห์ช่องว่าง (Gap Analysis) เป้าหมายระดับศักยภาพ และแผนการยกระดับศักยภาพ (Improvement Plan) (รายละเอียดตามข้อ 4.5.5 (1))

โดยผู้รับจ้างจะต้องส่งมอบให้แก่ กพท. ในรูปแบบเอกสารและไฟล์เอกสาร (USB Drive) จำนวน 1 ชุด และคณะกรรมการตรวจรับได้ทำการตรวจรับงานจ้างเรียบร้อยแล้ว

งวดที่ 3 เป็นจำนวนเงินในอัตราร้อยละ 10 ของวงเงินตามสัญญาทั้งหมด เมื่อผู้รับจ้างได้ปฏิบัติงานในเดือนที่ 8 – 10 โดยมีรายละเอียดดังต่อไปนี้

- จัดทำรายงานผลการดำเนินงานรายเดือน และรายงานสรุปประจำงวดงาน (รายละเอียดตามข้อ 4.3)

- จัดทำและเผยแพร่ข่าวสารด้านความมั่นคงปลอดภัยไซเบอร์ (รายละเอียดตามข้อ 4.3.5)

- รายงานผลนำเข้าข้อมูล Indicators of Compromise (IOC) เข้าสู่แพลตฟอร์มบริหารจัดการ สำหรับการจัดเก็บ รวบรวม วิเคราะห์ และแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ (รายละเอียดตามข้อ 4.3.8)

- จัดทำรายงานผลการปฏิบัติงานของบุคลากร (Operation และ Specialist Team) (รายละเอียดตามข้อ 4.5.4 (2))

(นายวีระ ระบายศรี) ประธานกรรมการ (นางสาวอรรวรรณ ใจเอื้อ) กรรมการ (นาวาอากาศเอก กรเอก ชิษณุชาบุญวิภัค) กรรมการ (นายรักพิรุนห์ รุจิรวงษ์สกุล) กรรมการ (นายจักรพรรณ มีนคร) กรรมการ

โดยผู้รับจ้างจะต้องส่งมอบให้แก่ กพท. ในรูปแบบเอกสารและไฟล์เอกสาร (USB Drive) จำนวน 1 ชุด และคณะกรรมการตรวจรับได้ทำการตรวจรับงานจ้างเรียบร้อยแล้ว

งวดที่ 4 เป็นจำนวนเงินในอัตราร้อยละ 10 ของวงเงินตามสัญญาทั้งหมด เมื่อผู้รับจ้างได้ปฏิบัติงานในเดือนที่ 11 – 13 โดยมีรายละเอียดดังต่อไปนี้

- จัดทำรายงานผลการดำเนินงานรายเดือน และรายงานสรุปประจำงวดงาน (รายละเอียดตามข้อ 4.3)
- จัดทำและเผยแพร่ข่าวสารด้านความมั่นคงปลอดภัยไซเบอร์ (รายละเอียดตามข้อ 4.3.5)
- รายงานผลนำเข้าข้อมูล Indicators of Compromise (IOC) เข้าสู่แพลตฟอร์มบริหารจัดการ สำหรับการจัดเก็บ รวบรวม วิเคราะห์ และแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ (รายละเอียดตามข้อ 4.3.8)
- จัดทำรายงานผลการปฏิบัติงานของบุคลากร (Operation และ Specialist Team) (รายละเอียดตามข้อ 4.5.4 (2))
- รายงานการฝึกอบรมหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์ระดับผู้เชี่ยวชาญ (รายละเอียดตามข้อ 4.5.1 (1))
- จัดทำรายงานผลการดำเนินงานประจำปี (Annual Report) ปีที่ 1 (รายละเอียดตามข้อ 4.6.3)
- รายงานผลการประเมินระดับศักยภาพ (Maturity Assessment) รอบที่ 1 พร้อมผลการวิเคราะห์ช่องว่าง (Gap Analysis) และการเปรียบเทียบกับเป้าหมายที่กำหนด (รายละเอียดตามข้อ 4.5.5 (1))

โดยผู้รับจ้างจะต้องส่งมอบให้แก่ กพท. ในรูปแบบเอกสารและไฟล์เอกสาร (USB Drive) จำนวน 1 ชุด และคณะกรรมการตรวจรับได้ทำการตรวจรับงานจ้างเรียบร้อยแล้ว

งวดที่ 5 เป็นจำนวนเงินในอัตราร้อยละ 10 ของวงเงินตามสัญญาทั้งหมด เมื่อผู้รับจ้างได้ปฏิบัติงานในเดือนที่ 14–16 โดยมีรายละเอียดดังต่อไปนี้

- จัดทำรายงานผลการดำเนินงานรายเดือน และรายงานสรุปประจำงวดงาน (รายละเอียดตามข้อ 4.3)
- จัดทำและเผยแพร่ข่าวสารด้านความมั่นคงปลอดภัยไซเบอร์ (รายละเอียดตามข้อ 4.3.5)
- รายงานผลนำเข้าข้อมูล Indicators of Compromise (IOC) เข้าสู่แพลตฟอร์มบริหารจัดการ สำหรับการจัดเก็บ รวบรวม วิเคราะห์ และแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ (รายละเอียดตามข้อ 4.3.8)
- จัดทำรายงานผลการปฏิบัติงานของบุคลากร (Operation และ Specialist Team) (รายละเอียดตามข้อ 4.5.4 (2))
- จัดทำรายงานผลการฝึกซ้อมและข้อเสนอแนะ (รายละเอียดตามข้อ 4.5.3 (5))

โดยผู้รับจ้างจะต้องส่งมอบให้แก่ กพท. ในรูปแบบเอกสารและไฟล์เอกสาร (USB Drive) จำนวน 1 ชุด และคณะกรรมการตรวจรับได้ทำการตรวจรับงานจ้างเรียบร้อยแล้ว

งวดที่ 6 เป็นจำนวนเงินในอัตราร้อยละ 10 ของวงเงินตามสัญญาทั้งหมด เมื่อผู้รับจ้างได้ปฏิบัติงานในเดือนที่ 17 – 19 โดยมีรายละเอียดดังต่อไปนี้

- จัดทำรายงานผลการดำเนินงานรายเดือน และรายงานสรุปประจำงวดงาน (รายละเอียดตามข้อ 4.3)
- จัดทำและเผยแพร่ข่าวสารด้านความมั่นคงปลอดภัยไซเบอร์ (รายละเอียดตามข้อ 4.3.5)
- รายงานผลนำเข้าข้อมูล Indicators of Compromise (IOC) เข้าสู่แพลตฟอร์มบริหารจัดการ สำหรับการจัดเก็บ รวบรวม วิเคราะห์ และแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ (รายละเอียดตามข้อ 4.3.8)
- จัดทำรายงานผลการปฏิบัติงานของบุคลากร (Operation และ Specialist Team) (รายละเอียดตามข้อ 4.5.4 (2))

(นายวีระ ระบายศรี)	(นางสาวอรรวรรณ ใจเอื้อ)	(นาวาอากาศเอก กรเอก ชิษณุชาบุญวิภัค)	(นายรักพิรุนห์ รุจิรวงษ์สกุล)	(นายจักรพรรณ มีนคร)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

โดยผู้รับจ้างจะต้องส่งมอบให้แก่ กพท. ในรูปแบบเอกสารและไฟล์เอกสาร (USB Drive) จำนวน 1 ชุด และคณะกรรมการตรวจรับได้ทำการตรวจรับงานจ้างเรียบร้อยแล้ว

งวดที่ 7 เป็นจำนวนเงินในอัตราร้อยละ 10 ของวงเงินตามสัญญาทั้งหมด เมื่อผู้รับจ้างได้ปฏิบัติงานในเดือนที่ 20 – 22 โดยมีรายละเอียดดังต่อไปนี้

- จัดทำรายงานผลการดำเนินงานรายเดือน และรายงานสรุปประจำงวดงาน (รายละเอียดตามข้อ 4.3)
- จัดทำและเผยแพร่ข่าวสารด้านความมั่นคงปลอดภัยไซเบอร์ (รายละเอียดตามข้อ 4.3.5)
- รายงานผลนำเข้าข้อมูล Indicators of Compromise (IOC) เข้าสู่แพลตฟอร์มบริหารจัดการ สำหรับการจัดเก็บ รวบรวม วิเคราะห์ และแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ (รายละเอียดตามข้อ 4.3.8)
- จัดทำรายงานผลการปฏิบัติงานของบุคลากร (Operation และ Specialist Team) (รายละเอียดตามข้อ 4.5.4 (2))

โดยผู้รับจ้างจะต้องส่งมอบให้แก่ กพท. ในรูปแบบเอกสารและไฟล์เอกสาร (USB Drive) จำนวน 1 ชุด และคณะกรรมการตรวจรับได้ทำการตรวจรับงานจ้างเรียบร้อยแล้ว

งวดที่ 8 เป็นจำนวนเงินในอัตราร้อยละ 10 ของวงเงินตามสัญญาทั้งหมด เมื่อผู้รับจ้างได้ปฏิบัติงานในเดือนที่ 23 – 25 โดยมีรายละเอียดดังต่อไปนี้

- จัดทำรายงานผลการดำเนินงานรายเดือน และรายงานสรุปประจำงวดงาน (รายละเอียดตามข้อ 4.3)
- จัดทำและเผยแพร่ข่าวสารด้านความมั่นคงปลอดภัยไซเบอร์ (รายละเอียดตามข้อ 4.3.5)
- รายงานผลนำเข้าข้อมูล Indicators of Compromise (IOC) เข้าสู่แพลตฟอร์มบริหารจัดการ สำหรับการจัดเก็บ รวบรวม วิเคราะห์ และแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ (รายละเอียดตามข้อ 4.3.8)
- จัดทำรายงานผลการปฏิบัติงานของบุคลากร (Operation และ Specialist Team) (รายละเอียดตามข้อ 4.5.4 (2))
- จัดทำรายงานผลการดำเนินงานประจำปี (Annual Report) ปีที่ 2 (รายละเอียดตามข้อ 4.6.3)
- รายงานผลการประเมินระดับศักยภาพ (Maturity Assessment) รอบที่ 2 พร้อมผลการวิเคราะห์ช่องว่าง (Gap Analysis) และการเปรียบเทียบกับเป้าหมายที่กำหนด (รายละเอียดตามข้อ 4.5.5 (2))

โดยผู้รับจ้างจะต้องส่งมอบให้แก่ กพท. ในรูปแบบเอกสารและไฟล์เอกสาร (USB Drive) จำนวน 1 ชุด และคณะกรรมการตรวจรับได้ทำการตรวจรับงานจ้างเรียบร้อยแล้ว

งวดที่ 9 เป็นจำนวนเงินในอัตราร้อยละ 10 ของวงเงินตามสัญญาทั้งหมด เมื่อผู้รับจ้างได้ปฏิบัติงานในเดือนที่ 26 – 28 โดยมีรายละเอียดดังต่อไปนี้

- จัดทำรายงานผลการดำเนินงานรายเดือน และรายงานสรุปประจำงวดงาน (รายละเอียดตามข้อ 4.3)
- จัดทำและเผยแพร่ข่าวสารด้านความมั่นคงปลอดภัยไซเบอร์ (รายละเอียดตามข้อ 4.3.5)
- รายงานผลนำเข้าข้อมูล Indicators of Compromise (IOC) เข้าสู่แพลตฟอร์มบริหารจัดการ สำหรับการจัดเก็บ รวบรวม วิเคราะห์ และแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ (รายละเอียดตามข้อ 4.3.8)
- จัดทำรายงานผลการปฏิบัติงานของบุคลากร (Operation และ Specialist Team) (รายละเอียดตามข้อ 4.5.4 (2))
- จัดทำรายงานสรุปผลการดำเนินโครงการ (Final Report)

(นายวีระ ระบายศรี)	(นางสาวอรรวรรณ ใจเอื้อ)	(นาวาอากาศเอก กรเอก ชิษณุชาบุญวิภัค)	(นายรักพิรุนห์ รุจิรวงษ์สกุล)	(นายจักรพรรณ มีนคร)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

- จัดทำแผนพัฒนาศักยภาพ TA-CERT (Roadmap) ระยะไม่น้อยกว่า 3 ปี และจัดทำ Dashboard สรุปผลการประเมินระดับศักยภาพ (รายละเอียดตามข้อ 4.5.5 (2.4 – 2.5))

- ส่งมอบซอร์สโค้ดฉบับสมบูรณ์ล่าสุด พร้อมหนังสือรับรองความตรงกันกับระบบที่ใช้งานจริง (รายละเอียดตามข้อ 4.4.7)

- ถ่ายทอดองค์ความรู้ให้เจ้าหน้าที่ กพท. และส่งมอบหนังสือรับรองการลบข้อมูล (Certificate of Data Destruction) (ถ้ามี)

โดยผู้รับจ้างจะต้องส่งมอบให้แก่ กพท. ในรูปแบบเอกสารและไฟล์เอกสาร (USB Drive) จำนวน 1 ชุด และคณะกรรมการตรวจรับได้ทำการตรวจรับงานจ้างเรียบร้อยแล้ว

9. การรับประกันความชำรุดบกพร่อง

ผู้ยื่นข้อเสนอซึ่งได้ทำสัญญาจ้าง หรือข้อตกลงเป็นหนังสือ จะต้องรับประกันความชำรุดบกพร่องของงานที่เกิดขึ้นภายในระยะเวลาไม่น้อยกว่า 1 ปี นับถัดจากวันที่สำนักงาน ได้รับมอบงานงวดสุดท้ายและคณะกรรมการตรวจรับได้ดำเนินการตรวจรับพัสดุเรียบร้อยแล้ว โดยต้องรีบจัดการซ่อมแซมแก้ไขให้ใช้การได้ดีดังเดิมภายใน 2 วัน นับถัดจากวันที่ได้รับแจ้งความชำรุดบกพร่อง

10. อัตราค่าปรับ

ค่าปรับตามสัญญาจ้างหรือข้อตกลงจ้างเป็นหนังสือจะกำหนด ดังนี้

10.1 กรณีผู้รับจ้างนำงานที่รับจ้างช่วงให้ผู้อื่นทำอีกทอดหนึ่งโดยไม่ได้รับอนุญาตจากสำนักงานจะกำหนดค่าปรับสำหรับการฝ่าฝืนดังกล่าวเป็นจำนวนร้อยละ 10 ของวงเงินของงานจ้างช่วงนั้น

10.2 กรณีผู้รับจ้างปฏิบัติผิดสัญญาจ้าง นอกเหนือจากข้อ 10.1 จะกำหนดค่าปรับแป็นรายวันเป็นจำนวนเงินตายตัวในอัตราร้อยละ 0.10 ของราคางานจ้าง แต่ต้องไม่ต่ำกว่าวันละ 100 บาท

10.3 หากระบบในโครงการยกระดับศักยภาพการดำเนินงานศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคการบิน (TA-CERT) ไม่สามารถใช้งานได้ทั้งหมดหรือบางส่วน โดยที่ผู้รับจ้างไม่สามารถแก้ไขให้แล้วเสร็จ ตามข้อ 4.8 หลังจากได้รับแจ้งจาก กพท. ผู้รับจ้างจะต้องจ่ายค่าปรับให้แก่ กพท. เป็นรายชั่วโมงในอัตราร้อยละ 0.035 ของราคาค่าจ้างตามสัญญา ในช่วงเวลาที่ไม่สามารถใช้งานได้ในส่วนที่เกินกว่ากำหนด

11. ข้อตกลงห้ามเปิดเผยข้อมูล

ข้อมูล เอกสาร หรือสัญญาที่เกี่ยวข้องกับโครงการนี้ทั้งหมดที่ กพท. จัดหาให้ หรือผู้ยื่นข้อเสนอดำเนินการและจัดหาให้ กพท. ถือเป็นความลับ และเป็นสมบัติของ กพท. โดยผู้ยื่นข้อเสนอต้องไม่เปิดเผยข้อมูลและผลการดำเนินการให้แก่ผู้ใด ยกเว้นแต่จะได้รับอนุญาตจาก กพท. เป็นลายลักษณ์อักษร หากผู้ยื่นข้อเสนอละเมิดโดยมีการนำไปเผยแพร่ และเปิดเผยโดยไม่ได้รับอนุญาต กพท. มีสิทธิ์ฟ้องร้องเรียกค่าเสียหายและดำเนินการตามกฎหมายได้

12. ความคุ้มครองเกี่ยวกับลิขสิทธิ์

ในกรณีที่บุคคลภายนอกกล่าวอ้างหรือใช้สิทธิเรียกร้องใด ๆ ว่ามีการละเมิดลิขสิทธิ์เกี่ยวกับงานจ้างตามสัญญานี้ โดย กพท. มิได้แก้ไขดัดแปลงไปจากเดิม ผู้ยื่นข้อเสนอจะต้องดำเนินการทั้งปวงเพื่อให้การกล่าวอ้างหรือการเรียกร้องดังกล่าวระงับสิ้นไปโดยเร็ว เพื่อให้ กพท. สามารถใช้งานจ้างนั้นต่อไปได้ หากผู้ยื่นข้อเสนอมิอาจกระทำได้และ กพท. ต้องรับผิดชอบชดใช้ค่าเสียหายต่อบุคคลภายนอก เนื่องจากผลแห่งการละเมิดลิขสิทธิ์ดังกล่าว ผู้ยื่นข้อเสนอต้องเป็นผู้ชำระค่าเสียหาย ค่าปรับและค่าใช้จ่ายอื่น ๆ รวมทั้งค่าธรรมเนียม และค่าทนายความ ทั้งนี้ กพท. จะแจ้งผู้ยื่นข้อเสนอทราบเป็นลายลักษณ์อักษรในเมื่อได้มีการกล่าวอ้างหรือใช้สิทธิเรียกร้องดังกล่าว โดยไม่ชักช้า

(นายวีระ ระบายศรี)	(นางสาวอรรวรรณ ใจเอื้อ)	(นาวาอากาศเอก กรเอก ชิษณุชาบุญวิภัค)	(นายรักพิรุนห์ รุจิรวงษ์สกุล)	(นายจักรพรรณ มีนคร)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

13. เงื่อนไขอื่น ๆ

13.1 ผู้ยื่นข้อเสนอต้องปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ นโยบายคุ้มครองข้อมูลส่วนบุคคล และประมวลแนวทางปฏิบัติและกรอบมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ของ กพท. รวมถึงกฎหมาย นโยบาย คำสั่งและขั้นตอนปฏิบัติอื่น ๆ ที่เกี่ยวข้อง

13.2 ในกรณีที่ผู้ยื่นข้อเสนอได้รับอนุญาตจาก กพท. ให้ว่าจ้าง มอบหมาย หรือแต่งตั้งผู้ให้บริการช่วง ผู้รับจ้างช่วง หรือผู้ประมวลผลข้อมูลช่วง ผู้ยื่นข้อเสนอต้องกำหนดให้บุคคลดังกล่าวปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ นโยบายคุ้มครองข้อมูลส่วนบุคคล และประมวลแนวทางปฏิบัติและกรอบมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ของ กพท. รวมถึงนโยบาย คำสั่งและขั้นตอนปฏิบัติอื่น ๆ ที่เกี่ยวข้อง

13.3 ผู้ยื่นข้อเสนอต้องใช้พัสดุที่ผลิตภายในประเทศ โดยต้องใช้ไม่น้อยกว่าร้อยละ 60 ของมูลค่าพัสดุที่จะใช้ในงานจ้างทั้งหมดตามสัญญา

13.4 ผู้ยื่นข้อเสนอต้องจัดทำแผนการใช้พัสดุที่ผลิตภายในประเทศ โดยยื่นให้แก่ผู้ว่าจ้างภายใน 60 วัน นับถัดจากวันลงนามในสัญญา

13.5 ผู้ยื่นข้อเสนอจะต้องจัดทำและนำเสนอ แผนการดำเนินงานโครงการทั้งหมด โดยมีรายละเอียดครบถ้วน เพื่อให้ กพท. พิจารณาและให้ความเห็นชอบ ภายใน 15 วันนับถัดจากวันลงนามในสัญญา

14. หน่วยงานผู้รับผิดชอบโครงการ

ฝ่ายบริหารเทคโนโลยีดิจิทัล กองพัฒนามาตรฐานการจัดการและความปลอดภัยไซเบอร์ สำนักงานการบินพลเรือนแห่งประเทศไทย เลขที่ 222 ซอยวิภาวดีรังสิต 28 ถนนวิภาวดีรังสิต แขวงจตุจักร เขตจตุจักร กรุงเทพมหานคร 10900 โทรศัพท์ 02 568 8809 อีเมล์ itd_is@caat.or.th

(นายวีระ ระบายศรี)	(นางสาวอรรวรรณ ใจเอื้อ)	(นาวาอากาศเอก กรเอก ชิษณุชาบุญวิภัค)	(นายรักพิรุนห์ รุจิรวงษ์สกุล)	(นายจักรพรรณ มีนคร)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

ภาคผนวก 1

ระบบบริหารจัดการและแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์

ผู้ยื่นข้อเสนอต้องจัดให้มีระบบสำหรับบริหารจัดการและแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ เพื่อสนับสนุนการรับ รวบรวม จัดเก็บ บริหารจัดการ และแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ รวมถึง Indicators of Compromise (IOC) โดยมีคุณสมบัติและความสามารถอย่างน้อยดังนี้

1. ผู้รับจ้างต้องจัดเตรียมทรัพยากรและโครงสร้างพื้นฐานสำหรับการติดตั้งและให้บริการแพลตฟอร์มบริหารจัดการ สำหรับการจัดเก็บ รวบรวม วิเคราะห์ และแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ ที่มีความมั่นคงปลอดภัยสูงตลอดระยะเวลาสัญญา จำนวนอย่างน้อย 1 Node โดยมีสถาปัตยกรรมระบบอย่างน้อยดังนี้

1.1 ติดตั้งบนระบบ Cloud ที่มีความมั่นคงปลอดภัยและเป็นไปตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2568 (หรือฉบับล่าสุด)

1.2 ทำหน้าที่เป็น Node หลักสำหรับเชื่อมต่อเพื่อแลกเปลี่ยนข้อมูล กับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และให้บริการแก่หน่วยงานสมาชิก TA-CERT รวมถึงเชื่อมต่อข้อมูลไปยัง Node ภายในของ กพท.

1.3 ระบบสามารถรองรับการประมวลผลข้อมูลจำนวนมาก (Correlation) ผู้รับจ้างต้องจัดหาทรัพยากร Cloud ที่มีคุณลักษณะทางเทคนิคขั้นต่ำ ดังนี้

- หน่วยประมวลผล (vCPU) ไม่น้อยกว่า 8 vCPU
- หน่วยความจำ (RAM) ไม่น้อยกว่า 32 GB
- พื้นที่จัดเก็บข้อมูล (Storage) ไม่น้อยกว่า 1 TB (รองรับการขยายตัวของข้อมูลตลอดอายุสัญญา)

2. ผู้รับจ้างต้องตั้งค่าโดเมนและความปลอดภัย (Domain and Security Configuration) อย่างน้อยดังนี้

2.1 ตั้งค่าการใช้งานระบบภายใต้ชื่อโดเมนย่อย (Sub-domain) ของ caat.or.th ตามที่ กพท. กำหนด

2.2 ดำเนินการติดตั้งและบริหารจัดการใบรับรองความปลอดภัย (SSL/TLS Certificate) ให้กับโดเมนดังกล่าวให้มีความปลอดภัยและเป็นปัจจุบันตลอดระยะเวลาสัญญา

3. แพลตฟอร์มที่นำเสนอต้องมีคุณสมบัติด้านการแลกเปลี่ยนและวิเคราะห์ข้อมูลอย่างน้อยดังนี้

3.1 ต้องสามารถเชื่อมต่อและแลกเปลี่ยนข้อมูลกับระบบ MISP ของ สกมช. ได้

3.2 ผู้รับจ้างต้องติดตั้ง กำหนดค่า และปรับแต่งแพลตฟอร์มให้มีการแสดงผล Dashboard ตรงตามความต้องการของ กพท.

3.3 สามารถรับข้อมูลสัญญาณบ่งชี้การบุกรุก (Indicator of Compromise) ภัยคุกคามทางไซเบอร์จากหน่วยงานภายนอกได้อัตโนมัติ

3.4 สามารถเพิ่มข้อมูลสัญญาณบ่งชี้การบุกรุก (Indicator of Compromise) ได้เอง

3.5 สามารถกำหนดระดับชั้นของข้อมูล Traffic Light Protocol (TLP) ของเหตุการณ์ได้

(นายวีระ ระบายศรี)	(นางสาวอรรวรรณ ใจเอื้อ)	(นาวาอากาศเอก กรเอก ชิษณุชาบุญวิภัค)	(นายรักพิรุนห์ รุจิรวงษ์สกุล)	(นายจักรพรรณ มีนคร)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

3.6 รองรับการส่งข้อมูลสัญญาณบ่งชี้การบุกรุก (Indicator of Compromise) ภัยคุกคามทางไซเบอร์ไปยังหน่วยงานสมาชิกของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคการบิน (Thailand Aviation - Computer Emergency Response Team : TA-CERT)

3.7 สัญญาณบ่งชี้การบุกรุก (Indicator of Compromise) ต้องรองรับข้อมูลอย่างน้อย ดังนี้

(1) ข้อมูล IP Address

(2) ข้อมูล Hash

(3) ข้อมูลชื่อโดเมน

(4) ข้อมูลชื่อไฟล์

(5) โดยต้องทำการปกปิดข้อมูลที่สามารถระบุตัวตนขององค์กรได้ เช่น IP, ชื่อองค์กร. ชื่อผู้ใช้งานเป็นต้น

3.8 สามารถหาความสัมพันธ์ระหว่าง สัญญาณบ่งชี้การบุกรุก (Indicator of Compromise) ได้อัตโนมัติ

3.9 สามารถนำข้อมูลออก (Export) ด้วยรูปแบบอย่างน้อย ดังนี้ STIX, PDF, plain text, CSV, JSON.

3.10 สามารถนำข้อมูลเข้า (Import) ด้วยรูปแบบอย่างน้อยดังนี้ STIX, PDF, plain text, CSV, JSON.

3.11 ระบบต้องสามารถบริหารจัดการผู้ใช้งานและสิทธิ์การเข้าถึงอย่างน้อยดังนี้

(1) สามารถสร้างและบริหารจัดการบัญชีผู้ใช้งานได้ไม่จำกัดจำนวน

(2) สามารถบริหารจัดการสิทธิ์การเข้าถึงข้อมูลในระดับองค์กร และระดับบัญชีผู้ใช้งานได้อย่างละเอียด เพื่อควบคุมการมองเห็นและใช้งานข้อมูล

(3) รองรับการยืนยันตัวตนแบบหลายปัจจัย (2-Factor Authentication : 2FA) เป็นอย่างน้อย

3.12 รองรับการเชื่อมต่อผ่านช่องทาง API, STIX, TAXII ได้กับหน่วยงานสมาชิก TA-CERT

3.13 รองรับการสนับสนุนการเชื่อมต่อสำหรับหน่วยงานสมาชิกที่ต้องการเชื่อมต่อ (Member Node Connectivity Support) โดยผู้รับจ้างต้องให้การสนับสนุนทางเทคนิค สมาชิกของศูนย์ฯ ในกรณีที่หน่วยงานดังกล่าวมีความประสงค์จะจัดตั้งระบบ MISP เป็นของตนเอง (Member Node) และต้องการเชื่อมต่อเพื่อแลกเปลี่ยนข้อมูลกับระบบ MISP บน Node ของศูนย์ฯ โดยผู้รับจ้างต้องสนับสนุนตั้งแต่ขั้นตอนการตั้งค่าการเชื่อมต่อ การทดสอบการรับส่งข้อมูล และการแก้ปัญหาที่เกี่ยวข้องกับการเชื่อมต่อดังกล่าว ตลอดระยะเวลาสัญญา

4. การทดสอบความมั่นคงปลอดภัยของระบบ (Security Testing)

4.1 ผู้รับจ้างต้องดำเนินการประเมินช่องโหว่ (Vulnerability Assessment) และทดสอบเจาะระบบ (Penetration Testing) ก่อนการเปิดให้บริการอย่างเป็นทางการ (Go-Live)

4.2 ผู้รับจ้างต้องจัดทำรายงานสรุปผลการทดสอบ พร้อมระบุระดับความรุนแรงของช่องโหว่ที่ตรวจพบและเสนอแนวทางการแก้ไข

4.3 ผู้รับจ้างต้องดำเนินการปิดช่องโหว่ที่มีความรุนแรงระดับร้ายแรง (Critical) และระดับสูง (High) ให้แล้วเสร็จ พร้อมส่งมอบรายงานผลการแก้ไข (Remediation Report) ก่อนการเปิดให้บริการอย่างเป็นทางการ

(นายวีระ ระบายศรี)	(นางสาวอรรวรรณ ใจเอื้อ)	(นาวาอากาศเอก กรเอก ชิษณุชาบุญวิภัค)	(นายรักพิรุนห์ รุจิรวงษ์สกุล)	(นายจักรพรรณ มีนคร)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

ภาคผนวก 2

ระบบหรือโมดูลด้านข่าวกรองภัยคุกคามทางไซเบอร์ (Threat Intelligence)

ผู้ยื่นข้อเสนอต้องจัดให้มีระบบหรือโมดูลด้านข่าวกรองภัยคุกคาม (Threat Intelligence) สำหรับสนับสนุนการดำเนินงานของ TA-CERT ในการรวบรวม สืบค้น ติดตาม วิเคราะห์ และเชื่อมโยงข้อมูลภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับ กพท. หน่วยงานสมาชิก TA-CERT และภาคการบิน โดยมีคุณสมบัติและความสามารถอย่างน้อยดังนี้

1. ระบบที่เสนอต้องเป็นซอฟต์แวร์พร้อมใช้งาน ที่ผู้ใช้บริการสามารถใช้งานผ่านอินเทอร์เน็ตได้ โดยมี Dashboard แสดงข้อมูลในรูปแบบกราฟิก เช่น การแจ้งเตือน, รายงาน และ Digital Footprint เป็นต้น โดยได้รับการรับรองความปลอดภัยแบบ ISO 27001:2022 certification และ SOC 2 Type II compliance เป็นอย่างน้อย
2. ระบบที่เสนอต้องสามารถทำการตรวจสอบสิทธิ์แบบหลายปัจจัย (MFA) เพื่อเข้าสู่ระบบได้
3. ระบบที่เสนอต้องสามารถกำหนด IP Address ที่สามารถเข้าสู่ระบบได้ หรือ รองรับการเชื่อมต่อกับระบบยืนยันตัวตนแบบรวมศูนย์ (Single Sign-On) ผ่านมาตรฐาน SAML 2.0 หรือ OpenID Connect กับ Identity Provider ที่ กพท. กำหนด ร่วมกับการกำหนดสิทธิ์การเข้าถึงตามบทบาทผู้ใช้งาน (RBAC) ได้
4. ระบบที่เสนอต้องสามารถแสดงภาพรวมของคะแนนความปลอดภัย (Security Score) หน่วยงานสมาชิก TA-CERT พร้อมทั้งรายละเอียดเกี่ยวกับความเสี่ยงด้านความปลอดภัยทางไซเบอร์ของหน่วยงานสมาชิก TA-CERT
5. ระบบที่เสนอต้องสามารถจัดเรียงและคัดกรองการแจ้งเตือน ความเสี่ยงด้านความปลอดภัยทางไซเบอร์ขององค์กรตามระดับความรุนแรง ได้แก่ Very High หรือ Critical, High, Medium และ Low ได้เป็นอย่างน้อย
6. ระบบที่เสนอต้องสามารถสร้างรายงานการแจ้งเตือน ความเสี่ยงด้านความปลอดภัยทางไซเบอร์ในรูปแบบ PDF และ CSV ได้เป็นอย่างน้อย
7. ต้องมีระบบ Sandbox สำหรับตรวจจับมัลแวร์ จากไฟล์ที่ต้องการ หรือสามารถเสนอระบบ cloud sandbox เพิ่มเติมได้
8. ระบบต้องสามารถเชื่อมต่อ (Integrate) หรือรับข้อมูลฟีด (Data Feed) จากแหล่งข่าวกรอง Open Source Intelligence (OSINT) และรองรับการเชื่อมต่อกับแหล่งข้อมูลเฉพาะทาง (Industry-specific ISAC) ผ่านมาตรฐาน STIX/TAXII หรือ API ได้
9. ระบบที่เสนอต้องสามารถค้นหาสินทรัพย์ดิจิทัล (Digital Asset) ของหน่วยงานสมาชิก TA-CERT ที่มีการสื่อสาร หรือให้บริการผ่านช่องทางอินเทอร์เน็ตแบบอัตโนมัติ ไม่น้อยกว่า 200 asset โดยสามารถค้นหาผ่านช่องทาง ดังนี้ เป็นอย่างน้อยดังนี้
    - 9.1 การสแกน IP ภายนอก
    - 9.2 การวิเคราะห์การจดทะเบียนโดเมนและข้อมูล WHOIS ที่เกี่ยวข้อง
    - 9.3 รายการ Subdomain ที่ถูกสร้างขึ้น
    - 9.4 การวิเคราะห์บริการคลาวด์เพื่อค้นหาสินทรัพย์ที่เกี่ยวข้อง เช่น AWS S3 Buckets
10. ระบบที่เสนอต้องสามารถแจ้งเตือนความเสี่ยงด้านความปลอดภัยทางไซเบอร์ ของหน่วยงานสมาชิก TA-CERT ดังต่อไปนี้:
    - 10.1 Vulnerabilities
    - 10.2 Certificate Authority Issues

(นายวีระ ระบายศรี)	(นางสาวอรรวรรณ ใจเอื้อ)	(นาวาอากาศเอก กรเอก ชิษณุชาบุญวิภัค)	(นายรักพิรุนห์ รุจิรวงษ์สกุล)	(นายจักรพรรณ มีนคร)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

10.3 Email Security

10.4 Exploitable Ports

10.5 Exposed Web Interfaces

10.6 SSL/TLS Issues

11. ระบบที่นำเสนอต้องสามารถรวบรวมข้อมูลจาก Open Web, Deep Web และ Darknet โดยสามารถเก็บข้อมูลข่าวกรองจากหลายภาษา และสามารถแปลข่าวกรองจากภาษาต่าง ๆ เป็นภาษาอังกฤษได้โดยอัตโนมัติ

12. ระบบต้องมีคุณสมบัติในการวิเคราะห์ไฟล์ต้องสงสัย (File Analysis) หรือ สามารถเชื่อมต่อกับระบบ Malware Analysis ภายนอกได้

13. มีระบบค้นหา และแสดงข้อมูลข่าวสารด้านไซเบอร์ โดยประกอบด้วย

13.1 ฟีดข่าวจากหลากหลายเว็บไซต์ หรือ Blogs ด้านความปลอดภัยไซเบอร์

13.2 ข่าวแยกตามภูมิภาค หรือ กลุ่มโจมตี หรือ อุตสาหกรรม

14. ระบบที่นำเสนอสามารถค้นหาข้อมูล Threat Intelligence จากฐานข้อมูล Threat Intelligence Database ได้

15. ระบบที่นำเสนอต้องสามารถคัดกรองข่าวกรอง ตามผู้เขียน, ความรุนแรง, แหล่งที่มา, วันที่สร้าง, วันที่เผยแพร่ และความเชื่อมโยงกับหน่วยงานสมาชิก TA-CERT

16. ระบบที่นำเสนอต้องสามารถตรวจจับกรณีเกิดการละเมิดข้อมูลและการใช้เครื่องมือโจมตีต่อไปนี้ได้อย่างน้อยดังนี้

16.1 Phishing Website

16.2 Compromised Credentials

16.3 Ransomware

16.4 Malware

16.5 Reconnaissance

17. ระบบที่เสนอต้องสามารถกำหนดข้อมูลองค์กรเพื่อค้นหาและแจ้งเตือนการละเมิดสิทธิของหน่วยงานสมาชิก TA-CERT ได้

18. ระบบที่เสนอต้องสามารถแจ้งเตือนความเสี่ยงด้านความปลอดภัยทางไซเบอร์จากหน่วยงานสมาชิก TA-CERT ไม่น้อยกว่า 14 domains โดยสามารถแสดงภาพรวมของคะแนนความมั่นคงปลอดภัย รวมถึงแจ้งเตือนเมื่อเกิดเหตุการณ์ที่มีความเสี่ยงทางไซเบอร์ หรือสามารถเสนอระบบเพิ่มเติมเพื่อสามารถให้ข้อมูลที่เทียบเท่าได้

19. ระบบที่เสนอสามารถเชื่อมต่อกับระบบ SIEM, SOAR และ Ticketing ผ่าน REST API เพื่อรับข้อมูลการแจ้งเตือน

(นายวีระ ระบายศรี)	(นางสาวอรรวรรณ ใจเอื้อ)	(นาวาอากาศเอก กรเอก ชิษณุชาบุญวิภัค)	(นายรักพิรุนห์ รุจิรวงษ์สกุล)	(นายจักรพรรณ มีนคร)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

ภาคผนวก 3

การพัฒนา TA-CERT Web Application

ผู้ยื่นข้อเสนอต้องดำเนินการวิเคราะห์ ออกแบบ พัฒนา ติดตั้ง กำหนดค่า ทดสอบ และเปิดใช้งานเว็บแอปพลิเคชันของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคการบิน (TA-CERT Web Application) เพื่อสนับสนุนการบริหารจัดการข้อมูลและการดำเนินงานของ TA-CERT รวมถึงใช้เป็นช่องทางในการเผยแพร่และแลกเปลี่ยนข้อมูลที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยระบบต้องมีคุณสมบัติและความสามารถอย่างน้อยดังนี้

1. ขอบเขตของระบบงานและโครงสร้างเมนู

ระบบบริหารจัดการข้อมูลสมาชิกศูนย์ประสานฯ จะต้องแสดงเมนู โดยผู้ดูแลระบบสามารถ เพิ่ม/ลบ แก้ไข ปรับปรุงข้อมูลได้ โดยมีรายละเอียด ดังนี้

1.1 หน้าหลัก

1.2 เกี่ยวกับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคการบิน (TA-CERT) ประกอบด้วย ความเป็นมา วิสัยทัศน์ พันธกิจ โครงสร้างคณะทำงานฯ. อำนาจหน้าที่ แผนการดำเนินการ เป็นอย่างน้อย

1.3 มี Dashboard แสดงข้อมูลการโจมตีทางไซเบอร์ในภาคการบิน (Aviation Cyber Attack Dashboard) เพื่อสนับสนุนภารกิจของ TA-CERT ระบบต้องมี Dashboard สำหรับแสดงสถิติและสถานะภัยคุกคามไซเบอร์ภาคการบิน โดยมีคุณลักษณะอย่างน้อยดังนี้

1.3.1 การรวบรวมและแสดงผลข้อมูล

(1) แสดงสถิติเหตุการณ์ภัยคุกคามไซเบอร์ที่ได้รับรายงานจากสมาชิก TA-CERT จำแนกตามประเภทการโจมตี (เช่น Phishing, Ransomware, DDoS) และระดับความรุนแรง

(2) แสดงผลในรูปแบบกราฟวิเคราะห์แนวโน้มและสัดส่วนของเหตุการณ์

1.3.2 การอ้างอิงมาตรฐานและระดับการเฝ้าระวัง

(1) จำแนกประเภทการโจมตีโดยอ้างอิงมาตรฐานสากล เช่น MITRE ATT&CK for ICS/Enterprise หรือมาตรฐานที่เกี่ยวข้องกับภาคการบิน

(2) แสดงระดับการเฝ้าระวัง (Alert Level) ตามระดับความเสี่ยงที่กำหนดโดย กพท. หรือหน่วยงานกำกับดูแล

1.3.3 การคัดกรองและวิเคราะห์ข้อมูล

(1) เลือกดูข้อมูลย้อนหลังได้ตามช่วงเวลา (รายวัน รายสัปดาห์ รายเดือน รายปี)

(2) คัดกรองข้อมูลตามกลุ่มผู้ประกอบการหรือประเภทระบบงานที่ถูกโจมตีได้

(3) รองรับการแสดงรายละเอียดเชิงลึกของเหตุการณ์

1.4 ข้อมูลหน่วยงานสมาชิกของศูนย์ประสานฯ โดยสามารถแสดงเป็นตราสัญลักษณ์ของหน่วยงานได้

1.5 ผลลัพธ์การดำเนินงานที่สำคัญของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคการบิน (TA-CERT)

1.6 การเผยแพร่ข่าวสาร ข่าวประชาสัมพันธ์ กิจกรรม และประกาศ ของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคการบิน (TA-CERT)

(นายวีระ ระบายศรี)	(นางสาวอรรวรรณ ใจเอื้อ)	(นาวาอากาศเอก กรเอก ชิษณุชาบุญวิภัค)	(นายรักพิรุนห์ รุจิรวงษ์สกุล)	(นายจักรพรรณ มีนคร)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

1.7 ติดต่อศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคการบิน (Thailand Aviation - Computer Emergency Response Team : TA-CERT) ประกอบด้วย ที่ตั้งพร้อมแผนที่ เบอร์โทรศัพท์ และอีเมล เป็นอย่างน้อย

1.8 แผนที่เว็บไซต์ แสดงแผนผังของหน้าต่างๆ ภายในเว็บไซต์ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคการบิน (Thailand Aviation - Computer Emergency Response Team : TA-CERT)

2. ระบบบริหารจัดการบัญชีผู้ใช้

แบ่งประเภทผู้ใช้งาน เป็นผู้ดูแลระบบสูงสุด, ผู้ดูแลระบบทั่วไป และผู้ใช้งาน โดยมีความสามารถอย่างน้อยดังนี้

2.1 ลงทะเบียนข้อมูลผู้ใช้งาน โดยสามารถปรับปรุง แก้ไขข้อมูลผู้ใช้งาน

2.2 การยืนยันตัวตนผู้ใช้และผู้ดูแลระบบ แบบ 2FA หรือระบบอื่นที่ได้รับความเห็นชอบจาก กพท.

2.3 มีการระบุเงื่อนไขการเข้าใช้ระบบฯ และการยอมรับแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของระบบฯ

2.4 การแสดงประกาศความเป็นส่วนตัว และการจัดการความยินยอมและประมวลผลข้อมูลส่วนบุคคล

2.5 การจัดการข้อมูลยืนยันตัวตนผู้ใช้งาน การตั้งค่ารหัสผ่านใหม่ การลืมรหัสผ่านเป็นอย่างน้อย

2.6 การลบบัญชีผู้ใช้งาน

2.7 ดูสถานะยืนยันการลงทะเบียนผู้ใช้งาน

2.8 การยืนยันการลงทะเบียนโดยผู้ดูแลระบบ

2.9 แจ้งเตือนเมื่อการลงทะเบียนเสร็จสมบูรณ์ เช่น อีเมล ให้กับผู้ใช้งานและผู้ดูแลระบบ

2.10 การแสดงผลและออกรายงานข้อมูลผู้ใช้งาน

3. คุณสมบัติของเว็บแอปพลิเคชันและ Application Programming Interface (API) มีความต้องการอย่างน้อย ดังต่อไปนี้

3.1 ระบบสามารถรองรับการใช้งานโดยผู้ใช้พร้อมกันจำนวนไม่น้อยกว่า 150 ราย

3.2 ระบบที่นำเสนอต้องป้องกันการโจมตีตามข้อมูลจาก OWASP Top 10

3.3 มีการจัดการข้อผิดพลาด (Error Handling) อย่างเหมาะสม เช่น การแสดงหน้าข้อผิดพลาดของเพจ

3.4 สามารถส่ง Log หรือ Event Alert ไปยังระบบเฝ้าระวังความมั่นคงปลอดภัยตามที่ผู้ว่าจ้างกำหนด

3.5 ระบบที่นำเสนอต้องสอดคล้องตามแนวปฏิบัติการรักษาความมั่นคงปลอดภัยเว็บไซต์ (Website Security Guideline) ที่ประกาศโดย สกมช.

3.6 ระบบที่พัฒนาเสร็จเรียบร้อยแล้วจะต้องมีการติดตั้งใช้งานบนระบบคลาวด์ที่ผู้รับจ้างจัดเตรียมหรือระบบคลาวด์ที่ผู้ว่าจ้างกำหนด

3.7 ระบบที่นำเสนอต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของเว็บแอปพลิเคชัน โดยมีแนวทางดังนี้

3.7.1 Secure Coding การเขียนโปรแกรมจะต้องมีความปลอดภัย

3.7.2 ระบบการรักษาความปลอดภัยอื่น ๆ เช่น WAF, Dedicated Firewall และ Application Performance Monitoring Tools

(นายวีระ ระบายศรี)	(นางสาวอรรวรรณ ใจเอื้อ)	(นาวาอากาศเอก กรเอก ชิษณุชาบุญวิภัค)	(นายรักพิรุนห์ รุจิรวงษ์สกุล)	(นายจักรพรรณ มีนคร)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

3.7.3 มีระบบสำรองข้อมูล (Backup) เพื่อรองรับในกรณีที่ระบบมีปัญหา เพื่อให้สามารถนำข้อมูลที่สำรองกลับมาให้บริการภายใน 24 ชั่วโมง โดยมี Software ทำการ Backup และมี Policy การ Backup และการทดสอบการกู้คืน

4. การแสดงผลและการรองรับการใช้งาน

เว็บแอปพลิเคชันที่นำมาใช้งานต้องมีคุณลักษณะสามารถทำงานบนเครื่องคอมพิวเตอร์ สมาร์ทโฟน และ Tablet ได้ โดยแสดงผลรูปแบบ Responsive Web Design และทำงานบน Google Chrome, Firefox, Microsoft Edge และ Safari เป็นอย่างน้อย

4.1 สามารถสร้าง Menu เพื่อ Link ไปยังเนื้อหาส่วนต่าง ๆ ได้

4.2 สามารถเพิ่ม ลบ แก้ไขหมวดหมู่เนื้อหาและเนื้อหา ส่วนแสดงผลหน้าบ้าน (Front-End) ได้

4.3 สามารถเพิ่ม ลบ ส่วนกำหนดรูปแบบการแสดงผล (Theme) ได้ เช่น Dark Mode

4.4 ผู้รับจ้างต้องใช้โปรแกรมที่ถูกต้องตามกฎหมายในการจัดทำระบบ โดยผู้รับจ้างต้องรับผิดชอบค่าใช้จ่ายใด ๆ ที่เกิดจากการใช้โปรแกรมถูกต้องตามกฎหมาย

(นายวีระ ระบายศรี)	(นางสาวอรรวรรณ ใจเอื้อ)	(นาวาอากาศเอก กรเอก ชิษณุชาบุญวิภัค)	(นายรักพิรุนห์ รุจิรวงษ์สกุล)	(นายจักรพรรณ มีนคร)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ