ข้อกำหนดขอบเขตของงาน (Term of Reference: TOR)
งานจัดซื้อสิทธิการใช้งานเครื่องมือสนับสนุนการบริหารจัดการภัยคุกคามทางไซเบอร์ (SIEM)
ของ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

1. ความเป็นมา

เนื่องในปัจจุบันระบบสารสนเทศต่างๆ มีการใช้บริการอยู่บนโครงสร้างพื้นฐานที่ สพร.ให้บริการอยู่ซึ่งเป็นระบบให้บริการกับภาครัฐ และประชาชนทั่วไป รวมถึงใช้ภายในหน่วยงานเอง จึงจำเป็นที่จะต้องอนุญาตให้ระบบเครือข่ายทั่วไปเข้าถึงได้ ซึ่งอาจเป็นช่องทางให้ผู้ไม่ประสงค์ดี ที่แฝงอยู่กับผู้ใช้งานทั่วไปเข้ามาทำให้เกิดเหตุขัดข้องกับระบบงานรวมถึงการจารกรรมข้อมูลซึ่งอาจจะก่อให้เกิดความเสียที่ประเมินมูลค่าไม่ได้ ซึ่งการตรวจจับเหตุการณ์จำเป็นต้องใช้งานซอฟต์แวร์สำหรับศูนย์ปฏิบัติการความมั่นคงปลอดภัยทางไซเบอร์เพื่อเฝ้าระวังภัยและป้องกันคุกคามทางไซเบอร์ที่อาจจะเกิดขึ้น

ดังนั้น เพื่อเป็นการป้องกันเหตุการณ์ดังกล่าวจำเป็นมีการต้องมีการจัดหาซอฟต์แวร์สำหรับศูนย์ปฏิบัติการความมั่นคงปลอดภัยทางไซเบอร์ สำหรับเฝ้าระวังภัยคุกคามทางไซเบอร์ที่อาจจะเกิดขึ้น

2. วัตถุประสงค์

เพื่อจัดหาซอฟต์แวร์ระบบบริหารจัดการภัยคุกคามสารสนเทศ เพื่อให้มีระบบตรวจจับภัยคุกคามทางไซเบอร์ได้อย่างต่อเนื่องและมีประสิทธิภาพ

3. คุณสมบัติผู้ยื่นข้อเสนอ

3.1 มีความสามารถตามกฎหมาย
3.2 ไม่เป็นบุคคลล้มละลาย
3.3 ไม่อยู่ระหว่างเลิกกิจการ
3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

ลงนามผู้กำหนดขอบเขตของงาน

ประธานกรรมการ	(นาย ปณิธาน เขินอำนวย)	ลงนาม.....ปณิธาน เขินอำนวย.....	วันที่...15/08/2567....
กรรมการ	(นาย ณัฐพล สายรัตน์)	ลงนาม.....ณัฐพล สายรัตน์.....	ครั้งที่.....1.....
กรรมการและเลขานุการ	(นาย นฤเทพ ฉัตรวนิชกุล)	ลงนาม...นฤเทพ ฉัตรวนิชกุล.....	

3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 เป็นบุคคลธรรมดาหรือนิติบุคคลผู้มีอาชีพรับจ้างงานดังกล่าว

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่ สพร. หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการยื่นข้อเสนอครั้งนี้

3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

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

3.11 ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ ดังนี้

(1) กรณีเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยซึ่งได้จดทะเบียนเกินกว่า 1 ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก 1 ปีสุดท้ายก่อนวันยื่นข้อเสนอ

(2) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่ตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอไม่น้อยกว่า 8,000,000 บาท (แปดล้านบาทถ้วน)

(3) กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอ ผู้ยื่นข้อเสนอต้องมีวงเงินสินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์ และประกอบธุรกิจค้าประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยมียอดเงินรวมของวงเงินสินเชื่อไม่น้อยกว่า 7,901,250 บาท (เจ็ดล้านเก้าแสนหนึ่งพันสองร้อยห้าสิบบาทถ้วน) คิดเป็น 1 ใน 4 ของมูลค่าโครงการหรือรายการที่ยื่นเสนอในแต่ละครั้ง ซึ่งสำนักงานใหญ่รับรองหรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ออกให้แก่ผู้ยื่นข้อเสนอนับถึงวันยื่นข้อเสนอไม่เกิน 90 วัน

(4) กรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดาจะต้องแสดงหนังสือรับรองบัญชีเงินฝากไม่เกิน 90 วัน ก่อนวันยื่นข้อเสนอ โดยต้องมีเงินฝากคงเหลือในบัญชีธนาคารเป็นมูลค่าไม่น้อยกว่า 7,901,250 บาท (เจ็ดล้านเก้าแสนหนึ่งพันสองร้อยห้าสิบบาทถ้วน) คิดเป็น 1 ใน 4 ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง และหากเป็นผู้ชนะการจัดซื้อจัดจ้างหรือเป็นผู้ได้รับการคัดเลือกจะต้องแสดงหนังสือรับรองบัญชีเงินฝากที่มีมูลค่าดังกล่าวอีกครั้งหนึ่งในวันลงนามในสัญญา

ลงนามผู้กำหนดขอบเขตของงาน

ประธานกรรมการ	(นาย ปณิธาน เขินอำนวย)	ลงนาม.....ปณิธาน เขินอำนวย.....	วันที่...15/08/2567....
กรรมการ	(นาย ณัฐพล สายรัตน์)	ลงนาม.....ณัฐพล สายรัตน์.....	ครั้งที่.....1.....
กรรมการและเลขานุการ	(นาย นฤเทพ ฉัตรวนิชกุล)	ลงนาม...นฤเทพ ฉัตรวนิชกุล.....	

คุณสมบัติในข้อนี้ ยกเว้นกรณีที่ผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐ หรือนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการตามพระราชบัญญัติล้มละลาย (ฉบับที่ 10) พ.ศ. 2561

3.12 ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ "กิจการร่วมค้า" ต้องมีคุณสมบัติดังนี้

กิจการร่วมค้าที่ยื่นข้อเสนอ ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน เว้นแต่ในกรณีกิจการร่วมค้าที่มีข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก กิจการร่วมค้านั้นสามารถใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียว เป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลักข้อตกลงดังกล่าวจะต้องมีการกำหนดสัดส่วนหน้าที่ และความรับผิดชอบในปริมาณงาน สิ่งของ หรือมูลค่าตามสัญญา มากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

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

3.13 ผู้เสนอราคาจะต้องมีผลงานเกี่ยวกับการติดตั้งหรือดูแลระบบความมั่นคงปลอดภัยทางไซเบอร์ในวงเงินไม่น้อยกว่า 5,000,000 บาท (ห้าล้านบาทถ้วน) จำนวน 1 ผลงาน โดยต้องเป็นผลงานสัญญาเดียว ย้อนหลังไม่เกิน 3 ปี นับจากวันที่งานแล้วเสร็จจนถึงวันที่ยื่นเอกสาร ซึ่งเป็นผลงานที่เป็นคู่สัญญาโดยตรงกับหน่วยงานภาครัฐ หรือหน่วยงานเอกชนที่ สพร. เชื่อถือ โดยจะต้องแนบสำเนาหนังสือรับรองผลงานและสำเนาสัญญา พร้อมรับรองสำเนาถูกต้องมาพร้อมกันในวันยื่นข้อเสนอโครงการ

3.14 ผู้เสนอราคาต้องได้รับการตั้งให้เป็นตัวแทนจำหน่ายหรือผู้ให้บริการ จากเจ้าของผลิตภัณฑ์หรือสาขาของเจ้าของผลิตภัณฑ์ในประเทศไทย หรือตัวแทนของเจ้าของผลิตภัณฑ์ในประเทศไทย (Distributor)

4. รายละเอียดขอบเขตงานดำเนินงาน

4.1 ให้บริการระบบบริหารจัดการภัยคุกคามสารสนเทศ (SIEM) บนระบบ Cloud

4.2 จัดทำขั้นตอนการตรวจจับการวิเคราะห์ภัยคุกคาม (Detection and Analysis) ประกอบด้วยการเฝ้าระวัง การตรวจสอบรายละเอียดเกี่ยวกับเหตุการณ์ภัยคุกคามทางไซเบอร์ การวิเคราะห์เหตุการณ์ภัยคุกคาม กระบวนการบันทึกผลการวิเคราะห์เหตุการณ์ภัยคุกคาม การจัดลำดับความสำคัญของเหตุการณ์ภัยคุกคาม การรายงานเบื้องต้นเกี่ยวกับเหตุการณ์ภัยคุกคามให้ผู้ที่เกี่ยวข้องทราบ

4.3 จัดทำหน้าจอแสดงผลระบบรักษาความปลอดภัย (Dashboard) ของ ระบบบริหารจัดการภัยคุกคามสารสนเทศ (SIEM) จำนวนอย่างน้อย 10 การแสดงผล

ลงนามผู้กำหนดขอบเขตของงาน

ประธานกรรมการ	(นาย ปณิธาน เขินอำนวย)	ลงนาม.....ปณิธาน เขินอำนวย.....	วันที่...15/08/2567....
กรรมการ	(นาย ณัฐพล สายรัตน์)	ลงนาม.....ณัฐพล สายรัตน์.....	ครั้งที่.....1.....
กรรมการและเลขานุการ	(นาย นฤเทพ ฉัตรวนิชกุล)	ลงนาม...นฤเทพ ฉัตรวนิชกุล.....	

4.4 จัดทำกรณีศึกษา (Use Case) ของ ระบบโซลูชันการรักษาความปลอดภัยที่ช่วยองค์กรตรวจหาภัยคุกคาม (SIEM) จำนวนอย่างน้อย 20 เหตุการณ์

4.5 จัดทำเอกสารกระบวนการทดสอบการใช้งานโดยผู้ใช้งานจริง (User Acceptance Test) เพื่อทำงานทดสอบการทำงานของระบบ

4.6 ระบบคลาวน์สำหรับการบันทึกข้อมูล Log เพื่อการวิเคราะห์และรักษาความปลอดภัยระบบคอมพิวเตอร์ จำนวน 1 ระบบ มีคุณลักษณะอย่างน้อยดังต่อไปนี้

4.6.1 ระบบที่นำเสนอต้องสามารถรองรับการทำงานด้วยสถาปัตยกรรมแบบกระจาย (Distributed architecture) และสามารถจัดเก็บข้อมูลแบบ High Availability (HA) หรือ Clustering

4.6.2 ระบบที่นำเสนอต้องสามารถใช้งานร่วมกับระบบเดิมของ สพร. ได้

4.6.3 ระบบที่นำเสนอต้องให้บริการแบบ On-Cloud (Software as a Service)

4.6.4 ระบบสามารถทำ multi-Tenant ได้โดยไม่มีค่าลิขสิทธิ์เพิ่ม

4.6.5 ระบบที่นำเสนอต้องรองรับ mobile application บน smart device iOS หรือ Android ในการดู Alert, Report และ Dashboard

4.6.6 ระบบที่นำเสนอต้องสามารถกำหนดสิทธิ์การใช้งานระบบของผู้ดูแลระบบ แต่ละคนได้แตกต่างกัน (Role Base Access Control)

4.6.7 ระบบที่นำเสนอต้องสามารถบริหารจัดการระบบผ่าน Web Browser หรือ CLI ได้

4.6.8 ระบบที่นำเสนอต้องสามารถพิสูจน์ตัวตนของผู้ใช้ระบบบน Local system หรือ LDAP Server และรองรับการทำ Single sign-on (SSO) ด้วย SAML

4.6.9 มีระบบ Monitoring Platform Health เพื่อตรวจสอบ ประสิทธิภาพของระบบได้

4.6.10 มีระบบ Deployment ส่วนกลางที่สามารถบริหารจัดการ และปรับแต่งค่า configure ของ Agent ได้

4.6.11 ระบบที่นำเสนอต้องมีความสามารถในการตรวจจับการวิเคราะห์ภัยคุกคาม (Detection and Analysis) ประกอบด้วยการเฝ้าระวัง การตรวจสอบรายละเอียดเกี่ยวกับเหตุการณ์ภัยคุกคามทางไซเบอร์ การวิเคราะห์เหตุการณ์ภัยคุกคาม กระบวนการบันทึกผลการวิเคราะห์เหตุการณ์ภัยคุกคาม การจัดลำดับความสำคัญของเหตุการณ์ภัยคุกคาม การรายงานเบื้องต้นเกี่ยวกับเหตุการณ์ภัยคุกคาม

4.6.12 ผู้ขายต้องจัดทำขั้นตอนการตรวจจับการวิเคราะห์ภัยคุกคาม (Detection and Analysis) ประกอบด้วย การเฝ้าระวัง การตรวจสอบรายละเอียดเกี่ยวกับเหตุการณ์ภัยคุกคามทางไซเบอร์ การวิเคราะห์เหตุการณ์ ภัยคุกคาม กระบวนการบันทึกผลการวิเคราะห์เหตุการณ์ภัยคุกคาม

ลงนามผู้กำหนดขอบเขตของงาน

ประธานกรรมการ	(นาย ปณิธาน เขินอำนวย)	ลงนาม.....ปณิธาน เขินอำนวย.....	วันที่...15/08/2567....
กรรมการ	(นาย ณัฐพล สายรัตน์)	ลงนาม.....ณัฐพล สายรัตน์.....	ครั้งที่.....1.....
กรรมการและเลขานุการ	(นาย นฤเทพ ฉัตรวนิชกุล)	ลงนาม...นฤเทพ ฉัตรวนิชกุล.....	

การจัดลำดับความสำคัญของเหตุการณ์ภัยคุกคาม การรายงานเบื้องต้นเกี่ยวกับเหตุการณ์ภัยคุกคามให้ผู้เกี่ยวข้องทราบ

4.6.13 ผู้ขายต้องทำการปรับแต่ง (Customize) กรณีศึกษา (Use Case) จากระบบ SIEM เดิมของ สพร. ให้มีความทันสมัยตามเทคโนโลยีปัจจุบัน

4.6.14 ระบบที่นำเสนอต้องสามารถค้นหาข้อมูลแบบกำหนดช่วงเวลาได้ และสามารถเชื่อมโยงความสัมพันธ์ของเหตุการณ์ (Event correlation) ได้

4.6.15 ระบบที่นำเสนอต้องมีระบบ Machine Learning ที่ช่วยในการสร้าง Model และสามารถนำไปใช้กับข้อมูลที่จัดเก็บในระบบ เพื่อทำนายผลลัพธ์ที่จะเกิดขึ้นในอนาคตของฟิลด์ข้อมูลได้

4.6.16 ระบบที่นำเสนอต้องเป็นระบบที่ถูกออกแบบมาเพื่อใช้งานเป็น Security Information and Event Management (SIEM) และอยู่ในกลุ่ม Leader ของ Gartner Magic Quadrant สำหรับ Security Information and Event Management ปี 2022 หรือปีล่าสุด

4.6.17 ระบบที่นำเสนอต้องสามารถค้นหาความสัมพันธ์ของเหตุการณ์ (Correlation) และมีรูปแบบสำเร็จรูปพร้อมใช้ (Out of the box) ไม่น้อยกว่า 1,000 rules และสามารถทำ Custom Rule ตามความต้องการได้

4.6.18 ระบบที่นำเสนอต้องสามารถกำหนดค่าความสำคัญ (Priority) ของตัวตนผู้ใช้งาน (User Identity) และอุปกรณ์(Asset) ได้ และสามารถนำมาใช้ในการคำนวณค่าความเร่งด่วน (Urgency) หรือความรุนแรง (Severity) ของการแจ้งเตือน (Alert) ได้

4.6.19 ระบบที่นำเสนอต้องสามารถสร้างนโยบายตรวจจับ (Detection Rule) ตามค่าคะแนนความเสี่ยง (Risk Score) โดยดูจากพฤติกรรม (Behavior) ความสัมพันธ์ และพร้อมกับช่วงระยะเวลา (Time Period) ได้

4.6.20 ระบบที่นำเสนอต้องสามารถสร้างนโยบาย (Rule) ในการตรวจจับโดยอ้างอิงกับ Security Framework เช่น MITRE ATT&CK, Lockheed Martin Kill Chain phases, CIS controls และ NIST ได้

4.6.21 ระบบที่นำเสนอต้องสามารถแสดงค่าคะแนนความเสี่ยง (Risk Score) ของ Object เช่น ผู้ใช้ (Users) และอุปกรณ์ (Asset) ได้

4.6.22 ระบบที่นำเสนอต้องสามารถรองรับการนำเข้าข้อมูล Threat intelligence จากภายนอก ในรูปแบบ STIX หรือ OpenIOC ได้ และรองรับการ Correlate ข้อมูลโดยใช้การค้นหาร่วมกับข้อมูลที่เก็บอยู่ได้

ลงนามผู้กำหนดขอบเขตของงาน

ประธานกรรมการ	(นาย ปณิธาน เขินอำนวย)	ลงนาม.....ปณิธาน เขินอำนวย.....	วันที่...15/08/2567....
กรรมการ	(นาย ณัฐพล สายรัตน์)	ลงนาม.....ณัฐพล สายรัตน์.....	ครั้งที่.....1.....
กรรมการและเลขานุการ	(นาย นฤเทพ ฉัตรวนิชกุล)	ลงนาม...นฤเทพ ฉัตรวนิชกุล.....	

4.6.23 ระบบที่นำเสนอต้องสามารถรองรับรูปแบบของ Threat Intelligence ดังต่อไปนี้เช่น Email, File name, Hash, URL, IP Address, Domain, Process, Registry และ Service เป็นอย่างน้อย

4.6.24 ระบบที่นำเสนอต้องมีระบบแสดงผลการตรวจสอบแบบ Swim lane ครอบคลุมหัวข้อไปนี้ได้ เพื่อแสดงเหตุการณ์ของผู้ใช้ หรืออุปกรณ์ ตามประเภทของเหตุการณ์ และสามารถเลือกช่วงเวลาได้

- Authentication
- Threat Activity
- Malware Attack
- Alert events
- Risk Modifier

4.6.25 ระบบที่นำเสนอต้องสามารถจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยด้านสารสนเทศ (Security Incident) ได้โดยสามารถมอบหมายเหตุการณ์ให้กับผู้ดูแลแต่ละคนได้

4.6.26 ระบบที่นำเสนอต้องมีเครื่องมือหรือแอพพลิเคชั่นสำหรับการแนะนำการเลือกใช้การตรวจจับเพื่อวางแนวทางเป็น Roadmap โดยมีความสามารถดังต่อไปนี้

- มี Content Library ในการตรวจจับสำเร็จรูปพร้อมใช้จำนวนไม่น้อยกว่า 1,000 รูปแบบการตรวจจับมีการเชื่อมโยงถึง MITRE ATT&CK Tactics, Techniques, Threat Group และ Kill Chain Phases
- สามารถเลือก Content และทำการ Bookmark เพื่อติดตามผลการติดตั้งได้
- มีเครื่องมือในการตรวจเช็คความครบถ้วนของข้อมูล (Log หรือ Data Source) ที่จำเป็นต้องมีสำหรับการตรวจจับ
- มี Dashboard แสดงผลของรูปแบบการตรวจจับที่มีการใช้งาน โดยเชื่อมโยงกับ MITRE ATT&CK Framework และ Cyber Kill Chain

4.6.27 ระบบที่นำเสนอต้องมีหน้าแสดงผล Dashboard เพื่อแสดงข้อมูลดังต่อไปนี้

- เหตุการณ์ (Event) แยกตามระดับความเร่งด่วน (Urgency/Severity)
- จัดอันดับเหตุการณ์ที่เกิดขึ้นอันดับต้นๆ (Top Event)
- Timeline ของจำนวนเหตุการณ์ที่เกิดขึ้น
- ระยะเวลาเฉลี่ยในการทำการวิเคราะห์เหตุการณ์ (Mean time to Triage)

ลงนามผู้กำหนดขอบเขตของงาน

ประธานกรรมการ	(นาย ปณิธาน เขินอำนวย)	ลงนาม.....ปณิธาน เขินอำนวย.....	วันที่...15/08/2567....
กรรมการ	(นาย ณัฐพล สายรัตน์)	ลงนาม.....ณัฐพล สายรัตน์.....	ครั้งที่.....1.....
กรรมการและเลขานุการ	(นาย นฤเทพ ฉัตรวนิชกุล)	ลงนาม...นฤเทพ ฉัตรวนิชกุล.....	

- ระยะเวลาเฉลี่ยในการแก้ไขปัญหาของเหตุการณ์ (Mean time to Resolution)

4.6.28 ระบบที่นำเสนอต้องสามารถแจ้งเตือนทาง E-mail หรือ Webhook เมื่อมีเหตุการณ์ที่ตรงกับเงื่อนไขของการตรวจสอบได้

4.6.29 ระบบที่ผู้ขายนำเสนอต้องสามารถจัดเก็บข้อมูลจากอุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์แม่ข่ายได้

4.6.30 สามารถรองรับปริมาณข้อมูล LOG ได้ไม่น้อยกว่า 300 GB ต่อวัน หรือไม่น้อยกว่า 12,500 EPS

4.6.31 ระบบที่นำเสนอต้องสามารถกำหนดกลุ่ม (Index) ของข้อมูลที่จัดเก็บได้ และสามารถกำหนดนโยบายการเก็บรักษาข้อมูลตามอายุและกำหนดสิทธิ์ในการเข้าถึงได้

4.6.32 ซอฟแวร์สำหรับการเก็บและส่งต่อข้อมูล (Forwarder) จากคอมพิวเตอร์แม่ข่ายต้องรองรับระบบปฏิบัติการต่อไปนี้ เช่น Microsoft Windows Server, CentOS Linux และ Ubuntu Linux ได้เป็นอย่างน้อย

4.6.33 ระบบที่นำเสนอต้องสามารถรับข้อมูลจากอุปกรณ์ต่อไปนี้ได้เป็นอย่างน้อย

- อุปกรณ์ Firewall, IPS, Web Proxy, WAF, และ Endpoint Security
- Windows Event Log
- Linux System Log
- Mail Gateway และ DNS Server
- อุปกรณ์ Vulnerability Scanner

4.6.34 ระบบที่นำเสนอต้องสามารถนำเข้าข้อมูลในรูปแบบดังต่อไปนี้ได้

- บรรทัดเดียว หลายบรรทัด และแบบมีโครงสร้างเช่น XML
- มอนิเตอร์ file หรือ directory
- มอนิเตอร์ Windows event log, registry, window management instrumentation (WMI) และ Active directory
- ข้อมูล NetFlow

4.6.35 ระบบที่นำเสนอต้องสามารถจัดเก็บข้อมูลได้โดยไม่ต้องทำการ Parsing หรือ Normalization ข้อมูลก่อนและสามารถทำการค้นหา (Search), สร้างรายงาน (report) และทำเป็น Dashboard ได้

4.6.36 ระบบที่นำเสนอต้องมี Wizard สำหรับใช้สร้าง Parsers และ ทดสอบข้อมูลปัจจุบันหรือข้อมูลย้อนหลังในระบบจากหน้า Web interface ได้

ลงนามผู้กำหนดขอบเขตของงาน

ประธานกรรมการ	(นาย ปณิธาน เขินอำนวย)	ลงนาม.....ปณิธาน เขินอำนวย.....	วันที่...15/08/2567....
กรรมการ	(นาย ณัฐพล สายรัตน์)	ลงนาม.....ณัฐพล สายรัตน์.....	ครั้งที่.....1.....
กรรมการและเลขานุการ	(นาย นฤเทพ ฉัตรวนิชกุล)	ลงนาม...นฤเทพ ฉัตรวนิชกุล.....	

4.6.37 ระบบที่นำเสนอต้องสามารถบริหารจัดการข้อมูลโดยทำการ Filtering ข้อมูลก่อนทำการจัดเก็บลง Index ได้อย่างน้อยดังต่อไปนี้

- สามารถทำการซ่อน (masking) ข้อมูลได้
- สามารถทำเลือกส่ง (Route) ข้อมูลเก็บลงใน Index ตามต้องการได้
- สามารถทำการลบ (Discard) ข้อมูลที่ไม่ต้องการได้

4.6.38 ระบบสามารถรองรับข้อมูล log และสามารถค้นหาข้อมูล log นั้นได้ ในกรณีที่รับข้อมูล log เข้ามาในรูปแบบที่ไม่รู้จักได้

4.6.39 ระบบที่นำเสนอต้องสามารถใช้ชุดคำสั่งเพื่อค้นหาข้อมูลได้หลายชุดคำสั่งต่อเนื่องกัน โดยสามารถนำผลลัพธ์ของชุดคำสั่งก่อนหน้ามาป้อนเข้าชุดคำสั่งถัดไปได้

4.6.40 ระบบที่นำเสนอจะต้องสามารถรองรับ caching mode ของการถ่ายโอนชุดข้อมูล log ในกรณีที่ระบบเครือข่ายขาดหาย (network loss) จะสามารถดำเนินการส่งข้อมูลต่อเมื่อมีการเชื่อมต่อเครือข่ายกลับคืนมาปกติ

4.7 บริการระบบบริหารการจัดการและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ (Security Orchestration Automation and Response: SOAR จำนวน 1 ระบบ

4.7.1 ระบบที่เสนอสามารถบริหารจัดการและตอบสนองต่อเหตุการณ์ภัยคุกคามที่เกิดขึ้นบนระบบเครือข่ายคอมพิวเตอร์ได้อย่างอัตโนมัติ (Security Orchestration, Automation and Response : SOAR) และมีระบบ Threat Intelligence Management (TIM) อยู่ภายในระบบเดียวกัน แบบพร้อมใช้งานภายในระบบดังกล่าว หรือนำเสนอ Threat Intelligence Management (TIM) หรือ Threat Intelligence Platform (TIP) เพิ่มเติม โดยระบบที่นำเสนอจะต้องเป็นสินค้าที่มีจำหน่ายอย่างเป็นทางการในประเทศไทย และมีตัวแทนจำหน่ายในประเทศไทยที่สามารถให้บริการหลังการขายได้

4.7.2 ระบบที่เสนอสามารถบริหารจัดการความปลอดภัยของระบบปฏิบัติการ SOAR เช่น มีการใช้ Docker เพื่อแยกกระบวนการในการเชื่อมต่อกับอุปกรณ์ต่างๆ (Integration isolation) ที่ใช้ในการทำ configuration หรือ automation ของอุปกรณ์ปลายทาง ด้วยสิทธิ์ของผู้ดูแลระบบ (administrative privilege) หรือเสนอวิธีการที่ทำให้ระบบ SOAR มีความปลอดภัยเพียงพอ

4.7.3 ระบบที่เสนอสามารถทำการกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงข้อมูล (Role-Based Access Management) เช่น Rules, Playbooks, Attachment และ Report ได้ และสามารถกำหนดสิทธิ์การ Create, Read, Update และ Delete ให้กับผู้ใช้งานระบบได้

4.7.4 ระบบที่เสนอสามารถทำงานร่วมกันในลักษณะ Collaborate and Learn แบบ Virtual War Room และมีระบบ Machine Learning มาช่วยในการวิเคราะห์และเชื่อมโยงเหตุการณ์ต่าง ๆ ที่เกิดขึ้นได้ หรือนำเสนอระบบเพิ่มเติมเพื่อทำตามความต้องการดังกล่าว โดยระบบ Collaborate

and Learn ที่นำเสนอเพิ่มเติม จะต้องมีระบบ Machine Learning มาช่วยในการวิเคราะห์และเชื่อมโยงเหตุการณ์ต่าง ๆ ที่เกิดขึ้น จากระบบ SOAR ไปยังระบบ Collaborate and Learn ได้ทันทีโดยไม่ต้องทำการค้นหาเพิ่มเติม

4.7.5 ระบบที่เสนอสามารถใช้งานระบบ Playbook แบบ Drag and Drop ได้ โดยมีรูปแบบ OOB (Out-of-Box) Predefined Connector มาให้ และรูปแบบการสั่งการแบบอัตโนมัติ (Predefined Automated action)

4.7.6 ระบบที่เสนอ มีรูปแบบ OOB (Out-of-Box) Playbook มาให้ ไม่น้อยกว่า 100 playbook เช่น

- Block Account – Generic
- Block IP – Generic
- IOC Alert
- NGFW Scan
- Spear Phishing Investigation

4.7.7 ระบบที่เสนอสามารถแลกเปลี่ยนข้อมูลโดยตรงกับ Threat Intelligence Partner

4.7.8 ระบบที่เสนอมีหน้าจอแสดงผล (Dashboard) ที่สามารถปรับแต่งค่าการแสดงผลสำหรับนักวิเคราะห์ระบบและผู้ดูแลระบบได้

4.7.9 ระบบที่เสนอสามารถแสดงผลในรูปแบบต่าง ๆ เช่น ตาราง (Chart), รายการ (List) และจำนวน (Counter) ได้

4.7.10 ระบบที่เสนอสามารถทำการออกรายงานและส่งอีเมลในรูปแบบ PDF, Doc และ CSV ได้เป็นอย่างน้อย

4.7.11 ระบบที่เสนอสามารถทำการนำเข้า (Import) และส่งออก (Export) รูปแบบของ Playbook ได้

4.7.12 ระบบที่เสนอสามารถทำงานร่วมกับระบบพิสูจน์ตัวตน เช่น Active Directory หรือ LDAP และ SAML ได้ รวมถึงสามารถกำหนดและควบคุมสิทธิ์ผู้ใช้งานในการเข้าใช้ระบบได้

4.7.13 ระบบที่เสนอสามารถทำการสร้างกระบวนการทำงานตอบสนองต่อเหตุการณ์ (Playbook) และเรียกใช้งาน ได้ทั้งแบบอัตโนมัติ และกำหนดเอง

4.7.14 ระบบที่เสนอสามารถทำการสร้าง Playbook ได้อย่างน้อยดังนี้

- Manual action and Task
- การสร้างขั้นตอนในการตัดสินใจและอนุมัติ
- การเรียกใช้งาน Playbook ที่ซ้อนกันได้
- การกำหนดเงื่อนไขและลูป
- การหยุดหรือดำเนินการต่อเมื่อเกิดข้อผิดพลาดใน Playbook

4.7.15 ระบบที่เสนอสามารถทำการเก็บข้อมูลในรูปแบบ Snapshot เพื่อทำการย้อนกลับ (Roll back) ในกรณีที่ Playbook เกิดปัญหาได้ หรือการทำ Playbook Version History

4.7.16 ระบบที่เสนอสามารถทำการจำลองขั้นตอนของ Playbook เพื่อทดสอบการทำงานได้

ลงนามผู้กำหนดขอบเขตของงาน

ประธานกรรมการ	(นาย ปณิธาน เขินอำนวย)	ลงนาม.....ปณิธาน เขินอำนวย.....	วันที่...15/08/2567....
กรรมการ	(นาย ณัฐพล สายรัตน์)	ลงนาม.....ณัฐพล สายรัตน์.....	ครั้งที่.....1.....
กรรมการและเลขานุการ	(นาย นฤเทพ ฉัตรวนิชกุล)	ลงนาม...นฤเทพ ฉัตรวนิชกุล.....	

4.7.17 ระบบที่เสนอสามารถรับข้อมูลจากรูปแบบ PDF หรือ Image เพื่อนำไปสร้างเป็น Indicator ให้กับระบบได้

4.7.18 ระบบที่เสนอสามารถรับข้อมูลจาก Indicator of Compromise (IOCs) จากแหล่งที่มีความน่าเชื่อถือและได้รับการสนับสนุนจากหน่วยงาน Cyber Threat Alliance หรือ ICSA Labs หรือ NSS Labs หรือ NASA หรือ NATO หรือ Common Criteria หรือ Mitre เป็นอย่างน้อย

4.7.19 ระบบที่เสนอสามารถเชื่อมโยงกับอุปกรณ์อื่นจากผู้ผลิตภายนอก (3rd party) ผ่านการเรียกใช้ API

4.7.20 ระบบที่เสนอรองรับการทำ High Availability แบบ Active/Active, Active/Passive และ Cluster ได้

4.7.21 ระบบที่เสนอสามารถทำการพัฒนารายงาน และ Dashboard ให้ครอบคลุมอย่างน้อยดังนี้

- จำนวน Active Incident ทั้งหมดในแต่ละวันแยกประเภทตาม Incident Type
- จำนวน Active Incident ทั้งหมดในแต่ละวันแยกประเภทตาม Severity เช่น High, Medium, Low
- จำนวน Active Incident ทั้งหมดในแต่ละวันแยกประเภทตาม Owner
- จำนวน Active Incident ทั้งหมดในแต่ละวันแยกประเภทตาม Phase เช่น Response, Triage, Containment
- จำนวน Incident ทั้งหมดในแต่ละวันแยกประเภทตาม Closed Reason เช่น False Positive, Duplicate เป็นต้น
- จำนวน Incident ในแต่ละสถานะว่ายังอยู่ใน Remediation SLA ที่กำหนด เช่น จำนวน Incident สถานะมีความเสี่ยงที่จะเกิน SLA, สถานะที่อยู่ใน SLA และ สถานะเกิน SLA
- จำนวน Incident ในแต่ละสถานะว่ายังอยู่ใน Detection SLA ที่กำหนด เช่น จำนวน Incident สถานะมีความเสี่ยงที่จะเกิน SLA, สถานะที่อยู่ใน SLA และ สถานะเกิน SLA
- จำนวน Indicator ในช่วงเวลา แยกตามประเภท เช่น IP, URL, Domain อื่น ๆ และแยกตาม Reputation เช่น Bad, Good เป็นต้น
- จำนวน Indicator ในช่วงเวลา แยกตามแหล่ง Threat Intelligence ต่าง ๆ เช่น IP, URL, Domain อื่น ๆ และแยกตาม Reputation เช่น Bad, Good เป็นต้น

4.7.22 ผู้ให้บริการจะต้องให้บริการระบบบริหารการจัดการและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ (Security Orchestration Automation and Response: SOAR) แบบ as a service ให้แก่ สพร และให้สิทธิแก่ สพร ในการเข้าถึง จำนวน 1 สิทธิ

ลงนามผู้กำหนดขอบเขตของงาน

ประธานกรรมการ	(นาย ปณิธาน เขินอำนวย)	ลงนาม.....ปณิธาน เขินอำนวย.....	วันที่...15/08/2567....
กรรมการ	(นาย ณัฐพล สายรัตน์)	ลงนาม.....ณัฐพล สายรัตน์.....	ครั้งที่.....1.....
กรรมการและเลขานุการ	(นาย นฤเทพ ฉัตรวนิชกุล)	ลงนาม...นฤเทพ ฉัตรวนิชกุล.....	

4.7.23 ผู้ให้บริการจะต้องทำการติดตั้งระบบบริหารการจัดการและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ (Security Orchestration Automation and Response: SOAR) บนระบบ Cloud และในส่วนอุปกรณ์ต่อเชื่อมไว้ที่ สพร โดย สพร จะเป็นผู้ดำเนินการจัดหาอุปกรณ์แม่ข่ายเอง

4.7.24 ผู้ให้บริการจะต้องทำการตั้งค่าที่ระบุใน Playbook บนระบบบริหารการจัดการและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ (Security Orchestration Automation and Response: SOAR) จำนวนไม่น้อยกว่า 5 Playbooks

4.7.25 ผู้ให้บริการจะต้องทำการตั้งค่าระบบบริหารการจัดการและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ (Security Orchestration Automation and Response: SOAR) ให้สามารถทำงานร่วมกับระบบบริหารจัดการภัยคุกคามสารสนเทศ (SIEM) ที่นำเสนอในโครงการนี้

4.7.26 ผู้ให้บริการจะต้องจัดให้มีเจ้าหน้าที่ผู้เชี่ยวชาญที่มีความรู้ความสามารถด้านภัยคุกคามทางไซเบอร์ เพื่อให้คำแนะนำในการปรับแก้ไข Playbook ให้แก่เจ้าหน้าที่ของ สพร ในระหว่างสัญญาการให้บริการ

4.7.27 ผู้ให้บริการต้องดำเนินการเชื่อมต่อระบบติดตามข้อมูลข่าวสารภัยคุกคามไซเบอร์ (Threat Intelligence) กับระบบ SOAR ที่ให้บริการ

4.8 ผู้ขายต้องให้บริการรับแจ้งเหตุขัดข้องแบบ 24x7 (24 ชั่วโมง x 7 วัน) โดยผ่านช่องทางดังต่อไปนี้

- ติดต่อผ่าน E-Mail
- ติดต่อผ่านโทรศัพท์ (Hotline หรือ Helpdesk หรือ Call Center)
- ติดต่อผ่านโทรศัพท์เคลื่อนที่

5 กำหนดระยะเวลาส่งมอบพัสดุ

ผู้ขายต้องส่งมอบงานพัสดุภายใน 120 วัน นับถัดจากวันที่ลงนามในสัญญา และให้มีระยะเวลาใช้งาน 1 ปี นับถัดจากวันที่ตรวจรับแล้วเสร็จ

6 หลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอ

สพร. จะพิจารณาคัดเลือกเลือกข้อเสนอผู้ยื่นข้อเสนอที่มีคุณสมบัติและยื่นเอกสารหลักฐานครบถ้วนถูกต้อง โดยใช้เกณฑ์ราคา

7 วงเงินงบประมาณ

ภายในจำนวนเงินทั้งสิ้น 31,605,000 (สามสิบเอ็ดล้านหกแสนห้าพันบาทถ้วน) ซึ่งเป็นราคาที่รวมภาษีมูลค่าเพิ่มและค่าใช้จ่ายทั้งปวงแล้ว

ลงนามผู้กำหนดขอบเขตของงาน

ประธานกรรมการ	(นาย ปณิธาน เขินอำนวย)	ลงนาม.....ปณิธาน เขินอำนวย.....	วันที่...15/08/2567....
กรรมการ	(นาย ณัฐพล สายรัตน์)	ลงนาม.....ณัฐพล สายรัตน์.....	ครั้งที่.....1.....
กรรมการและเลขานุการ	(นาย นฤเทพ ฉัตรวนิชกุล)	ลงนาม...นฤเทพ ฉัตรวนิชกุล.....	

8 งวดงานและการจ่ายเงิน

กำหนดการส่งมอบงานและการจ่ายเงินจำนวน 3 งวด โดยมีรายละเอียดและที่ต้องส่งมอบ (ในรูปแบบเอกสารจำนวน 1 ชุด และในรูปแบบไฟล์อิเล็กทรอนิกส์บันทึกลงใน Flash Drive จำนวน 1 ชุด) และมีอัตราการจ่ายเงินดังนี้

8.1 ชำระเงินงวดที่ 1 จำนวนร้อยละ 20 เมื่อคณะกรรมการได้ตรวจรับเรียบร้อยแล้ว โดยผู้รับจ้างต้องส่งแผนการดำเนินงานภายใน 30 วัน นับถัดจากวันที่ลงนามในสัญญา โดยมีงานที่ต้องส่งมอบ ดังนี้

8.1.1 ส่งแผนการดำเนินงานโครงการระบบคลาวน์สำหรับการบันทึกข้อมูล Log เพื่อการวิเคราะห์และรักษาความปลอดภัยระบบคอมพิวเตอร์

8.1.2 ส่งแบบ System Architecture ของโครงการระบบคลาวน์สำหรับการบันทึกข้อมูล Log เพื่อการวิเคราะห์และรักษาความปลอดภัยระบบคอมพิวเตอร์

8.2 ชำระเงินงวดที่ 2 จำนวนร้อยละ 30 เมื่อคณะกรรมการได้ตรวจรับเรียบร้อยแล้ว โดยผู้รับจ้างต้องส่งงานภายใน 90 วัน นับถัดจากวันที่ลงนามในสัญญา ดังนี้

8.2.1 ดำเนินการติดตั้งระบบคลาวน์สำหรับการบันทึกข้อมูล Log เพื่อการวิเคราะห์และรักษาความปลอดภัยระบบคอมพิวเตอร์ จัดทำระบบโซลูชันการรักษาความปลอดภัยที่ช่วยองค์กรตรวจหาภัยคุกคาม (SIEM) ให้เป็นไปตามขอบเขตการดำเนินงานข้อที่ 4.6

8.2.2 ดำเนินการติดตั้งขั้นตอนการตรวจจับการวิเคราะห์ภัยคุกคาม (Detection and Analysis) ให้เป็นไปตามขอบเขตการดำเนินงานข้อที่ 4.7

8.2.3 ดำเนินการติดตั้งหน้าจอแสดงผลระบบรักษาความปลอดภัย (Dashboard) ให้เป็นไปตามรายละเอียดขอบเขตงานดำเนินงาน

8.2.4 ดำเนินการติดตั้งกรณีศึกษา (Use Case) ให้เป็นไปตามรายละเอียดขอบเขตงานดำเนินงาน

8.2.5 ดำเนินการติดตั้งระบบบริหารการจัดการและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ

8.3 ชำระเงินงวดที่ 3 จำนวนร้อยละ 50 เมื่อคณะกรรมการได้ตรวจรับเรียบร้อยแล้ว ผู้รับจ้างต้องส่งงานภายใน 120 วัน นับถัดจากวันที่ลงนามในสัญญา โดยมีงานที่ต้องส่งมอบดังนี้

8.3.1 ส่งเอกสารการออกแบบระบบพร้อมกับการตั้งค่าคำสั่ง (System Design and Configuration)

8.3.2 ส่งเอกสารคู่มือการดูแลระบบ (Operations Guide)

8.3.3 ส่งเอกสารกระบวนการทดสอบการใช้งานโดยผู้ใช้งานจริง (User Acceptance Test) เพื่อทำงานทดสอบการทำงานของระบบ

8.3.4 ดำเนินการตั้งค่าที่ระบุใน Playbook บนระบบบริหารการจัดการและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ

ลงนามผู้กำหนดขอบเขตของงาน

ประธานกรรมการ	(นาย ปณิธาน เขินอำนวย)	ลงนาม.....ปณิธาน เขินอำนวย.....	วันที่...15/08/2567....
กรรมการ	(นาย ณัฐพล สายรัตน์)	ลงนาม.....ณัฐพล สายรัตน์.....	ครั้งที่.....1.....
กรรมการและเลขานุการ	(นาย นฤเทพ ฉัตรวนิชกุล)	ลงนาม...นฤเทพ ฉัตรวนิชกุล.....	

8.3.5 ส่งมอบสิทธิ์ในการเข้าใช้บริการระบบบริหารการจัดการและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ

9 ค่าปรับ

ผู้ขายจะต้องชำระค่าปรับให้ผู้ซื้อเป็นรายวันในอัตราร้อยละ 0.20 ของราคาสิทธิการใช้งานฯ ที่ยังไม่ได้รับมอบ นับถัดจากวันครบกำหนดตามสัญญา จนถึงวันที่ผู้ขายได้นำสิทธิการใช้งานฯ มาส่งมอบให้แก่ผู้ซื้อจนถูกต้องครบถ้วน

10 การจัดทำข้อเสนอ

ผู้ยื่นข้อเสนอต้องจัดทำข้อเสนอตามรายการ อย่างน้อย ดังนี้

10.1 **เอกสารแสดงคุณสมบัติทั่วไปของผู้ยื่นข้อเสนอ** ให้จัดทำตามรายการเอกสารหลักฐานที่กำหนด และเอกสารหลักฐานผลงานของผู้ยื่นข้อเสนอตามคุณสมบัติของผู้ยื่นข้อเสนอ ในข้อ 3

10.2 เอกสารข้อเสนอด้านเทคนิคหรือข้อเสนออื่น ประกอบด้วย

10.2.1 เอกสารการยอมรับดำเนินงานตามข้อกำหนด ตามตัวอย่างตารางเปรียบเทียบ ดังนี้

ขอบเขตการดำเนินงาน สพร. กำหนด	ขอบเขตการดำเนินงาน ที่ผู้เสนอราคา เสนอ	เปรียบเทียบขอบเขตการดำเนินงานที่ผู้เสนอราคาเสนอ	เอกสารอ้างอิง
ให้ขอบเขตการดำเนินงาน ที่ สำนักงานกำหนด	ให้ระบุขอบเขตการดำเนินงานที่ผู้เสนอราคาเสนอ	ให้ระบุจุดที่ดีกว่า หรือเทียบเท่า	ให้ระบุเอกสารอ้างอิง (ถ้ามี)

10.2.2 ผู้รับจ้างต้องส่งแผนการทำงานให้ผู้ว่าจ้างภายใน 30 วัน นับถัดจากวันลงนามในสัญญา

10.3 ข้อเสนอทางด้านราคา

ผู้ยื่นข้อเสนอจะต้องเสนอราคาตามขอบเขตงาน และเสนอราคาในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ของกรมบัญชีกลาง ตามแบบและเงื่อนไขที่กำหนดในเอกสารการประกวดราคาอิเล็กทรอนิกส์ (e-bidding) โดยเสนอราคาเป็นค่าจ้างรวมทั้งสิ้น ซึ่งรวมภาษีมูลค่าเพิ่มและค่าใช้จ่ายทั้งปวงไว้เรียบร้อยแล้ว ทั้งนี้ไม่ต้องจัดทำเอกสารแจกแจงรายละเอียดประกอบราคายื่นเสนอ ยกเว้น แต่ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกจะต้องจัดทำเอกสารแจกแจงรายละเอียดประกอบราคาที่เสนอจำแนกตามประเภทของรายจ่ายให้

สอดคล้องกับราคาที่เสนอ ตามที่ สพร. แจ้งพร้อมทั้งปรับปรุงรายละเอียดค่าจ้างให้สอดคล้องกับราคาที่เสนอหรือค่าจ้างตามผลการเจรจาต่อรอง ทั้งนี้ ผู้ยื่นข้อเสนอจะต้องเสนอกำหนดยืนราคาไม่น้อยกว่า 90 วัน ผู้ยื่นข้อเสนอต้องรับผิดชอบราคาที่ตนได้เสนอไว้และจะถอนการเสนอราคามิได้

11 การเก็บรักษาข้อมูลที่เป็นความลับ

ผู้ขายจะต้องจัดการเก็บรักษาข้อมูลต่าง ๆ ที่เกี่ยวกับการดำเนินงานตามสัญญานี้ที่ผู้ขายได้รับจากผู้ซื้อ ซึ่งรวมถึงข้อมูลต่าง ๆ ที่ ผู้ซื้อได้จัดทำขึ้นเนื่องจากการดำเนินงานนี้อย่างเป็นความลับ และ/หรือความลับทางการค้าของผู้ซื้อ และผู้ขายต้องหามาตรการในการจัดเก็บข้อมูลที่เป็นความลับให้มิดชิด ทั้งนี้ ผู้ขายจะต้องลงนามใน “สัญญาไม่เปิดเผยข้อมูลที่เป็นความลับ” พร้อมสัญญา

12 ข้อตกลงประมวลผลข้อมูลส่วนบุคคล

ผู้ขายตกลงรับทำงานในโครงการฯ นี้ ซึ่งในการดำเนินการดังกล่าว ผู้ซื้อได้มอบหมายหรือแต่งตั้งให้ผู้ขายเป็นผู้ดำเนินการกระบวนการเก็บรวบรวม ใช้ หรือเปิดเผย ข้อมูลส่วนบุคคล (“การประมวลผลข้อมูล”) แทนหรือในนามของผู้ซื้อ ดังนั้น ผู้ขายในฐานะผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องปฏิบัติตามข้อตกลงการประมวลผลข้อมูลส่วนบุคคล ตามข้อกำหนดใน “ข้อตกลงประมวลผลข้อมูลส่วนบุคคล” ที่แนบท้ายสัญญา

13 เงื่อนไขอื่น ๆ

13.1 สพร. ทรงไว้ซึ่งสิทธิ์ที่จะยกเลิกการดำเนินการจ้างโดยไม่พิจารณาจัดจ้างเลยก็ได้สุดแต่จะพิจารณาทั้งนี้เพื่อประโยชน์ของทางราชการเป็นสำคัญ

13.2 สพร. สงวนสิทธิ์ที่จะดำเนินการจัดทำสัญญาเมื่อได้รับการจัดสรรงบประมาณแล้วเท่านั้น

13.3 ผู้เสนอราคา ซึ่ง สพร. ได้คัดเลือกไว้แล้ว ไม่มาทำสัญญาหรือข้อตกลงภายในกำหนดเวลา โดยไม่มีเหตุอันสมควร สพร. สงวนสิทธิ์ที่จะพิจารณาว่าผู้เสนอราคานั้น เป็นผู้ทิ้งงานและแจ้งเวียนให้ส่วนราชการต่าง ๆ ทราบต่อไป

13.4 สพร. สงวนสิทธิ์ที่จะแก้ไขเพิ่มเติมเงื่อนไข หรือข้อกำหนดในแบบสัญญาให้เป็นไปตามความเห็นของสำนักงานอัยการสูงสุด (ถ้ามี)

13.5 ผู้เสนอราคาที่ได้รับการคัดเลือกให้ไปทำสัญญาจะต้องวางหลักประกันสัญญาจำนวนร้อยละ 5 ของมูลค่าสัญญา

13.6 ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกจะต้องไม่เอางานทั้งหมดหรือแต่บางส่วนแห่งสัญญานี้ไปจ้างช่วงอีกทอดหนึ่ง เว้นแต่การจ้างช่วงงานแต่บางส่วนที่ได้รับอนุญาตเป็นหนังสือจาก สพร. แล้ว

ลงนามผู้กำหนดขอบเขตของงาน

ประธานกรรมการ	(นาย ปณิธาน เขินอำนวย)	ลงนาม.....ปณิธาน เขินอำนวย.....	วันที่...15/08/2567....
กรรมการ	(นาย ณัฐพล สายรัตน์)	ลงนาม.....ณัฐพล สายรัตน์.....	ครั้งที่.....1.....
กรรมการและเลขานุการ	(นาย นฤเทพ ฉัตรวนิชกุล)	ลงนาม...นฤเทพ ฉัตรวนิชกุล.....	

13.7 ข้อมูลและเอกสารใด ๆ ที่ผู้รับจ้างได้รับทราบหรือได้รับจาก สพร. หรือลูกค้าของ สพร. รวมทั้งผลงานที่ส่งมอบ ผู้รับจ้างจะต้องถือเป็นความลับ ไม่นำไปเผยแพร่ให้บุคคลใดทราบเป็นอันขาด เว้นแต่จะได้รับการอนุญาตเป็นลายลักษณ์อักษรจาก สพร.

13.8 สพร. ขอสงวนสิทธิ์ที่จะยกเลิกการจ่ายเงินทันที และ/หรือเรียกเงินคืน หากผู้รับจ้างไม่สามารถส่งมอบงานได้ตามข้อกำหนดและเงื่อนไขการจ้าง (TOR) ข้อหนึ่งข้อใดก็ดี เว้นแต่การที่ผู้รับจ้างไม่สามารถส่งมอบงานได้ดังกล่าวเป็นผลมาจากเหตุสุดวิสัย ความผิดของ สพร. หรือมิได้เกิดจากความผิดของฝ่ายหนึ่งฝ่ายใด

14 หน่วยงานที่รับผิดชอบ

ทีมปฏิบัติการการให้บริการด้านความมั่นคงปลอดภัยทางไซเบอร์ ฝ่ายความมั่นคงปลอดภัยทางไซเบอร์ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

15 สถานที่ติดต่อเพื่อขอทราบรายละเอียดเพิ่มเติม

- สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) เลขที่ 999 ชั้น 4 อาคารสถาบันเพื่อการยุติธรรมแห่งประเทศไทย (องค์การมหาชน) ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210
- E-mail: cmp_division@dga.or.th
- Website: www.dga.or.th
- โทรศัพท์ 0-2612-6000

ลงนามผู้กำหนดขอบเขตของงาน

ประธานกรรมการ	(นาย ปณิธาน เงินอำนวย)	ลงนาม.....ปณิธาน เงินอำนวย.....	วันที่...15/08/2567....
กรรมการ	(นาย ณัฐพล สายรัตน์)	ลงนาม.....ณัฐพล สายรัตน์.....	ครั้งที่.....1.....
กรรมการและเลขานุการ	(นาย นฤเทพ ฉัตรวนิชกุล)	ลงนาม...นฤเทพ ฉัตรวนิชกุล.....	