รายละเอียดคุณลักษณะเฉพาะ (Terms of Reference : TOR) โครงการพัฒนาระบบบูรณาการด้านการข่าวเพื่อการแจ้งเตือนภัยคุกคามทางไซเบอร์ แขวงพญาไท เขตพญาไท กรุงเทพฯ
กิจกรรมที่ 1 ต่ออายุระบบบริหารจัดการความปลอดภัยโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล

1. ความเป็นมา

สำนักข่าวกรองแห่งชาติ เริ่มจัดตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Operation Center : CSOC) ตั้งแต่ปีงบประมาณ พ.ศ. 2562 วัตถุประสงค์เพื่อเฝ้าระวัง ตรวจจับ ระงับ ยับยั้ง และแจ้งเตือนภัยคุกคามทางไซเบอร์ รวมทั้งกำกับดูแลและควบคุมมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ภายในสำนักข่าวกรองแห่งชาติ ซึ่งการดำเนินงานจัดให้มีเจ้าหน้าที่เวรประจำวันปฏิบัติหน้าที่ในการเฝ้าระวังและแก้ไขปัญหาภัยคุกคามทางไซเบอร์อย่างต่อเนื่อง ตลอด 24 ชั่วโมง ไม่เว้นวันหยุดราชการ และได้จัดหาเทคโนโลยีเครื่องมือป้องกันภัยคุกคามทั้งในมิติเชิงรุกและเชิงรับที่หลากหลาย เพื่อสนับสนุนการปฏิบัติงานของเจ้าหน้าที่ให้สามารถรับมือและตอบสนองต่อภัยคุกคามที่เกิดขึ้นได้อย่างมีประสิทธิภาพ โดยปีงบประมาณ พ.ศ. 2566 ได้จัดซื้อระบบบริหารจัดการความปลอดภัยโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล ทำให้การจัดการฐานข้อมูลทรัพย์สินสารสนเทศ และการปรับปรุงซอฟต์แวร์โดยอัตโนมัติ รวมทั้งการรักษาความปลอดภัยระบบคอมพิวเตอร์ภายในสำนักข่าวกรองแห่งชาติครอบคลุมทุกพื้นที่ปฏิบัติงาน รองรับการตรวจจับและระงับเหตุการณ์โจมตีทางไซเบอร์ที่มีความซับซ้อน ช่วยลดความเสี่ยงและความเสียหายที่อาจนำไปสู่ผลกระทบในระดับร้ายแรงได้ทันท่วงที

พระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ. 2562 และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กำหนดให้สำนักข่าวกรองแห่งชาติมีหน้าที่ และอำนาจในด้านการข่าวกรอง การต่อต้านข่าวกรอง การข่าวกรองทางการสื่อสาร และการรักษาความปลอดภัยฝ่ายพลเรือน รวมถึงการประสานงานกับหน่วยงานอื่นในการเฝ้าระวังและแจ้งเตือนภัยคุกคามทางไซเบอร์ อีกทั้ง สำนักข่าวกรองแห่งชาติได้รับการมอบหมายจากสำนักงานสภาความมั่นคงแห่งชาติ (สมช.) ให้ปฏิบัติหน้าที่สำคัญ 2 ประการ คือ 1) เป็นศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านความมั่นคงของรัฐฝ่ายพลเรือน (Thailand Civilian Sector CERT: TCS-CERT) และ 2) ได้รับการมอบหมายให้เป็นหน่วยงานควบคุมและกำกับดูแล (Regulator) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure – CII) ด้านความมั่นคงของรัฐ กลุ่มหน่วยงานที่มีภารกิจเกี่ยวข้องกับความมั่นคงอื่น และถูกกำหนดให้เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญสารสนเทศ (CII) ประกอบกับนโยบายและแผนความมั่นคงที่ 15 การพัฒนาระบบข่าวกรองแห่งชาติ ซึ่งมีเป้าหมายในการยกระดับระบบข่าวกรองเพื่อการเฝ้าระวัง ประเมิน ตอบสนอง และแจ้งเตือนสถานการณ์ที่มีความเสี่ยงอันจะนำไปสู่ภัยคุกคามความมั่นคงแห่งชาติและผลประโยชน์ชาติ โดยกำหนดตัวชี้วัดการมีระบบเชื่อมโยงและบูรณาการข้อมูลด้านการข่าวเพื่อการแจ้งเตือนภัยคุกคามทางไซเบอร์ภายในปี 2570 และกำหนดกลยุทธ์การเชื่อมโยง บูรณาการและแจ้งเตือนข้อมูลด้านการข่าวเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์

ด้วยเหตุนี้ สำนักข่าวกรองแห่งชาติ จึงมีความจำเป็นต้องต่ออายุลิขสิทธิ์ระบบบริหารจัดการความปลอดภัยโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล โปรแกรมตรวจจับภัยคุกคามทางไซเบอร์แบบปัญญาประดิษฐ์ จำนวน 1,000 หน่วย ที่ระยะเวลาสิทธิ์การใช้งานจะสิ้นสุดใน ธ.ค.69 เพื่อให้สามารถใช้งานระบบดังกล่าวได้อย่างต่อเนื่อง อันจะเกิดประโยชน์สูงสุดต่อหน่วยงาน ในการป้องกันการโจมตี และต่อต้านการจารกรรมทางไซเบอร์ขั้นสูงได้อย่างมีประสิทธิภาพ พร้อมเสริมสมรรถนะความสามารถเพิ่มเติมของระบบให้รองรับการบริหารจัดการและควบคุมอุปกรณ์เชื่อมต่อระหว่างเครื่องคอมพิวเตอร์ได้อย่างครอบคลุม ยกระดับมาตรการรักษาความปลอดภัยของข้อมูล และขยายสิทธิ์การเข้าถึงระบบฐานข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์ (Threat Intelligence) สำหรับใช้วิเคราะห์เหตุการณ์ภัยคุกคามที่เกิดขึ้น เพื่อนำข้อมูลที่ได้ไปกำหนดนโยบายและมาตรการรักษาความปลอดภัยภายในหน่วยงานได้ดียิ่งขึ้น และใช้เป็นส่วนประกอบสำคัญในการผลิตรายงานข่าวกรองภัยคุกคามทางไซเบอร์

แจกจ่ายให้กับหน่วยประชาคมข่าวกรองทางไซเบอร์ในปัจจุบัน และอนาคต ควบคู่การพัฒนาทักษะความสามารถของผู้ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้สามารถใช้งานระบบได้มีประสิทธิภาพในระดับมาตรฐานสากล พร้อมรับมือภัยคุกคามรูปแบบใหม่ในสภาวะที่ปัญญาประดิษฐ์เริ่มมีบทบาทสำคัญในทุกมิติ

2. วัตถุประสงค์

2.1 เพื่อให้สามารถใช้งานระบบบริหารจัดการความปลอดภัยโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล ในการเฝ้าระวัง ตรวจจับ ระงับ ยับยั้ง และแก้ไขปัญหาภัยคุกคามทางไซเบอร์ได้อย่างต่อเนื่องและมีประสิทธิภาพ

2.2 เพื่อให้สามารถผลิตรายงานข่าวกรองด้านภัยคุกคามทางไซเบอร์ที่มีคุณภาพ แจกจ่ายให้หน่วยประชาคมสามารถนำข้อมูลไปใช้ประโยชน์ในการสืบสวนเชิงลึก รวมถึงป้องกันหรือแก้ไขปัญหาภัยคุกคามทางไซเบอร์ภายในหน่วยงานของตนเองได้

2.3 เพื่อพัฒนาเจ้าหน้าที่ผู้ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักข่าวกรองแห่งชาติให้มีทักษะความรู้ด้านการบริหารจัดการความปลอดภัยโครงสร้างพื้นฐานเทคโนโลยีดิจิทัลที่มีประสิทธิภาพระดับสากล

3. คุณสมบัติของผู้ยื่นข้อเสนอ

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราวเนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าด้วยกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการ ผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 เป็นนิติบุคคลผู้มีอาชีพขายพัสดุที่ประกวดราคาซื้อด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่ สำนักข่าวกรองแห่งชาติ ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรม ในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละสิทธิ์และความคุ้มกันเช่นว่านั้น

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

3.11 ผู้ยื่นข้อเสนอซึ่งได้รับคัดเลือกเป็นคู่สัญญาต้องรับและจ่ายเงินผ่านบัญชีธนาคาร เว้นแต่การจ่ายเงินแต่ละครั้งซึ่งมีมูลค่าไม่เกินสามหมื่นบาทคู่สัญญาอาจจ่ายเป็นเงินสดก็ได้

3.12 ผู้ยื่นข้อเสนอต้องเป็นนิติบุคคลที่จดทะเบียนก่อตั้งมาแล้วไม่น้อยกว่า 3 ปี ขึ้นไป นับถึงวันที่ยื่นข้อเสนอราคา และมีทุนจดทะเบียนไม่น้อยกว่า 2,000,000 บาท (สองล้านบาทถ้วน) ชำระเต็มมูลค่า โดยมีหลักฐานการจดทะเบียนซึ่งกรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์ ออกให้หรือรับรองให้ไม่เกิน 6 เดือน นับจากวันยื่นข้อเสนอ

3.13 ผู้ยื่นข้อเสนอต้องได้รับการสนับสนุนทางเทคนิค และได้รับการแต่งตั้งเป็นตัวแทนจำหน่ายระบบจากบริษัทเจ้าของผลิตภัณฑ์หรือสาขาของเจ้าของผลิตภัณฑ์ หรือตัวแทนจำหน่ายในประเทศไทย พร้อมแสดงเอกสารการแต่งตั้งเป็นตัวแทนจำหน่ายฉบับจริง โดยให้ยื่นเอกสารขณะเข้าเสนอราคา

4. รายละเอียดคุณลักษณะเฉพาะ

4.1 ต่ออายุสิทธิ์การใช้งานโปรแกรมตรวจจับภัยคุกคามทางไซเบอร์แบบปัญญาประดิษฐ์ จำนวน 1,000 หน่วย

4.1.1 โปรแกรมที่นำเสนอต้องเป็นผลิตภัณฑ์ที่อยู่ในกลุ่ม Leader Gartner Magic Quadrant ด้าน Endpoint Protection Platforms ปี 2026 และต้องเป็นผลิตภัณฑ์ที่อยู่ในกลุ่ม Leader The Forrester Wave ด้าน Extended Detection And Response Platforms ปี 2026 เพื่อให้มั่นใจว่าโปรแกรมที่นำเสนอยังคงพัฒนาโปรแกรมอย่างต่อเนื่อง

4.1.2 โปรแกรมที่นำเสนอต้องสามารถบริหารจัดการผ่านระบบคลาวด์ (cloud) ได้

4.1.3 การเชื่อมต่อระหว่างโปรแกรมตัวแทน (Agent) กับระบบคลาวด์ต้องมีการเข้ารหัสแบบ TLS-encrypted เพื่อความปลอดภัย

4.1.4 สามารถติดตั้งในเครื่องคอมพิวเตอร์ปลายทาง (Endpoint) บนระบบปฏิบัติการ Windows, Windows Server, Linux และ MacOS ได้เป็นอย่างน้อย

4.1.5 รองรับระบบยืนยันตัวตนแบบ 2 ปัจจัย (2 Factor Authentication)

4.1.6 สามารถตรวจจับมัลแวร์ (malware) โดยไม่อาศัย signature และไม่ต้องทำการ update signature บนเครื่องลูกข่าย โดยโปรแกรมที่ติดตั้งเป็นแบบ Lightweight Agent

4.1.7 สามารถป้องกัน known, unknown malware, adware และ potentially unwanted programs (PUPs) ด้วยเทคโนโลยี Machine learning

4.1.8 สามารถแสดงผลของภัยคุกคามที่เกิดขึ้นออกมาเป็นรูปภาพ process tree, process table และ events timeline ได้

4.1.9 สามารถตัดการเชื่อมต่อระบบเครือข่าย (network containment) ของเครื่องที่ติดตั้ง Agent ได้จากระบบคลาวด์บริหารจัดการจากส่วนกลาง

4.1.10 สามารถเชื่อมต่อระยะไกล (Real Time Response) เพื่อทำการ run คำสั่งกรณีที่ตรวจพบความผิดปกติในเครื่องคอมพิวเตอร์ปลายทางที่ติดตั้ง Agent

4.1.11 สามารถป้องกันพฤติกรรมการโจมตีช่องโหว่ (Exploitation behavior) และพฤติกรรมของ Ransomware ได้

4.1.12 สามารถแจ้งเตือนภัยคุกคาม (alerts) ตามลำดับความสำคัญในหน้าแสดงผลการตรวจจับ (Detection dashboard) และนำข้อมูลการตรวจจับมาจัดหมวดหมู่ตามประเภท Tactic หรือ Technique ได้

4.1.13 รองรับการค้นหาข้อมูลการใช้งาน IP addresses, bulk domains และ events ที่เกี่ยวข้องกับข้อมูลการใช้งานได้

4.1.14 มีระบบปัญญาประดิษฐ์ (Artificial Intelligence : AI) เพื่อใช้ในการสนทนา (AI conversations) ไม่น้อยกว่า 50 เครดิตต่อเดือน เพื่อให้สามารถนำ AI มาช่วยวิเคราะห์ข้อมูลภายในองค์กรได้

4.1.15 โปรแกรมที่นำเสนอต้องสามารถเก็บข้อมูลจากอุปกรณ์ภายนอก (third-party data) ได้ไม่น้อยกว่า 10 GB ต่อวัน และต้องเก็บย้อนหลังได้ไม่น้อยกว่า 7 วัน

4.1.16 มีบริการตรวจสอบภัยคุกคามเชิงรุก (Threat Hunting service) โดยผู้เชี่ยวชาญจากบริการของผลิตภัณฑ์ที่มีเครื่องหมายการค้าเดียวกันกับโปรแกรมที่นำเสนอ (Human Analysis) ตลอด 24 ชั่วโมง (24/7)

ครอบคลุมทุกเครื่องคอมพิวเตอร์ที่ติดตั้ง Agent เพื่อให้มีประสิทธิภาพในการรับมือภัยคุกคามรองรับระบบของสำนักข่าวกรองแห่งชาติที่มีอยู่เดิม โดยไม่ต้องติดตั้ง Agent ใหม่

4.1.17 มีลิขสิทธิ์การใช้งานไม่น้อยกว่า 1 ปี

4.1.18 โปรแกรมที่นำเสนอต้องเป็นผลิตภัณฑ์ที่ทางสำนักข่าวกรองแห่งชาติใช้งานอยู่เดิมเพื่อความต่อเนื่องในการป้องกันภัยคุกคามทางไซเบอร์

4.2 ระบบรวบรวมข่าวกรองภัยคุกคามทางไซเบอร์ (Threat Intelligence: TI) โดยต้องมีคุณสมบัติอย่างน้อย ดังนี้

4.2.1 ระบบที่นำเสนอต้องเป็นผลิตภัณฑ์ที่อยู่ในกลุ่ม Leader ของ Gartner Magic Quadrant ด้าน Cyber threat Intelligence Technologies ปี 2026 เพื่อให้มั่นใจว่าโปรแกรมที่เสนอมีประสิทธิภาพและได้รับการยอมรับในระดับสากล

4.2.2 ระบบที่นำเสนอต้องสามารถแสดงผลข้อมูล Indicators of Compromise (IOCs) โดยสามารถค้นหา หรือกรอง (Filter) ข้อมูลได้จากคุณสมบัติอย่างน้อยดังต่อไปนี้ Type, Published date, Confidence, Adversary, Malware family, Threat type และ Target เพื่อช่วยให้นักวิเคราะห์เข้าใจถึงผลกระทบและวางแผนตอบสนองต่อเหตุการณ์ได้อย่างเหมาะสม

4.2.3 มีฐานข้อมูลข่าวกรองภัยคุกคามที่ครอบคลุมกลุ่มผู้ไม่หวังดี (Adversary) มากกว่า 250 กลุ่ม โดยแสดงผลบนหน้าจอ management console เดียวกัน และสามารถค้นหา หรือกรอง (Filter) ข้อมูลได้จากคุณสมบัติอย่างน้อยดังต่อไปนี้ Target countries, Target industries, Motivation, Origin และ Published date และต้องแสดงรายละเอียดของกลุ่มผู้ไม่หวังดีได้อย่างน้อยดังต่อไปนี้ Kill chain, MITRE ATT&CK Matrix และรายงานที่เกี่ยวข้อง

4.2.4 สามารถนำส่งข้อมูลออก (Export) เพื่อใช้งานข้อมูลภัยคุกคาม IOCs ประเภทต่างๆ ได้อย่างน้อยดังต่อไปนี้ IP Address, Domain, SHA1 Hash, SHA256 Hash, Email Address, Coin Address และ URL ผ่านช่องทาง API หรือแบบ Manual เป็นไฟล์ CSV และ JSON ได้ไม่น้อยกว่า 1,000,000 รายการต่อครั้ง

4.2.5 มี Sandbox ที่มีเครื่องหมายการค้าเดียวกันกับผลิตภัณฑ์ Threat Intelligence เพื่อใช้วิเคราะห์ไฟล์/URL ทั้งในรูปแบบ Manual Upload และแบบอัตโนมัติจากไฟล์ที่ถูกกักกัน (Quarantined files) โดยรองรับ OS environment สำหรับการวิเคราะห์อย่างน้อยดังนี้ Windows 64 bit, Linux Ubuntu 64 bit, Android และ macOS

4.2.6 มีรายงานสรุป (Report) จากเจ้าของผลิตภัณฑ์ ตามประเภทของ Report ดังนี้ Alert, Intelligence Tipper, Intelligence Weekly Report และ Intelligence Report

4.2.7 สามารถเข้าถึงข้อมูลข่าวและรายงานภัยคุกคามไซเบอร์ของผู้ให้บริการได้ผ่าน Web Portal

4.2.8 มีลิขสิทธิ์การใช้งานไม่น้อยกว่า 1 ปี

4.2.9 โปรแกรมที่นำเสนอต้องเป็นผลิตภัณฑ์ที่ทางสำนักข่าวกรองแห่งชาติใช้งานอยู่เดิมเพื่อความต่อเนื่องในการป้องกันภัยคุกคามทางไซเบอร์

4.3 ระบบควบคุมการใช้งานอุปกรณ์เชื่อมต่อภายนอก (Device Control) จำนวน 1,000 สิทธิ์

4.3.1 สามารถกำหนด policy จาก USB device class ได้อย่างน้อยดังต่อไปนี้ Audio / Video, Imaging, Mass Storage, Mobile (MTP/PTP), Printer และ Wireless

4.3.2 สามารถกำหนดระดับการเข้าถึง (level of access) ของ USB device ได้อย่างน้อยดังต่อไปนี้ full access, full block, read write and execute, read and write only และ read only

4.4 ระบบป้องกันข้อมูลระบุยืนยันตัวบุคคล (Identity Protection) จำนวนไม่น้อยกว่า 800 สิทธิ์

4.4.1 โปรแกรมที่นำเสนอต้องถูกออกแบบมาเพื่อการป้องกันภัยคุกคามบนฐานข้อมูลบัญชีผู้ใช้งาน Identity Protection โดยทำการติดตั้งติดตั้ง sensor เข้าไปใน Domain Controller ตั้งแต่ Windows 2008 R2 SP1 ขึ้นไป

4.4.2 สามารถเรียนรู้พฤติกรรมการใช้งานของผู้ใช้งานแต่ละบัญชีผู้ใช้งาน (user behavior) เพื่อทำการกำหนดคะแนนความเสี่ยง (risk score) อย่างน้อยดังต่อไปนี้ ช่วงเวลาและตำแหน่งที่ทำการ login, role ของบัญชีผู้ใช้ที่อยู่ใน Organization, ระบบและเครื่องที่ทำการ login, และความแข็งแรงของรหัสผ่าน (password)

4.4.3 สามารถเก็บข้อมูลของ user หรือ endpoint จาก Active Directory (AD) หรือ Azure AD โดยสามารถแสดงออกมาเป็น Business card โดยสามารถแสดงข้อมูลต่างๆได้อย่างน้อยดังต่อไปนี้ Organizational Unit, Created, Account type, Domain, Title, Service Principal Names (SPNs), SID, Last Password Change, Password Policy Strength, Department, Managed by, Email address และ Classification

4.4.4 สามารถตรวจจับการโจมตี (Attack) ที่เกิดขึ้นใน Active Directory ได้อย่างน้อยดังต่อไปนี้ Suspicious domain replication, Golden Ticket attack, Password brute force attack, Credential scanning, NTLM relay activity, Suspicious Protocol implementation (Pass the Hash), Suspicious Kerberos ticket reuse, Skeleton key attack, Suspicious LDAP search, Unusual access to a user entity (Kerberoasting)

4.4.5 สามารถทำการติดตามและวิเคราะห์ Privileged identities เพื่อลดความเสี่ยงที่อาจเกิดขึ้นจากบัญชีเหล่านี้ได้ โดยแสดงรายละเอียดได้อย่างน้อยดังนี้

4.4.5.1 แสดง privileged users ทั้งหมด และการเปลี่ยนแปลงที่เกิดขึ้นในช่วงเวลาที่กำหนด

4.4.5.2 แสดง list ของ privileged users ที่มีการให้สิทธิที่ไม่ตรงตาม AD group (Stealthy)

4.4.5.3 แสดง privileged users ที่ไม่มีการใช้งานมามากกว่า 90 วัน (Stale)

4.4.5.4 แสดง privileged users ที่มีการกำหนดค่า Password Never Expired

4.4.5.5 แสดง privileged users ที่ login จากหลาย locations (Shared)

4.4.6 สามารถทำการวิเคราะห์เหตุการณ์ (event analysis) ที่เกิดขึ้นใน domain ตามช่วงเวลาที่กำหนด โดยสามารถแสดงรายละเอียดได้อย่างน้อยดังต่อไปนี้ Top Users Accounts Lockouts, Password Changes, Account Modified, New User Accounts, Disabled User Accounts, Top Users Login Failures, Login Failures by Department

4.4.7 สร้าง Automate Workflow โดยกำหนด trigger, condition และ action หากตรวจพบสิ่งผิดปกติจากระบบเดียวกัน

4.4.8 สามารถส่งแจ้งเตือนผ่านทาง email โดยอัตโนมัติหากตรวจพบภัยคุกคามในรูปแบบ privilege escalation ได้

4.4.9 สามารถเพิ่มรายชื่อ users เพื่อเฝ้าระวัง (watchlist) โดยอัตโนมัติหากตรวจพบภัยคุกคามในรูปแบบ Credential Access ได้

4.4.10 สามารถกำหนดรีเซ็ตรหัสผ่านหากตรวจพบ account ที่มีการใช้รหัสผ่านที่รั่วไหล (Compromised password) ได้โดยอัตโนมัติ และส่งแจ้งเตือนให้ users ทราบทันทีเมื่อระบบทำการสั่งรีเซ็ตรหัสผ่าน

4.4.11 สามารถตรวจสอบการยืนยันตัวตนบน AD/Domain Controller (Inspection Authentication Traffic) โดยสามารถตรวจสอบโปรโตคอลได้อย่างน้อยดังนี้ Kerberos, NTLM, RDP to DC, LDAP, LDAPS และ SMB to DC

4.4.12 มีความสามารถอย่างน้อยดังต่อไปนี้ Dark Web Monitoring, Brand and Domain Monitoring, Credential Monitoring และ Dark Web Activity Reports

4.4.13 สามารถเก็บและตรวจสอบข้อมูลจากแหล่งต่างๆ ได้เป็นอย่างน้อยดังต่อไปนี้ Dark Web, Social Media, Forums, Criminal Marketplaces และ Chat platforms

4.4.14 สามารถสร้าง Monitoring Rule เพื่อแจ้งเตือนภัยคุกคามที่ตรวจพบได้อย่างน้อยดังต่อไปนี้ Bank Identification Numbers (BINs), Brands & Products, Company domains, Company names, Email addresses, IP addresses, Suppliers และ Vulnerabilities (CVEs)

4.5 จัดหาสิทธิ์การฝึกอบรมเพื่อสร้างความเข้าใจหลักการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือการบริหารจัดการและตอบสนองเหตุการณ์ หรือการเฝ้าระวังและตรวจจับภัยคุกคามทางไซเบอร์ จากสถาบัน SANS Institute แบบร่วมกับวิทยากร ณ สถานที่จัดฝึกอบรม (In Person) หรืออบรมแบบตามอัธยาศัย (On-demand) พร้อมสิทธิ์การสอบวัดความรู้ (Certificate) ตามหลักสูตรที่ได้รับสิทธิ์เข้าร่วมอบรม จำนวนไม่น้อยกว่า 2 สิทธิ์

5. ข้อกำหนดทั่วไป

5.1 ผู้ยื่นข้อเสนอต้องยื่นเสนอรายละเอียดรายการผลิตภัณฑ์ คุณลักษณะเฉพาะ และต้องทำตารางเปรียบเทียบรายละเอียดคุณลักษณะพร้อมแนบแค็ตตาล็อก หรือเอกสารรายละเอียดของผลิตภัณฑ์ที่ยื่นเสนอ โดยให้ระบุให้เห็นอย่างชัดเจน สามารถตรวจสอบได้ว่าสิ่งที่ต้องการอ้างอิง อยู่ในส่วนใด ตำแหน่งใด ของเอกสารที่เสนอมา โดยเอกสารที่อ้างอิงข้อความหรือเอกสารในส่วนอื่นที่เสนอมา ให้หมายเหตุ หรือขีดเส้นใต้ หรือระบายสี พร้อมเขียนหัวข้อกำกับไว้ในเอกสารหรือแค็ตตาล็อกให้ชัดเจน ตามตารางที่สำนักข่าวกรองแห่งชาติกำหนด จะเสนอรายละเอียดที่คลุมเครือ หรือไม่ชัดเจน หรือไม่ครบถ้วน หรือไม่ตรงรายละเอียดที่สำนักข่าวกรองแห่งชาติกำหนดไว้ไม่ได้ หากคณะกรรมการพิจารณาผลการประกวดราคาพิจารณาแล้ว ปรากฏว่ารายละเอียดดังกล่าวไม่ชัดเจนตามข้างต้น จะถือว่าผู้เสนอราคารายนั้น เจตนาที่จะเอาเปรียบและทำให้เกิดความไม่เป็นธรรมกับผู้เสนอราคารายอื่น คณะกรรมการพิจารณาผลการประกวดราคาจะพิจารณาตัดสิทธิ์ผู้เสนอราคารายนั้นทันที

อ้างถึงข้อ	คุณลักษณะเฉพาะของสำนักข่าวกรองแห่งชาติ	คุณลักษณะที่เสนอ	เอกสารอ้างอิง
ระบุหัวข้อให้ตรงกับหัวข้อที่ระบุในเอกสารรายละเอียดคุณลักษณะเฉพาะ (Terms of Reference : TOR) โครงการพัฒนาระบบบูรณาการด้านการข่าว เพื่อการแจ้งเตือนภัยคุกคามทางไซเบอร์ กิจกรรมที่ 1 ต่ออายุระบบบริหารจัดการความปลอดภัยโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล	ให้คัดลอกข้อกำหนดคุณลักษณะเฉพาะที่สำนักข่าวกรองแห่งชาติกำหนดมาใส่ในช่องนี้	ให้ระบุคุณลักษณะที่เสนอ	ระบุหมายเลขหน้าเอกสารอ้างอิงของผู้เสนอ

5.2 ผู้ยื่นข้อเสนอต้องส่งแค็ตตาล็อกรายละเอียดคุณลักษณะของทุกรายการที่ยื่นเสนอ พร้อมระบุชื่อผลิตภัณฑ์ และรุ่นที่นำเสนอให้ชัดเจน กรณีที่อุปกรณ์มีหลายรุ่น (Model) หรือมี Option ต้องระบุให้ชัดเจนว่าจะส่งมอบรุ่น หรือ Series ใด และ Option ใด เพื่อประกอบการพิจารณาของคณะกรรมการฯ

6. กำหนดเวลาส่งมอบพัสดุ

ผู้ขายจะต้องติดตั้ง ตรวจสอบส่งมอบโปรแกรมและระบบคอมพิวเตอร์ที่เสนอ พร้อมจัดทำเอกสารการตั้งค่าคู่มือ ส่งมอบในรูปสื่อดิจิทัล (Digital File) จำนวน 5 ชุด และเอกสารพิมพ์ (Hard Copy) 2 ชุด ส่งให้ ณ สำนักข่าวกรองแห่งชาติ พร้อมดำเนินงานตามขอบเขตงานให้เสร็จสิ้นภายใน 120 วัน นับถัดจากวันลงนามในสัญญา

ซึ่งผู้ขายจะต้องแจ้งกำหนดเวลาการส่งมอบงานแต่ละงวดเป็นลายลักษณ์อักษรให้สำนักข่าวกรองแห่งชาติทราบล่วงหน้าก่อนส่งมอบงานล่วงหน้าอย่างน้อย 7 วันทำการ โดยแบ่งงวดงานเป็น 2 งวด

6.1 งวดที่ 1 ผู้ขายส่งมอบระบบ ตามข้อที่ 4.1 - 4.4 ภายใน 60 วัน นับถัดจากวันลงนามในสัญญา

6.2 งวดที่ 2 ผู้ขายส่งมอบระบบและสิทธิ์การอบรม ตามข้อที่ 4.5 ภายใน 120 วัน นับถัดจากวันลงนามในสัญญา

7. หลักเกณฑ์ในการพิจารณาคัดเลือกข้อเสนอ

สำนักข่าวกรองแห่งชาติกำหนดเกณฑ์การพิจารณา โดยใช้เกณฑ์ราคา

8. วงเงินงบประมาณ

วงเงินงบประมาณ 7,049,200.00 บาท (เจ็ดล้านสี่หมื่นเก้าพันสองร้อยบาทถ้วน) ซึ่งรวมภาษีมูลค่าเพิ่มตลอดจนภาษีอากรอื่น ๆ และค่าใช้จ่ายทั้งปวงด้วยแล้ว

9. งวดงานและการจ่ายเงิน

สำนักข่าวกรองแห่งชาติจะชำระเงินตามจำนวนในสัญญาหลังจากที่ผู้ขายส่งมอบงานถูกต้องเรียบร้อยแล้ว และคณะกรรมการตรวจรับพัสดุได้ตรวจรับงานตามที่สำนักข่าวกรองแห่งชาติกำหนดครบถ้วน โดยจะชำระเงินตามเงื่อนไขและกำหนดเวลา ดังนี้

งวดที่ 1 ชำระเงินในอัตราร้อยละ 70 ของจำนวนเงินในสัญญา เมื่อผู้ขายส่งมอบงานงวดที่ 1 ตามข้อ 6.1 และสำนักข่าวกรองแห่งชาติได้ตรวจรับงานเรียบร้อยแล้ว

งวดที่ 2 ชำระเงินในอัตราร้อยละ 30 ของจำนวนเงินในสัญญา เมื่อผู้ขายส่งมอบงานงวดที่ 2 ตามข้อ 6.2 และสำนักข่าวกรองแห่งชาติได้ตรวจรับงานเรียบร้อยแล้ว

10. อัตราค่าปรับ

หากผู้ขายไม่สามารถส่งมอบพัสดุได้ภายในเวลาที่กำหนดไว้ในสัญญา จะต้องชำระค่าปรับให้แก่สำนักข่าวกรองแห่งชาติ เป็นรายวัน อัตราร้อยละ 0.20 (ศูนย์จุดสองศูนย์) ของราคาพัสดุที่ยังไม่ได้รับมอบ

11. การฝึกอบรม

ผู้ขายต้องทำการอบรม ในรูปแบบการลงมือปฏิบัติจริง (Hands-on) และเสนอแนะการใช้งานให้เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร จำนวนไม่น้อยกว่า 10 คน โดยมีระยะเวลาอบรมไม่น้อยกว่า 1 วัน และผู้จัดการอบรมต้องรับผิดชอบการจัดเตรียมเอกสารประกอบการเรียนการสอน อาหารว่างและอาหารกลางวันสำหรับผู้เข้ารับการอบรม ณ สถานที่ซึ่งสำนักข่าวกรองแห่งชาติจัดเตรียมไว้ให้

12. การรับประกันความชำรุดบกพร่องของพัสดุที่ส่งมอบ

12.1 ผู้ขายต้องให้บริการบำรุงรักษา ตั้งค่าระบบเพิ่มเติมตามที่ผู้ซื้อกำหนด และสนับสนุนเจ้าหน้าที่ของผู้ซื้อโดยให้สามารถใช้งานระบบที่ได้จัดหาและพัฒนาได้อย่างต่อเนื่อง ตลอดช่วงเวลาราชการเป็นระยะเวลา 1 ปี นับจากวันรับมอบงานงวดสุดท้าย

12.2 สำนักข่าวกรองแห่งชาติสามารถขอรับคำปรึกษาด้านเทคนิคทางโทรศัพท์ได้โดยไม่จำกัดจำนวนครั้ง ตลอดช่วงเวลาราชการเป็นระยะเวลา 1 ปี นับจากวันรับมอบงานงวดสุดท้าย

12.3 ผู้ขายจะต้องรับประกันความชำรุดบกพร่องของครุภัณฑ์ที่ซื้อขายตามเอกสารแนบรายละเอียดคุณลักษณะเฉพาะ (Terms of Reference : TOR) โครงการพัฒนาระบบบูรณาการด้านการข่าว เพื่อการแจ้งเตือนภัยคุกคามทางไซเบอร์ กิจกรรมที่ 1 ต่ออายุระบบบริหารจัดการความปลอดภัยโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล ตามรายละเอียดคุณลักษณะเฉพาะ นับถัดจากวันที่สำนักข่าวกรองแห่งชาติ ได้รับมอบครุภัณฑ์โดยต้องรีบ

จัดการซ่อมแซมแก้ไขภายใน 72 ชั่วโมง นับถัดจากวันที่ได้รับแจ้งความชำรุดบกพร่อง โดยมีการบริการ On-site service ณ สำนักข่าวกรองแห่งชาติ นับแต่ได้รับแจ้งตามสัญญาการให้บริการ

12.4 ผู้ขายมีหน้าที่บำรุงรักษาและซ่อมแซมแก้ไขครุภัณฑ์คอมพิวเตอร์หรือชุดโปรแกรมให้อยู่ในสภาพใช้งานได้ดีอยู่เสมอตามเงื่อนไขรับประกันสินค้าของผู้ผลิต โดยให้มีเวลาครุภัณฑ์คอมพิวเตอร์หรือชุดโปรแกรมขัดข้องรวมตามเกณฑ์การคำนวนเวลาขัดข้องไม่เกินเดือนละ 72 ชั่วโมง หรือร้อยละ 10 ของเวลาใช้งานทั้งหมดของคอมพิวเตอร์เดือนนั้น ถ้าครุภัณฑ์คอมพิวเตอร์หรือชุดโปรแกรมขัดข้องเกินระยะเวลาดังกล่าว สำนักข่าวกรองแห่งชาติจะคิดค่าปรับในส่วนที่เกินอัตราชั่วโมงละ 0.035 ของราคาอุปกรณ์คอมพิวเตอร์นั้น ๆ เกณฑ์การคำนวนนับวันและค่าตัวถ่วง เป็นดังนี้

จำนวนชั่วโมงที่ขัดข้องในขณะใดขณะหนึ่งเท่ากับค่าสูงสุดของจำนวนชั่วโมงที่ขัดข้องในขณะนั้นของอุปกรณ์คูณด้วยค่าตัวถ่วง

จำนวนชั่วโมง = ค่าสูงสุด (ชั่วโมงที่ขัดข้อง x ค่าตัวถ่วง)

เศษของชั่วโมงนับเป็น 1 ชั่วโมง

ค่าปรับ = 0.035 x ผลรวมจำนวนชั่วโมง x ราคาครุภัณฑ์คอมพิวเตอร์

กำหนดค่าตัวถ่วงของคอมพิวเตอร์

ครุภัณฑ์ที่ขัดข้อง	ค่าถ่วง
โปรแกรมตรวจจับภัยคุกคามทางไซเบอร์แบบปัญญาประดิษฐ์ จำนวน 1,000 หน่วย	1

13. กรรมสิทธิ์และลิขสิทธิ์ของงาน ข้อมูล เอกสาร และโปรแกรมคอมพิวเตอร์

13.1 ผู้ขายต้องไม่เปิดเผยหรือเผยแพร่งาน ข้อมูล เอกสาร และโปรแกรมคอมพิวเตอร์ที่ผู้ขายส่งมอบให้แก่สำนักข่าวกรองแห่งชาติ ไม่ว่าทั้งหมดหรือเพียงบางส่วนให้แก่บุคคลใด เว้นแต่จะได้รับการอนุญาตอย่างเป็นลายลักษณ์อักษรจากสำนักข่าวกรองแห่งชาติ

13.2 ผู้ขายต้องรับประกันว่า งาน ข้อมูล เอกสาร และโปรแกรมคอมพิวเตอร์ทั้งหมดที่นำมาส่งมอบให้แก่สำนักข่าวกรองแห่งชาติ ในการดำเนินงานตามโครงการนี้ ผู้ขายต้องผ่านการได้รับสิทธิโดยชอบด้วยกฎหมายที่จะนำมาใช้ในการดำเนินงานและส่งมอบให้แก่ สำนักข่าวกรองแห่งชาติ ในการดำเนินงานตามโครงการนี้ เพื่อให้สำนักข่าวกรองแห่งชาติสามารถใช้งานได้โดยชอบด้วยกฎหมายและไม่มีข้อจำกัดใด ๆ

13.3 ในกรณีที่มีบุคคลใดกล่าวอ้างว่า สำนักข่าวกรองแห่งชาติ ละเมิดกรรมสิทธิ์หรือลิขสิทธิ์ในงาน ข้อมูล เอกสาร และโปรแกรมคอมพิวเตอร์ทั้งหมดที่ผู้ขายนำมาส่งมอบให้แก่สำนักข่าวกรองแห่งชาติในการดำเนินงานตามโครงการนี้ ผู้ขายจะต้องรับผิดชอบค่าใช้จ่ายทั้งหมดในการต่อสู้คดี และความเสียหายที่เกิดขึ้นแก่สำนักข่าวกรองแห่งชาติ

13.4 ผู้ขายจะต้องส่งเอกสาร สัญญารักษาความลับ (Non-disclosure Agreement) ที่ลงนามโดยบุคลากรที่เข้าร่วมดำเนินงานในโครงการทั้งหมด กรณีที่มีการเปลี่ยนแปลงหรือเพิ่มบุคลากรผู้เข้าร่วมโครงการจะต้องส่งเอกสารสัญญารักษาความลับของบุคลากรดังกล่าวให้แก่สำนักข่าวกรองแห่งชาติก่อนที่บุคลากรนั้นจะเข้าเริ่มงานในโครงการ

14. ลิขสิทธิ์หรือสิทธิ์ในทรัพย์สินทางปัญญาและการรักษาความลับ

14.1 ผู้ขายตกลงให้ลิขสิทธิ์ในรายงานและข้อมูลที่ผู้ขายจัดทำขึ้นจากการทำงานตามโครงการนี้เป็นของสำนักข่าวกรองแห่งชาติ โดยผู้ขายจะต้องไม่นำข้อมูลที่ได้รับจากการทำงาน รวมทั้งรายงานและข้อมูลที่ผู้ขายได้จัดทำขึ้นไปเปิดเผยหรือใช้งานต่อไป เว้นแต่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากสำนักข่าวกรองแห่งชาติ

14.2 ผู้ชนะการเสนอราคาที่ลงนามในสัญญาซื้อขายแล้ว จะต้องผ่านการตรวจสอบประวัติและพฤติการณ์บุคคล และผ่านกระบวนการรับรองความไว้วางใจจากสำนักข่าวกรองแห่งชาติพร้อมทั้งปฏิบัติตามระเบียบสำนักข่าวกรองแห่งชาติว่าด้วยการรักษาความปลอดภัย พ.ศ.2554

15. เงื่อนไขอื่น ๆ

15.1 สำนักข่าวกรองแห่งชาติขอสงวนสิทธิ์ในการพิจารณาขยายอายุสัญญาตามแนวทางการพิจารณาขยายอายุสัญญา หรือการงดหรือลดค่าปรับของสำนักข่าวกรองแห่งชาติ

15.2 สำนักข่าวกรองแห่งชาติขอสงวนสิทธิ์ในการปรับปรุงแก้ไข หรือยกเลิกข้อกำหนดดังกล่าวนี้บางส่วนหรือทั้งหมด และให้ถือว่าการพิจารณาวินิจฉัยชี้ขาดของสำนักข่าวกรองแห่งชาติเป็นที่สุด ทั้งนี้ผู้ชนะการเสนอราคาตกลงยินยอมไม่เรียกร้องค่าเสียหายไม่ว่าในกรณีใด ๆ ทั้งสิ้นจากสำนักข่าวกรองแห่งชาติ

15.3 ในระหว่างอายุสัญญาซื้อขาย หากสำนักข่าวกรองแห่งชาติเห็นว่าผู้ชนะการเสนอราคาไม่อาจปฏิบัติตามเงื่อนไขในสัญญาซื้อขายข้อใดข้อหนึ่งได้ สำนักข่าวกรองแห่งชาติมีสิทธิ์ยกเลิกสัญญาซื้อขายได้ โดยผู้ชนะการเสนอราคายินยอมที่จะชดใช้ค่าเสียหายต่าง ๆ ที่อาจเกิดขึ้นให้แก่สำนักข่าวกรองแห่งชาติ โดยไม่มีเงื่อนไขภายในกำหนด 15 วัน นับจากวันที่ได้รับแจ้ง

16. ผู้รับผิดชอบโครงการ

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักข่าวกรองแห่งชาติ เลขที่ 321 แขวงดุสิต เขตดุสิต กรุงเทพมหานคร 10300

---

1.	2.	3.	4.	5. .....
ประธานคณะกรรมการ	คณะกรรมการ	คณะกรรมการ	คณะกรรมการ	คณะกรรมการและเลขานุการ