ข้อกำหนดขอบเขตของงาน (Terms of Reference :TOR)
โครงการเช่าใช้บริการศูนย์คอมพิวเตอร์สำหรับวางอุปกรณ์คอมพิวเตอร์
และบริการศูนย์เฝ้าระวังและแจ้งเตือนภัยคุกคามทางคอมพิวเตอร์
ประจำปีงบประมาณ พ.ศ. 2567

1. หลักการและเหตุผล

กรมตรวจบัญชีสหกรณ์ มีความประสงค์เช่าใช้บริการศูนย์คอมพิวเตอร์สำหรับวางอุปกรณ์คอมพิวเตอร์ และบริการศูนย์เฝ้าระวังและแจ้งเตือนภัยคุกคามทางคอมพิวเตอร์ เพื่อใช้เป็นช่องทางการจัดเก็บข้อมูลระบบสารสนเทศที่สำคัญ และเป็นช่องทางติดต่อสื่อสาร เผยแพร่ข้อมูลข่าวสารต่าง ๆ แก่หน่วยงานภายใน และหน่วยงานภายนอกกรมตรวจบัญชีสหกรณ์ ซึ่งประกอบไปด้วยสหกรณ์และกลุ่มเกษตรกร รวมทั้งประชาชนทั่วไป ที่ผ่านมาระบบเทคโนโลยีสารสนเทศของกรมตรวจบัญชีสหกรณ์ได้มีการพัฒนาอย่างต่อเนื่อง มีระบบสารสนเทศที่ช่วยสนับสนุนการดำเนินงานของหน่วยงาน สำหรับให้ทุกหน่วยงานสามารถรับ - ส่งข้อมูลถึงกันได้ตลอดเวลา มีความรวดเร็วไม่เกิดความล่าช้าหรือขัดข้องของข้อมูล เพื่อเพิ่มประสิทธิภาพและความโปร่งใสตรวจสอบได้

ปัจจุบันกรมตรวจบัญชีสหกรณ์ มีความจำเป็นต้องเช่าใช้บริการศูนย์คอมพิวเตอร์สำหรับวางอุปกรณ์คอมพิวเตอร์ และบริการศูนย์เฝ้าระวังและแจ้งเตือนภัยคุกคามทางคอมพิวเตอร์ เพื่อให้บริการระบบสารสนเทศของกรมตรวจบัญชีสหกรณ์สามารถเชื่อมโยงข้อมูลได้อย่างมีประสิทธิภาพและมีเสถียรภาพ ซึ่งเป็นระบบหลักในการปฏิบัติงาน การบริหารงาน และการรายงานผลการปฏิบัติงานตามภารกิจของกรมตรวจบัญชีสหกรณ์ อีกทั้งทางกรมตรวจบัญชีสหกรณ์ได้คำนึงถึงความปลอดภัยของข้อมูล ดังนั้นการเก็บรักษาข้อมูลที่มีการบริหารจัดการฐานข้อมูลอย่างมีประสิทธิภาพอยู่ในศูนย์ข้อมูลไอทีที่มีมาตรฐานสากลรองรับ เน้นความปลอดภัยด้านระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศรับรองเหตุการณ์ภัยพิบัติที่ไม่คาดคิด ถือเป็นอีกช่องทางหนึ่งที่ส่งผลให้ระบบสารสนเทศของกรมตรวจบัญชีสหกรณ์ทำงานได้อย่างมีประสิทธิภาพสูงสุด

2. วัตถุประสงค์

2.1 เพื่อปรับปรุงโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ และการสื่อสารพื้นฐานของหน่วยงาน
2.2 เพื่อขยายขีดความสามารถในการรับ - ส่งข้อมูลภายในหน่วยงานของกรมตรวจบัญชีสหกรณ์ผ่านระบบเครือข่ายให้มีความปลอดภัย และใช้งานได้อย่างมีประสิทธิภาพ
2.3 เพื่อเพิ่มความปลอดภัยให้กับเว็บไซต์ของหน่วยงาน
2.4 เพื่อเฝ้าระวัง และเตือนภัยต่าง ๆ ในการใช้งานระบบสารสนเทศของหน่วยงาน

3. คุณสมบัติของผู้รับจ้าง

3.1 มีความสามารถตามกฎหมาย
3.2 ไม่เป็นบุคคลล้มละลาย
3.3 ไม่อยู่ระหว่างเลิกกิจการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5 ผู้ยื่นข้อเสนอต้องไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้าง และการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 ผู้ยื่นข้อเสนอต้องเป็นผู้มีอาชีพรับจ้างงานดังกล่าว

3.8 ผู้ยื่นข้อเสนอต้องไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอราคารายอื่นที่เข้ายื่นข้อเสนอให้แก่กรมตรวจบัญชีสหกรณ์ ณ วันประกาศประกวดราคา หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรม ในการยื่นข้อเสนอครั้งนี้

3.9 ผู้ยื่นข้อเสนอต้องไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

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

3.11 ผู้ยื่นข้อเสนอซึ่งได้รับคัดเลือกเป็นคู่สัญญาต้องลงทะเบียนในระบบจัดซื้อจัดจ้างภาครัฐ ด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement : e - GP) ของกรมบัญชีกลางตามที่คณะกรรมการ ป.ป.ช. กำหนด

3.12 ผู้ยื่นข้อเสนอต้องไม่อยู่ในฐานะเป็นผู้ไม่แสดงบัญชีรายรับรายจ่ายหรือแสดงบัญชีรายรับรายจ่ายไม่ถูกต้องครบถ้วนในสาระสำคัญ ตามที่คณะกรรมการ ป.ป.ช. กำหนด

3.13 ผู้ยื่นข้อเสนอซึ่งได้รับคัดเลือกเป็นคู่สัญญาต้องรับและจ่ายเงินผ่านบัญชีธนาคาร เว้นแต่การจ่ายเงินแต่ละครั้งซึ่งมีมูลค่าไม่เกินสามหมื่นบาทคู่สัญญาอาจจ่ายเป็นเงินสดก็ได้ ตามที่คณะกรรมการ ป.ป.ช. กำหนด

3.14 ผู้ยื่นข้อเสนอต้องเป็นนิติบุคคลที่จดทะเบียนจัดตั้งตามกฎหมายไทย ซึ่งประกอบธุรกิจเกี่ยวกับการเป็นผู้ให้เช่าพื้นที่ศูนย์คอมพิวเตอร์ ที่ให้บริการระบบเครือข่ายเทคโนโลยีสารสนเทศ โดยมีวัตถุประสงค์ในการประกอบกิจการเกี่ยวกับงานจ้างตามประกาศนี้มาแล้วไม่น้อยกว่า 3 ปี

3.15 ผู้ยื่นข้อเสนอต้องสามารถให้บริการอินเทอร์เน็ตตามใบอนุญาตการให้บริการอินเทอร์เน็ตแบบที่หนึ่ง หรือใบอนุญาตประกอบกิจการโทรคมนาคมแบบที่หนึ่ง หรืออย่างใดอย่างหนึ่ง

3.16 ผู้ยื่นข้อเสนอจะต้องมีผู้ชำนาญงานพร้อมปฏิบัติงาน (On-Call Service) ตลอด 24 ชั่วโมง 7 วันต่อสัปดาห์ และมีผู้ชำนาญงานพร้อมให้คำปรึกษาและพร้อมปฏิบัติงาน ในกรณีที่มีปัญหาเร่งด่วน (Urgent Case) ตลอดอายุสัญญา

3.17 ผู้ยื่นข้อเสนอต้องมีทุนจดทะเบียนไม่น้อยกว่า 200,000,000.00 บาท (สองร้อยล้านบาทถ้วน) โดยมีหลักฐานการจดทะเบียน ซึ่งกรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์ออกให้หรือรับรองไม่เกิน 3 เดือน

3.18 ผู้ยื่นข้อเสนอจะต้องได้รับการรับรองมาตรฐาน มาตรฐาน ISO/IEC 27001, ISO/IEC 20000, ISO 22301 และ ISO 27017 เป็นอย่างน้อย

3.19 ผู้ยื่นข้อเสนอต้องเป็นนิติบุคคลและมีผลงานการเป็นผู้ให้เช่าพื้นที่ศูนย์คอมพิวเตอร์ ที่ให้บริการระบบเครือข่ายเทคโนโลยีสารสนเทศ หรือ ศูนย์เฝ้าระวังและแจ้งเตือนภัยคุกคามทางคอมพิวเตอร์ (Security Operation Center : SOC) ในวงเงินไม่น้อยกว่า 1,500,000.00 บาท (หนึ่งล้านห้าแสนบาทถ้วน) จำนวนไม่น้อยกว่า 2 ผลงาน ซึ่งเป็นผลงานที่สิ้นสุดสัญญาแล้วในระยะเวลาไม่เกิน 3 ปี ที่ผ่านมานับจากวันที่ยื่นเสนอราคา หรือที่อยู่ในระหว่างให้บริการมาแล้วไม่น้อยกว่า 1 ปี โดยจะต้องแนบสำเนาหนังสือรับรองผลงาน และเป็นผลงานที่เป็นคู่สัญญาโดยตรงกับส่วนราชการ หน่วยงานตามกฎหมายว่าด้วยการระเบียบบริหารราชการส่วนท้องถิ่น หน่วยงานอื่นซึ่งมีกฎหมายบัญญัติให้มีฐานะเป็นราชการบริหารส่วนท้องถิ่นรัฐวิสาหกิจหรือหน่วยงานเอกชนที่กรมตรวจบัญชีสหกรณ์ เชื่อถือ

3.20 ผู้ยื่นข้อเสนอต้องมีศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) ตั้งอยู่ในประเทศไทย อย่างน้อย 3 ศูนย์ข้อมูล

3.21 ผู้ยื่นข้อเสนอต้องมีวงจรเชื่อมโยงกับศูนย์แลกเปลี่ยนข้อมูลอินเทอร์เน็ตภายในประเทศ (National Internet Exchange: NIX) ไม่น้อยกว่า 5 แห่ง และวงจรเชื่อมโยงกับศูนย์แลกเปลี่ยนข้อมูลอินเทอร์เน็ตเพื่อออกต่างประเทศ (International Internet Gateway: IIG) ไม่น้อยกว่า 3 แห่ง ในกรณีที่ Gateway ใด Gateway หนึ่งขัดข้องก็สามารถใช้งานอีก Gateway ได้โดยอัตโนมัติ

3.22 ผู้ยื่นข้อเสนอต้องมีเจ้าหน้าที่ผู้เชี่ยวชาญสำหรับดำเนินงาน และให้คำแนะนำด้านเทคนิค โดยมีใบรับรอง CompTIA Security, Certified Ethical Hacker และ ITIL Foundation เป็นอย่างน้อย

4. รายละเอียดคุณสมบัติของบริการให้เช่าใช้บริการศูนย์คอมพิวเตอร์สำหรับวางอุปกรณ์คอมพิวเตอร์และบริการศูนย์เฝ้าระวังและแจ้งเตือนภัยคุกคามทางคอมพิวเตอร์

คุณสมบัติพื้นที่วางเครื่องคอมพิวเตอร์แม่ข่าย (Co-Location)

4.1 ผู้รับจ้างจะต้องให้บริการพื้นที่บนตู้ Rack ให้กับผู้ใช้บริการเพื่อติดตั้งระบบ Server ขนาด 42U และมีไฟฟ้าให้ใช้งานได้เพียงพอ

4.2 ผู้รับจ้างต้องจัดเตรียมรางไฟ หรือ Power Distribution Unit (PDU) ชนิด 24 Outlet จำนวน 2 ชุด

4.3 ผู้รับจ้างจะต้องจัดเตรียม Fixed Shelf Rack สำหรับวางอุปกรณ์ภายใน Rack จำนวน 3 ชุด

4.4 ผู้รับจ้างจะต้องจัดเตรียมอุปกรณ์ Gigabit Switch (24-Port) สำหรับภายในตู้ Rack จำนวน 1 ตัว

4.5 ผู้รับจ้างจะต้องมีระบบรักษาความปลอดภัย ณ ศูนย์คอมพิวเตอร์ โดยสามารถสแกนรหัสผ่านนิ้วมือ หรือสามารถใช้บัตรผ่านเข้า - ออกได้

4.6 ผู้รับจ้างจะต้องมีระบบป้องกัน และระงับอัคคีภัยที่สามารถทำงานได้หากมีเหตุเพลิงไหม้เกิดขึ้น

4.7 ผู้รับจ้างจะต้องมีระบบรองรับการทำงานของระบบป้องกันน้ำรั่ว (Water Detector) ที่สามารถแจ้งเตือนตำแหน่งที่เกิดปัญหาน้ำรั่วไหล

4.8 ผู้รับจ้างจะต้องมีระบบรองรับการทำงานของระบบสำรองไฟฟ้าแบบต่อเนื่อง (UPS) พร้อมด้วยเครื่องกำเนิดไฟฟ้าที่สามารถทำงานโดยอัตโนมัติ (Generator) ที่ทำงานในลักษณะ N+1 เมื่อเกิดปัญหา

4.9 ผู้รับจ้างเช่าใช้บริการศูนย์คอมพิวเตอร์สำหรับวางอุปกรณ์คอมพิวเตอร์ จะต้องเป็นผู้ที่ได้รับมาตรฐาน ISO/IEC 27001, ISO/IEC 20000, ISO 22301 และ ISO 27017 เป็นอย่างน้อย

4.10 ผู้รับจ้างมีระบบโทรทัศน์วงจรปิดดูแลศูนย์บริการข้อมูลตลอด 24 ชั่วโมง 7 วันต่อสัปดาห์ โดยสามารถเก็บข้อมูลย้อนหลังได้ถึง 90 วัน

4.11 ผู้รับจ้างจะต้องมีศูนย์บริการเครือข่ายที่มีเจ้าหน้าที่ประจำในการรับแจ้งเหตุขัดข้องที่เกี่ยวกับการให้บริการ และสามารถแก้ไขเหตุขัดข้องและปัญหาได้ตลอด 24 ชั่วโมง 7 วันต่อสัปดาห์

4.12 ผู้รับจ้างมีเจ้าหน้าที่ประจำ Call Center เพื่อคอยช่วยเหลือกรณีหน่วยงานมีปัญหาการใช้งานได้ตลอด 24 ชั่วโมง 7 วันต่อสัปดาห์

คุณสมบัติโครงข่ายสัญญาณข้อมูล (Network) และอินเทอร์เน็ต (Internet)

4.13 ผู้รับจ้างต้องจัดหา IP Address (IPv4) ไม่น้อยกว่า 35 IP

4.14 ผู้รับจ้างจะต้องจัดเตรียม Port เชื่อมต่อการให้บริการอินเทอร์เน็ต อย่างน้อยขนาด 1 Gigabit Ethernet (UTP CAT 6) จำนวน 5 Port

4.15 ผู้รับจ้างจะต้องจัดเตรียมอินเทอร์เน็ตภายในประเทศ ความเร็วอย่างน้อย 100 Mbps. และต่างประเทศ ความเร็วอย่างน้อย 1 Mbps.

4.16 ผู้รับจ้างต้องไม่จำกัดปริมาณการรับ – ส่งข้อมูลทั้งภายในประเทศและต่างประเทศในความเร็วที่กำหนด ตามข้อ 4.15

4.17 ผู้รับจ้างจะต้องให้บริการเครือข่ายสัญญาณสื่อสารข้อมูลแบบส่วนตัว (Private Link) ระหว่างกรมตรวจบัญชีสหกรณ์กับสถานที่เช่าใช้บริการศูนย์คอมพิวเตอร์สำหรับวางอุปกรณ์คอมพิวเตอร์ของกรมตรวจบัญชีสหกรณ์ ความเร็วไม่น้อยกว่า 35 Mbps. จำนวน 1 วงจร

4.18 ผู้รับจ้างสามารถให้บริการและรองรับการใช้งาน IPv6/64 ได้เป็นอย่างน้อย

คุณสมบัติด้าน Security

4.19 ผู้รับจ้างต้องให้บริการเว็บแอปพลิเคชันไฟล์วอลล์เพื่อป้องกันการโจมตี และรายงานผลภัยคุกคามเว็บไซต์ภายใต้โดเมน cad.go.th โดยมี Bandwidth ไม่เกิน 1 Terabytes (TB) ต่อเดือน

4.20 ผู้รับจ้างจะต้องมีระบบตรวจสอบปริมาณข้อมูลการใช้งานแบบ Online ผ่าน Web browser โดยสามารถแสดงเป็นกราฟการใช้งานและเรียกดูย้อนหลังได้

4.21 ผู้รับจ้างจะต้องมีคุณสมบัติและความสามารถทางเทคนิคในการป้องกันการโจมตีในระดับเว็บแอปพลิเคชัน (Web Application Firewall) อย่างน้อยดังต่อไปนี้

4.21.1 รองรับการใช้งานโปรโตคอล HTTP หรือ HTTPS ได้เป็นอย่างน้อย

4.21.2 รองรับการทำ SSL Inspection

4.21.3 สามารถตรวจสอบภัยคุกคามด้านความปลอดภัยเว็บแอปพลิเคชันหรือการใช้งานที่ผิดปกติได้โดยใช้เทคนิคหรือวิธีการดังต่อไปนี้

4.21.3.1 SQLi -Common Patterns

4.21.3.2 Application Attack Signatures

4.21.3.3 HTTP Request Smuggling Attack , HTTP Response Splitting Attack

4.21.4 สามารถป้องกันการโจมตีเหล่านี้ได้เป็นอย่างน้อย

4.21.4.1 Cross Site Scripting (XSS)

4.21.4.2 SQL Injection

4.21.4.3 session fixation attack

4.21.4.4 Buffer Overflow

4.21.4.5 Anomaly:Header:Cookie

4.21.4.6 XSS, HTML Injection - Malicious HTML Encoding Multiple URL Encoding Detected

4.21.4.7 Directory Traversal

4.21.4.8 SQLi - String Function

4.21.4.9 SQLi - AND/OR Digit Operator Digit

4.21.4.10 SQLi - Math Comparison

4.21.4.11 HTML Injection - A Tag

4.21.4.12 Java - Deserialization, Code Injection

4.21.4.13 HTML Injection - HTML Tag

4.21.4.14 Apache Struts - Code Injection - CVE:CVE-2017-9805

4.21.4.15 Microsoft ASP.NET - Code Injection - Function response.write

4.21.5 สามารถรองรับการทำงานได้ 3 Mode ได้แก่ Simulate, Legacy Captcha, Block

4.21.6 สามารถป้องกันการโจมตี Web Application ตาม OWASP Top 10

4.21.7 สามารถทำการ Updates Signature ได้ทั้งแบบ Manual หรือแบบ Automatic

4.21.8 สามารถตั้งค่า Web Application Firewall (WAF) ได้แบบไม่จำกัดจำนวน และการตั้งค่าการเปิดปิด WAF Rule ต้องมีผลบังคับใช้ (Effective) ภายในเวลาไม่เกิน 30 วินาที

4.21.9 ป้องกันการร้องขอ (Request) ที่เป็นอันตรายได้โดยการ Block by Request และ Block by IP Address โดยสามารถกำหนดระยะเวลาที่ทำการ Block ได้ เช่น 30 วินาที และ 1 นาที เป็นต้น

4.21.10 มีระบบแสดงผลภัยคุกคามทางเว็บแอปพลิเคชันต่าง ๆ โดยสามารถร้องขอผลแสดงภัยคุกคามกับทางผู้รับจ้างได้

4.21.11 สามารถแสดงรายงานผลภัยคุกคามเชิงลึกแบบละเอียดผ่านหน้า Dashboard ได้ กรมตรวจบัญชีสหกรณ์สามารถขอให้ผู้รับจ้างส่งข้อมูลย้อนหลังได้เพิ่มเติม

4.21.12 ให้คำปรึกษาเกี่ยวกับบริการวิเคราะห์เฝ้าระวังภัยคุกคามต่าง ๆ ที่เกิดขึ้นและสนับสนุนการทำงานเกี่ยวกับระบบเว็บแอปพลิเคชันไฟร์วอลล์ในวันทำการแบบ 5 วัน 8 ชั่วโมง ระหว่างเวลา 08.30 น. - 17.30 น.

4.21.13 ผู้รับจ้างต้องจัดเตรียมระบบเว็บแอปพลิเคชันไฟร์วอลล์ และระบบสำหรับจัดเก็บข้อมูลการโจมตีที่เกิดจากเว็บแอปพลิเคชันไฟร์วอลล์ กรมตรวจบัญชีสหกรณ์สามารถขอให้ผู้รับจ้างส่งข้อมูลย้อนหลังได้เพิ่มเติม

4.21.14 ผู้รับจ้างต้องจัดให้มีเจ้าหน้าที่ที่มีความเชี่ยวชาญด้านเว็บแอปพลิเคชันไฟร์วอลล์และด้านการวิเคราะห์และป้องกันภัยคุกคามทางด้านเว็บแอปพลิเคชัน เพื่อทำหน้าที่ในการปรับแต่งและกำหนดค่าการทำงานของอุปกรณ์และระบบต่าง ๆ ที่เกี่ยวข้องเพื่อให้สามารถวิเคราะห์ ป้องกัน และรายงานผลภัยคุกคามที่เกิดขึ้นกับระบบงานเว็บแอปพลิเคชันของกรมตรวจบัญชีสหกรณ์ ที่เปิดให้บริการทางเครือข่ายอินเทอร์เน็ตอย่างมีประสิทธิภาพ

4.21.15 สามารถแสดงรายงาน (Analytic) บน Dashboard โดย Dashboard ที่แสดงต้องประกอบด้วยข้อมูล Total Requests, Cached Request, Bandwidth, Top Threat Countries และ Top Traffic Countries ได้เป็นอย่างน้อย

4.22 ผู้รับจ้างต้องให้บริการศูนย์เฝ้าระวังและแจ้งเตือนภัยคุกคามทางคอมพิวเตอร์ Security Operation Center (SOC) โดยมีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ เพื่อทำการวิเคราะห์และแจ้งเตือนภัยคุกคามฯ ให้กับผู้ใช้บริการ โดยมีขอบเขตดังต่อไปนี้

4.22.1 ผู้รับจ้างต้องดำเนินการจัดเก็บข้อมูลบันทึกประวัติการทำงานของระบบคอมพิวเตอร์ (Log) จากอุปกรณ์เครือข่าย/อุปกรณ์ด้านความมั่นคงปลอดภัย และเครื่องคอมพิวเตอร์แม่ข่ายที่สำคัญของกรมตรวจบัญชีสหกรณ์ ด้วยในรูปแบบ Centralize Log โดยระบบดังกล่าวต้องจัดเก็บข้อมูลได้ไม่น้อยกว่า 90 วัน และสามารถนำข้อมูลดังกล่าวมาทำการจัดเรียง วิเคราะห์ ตรวจสอบ พร้อมทั้งแสดงผลได้ตามหัวข้อดังต่อไปนี้

4.22.1.1 เว็บไซต์แสดงผลการวิเคราะห์ข้อมูลการใช้งานตามข้อมูลที่จัดเก็บ

4.22.1.2 แถบค้นหาข้อมูลจราจรแบบเดียวกับกูเกิ้ล (Search)

4.22.1.3 แจ้งเตือนฉุกเฉินเมื่อเกิดเหตุ (Incident Response)

4.22.1.4 รายงานด้านความปลอดภัยทางคอมพิวเตอร์

4.22.1.5 รายงานความเสี่ยงและภัยคุกคามทางคอมพิวเตอร์

4.22.2 ระบบจัดเก็บข้อมูล Log จะต้องสามารถรองรับปริมาณข้อมูล Log ได้ไม่น้อยกว่า 5 GB ต่อวันและต้องสามารถส่งข้อมูลดังกล่าวไปยังระบบ SOC เพื่อทำการวิเคราะห์และบริหารจัดการข้อมูลดังกล่าวได้

4.22.3 ระบบจัดเก็บข้อมูล Log จะต้องมีระบบทดแทน (HA) หรือทำงานร่วมกันแบบกลุ่ม (Cluster) หรือทำงานร่วมกันไม่น้อยกว่า 2 ตัว (Multiple Node) หรือ มีการสำรองข้อมูลเพื่อรองรับการกู้คืนระบบ กรณีเกิดความเสียหายของระบบ (Snapshot backup) และรองรับการขยายพื้นที่จัดเก็บข้อมูล (Storage) ของ Log ได้

4.22.4 ผู้รับจ้างต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัย เพื่อป้องกันการเข้าถึงข้อมูล Log โดยไม่ได้รับอนุญาต

4.22.5 ระบบจัดเก็บข้อมูล Log ต้องมีช่องทางสำหรับให้เจ้าหน้าที่ของกรมตรวจบัญชีสหกรณ์ สามารถเข้าตรวจสอบหรือค้นหาข้อมูล Log ที่จัดเก็บได้แบบเรียลไทม์ (Real Time)

4.22.6 ผู้รับจ้างต้องจัดให้มีการเทียบสัญญาณนาฬิกาบนเครื่องคอมพิวเตอร์จากเครื่องให้บริการเทียบเวลาที่เป็นมาตรฐาน เช่น สถาบันมาตรวิทยาแห่งชาติ (NIMT) กรมอุทกศาสตร์ กองทัพเรือหรือ National Institute of Standards and Technology, US หรือ ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย เป็นต้น

4.22.7 การวิเคราะห์ (Correlation) และรายงานผลภัยคุกคามทางคอมพิวเตอร์ ผู้รับจ้างจะต้องดำเนินการร่วมกับเจ้าหน้าที่ของกรมตรวจบัญชีสหกรณ์ โดยการนำข้อมูล Log และข้อมูลที่ได้จากระบบเว็บแอปพลิเคชันไฟล์วอลล์ ดำเนินการตรวจสอบ และวิเคราะห์ข้อมูลตามกระบวนการ ซึ่งเป็นไปตามมาตรฐาน ดังนี้

4.22.7.1 สามารถวิเคราะห์ข้อมูลจาก Log ที่จัดเก็บได้

4.22.7.2 สามารถวิเคราะห์ความสัมพันธ์ของเหตุการณ์ต่าง ๆ ด้านความปลอดภัยสารสนเทศได้

4.22.7.3 สามารถแจ้งเตือนไปยังผู้รับจ้างได้แบบอัตโนมัติ ในกรณีที่เกิดภัยคุกคามหรือเป็นการใช้งานปกติของระบบแต่มีพฤติกรรมที่น่าสงสัย หรือระบบทำงานที่ผิดปกติ โดยผู้รับจ้างจะต้องวิเคราะห์ แนะนำ แนวทางแก้ไข และแจ้งเหตุดังกล่าวให้เจ้าหน้าที่ของกรมตรวจบัญชีสหกรณ์ ทราบ

4.22.7.4 สามารถกำหนดชนิดของอุปกรณ์หรือระบบต้นทางของข้อมูล Log ได้

4.22.7.5 มีผู้เชี่ยวชาญให้คำปรึกษาทางด้านเทคนิค และทำหน้าที่ปรับแต่ง กำหนดค่าการทำงานของระบบ SOC หรือ Log Analyze เพื่อวิเคราะห์ความสัมพันธ์ของเหตุการณ์และเฝ้าระวังภัยคุกคามทางคอมพิวเตอร์

4.22.8 จัดทำรายงานการปฏิบัติงานของศูนย์ Security Operation Center (SOC) ที่ประกอบด้วย

4.22.8.1 รายงานสรุปภัยคุกคามทางคอมพิวเตอร์สำหรับผู้บริหาร

4.22.8.2 รายงานสรุปเหตุการณ์ด้านความปลอดภัยของอุปกรณ์และบริการที่เฝ้าระวัง โดยแสดงสถานะ ระดับความรุนแรง ผลกระทบ สูงสุด 15 เหตุการณ์ (กรณีไม่ถึงให้สรุปเหตุการณ์ตามจำนวนที่เกิดขึ้นจริง)

4.22.9 ผู้รับจ้างจะต้องมีการแจ้งเตือนหากมีเหตุผิดปกติเกิดขึ้น กรณีมีการบุกรุกทางไซเบอร์ ระดับความรุนแรง ผลกระทบสูงสุด (Critical) ภายใน 15 นาที ระดับความรุนแรง ผลกระทบสูง (High) ภายใน 3 ชั่วโมง ผ่านทางแอปพลิเคชัน Line หรือ E-mail อย่างใดอย่างหนึ่งเป็นอย่างน้อย

4.23 การแจ้งเตือนในกรณีที่วิเคราะห์ข้อมูลแล้วพบเหตุการณ์ผิดปกติที่ก่อให้เกิดผลกระทบ หรือพบผู้บุกรุกให้ดำเนินการดังนี้

4.23.1 หากพิจารณาว่าเป็นการบุกรุกที่อาจส่งผลร้ายแรงต่อระบบงานของกรมตรวจบัญชีสหกรณ์ ผู้รับจ้างต้องดำเนินการแจ้งให้กรมตรวจบัญชีสหกรณ์ ทราบทันทีทางโทรศัพท์เคลื่อนที่ (Mobile Phone) หรือระบบการสื่อสารอื่น ๆ ที่เหมาะสม และให้คำแนะนำ พร้อมทั้งเสนอวิธีการแก้ปัญหาเฉพาะกิจ ทั้งนี้การบุกรุกที่อาจส่งผลร้ายแรง หมายถึง เหตุที่ทำให้ทราบได้ว่าอาจถูกบุกรุก

4.23.1.1 ผู้รับจ้างตรวจสอบได้ว่าถูกบุกรุกโจมตีที่ทำให้ระบบ ไม่สามารถทำงานได้หรือหยุดทำงาน

4.23.1.2 ผู้รับจ้างตรวจสอบได้ว่ารายละเอียดหน้าเว็บไซต์ของกรมตรวจบัญชีสหกรณ์ถูกแก้ไขเปลี่ยนแปลง

4.23.2 หากพิจารณาว่าเป็นการบุกรุกที่ไม่ส่งผลร้ายแรงต่อระบบงานของกรมตรวจบัญชีสหกรณ์ ผู้รับจ้างต้องดำเนินการแจ้งไปยังกรมตรวจบัญชีสหกรณ์ ทราบ ผ่านทาง แอปพลิเคชัน Line หรือ E-mail อย่างใดอย่างหนึ่งเป็นอย่างน้อย

4.23.3 หากมีวันหยุดติดต่อกันเกิน 2 วัน ผู้รับจ้างต้องวิเคราะห์ข้อมูลและส่งมอบผลลัพธ์จากการวิเคราะห์ภายในวันทำการถัดไป และกรณีพบการบุกรุกผู้รับจ้างต้องแจ้งต่อกรมตรวจบัญชีสหกรณ์ ทราบทันที

5. กำหนดส่งมอบงาน

5.1 ผู้รับจ้างต้องดำเนินการตามข้อที่ 4.1 – 4.22 ให้แล้วเสร็จ และส่งมอบงานในรูปแบบของเอกสารพร้อมแผ่นซีดี จำนวน 3 ชุด ซึ่งประกอบไปด้วย

1) เอกสารข้อเสนอทางด้านเทคนิค
2) รายละเอียดคุณสมบัติของการให้บริการ

ภายใน 15 วันนับถัดจากวันลงนามในสัญญา

5.2 เมื่อผู้รับจ้างส่งมอบงานตามข้อ 5.1 เรียบร้อยแล้ว ให้ดำเนินการส่งงานงวดที่ 1 – 10 ดังนี้ ผู้รับจ้างต้องส่งมอบผลการดำเนินงานในรูปแบบรายงานประจำเดือนให้กับกรมตรวจบัญชีสหกรณ์ในรูปแบบของเอกสาร จำนวน 3 ชุด ซึ่งประกอบไปด้วย

1) รายงานสรุปผลปริมาณการใช้งานศูนย์ข้อมูลคอมพิวเตอร์ (Data Center)
2) รายงานปัญหาการใช้บริการอินเทอร์เน็ต
3) รายงานการบันทึกประวัติการทำงานของระบบคอมพิวเตอร์ (Log) จากอุปกรณ์เครือข่าย/อุปกรณ์ด้านความมั่นคงปลอดภัย และเครื่องคอมพิวเตอร์แม่ข่าย
4) รายงานสรุปผลการปฏิบัติงานศูนย์เฝ้าระวังความปลอดภัยระบบคอมพิวเตอร์ และสารสนเทศ (Security Operation Center)
5) รายงานการใช้บริการการป้องกันการโจมตีในระดับเว็บแอปพลิเคชัน (Web Application Firewall)

6) รายงานข้อมูลภัยคุกคามเชิงลึก (Incident Report) พร้อมแผ่นซีดีที่บันทึกรายงาน เอกสารข้างต้น จำนวน 3 แผ่น ภายในวันที่ 10 ของเดือนถัดไป

6. ระยะเวลาการดำเนินการ

ระยะเวลาในการดำเนินการ 10 เดือน ของปีงบประมาณ พ.ศ. 2567

7. วงเงินในการจัดหา

จำนวน 1,722,700.00 บาท (หนึ่งล้านเจ็ดแสนสองหมื่นสองพันเจ็ดร้อยบาทถ้วน)

8. เงื่อนไขการชำระเงิน

ชำระเงินเป็นงวดตามสัญญาเช่ารายเดือน

9. ประโยชน์ที่คาดว่าจะได้รับ

กรมตรวจบัญชีสหกรณ์ มีพื้นที่สำหรับวางเครื่องคอมพิวเตอร์แม่ข่ายเพียงพอต่อความต้องการของระบบสารสนเทศ และข้อมูลสารสนเทศมีความปลอดภัย เนื่องจากมีระบบบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศตามมาตรฐาน ISO/IEC 27001 และด้านระบบบริหารจัดการบริการสารสนเทศตามมาตรฐาน ISO/IEC 20000