ข้อกำหนดขอบเขตของงาน (Terms of Reference: TOR)
โครงการจัดหาระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์และวิเคราะห์ภัยคุกคามบนเครือข่ายแบบรวมศูนย์
(Security Incident Event Management: SIEM)
สำนักงานเศรษฐกิจการคลัง กระทรวงการคลัง

---

1. ความเป็นมา

สำนักงานเศรษฐกิจการคลัง (สศค.) โดยศูนย์เทคโนโลยีสารสนเทศ เป็นหน่วยงานที่มีหน้าที่ความรับผิดชอบในงานด้านเทคโนโลยีสารสนเทศและการสื่อสารของ สศค. โดยทางศูนย์เทคโนโลยีสารสนเทศ ได้ให้บริการด้านอินเทอร์เน็ตแก่ข้าราชการและลูกจ้างของ สศค. รวมทั้งให้บริการงานระบบฯ ต่างๆ แก่บุคคลภายนอก และภายในสำนักงานฯ ผ่านทางอินเทอร์เน็ต และอินทราเน็ต

เนื่องในปัจจุบันศูนย์เทคโนโลยีสารสนเทศ ได้มีการนำระบบเทคโนโลยีสารสนเทศมาใช้กับระบบงานต่าง ๆ ที่สำคัญในหน่วยงานกันอย่างแพร่หลาย และยังเป็นระบบที่ให้บริการกับประชาชนทั่วไปผ่านเครือข่ายอินเทอร์เน็ต ซึ่งเป็นเหตุให้ผู้ที่ไม่ประสงค์ดีที่ปะปนอยู่กับผู้ใช้งานทั่วไป สามารถเข้าโจมตีระบบงานสำคัญต่างๆ และอาจก่อให้เกิดความเสียหายแก่หน่วยงานได้ โดยในปัจจุบันนั้นผู้ดูแลจะต้องใช้ระยะเวลาในตรวจสอบ รวบรวมข้อมูลเพื่อทำการวิเคราะห์การโจมตีที่เกิดขึ้นค่อนข้างนาน และเพื่อให้เป็นไปตามข้อกำหนดตามหลักเกณฑ์ของ “พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560”

ศูนย์เทคโนโลยีสารสนเทศ จึงสมควรที่จัดซื้อจัดหาโครงการจัดหาระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์และวิเคราะห์ภัยคุกคามบนเครือข่ายแบบรวมศูนย์ เพื่อรวบรวมข้อมูลและวิเคราะห์ข้อมูล Log จากอุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์แม่ข่าย ทำให้บริการจัดการข้อมูล Log ของหน่วยงานได้อย่างมีประสิทธิภาพ และตรงตามข้อกำหนดของพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์

2. วัตถุประสงค์

1 เพื่อจัดหาระบบรักษาความปลอดภัยสารสนเทศให้มีความทันสมัยตามเทคโนโลยีในปัจจุบัน และให้รองรับกับปริมาณข้อมูล Log ของระบบงานคอมพิวเตอร์ในปัจจุบัน

2 เพื่อเพิ่มประสิทธิภาพในการค้นหาและวิเคราะห์ภัยคุกคามต่าง ๆ ที่เกิดขึ้นในเครือข่าย สศค. ให้สามารถทำได้อย่างมีประสิทธิภาพและรวดเร็วยิ่งขึ้น

3 เพิ่มขีดความสามารถในการป้องกันภัยคุกคามใหม่ ๆ ที่จะเกิดขึ้นในอนาคตได้และป้องกันความเสี่ยงที่อาจเกิดจากภัยคุกคามทางไซเบอร์ได้

4 เพื่อให้เป็นไปตามข้อกำหนดตามหลักเกณฑ์ของ “พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

5 เพื่อใช้ในการบริหารจัดการเกี่ยวกับความมั่นคงปลอดภัยในระบบเครือข่ายสื่อสาร และข้อมูลสารสนเทศของ สศค. ที่เกิดจากการโจมตีภายนอก สร้างความเชื่อมั่นให้ระบบเครือข่ายสื่อสารมีเสถียรภาพ

3. คุณสมบัติผู้ยื่นเสนอราคา

3.1 ผู้ยื่นข้อเสนอต้องเป็นนิติบุคคลที่มีการจดทะเบียนก่อตั้งบริษัทมาแล้วไม่น้อยกว่า 3 ปี โดยมีหลักฐานการจดทะเบียน ณ กรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์ ซึ่งออกเอกสารหรือรับรองการจดทะเบียนให้ไม่เกิน 3 เดือนนับถึงวันที่เสนอราคา

3.2 ผู้ยื่นข้อเสนอต้องมีผลงานในการขายระบบเครือข่ายคอมพิวเตอร์หรือระบบรักษาความปลอดภัยระบบเครือข่าย และเป็นคู่สัญญาโดยตรงกับหน่วยงานราชการหรือรัฐวิสาหกิจ อย่างน้อย 1 สัญญา มูลค่าของสัญญาไม่น้อยกว่า 9,000,000 บาท (เก้าล้านบาทถ้วน) ซึ่งผลงานนั้นต้องมีระยะเวลาไม่เกิน 5 ปี นับถัดจากวันสิ้นสุดในสัญญา และต้องแสดงหลักฐานเอกสารรับรองผลงานโดยคู่สัญญาพร้อมสำเนาสัญญา ทั้งนี้ สศค. สงวนสิทธิ์ที่จะตรวจสอบข้อเท็จจริงโดยตรงจากหน่วยงานตามเอกสารที่เสนอนั้น

3.3 ผู้ยื่นข้อเสนอต้องได้รับการแต่งตั้งให้เป็นตัวแทนจำหน่ายจากบริษัทผู้ผลิตหรือบริษัทผู้ผลิตสาขาประจำประเทศไทย และต้องได้รับการรับรองว่าอุปกรณ์ที่เสนอเป็นอุปกรณ์ใหม่ ไม่เคยใช้งานมาก่อน ยังอยู่ในสายการผลิต สนับสนุนการรับประกัน (Warranty) สนับสนุนทางด้านเทคนิคและบริการหลังการขาย โดยแนบสำเนาหนังสือแต่งตั้งและหนังสือรับรองเสนอทาง e-GP สำหรับรายการที่ 5.1, 5.2, 5.3, 5.4, 5.5, 5.6 และ 5.7

3.4 ผู้ยื่นข้อเสนอต้องมีเจ้าหน้าที่ด้านเทคนิคที่ได้รับหนังสือรับรอง (Certificate) ในด้าน Network Security ระดับ Professional หรือดีกว่า จากบริษัทผู้ผลิตหรือบริษัทผู้ผลิตสาขาประจำประเทศไทยของอุปกรณ์ตามรายการที่ 5.1 และเป็นพนักงานประจำของผู้ยื่นข้อเสนอ อย่างน้อย 1 คน โดยแนบสำเนาหนังสือรับรองและหลักฐานทาง e-GP

3.5 หากมีการเปลี่ยนแปลงบุคลากรในภายหลังจากการชนะการประกวดราคาด้วยวิธีอิเล็กทรอนิกส์ และในช่วงดำเนินงานโครงการจนตรวจรับงานงวดสุดท้ายแล้วเสร็จสมบูรณ์ ผู้ยื่นเสนอราคาจะต้องแจ้งให้ สศค. ทราบเป็นลายลักษณ์อักษร และบุคลากรใหม่จะต้องมีคุณสมบัติเทียบเท่าหรือสูงกว่าบุคลากรเดิม และจะต้องได้รับการพิจารณาอนุมัติจาก สศค. จึงจะสามารถปฏิบัติงานต่อไปได้ นอกจากนี้ ในกรณีที่ สศค. พิจารณาแล้วเห็นว่าการทำงานของผู้ยื่นเสนอราคามีความล่าช้าในการดำเนินงาน และแจ้งให้ผู้ยื่นเสนอราคาทราบ เพื่อดำเนินการเพิ่มเติมบุคลากร ผู้ยื่นเสนอราคาจะต้องเพิ่มบุคลากรดังกล่าวตามความต้องการของ สศค. ได้ และในทำนองเดียวกัน ถ้า สศค. เห็นว่าบุคลากรของผู้ยื่นเสนอราคาไม่สามารถปฏิบัติงานได้อย่างมีประสิทธิภาพ สศค. สามารถที่จะขอเปลี่ยนแปลงบุคลากรได้เช่นเดียวกัน ซึ่งข้อพิจารณาดังกล่าว สศค. ขอสงวนสิทธิ์ในการที่จะดำเนินการได้

พิมลพรรณ

4. การเสนอราคา

ผู้ยื่นเสนอราคาต้องนำเสนอรายละเอียดเป็นตารางการเปรียบเทียบคุณสมบัติ ตามรูปแบบดังนี้

คุณลักษณะเฉพาะและข้อกำหนด (งานซื้อ) ที่ สศค. กำหนด	คุณสมบัติที่ผู้เสนอราคาเสนอ	เปรียบเทียบคุณสมบัติ หรือ ขอบเขตการดำเนินงานที่ผู้เสนอราคาเสนอ	เอกสารอ้างอิง
ให้คัดลอกคุณสมบัติที่สำนักงานกำหนด หรือขอบเขตการดำเนินงานที่ สศค. กำหนด	ให้ระบุคุณสมบัติที่ผู้เสนอราคาเสนอ พร้อมทั้งระบุยี่ห้อและรุ่น	ให้ระบุจุดที่ดีกว่า หรือเทียบเท่า	ให้ระบุเอกสารอ้างอิง (ถ้ามี)

ผู้ยื่นเสนอราคาจะต้องเสนอกำหนดยืนราคาไม่น้อยกว่า 90 วันนับแต่วันที่ยื่นยันราคาสุดท้าย โดยภายในกำหนดยืนราคาผู้ยื่นเสนอราคาหรือผู้มีสิทธิ์เสนอราคาจะต้องรับผิดชอบราคาที่ตนได้เสนอไว้และจะถอนการเสนอราคามิได้

5. รายละเอียดคุณลักษณะเฉพาะและข้อกำหนด

ผู้ยื่นเสนอราคาจะต้องเสนอรายการ ดังนี้

ลำดับที่	รายการ	จำนวน	หน่วย
1	อุปกรณ์วิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ (Security Incident Event Management: SIEM)	1	ชุด
2	ระบบบริหารจัดการและตอบสนองต่อเหตุการณ์ภัยคุกคามทางคอมพิวเตอร์ (Security Orchestration, Automation and Response: SOAR)	1	ระบบ
3	ซอฟต์แวร์ตรวจจับและตอบสนองต่อภัยคุกคามทางไซเบอร์ (Endpoint Detection and Response: EDR)	1	ระบบ
4	ระบบตรวจจับและตอบสนองต่อระบบเครือข่ายคอมพิวเตอร์ (Network Detection and Response: NDR)	1	ระบบ
5	เครื่องคอมพิวเตอร์แม่ข่าย แบบ Hyperconverged	2	ชุด
6	ชุดโปรแกรมระบบคอมพิวเตอร์เสมือนสำหรับเครื่องคอมพิวเตอร์แม่ข่าย	2	ชุด
7	ชุดโปรแกรมบริหารจัดการระบบคอมพิวเตอร์เสมือน	1	ชุด

รายละเอียดคุณลักษณะอุปกรณ์ของโครงการฯ มีดังนี้

5.1 อุปกรณ์วิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ (Security Incident Event Management: SIEM) จำนวน 1 ชุด โดยมีคุณลักษณะอย่างน้อยดังนี้

5.1.1 เป็นอุปกรณ์ Hardware แบบ Appliance ที่ออกแบบสำหรับเก็บบันทึกข้อมูลทางด้านการรักษาความปลอดภัยเครือข่ายโดยทำหน้าที่เป็น SIEM โดยเฉพาะ

5.1.2 ต้องสามารถรองรับการส่งข้อมูลเหตุการณ์ได้สูงสุด 7,000 เหตุการณ์ต่อวินาที (Event Per Second) เป็นอย่างน้อย

5.1.3 ระบบที่เสนอต้องมีขนาด Storage หรือพื้นที่รวมก่อนการทำ Raid ขนาดไม่น้อยกว่า 60 TB

5.1.4 มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 1/10 G Base-T หรือดีกว่า จำนวนไม่น้อยกว่า 2 ช่อง

5.1.5 ระบบต้องรองรับ log formats ในรูปแบบ Syslog, Syslog TLS, SNMP, NetFlow, OPSEC ได้เป็นอย่างน้อย

5.1.6 มีความสามารถในการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ และรักษาความถูกต้องของข้อมูลที่เก็บบันทึกไว้ด้วยการทำ Hashing แบบ SHA1 หรือดีกว่า

5.1.7 สามารถทำการส่งข้อมูล Log ไปยังอุปกรณ์จัดเก็บข้อมูลภายนอกได้

5.1.8 ระบบที่เสนอต้องมีความสามารถในการทำการบีบอัด (Compression) ข้อมูล Raw Log และสามารถปรับระดับของการบีบอัด (Compression Rate) ได้ไม่น้อยกว่า 3 ระดับ และต้องไม่น้อยกว่า 14:1 ส่วน

5.1.9 มีความสามารถในการสร้างความสัมพันธ์ (Correlation) ของข้อมูลเหตุการณ์ (Event) ได้เป็นอย่างน้อย และมี Pre-defined มาพร้อมกับระบบ 100 Correlation Rules เป็นอย่างน้อยและ สามารถสร้าง Correlation Rules ได้ไม่จำกัด

5.1.10 สามารถแสดง/ค้นหาข้อมูลที่บันทึกข้อมูล จากหมายเลข IPv4 และ IPv6 ได้

5.1.11 สามารถรับข้อมูล ภัยคุกคามจากภายนอกด้วย STIX/TAXII และแจ้งเตือนเมื่อมีการเชื่อมต่อไปยัง IP Address หรือ Domain ภายนอกองค์กรที่เป็นอันตรายได้

5.1.12 สามารถรับข้อมูลภัยคุกคามต่าง ๆ (Threat Intelligence) ทั้งจากภายนอก และของผลิตภัณฑ์เองได้ เช่นข้อมูล Botnet, Malware Domain, Malware IP, Malware URL, Malware Hash เพื่อใช้ในการวิเคราะห์ภัยคุกคามชนิดใหม่ที่เกิดขึ้นได้

5.1.13 สามารถแสดงผลแบบ Bar Chart, Pie Chart และ Distribution ได้

5.1.14 สามารถแสดงภาพรวมของระบบในลักษณะ Dashboard หรือแบบอื่น ๆ ที่สามารถแสดงสถานะของการใช้งานทรัพยากรต่าง ๆ ของระบบ ได้

5.1.15 มีความสามารถในการสร้างรายงานสำหรับ compliance ดังต่อไปนี้ ISO, PCI-DSS, FISMA, HIPPA, NERC-CIP, SOX, GLBA

5.1.16 ต้องสามารถจำกัดสิทธิการเข้าถึงข้อมูลของอุปกรณ์ ของแต่ละกลุ่มผู้ใช้งานได้

5.1.17 มีความสามารถในการเตือนผู้ใช้ผ่านทาง Email , SNMP และ Syslog ได้

5.1.18 สามารถออกรายงานในรูปแบบไฟล์ได้ ดังต่อไปนี้ HTML, PDF และ CSV ได้เป็นอย่างน้อย

5.1.19 มีระบบ Case Management หรือ Incident Workflow เพื่อให้สามารถติดตามและบริหารจัดการปัญหาที่เกิดขึ้นได้

5.1.20 อุปกรณ์ทั้งหมดต้องสามารถติดตั้งบนในตู้ Rack มาตรฐาน 19 นิ้วได้

5.1.21 มี Power Supply แบบ Redundant หรือ Hot Swap จำนวน 2 หน่วย

5.1.22 สามารถรับข้อมูลและจัดเก็บข้อมูลจราจร (Syslog) จากอุปกรณ์เครือข่ายเดิมของ สศค. ได้ ได้แก่ Firewall , Switch ,IPS, WAF และ DDoS

5.1.23 สามารถพิสูจน์ตัวตน (Authentication) ผู้ใช้งานได้ โดยรองรับฐานข้อมูลผู้ใช้แบบ Local, Microsoft AD ได้เป็นอย่างน้อย

5.2 **ระบบบริหารจัดการและตอบสนองต่อเหตุการณ์ภัยคุกคามทางคอมพิวเตอร์ (Security Orchestration, Automation and Response: SOAR) จำนวน 1 ระบบ โดยมีคุณลักษณะอย่างน้อยดังนี้**

5.2.1 เป็นระบบที่ถูกออกแบบมาเพื่อให้สามารถบริหารจัดการและตอบสนองต่อเหตุการณ์ภัยคุกคามที่เกิดขึ้นบนระบบเครือข่ายคอมพิวเตอร์ได้อย่างอัตโนมัติ (Security Orchestration, Automation and Response : SOAR)

5.2.2 มีลิขสิทธิ์สำหรับผู้ใช้งานระบบหลัก จำนวนไม่น้อยกว่า 2 ลิขสิทธิ์และสามารถเพิ่มเติมได้ในอนาคต

5.2.3 รองรับการทำงานแบบ Multi-tenancy ได้ โดยสามารถกำหนดการทำงานแบบอัตโนมัติ (Automation Workflow) ระบุแบ่งตาม Tenant ได้

5.2.4 สามารถบริหารจัดการความปลอดภัย เช่น Security alert, Incident, Indicator, Asset และ Task โดยผ่านหน้า GUI ได้เป็นอย่างน้อย

5.2.5 สามารถทำการกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงข้อมูล (Role-Based Access Management) เช่น Rules, Playbooks, Attachment และ Report ได้ และสามารถกำหนดสิทธิ์การ Create, Read, Update หรือ Modify และ Delete ให้กับผู้ใช้งานระบบได้

5.2.6 สามารถใช้งานระบบ Playbook แบบ Drag and Drop ได้ โดยมีรูปแบบ OOB (Out-of-Box) Predefined Connector มาให้จำนวนไม่น้อยกว่า 300 การเชื่อมต่อ และรูปแบบการสั่งการแบบอัตโนมัติ (Predefined Automated action) จำนวนไม่น้อยกว่า 3,000 แบบ

5.2.7 ระบบที่เสนอสามารถแลกเปลี่ยนข้อมูลโดยตรงกับ Threat Intelligence Partner ได้ไม่น้อยกว่า 200 หน่วยงาน

5.2.8 มีหน้าจอแสดงผล (Dashboard) ที่สามารถปรับแต่งค่าการแสดงผลสำหรับนักวิเคราะห์ระบบและผู้ดูแลระบบได้

5.2.9 สามารถแสดงผลในรูปแบบต่าง ๆ เช่น ตาราง (Chart), รายการ (List) และจำนวน (Counter) ได้

5.2.10 สามารถทำการออกรายงานและส่งอีเมล์ในรูปแบบ PDF และ CSV ได้เป็นอย่างน้อย

5.2.11 สามารถทำการนำเข้า (Import) และส่งออก (Export) รูปแบบของ Playbook ได้

5.2.12 สามารถทำงานร่วมกับระบบพิสูจน์ตัวตน เช่น Active Directory, LDAP และ SAML ได้ รวมถึงสามารถกำหนดและควบคุมสิทธิ์ผู้ใช้งานในการเข้าใช้ระบบได้

5.2.13 สามารถทำการสร้างกระบวนการทำงานตอบสนองต่อเหตุการณ์ (Playbook) และเรียกใช้งา ได้ทั้งแบบอัตโนมัติ และกำหนดเอง

5.2.14 สามารถทำการสร้าง Playbook ได้อย่างน้อยดังนี้

1) Manual action and Task
2) การสร้างขั้นตอนในการตัดสินใจและอนุมัติ
3) การเรียกใช้งาน Playbook ที่ซ้อนกันได้
4) การกำหนดเงื่อนไขและลูปได้
5) การหยุดหรือดำเนินการต่อเมื่อเกิดข้อผิดพลาดใน Playbook

5.2.15 สามารถทำการเก็บข้อมูลในรูปแบบ Snapshot เพื่อทำการย้อนกลับ (Roll back) ในกรณีที่ Playbook เกิดปัญหาได้

5.2.16 สามารถทำการจำลองขั้นตอนของ Playbook เพื่อทดสอบการทำงานได้

5.2.17 สามารถเชื่อมโยงกับอุปกรณ์อื่นจากผู้ผลิตภายนอก (3rd party) ผ่านการเรียกใช้ API

5.2.18 ระบบรองรับการทำ High Availability แบบ Active/Active, Active/Passive และ Cluster ได้

5.2.19 อุปกรณ์ที่เสนอต้องสามารถทำงานร่วมกับ อุปกรณ์วิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ (Security Incident Event Management: SIEM) ที่เสนอในการจัดซื้อครั้งนี้ได้

5.3 **ซอฟต์แวร์ตรวจจับและตอบสนองต่อภัยคุกคามทางไซเบอร์ (Endpoint Detection and Response: EDR) จำนวน 1 ระบบ โดยมีคุณลักษณะอย่างน้อยดังนี้**

5.3.1 เป็นซอฟต์แวร์ที่สามารถใช้งานได้กับเครื่องคอมพิวเตอร์ และเครื่องคอมพิวเตอร์แม่ข่าย ได้ไม่น้อยกว่า 550 เครื่อง

5.3.2 สามารถติดตั้งได้ทั้งแบบ On Cloud หรือ On Premise

5.3.3 รองรับการติดตั้งบนระบบปฏิบัติการต่างๆ ได้อย่างน้อยดังนี้

1) Windows XP, 7, 8 และ 10
2) Windows Server 2003, 2008, 2012, 2016 และ 2019
3) MacOS
4) Red Hat Enterprise
5) CentOS
6) Ubuntu
7) Oracle

5.3.4 สามารถทำ Virtual Patch ได้

5.3.5 สามารถตรวจสอบ Application ที่ใช้งานภายในองค์กร และรายการช่องโหว่ตาม Common Vulnerability Scoring System (CVSS) ได้ หรือ มีวิธีในการป้องกันและตอบสนองต่อภัยคุกคามทางด้านไซเบอร์ได้อย่างน้อยดังนี้ Scheduled Scan, Realtime Protection, Ransomware, WebShell, Brut-Force และ Advanced Threat Defense

5.3.6 สามารถป้องกันมัลแวร์ (Malware) ด้วย Machine Learning ได้ โดยไม่ต้องติดตั้ง Agent หรือ มีระบบวิเคราะห์และตรวจจับ (Security Engines) เพื่อเพิ่มประสิทธิภาพในการป้องกัน อย่างน้อยดังนี้ AI based engine, Cloud based engine, Gene engine และ Behavioral engine

5.3.7 สามารถป้องกัน Endpoint ได้ แม้อยู่ในสถานะออฟไลน์ (Offline)

5.3.8 สามารถแสดงภาพกราฟตามลำดับขั้นตอนของเหตุการณ์ที่เกิดขึ้นได้ หรือ มีความสามารถในการค้นหาไฟล์ต้องสงสัยที่อาจจะมีอยู่ในเครื่องคอมพิวเตอร์ (Infected File Tracking)

5.3.9 สามารถทำ Threat Hunting จาก Hash และ File name โดยกำหนดช่วงเวลาที่ต้องการค้นหาได้ หรือ มีความสามารถในการแยกเครื่องคอมพิวเตอร์ที่มีความเสี่ยงออกมาจากระบบเครือข่าย (Endpoint Isolation)

5.3.10 สามารถควบคุมการใช้งานอุปกรณ์ USB ได้

5.3.11 สามารถป้องกันการเข้าถึงเว็บไซต์ (Website) ที่ไม่ปลอดภัยได้

5.3.12 สามารถทำงานร่วมกับ Windows Security Center ได้

5.3.13 สามารถกำหนดเงื่อนไขในการแก้ไขปัญหาเมื่อตรวจพบมัลแวร์ (Malware) ได้อย่างน้อยดังนี้

1) Terminate Process

2) Delete File

3) Clean Persistent Data

4) Block Address on Firewall

5.3.14 สามารถอัพเดท Threat Intelligence จากฐานข้อมูลของเจ้าของผลิตภัณฑ์ที่เสนอได้อย่างต่อเนื่องตลอดอายุสัญญา

5.3.15 สามารถส่ง Log แบบ Syslog ได้

5.3.16 สามารถแจ้งเตือนผู้ดูแลระบบเมื่อตรวจพบมัลแวร์ (Malware) ผ่าน Email ได้เป็นอย่างน้อย

5.3.17 สามารถแสดงผลรายงานแบบ PDF ได้เป็นอย่างน้อย

5.4 **ระบบตรวจจับและตอบสนองต่อระบบเครือข่ายคอมพิวเตอร์ (Network Detection and Response: NDR) จำนวน 1 ระบบ โดยมีคุณลักษณะอย่างน้อยดังนี้**

5.4.1 มีอุปกรณ์ Hardware Appliance จำนวนอย่างน้อย 1 ชุด โดยมีคุณลักษณะอย่างน้อยดังนี้

1) มีช่องเชื่อมต่อเครือข่าย 10 Gigabit Ethernet SFP+ จำนวนไม่น้อยกว่า 2 พอร์ต พร้อมติดตั้ง Transceiver 10G SR จำนวนไม่น้อยกว่า 2 พอร์ต
2) มีช่องเชื่อมต่อเครือข่าย 10/100/1000Base-T จำนวนไม่น้อยกว่า 2 พอร์ต
3) มี SSD ขนาดไม่น้อยกว่า 128 Gb จำนวน 1 หน่วย
4) มี Harddisk ขนาดไม่น้อยกว่า 1.2 TB จำนวนไม่น้อยกว่า 4 หน่วย
5) มี Performance แบบ Mix Mode (Brand และ Sensor) ไม่น้อยกว่า 8 Gbps หากอุปกรณ์ไม่สามารถทำงานในแบบ Mix Mode ได้ให้เสนออุปกรณ์ภายนอกที่ทำหน้าที่เป็น Sensor โดยอุปกรณ์ภายนอกที่เสนอต้องมี Throughput ไม่น้อยกว่า 8 Gbps

หรือมีซอฟต์แวร์รวบรวมข้อมูลภายในระบบเครือข่าย (Sensor) จำนวน 1 ชุด พร้อมซอฟต์แวร์สำหรับการตรวจจับและตอบสนองต่อภัยคุกคามทางด้านไซเบอร์ (security detection and response) จำนวน 1 ชุด โดยมีคุณสมบัติต่อชุดดังนี้

1) ซอฟต์แวร์รวบรวมข้อมูลภายในระบบเครือข่าย (Sensor) มีคุณสมบัติต่อชุดดังนี้

- สามารถติดตั้งบนระบบ Virtualization
- ใช้ทรัพยากรหน่วยประมวลผลกลางแบบเสมือน (vCPU) 8 Core
- ใช้ทรัพยากรหน่วยความจำหลักแบบเสมือน (Virtual RAM) 8 GB
- ใช้ทรัพยากรหน่วยความจำสำรองแบบเสมือน (Virtual Disk) ไม่ต่ำกว่า 128 GB

- สามารถรวบรวมข้อมูลภายในระบบเครือข่ายด้วยวิธีการ SPAN หรือ Mirrored Traffic จากอุปกรณ์ Switch หรือ Virtual Switch ได้

2) ซอฟต์แวร์สำหรับการตรวจจับและตอบสนองต่อภัยคุกคามทางด้านไซเบอร์ (security detection and response)มีคุณสมบัติต่อชุดดังนี้

- สามารถติดตั้งบนระบบ Virtualization ใช้ทรัพยากรหน่วยประมวลผลกลางแบบเสมือน (vCPU) 8 Core
- ใช้ทรัพยากรหน่วยความจำหลักแบบเสมือน (Virtual RAM) 64 GB
- ใช้ทรัพยากรหน่วยความจำสำรองแบบเสมือน (Virtual Disk) 2 TB
- สามารถรับ Traffic Throughput ได้อย่างน้อย 2 Gbps
- สามารถทำการรวบรวมข้อมูลจากซอฟต์แวร์รวบรวมข้อมูลภายในระบบเครือข่าย (Sensor) ที่นำเสนอได้

5.4.2 ระบบที่เสนอต้องเป็นระบบทางด้าน Network Detection and Response (NDR) และใช้ข้อมูล Raw Network Packet เพื่อนำมาใช้ในการตรวจจับ และวิเคราะห์ภัยคุกคามขั้นสูงได้

5.4.3 ต้องมีความสามารถประมวลผลและวิเคราะห์ข้อมูลได้ในรูปแบบ On-Premise

5.4.4 ระบบที่เสนอต้องสามารถในการวิเคราะห์และตรวจจับภัยคุกคามขั้นสูงด้วยวิธีการ ดังต่อไปนี้

1) ต้องมีการใช้ Behavioral Techniques (Non-Signature-Based Detection) โดยการใช้ Machine Learning ในการตรวจวิเคราะห์ และต้องมีการใช้ Unsupervised Learning เป็นอย่างน้อย เพื่อสามารถตรวจจับ Network Traffic ที่ผิดปกติ (Anomaly Network Traffic) ได้
2) ต้องมีความสามารถในการใช้ Supervised Learning ในการสร้าง Model เพื่อใช้ในการตรวจจับภัยคุกคามทางด้าน Network ที่ใช้เทคนิคขั้นสูงได้
3) มีความสามารถในการปรับปรุงประสิทธิภาพ (Fine-tune) ในด้านความถูกต้องแม่นยำในการตรวจจับ (Accuracy of Detection)
4) ต้องสามารถวิเคราะห์ Network Packets ในรูปแบบ Encrypted Traffic และ Decrypted Traffic โดยสำหรับ Encrypted Traffic ต้องสามารถวิเคราะห์ด้วยวิธี JA3 Fingerprint และ JA3S Fingerprint

5.4.5 ระบบที่เสนอต้องมีความสามารถในการแสดงผลและสนับสนุนด้านการตอบสนองภัยคุกคามแบบ Manual Response หรือแบบ Automatic Response ได้ ดังต่อไปนี้

1) ต้องสามารถเรียกดูข้อมูลบนระบบที่ให้บริการอย่างน้อยดังต่อไปนี้ ย้อนหลังได้ไม่น้อยกว่า 90 วัน

- หน้า dashboard แสดงการใช้งาน Network ที่ผิดปกติที่ระบบสามารถตรวจจับได้ (All Alerts / Detections)
- ประเภทของการใช้งาน Network ผิดปกติที่ระบบสามารถตรวจจับได้ (Security Category)
- ระดับความรุนแรง (Severity) หรือค่าความเสี่ยง (Risk Score) ของการใช้งาน Network ผิดปกติที่ระบบสามารถตรวจจับได้
- ข้อมูลของ host ต่างๆ โดยสามารถดู detail และ Detection ได้ หรือมีความสามารถในการตรวจจับภัยคุกคามทางด้านไซเบอร์แบบเชิงรุก (Threat Hunting) โดยมีความสามารถดังนี้
  - สามารถวิเคราะห์และตรวจจับแหล่งที่มาของภัยคุกคาม (patient zero หรือ Entry Point)
  - สามารถเชื่อมโยงการแพร่กระจายหรือการโจมตีของภัยคุกคามที่เกิดขึ้นภายในระบบเครือข่ายได้

2) ต้องมีความสามารถ Correlate Security Events เพื่อให้ทราบว่าภัยคุกคามดังกล่าวมีความสัมพันธ์เชื่อมโยง
   - แสดงผลความเชื่อมโยงระหว่างเครือข่าย Network Lateral Movement ได้
   - สามารถ Map Security Events กับ MITRE Framework หรือ Cyber Kill Chain เพื่อให้ทราบว่าภัยคุกคามดังกล่าวเป็นภัยคุกคามประเภทใด และอยู่ใน Attack Phase ใดได้
3) ต้องสามารถนำข้อมูลที่เป็น Network Packet มาแสดงผล และสามารถ Export PCAP เพื่อนำไปทำ Network Forensics ได้
4) สามารถทำงานร่วมกับอุปกรณ์วิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ (Security Incident Event Management: SIEM) ที่เสนอในโครงการนี้ได้

5.5 **เครื่องคอมพิวเตอร์แม่ข่าย แบบ Hyperconverged จำนวน 2 ชุด โดยมีคุณลักษณะอย่างน้อยดังนี้**

5.5.1 เป็นเครื่องคอมพิวเตอร์แม่ข่ายที่ถูกออกแบบเป็น Hyperconverged โดยเฉพาะ มีหน่วยประมวลผลกลางชนิด Intel XEON Silver 4216 แบบ 16-Core Processor หรือดีกว่า โดยแต่ละหน่วยมีความเร็วสัญญาณนาฬิกาไม่ต่ำกว่า 2.1GHz จำนวนไม่น้อยกว่า 1 หน่วย และรองรับการเพิ่มจำนวนได้ไม่น้อยกว่า 2 หน่วย

5.5.2 มีหน่วยความจำหลักขนาดไม่น้อยกว่า 144GB แบบ DDR4 RDIMM หรือ LRDIMM หรือดีกว่า

5.5.3 มีหน่วยจัดเก็บข้อมูลแบบ Solid State Drives (SSD) หรือดีกว่า และมีความจุต่อหน่วยไม่น้อยกว่า 1.92TB จำนวนไม่น้อยกว่า 6 หน่วย

5.5.4 มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 1GbE Ethernet (RJ-45) หรือดีกว่า จำนวนไม่น้อยกว่า 4 ช่อง และแบบ 10/25GbE (SFP28) จำนวนไม่น้อยกว่า 2 ช่อง พร้อมสาย DAC 10Gb จำนวน 1 หน่วย

5.5.5 มี Power Supply แบบ Hot Plug หรือ Hot Swap ขนาดไม่น้อยกว่า 1600W จำนวน 2 หน่วย และมี Cooling Fans แบบ Redundant รองรับการถอดเปลี่ยนแบบ Hot Plug หรือ Hot Swap ได้

5.5.6 มีช่องเชื่อมต่อแบบ USB 3.0 port ไม่น้อยกว่า 5 ช่อง

5.5.7 มีสถาปัตยกรรมแบบ Scale-out และ Open architecture สามารถ share Data Store ให้ ESXi เครื่องอื่นได้

5.5.8 สามารถทำ Data Optimization แบบ Inline Deduplication และ Compression ได้พร้อมกัน

5.5.9 หน่วยจัดเก็บข้อมูล Hard Drive ชนิด SSD สามารถเสียหายพร้อมกันได้อย่างน้อย 1 หน่วย ต่อ Node โดยไม่ทำให้ข้อมูลเสียหายและไม่กระทบต่อประสิทธิภาพโดยรวมของระบบ หรือเสนออุปกรณ์ Hyper Converged รุ่นเดียวกันกับที่เสนอเพิ่มเติม เพื่อให้สามารถทำงานได้ตามข้อกำหนดข้างต้น

5.5.10 ระบบที่เสนอต้องสามารถทำการสำรองข้อมูลหรือมีซอฟต์แวร์สำหรับสำรองข้อมูล และกู้คืนข้อมูลได้ โดยมีคุณสมบัติอย่างน้อยดังนี้

1) การสำรองข้อมูล สามารถกำหนด Policy Backup, Retention time และตั้ง Frequency (หรือ Schedule) ได้
2) สามารถกู้คืน (Restore) ข้อมูลได้แบบ File และ Full VM เป็นอย่างน้อยสำหรับ Windows VM
3) สามารถสำรองข้อมูล หรือกู้คืนข้อมูลระดับ VM ขนาด 200GB จาก Local Datacenter เสร็จภายใน 60 วินาที

5.5.11 รองรับการเพิ่มขยายโหนด Hyperconverged ได้โดยไม่ต้องหยุดการทำงาน

5.5.12 รองรับ Hypervisor แบบ VMware vSphere หรือ Microsoft Hyper-V ได้เป็นอย่างน้อย และมี Certified สำหรับ Red Hat Enterprise Linux VM

5.5.13 มี Remote Management Port แบบ 1GbE Ethernet RJ-45 จำนวน 1 พอร์ตต่อ Node เพื่อช่วยในการจัดการ กับ Server จากระยะไกล ผ่าน Web Base Application (Remote) สามารถสั่ง Power ON, Power OFF, Restart เครื่อง Server และตั้งค่าใน Bios ได้ และสามารถทำ Virtual KVM Remote Graphical Console, Virtual Power Button Control, Virtual Media และ Virtual Folder ได้ รองรับการสั่งงานระยะไกล (Remote) ผ่าน Smart Phone หรือ Tablet ด้วย Mobile Application ที่ได้รับการออกแบบมาโดยเฉพาะจากผู้ผลิตทั้งบน Android หรือ iOS ได้เป็นอย่างน้อย

5.5.14 มี Software ช่วยในการจัดการกับอุปกรณ์ต่างๆ ของ Server ได้แบบ web base application โดยสามารถ access ผ่าน web browser ได้ สามารถบอกสถานะของอุปกรณ์ และแจ้งเตือนสิ่งผิดปกติที่เกิดขึ้นกับอุปกรณ์ผ่านทาง SNMP และ E-mail ได้

5.5.15 สามารถตรวจสอบสถานะของเครื่อง แจ้งซ่อมโดยอัตโนมัติ ผ่าน Cloud Service ที่ทางผู้ผลิตจัดหาไว้ให้

5.5.16 มีระบบ Artificial Intelligent (AI) ในการเรียนรู้และวิเคราะห์การทำงานของเครื่อง ในรูปแบบ global learning พร้อมให้คำแนะนำ หรือแก้ไขปัญหาที่เกิดขึ้นโดยอัตโนมัติ หรือเสนอระบบ Artificial Intelligent (AI) ในการเรียนรู้และวิเคราะห์การทำงานของเครื่อง เพิ่มเติมภายนอก

5.5.17 ระบบ Hyperconverged ที่เสนอจะต้องได้รับการประเมินจากหน่วยงานที่น่าเชื่อถือให้อยู่ในกลุ่มผู้นำ (Leaders) ของกลุ่มตลาดอุปกรณ์ Hyperconverged Infrastructure จาก Gartner Magic Quadrant ในปี 2019 หรือใหม่กว่า

5.6 **ชุดโปรแกรมระบบคอมพิวเตอร์เสมือนสำหรับเครื่องคอมพิวเตอร์แม่ข่าย จำนวน 2 ชุด โดยมีคุณลักษณะอย่างน้อยดังนี้**

5.6.1 รองรับการบริหารจัดการผ่านบราวเซอร์ได้

5.6.2 รองรับการแบ่งทรัพยากรของ Hardware ตามสถาปัตยกรรม hypervisor ออกเป็นเครื่องคอมพิวเตอร์เสมือน (Virtual Machine) ได้มากกว่า 1 เครื่องคอมพิวเตอร์เสมือน

5.6.3 สามารถกำหนดให้เครื่องคอมพิวเตอร์เสมือน (Virtual Machine) ประมวลผลหลายโปรเซสเซอร์แบบเสมือน (Virtual Symmetric Multiprocessing - SMP) ได้สูงสุดถึง 128 vCPU

5.6.4 สามารถกำหนดพื้นที่ Disk Space ให้คอมพิวเตอร์เสมือนในแบบ Thin Provisioning ได้

5.6.5 สามารถย้ายไฟล์ดิสค์เสมือน ของคอมพิวเตอร์เสมือนข้าม storage ได้โดยไม่ก่อให้เกิดความเสียหายต่องานที่ทำบนเครื่องคอมพิวเตอร์เสมือน (Virtual Machine) หรือส่งผลต่อผู้ใช้งานที่รับบริการอยู่

5.6.6 สามารถย้ายเครื่องคอมพิวเตอร์เสมือน (Virtual Machine) ข้ามเครื่องเซิร์ฟเวอร์ เมื่อต้องการบำรุงรักษาเครื่องเซิร์ฟเวอร์โดยไม่ก่อให้เกิดความเสียหายต่องานที่ทำบนเครื่องคอมพิวเตอร์เสมือน (Virtual Machine) หรือส่งผลต่อผู้ใช้งานที่รับบริการอยู่

5.6.7 รองรับการรีสตาร์ทเครื่องคอมพิวเตอร์เสมือน (Virtual Machine) ในแบบอัตโนมัติ เมื่อ Hardware หรือ ระบบปฏิบัติการ หยุดการทำงานหรือเกิดความเสียหายได้

5.6.8 สามารถกำหนดให้เครื่องคอมพิวเตอร์เสมือน (Virtual Machine) เข้าถึงอุปกรณ์จัดเก็บข้อมูลแบบแชร์ได้เช่น Fibre Chanel, iSCSI เป็นต้น

5.6.9 สามารถกำหนดให้ทุกแอปพลิเคชั่นทำงานได้ต่อเนื่องโดยไม่ทำเกิดให้ความเสียหายหรือหยุดให้บริการ เมื่อเกิดความเสียหายของ Hardware ได้และสามารถกำหนด Virtual CPU ได้สูงสุด 2 vCPU

5.6.10 สามารถเพิ่มขยาย CPU, Memory และ Disk ให้กับเครื่องคอมพิวเตอร์เสมือน (Virtual Machine)โดยไม่ทำให้เกิดความเสียหายหรือหยุดให้บริการได้

5.6.11 สามารถติดตั้งกับเครื่องคอมพิวเตอร์แม่ข่ายชนิด Hyperconverged ที่เสนอได้

5.7 **ชุดโปรแกรมบริหารจัดการระบบคอมพิวเตอร์เสมือน จำนวน 1 ชุด โดยมีคุณลักษณะอย่างน้อยดังนี้**

5.7.1 มีเครื่องมือในการบริหารจัดการเครื่องแม่ข่ายเสมือน (Hosts) และ เครื่องคอมพิวเตอร์เสมือน (Virtual machine) แบบศูนย์กลางการจัดการ ที่สามารถบริหารจัดการเครื่องแม่ข่ายเสมือน (Hosts)ได้ไม่น้อยกว่า 1000 เครื่อง

5.7.2 สามารถติดตั้ง Patch และ Update สำหรับ Hypervisor Server ได้จากส่วนกลาง

5.7.3 สามารถเข้าถึงผ่าน Web Brower ได้

5.7.4 สามารถตรวจสอบและสร้าง alarm สำหรับ Server Hardware , Virtual Machine , Host , Datastore หรือ Network ได้

5.7.5 สามารถบริหารจัดการกับชุดระบบปฏิบัติการแม่ข่ายคอมพิวเตอร์เสมือนที่เสนอได้

6. การติดตั้งและทดสอบอุปกรณ์ในโครงการ

6.1 ผู้ชนะการประกวดราคาต้องติดตั้งอุปกรณ์ในโครงการตามจุดที่หน่วยงานกำหนดอย่างถูกต้อง ครบถ้วน รวมทั้งจัดหาอุปกรณ์ต่าง ๆ ที่เกี่ยวกับสภาพแวดล้อมของสถานที่ที่ใช้ในการติดตั้งด้วย เช่น ปลั๊กไฟ รางสายไฟ และอื่น ๆ เป็นต้น พร้อมดำเนินการทดสอบการทำงานของระบบเครื่องคอมพิวเตอร์พร้อมอุปกรณ์ ซอฟต์แวร์ และระบบงานคอมพิวเตอร์ทั้งหมดในโครงการ

6.2 ในกรณีผลการทดสอบการทำงานของอุปกรณ์ในโครงการ ยังไม่สามารถทำงานได้อย่างถูกต้อง ครบถ้วนตามวัตถุประสงค์ของโครงการ ผู้ชนะการประกวดราคาจะต้องทำการปรับปรุงแก้ไขเพื่อให้การทดสอบผ่านเงื่อนไขตามข้อกำหนดดังกล่าว

6.3 ในระหว่างที่ทำการทดสอบระบบ หากอุปกรณ์ใดของสำนักงาน หรือหน่วยงานที่เกี่ยวข้องได้รับความเสียหายระหว่างการทดสอบ และส่งผลให้เกิดข้อบกพร่องของระบบคอมพิวเตอร์ โดยความเสียหายที่เกิดขึ้นระหว่างการทดสอบนั้นเกิดจากความบกพร่องของบุคลากรของผู้ชนะการประกวดราคา ผู้ชนะการประกวดราคาจะต้องทำการซ่อมแซม แก้ไขหรือเปลี่ยนแทนโดยไม่คิดค่าใช้จ่ายใด ๆ จากสำนักงาน

7. การฝึกอบรม

ผู้ชนะการประกวดราคาต้องจัดการฝึกอบรมเจ้าหน้าที่ของ สศค. พร้อมมีคู่มือและเอกสารประกอบการฝึกอบรม ผู้ชนะการประกวดราคาต้องรับผิดชอบค่าวิทยากร ค่าอาหารกลางวัน ค่าอาหารว่าง และค่าเอกสารตลอดการฝึกอบรม โดยมีหลักสูตรการฝึกอบรมอย่างน้อย ดังนี้

1. หลักสูตรการใช้งานระบบการวิเคราะห์ข้อมูล (SIEM) และการใช้งานระบบตอบสนองอัตโนมัติ (SOAR) ระยะเวลาไม่น้อยกว่า 2 วัน วันละไม่น้อยกว่า 6 ชั่วโมง จำนวนไม่น้อยกว่า 5 คน
2. หลักสูตรการใช้งานระบบตรวจจับและตอบสนองต่อภัยคุกคามทางไซเบอร์ (EDR) และต่อระบบเครือข่าย (NDR) ระยะเวลาไม่น้อยกว่า 2 วัน วันละไม่น้อยกว่า 6 ชั่วโมง จำนวนไม่น้อยกว่า 5 คน
3. หลักสูตรการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย (Hyperconverged) และระบบคอมพิวเตอร์เสมือน ระยะเวลาไม่น้อยกว่า 1 วัน วันละไม่น้อยกว่า 6 ชั่วโมง จำนวนไม่น้อยกว่า 5 คน

8. การสนับสนุนของ สศค.

สศค. จะอำนวยความสะดวกให้กับบริษัทคู่สัญญา เพื่อให้การดำเนินงานเรียบร้อยและมีประสิทธิภาพ ดังนี้

8.1 ประสานงานและดำเนินการจัดเจ้าหน้าที่อำนวยความสะดวกในการให้ข้อมูลเกี่ยวกับระบบความปลอดภัย และอื่น ๆ ที่เกี่ยวข้อง

8.2 อนุญาตให้บริษัทคู่สัญญาสามารถใช้และสามารถส่งข้อมูลผ่านระบบเครือข่ายสื่อสารของ สศค. ตามความเหมาะสม

9. ระยะเวลาดำเนินงานและการส่งมอบงาน

ผู้ชนะการประกวดราคาต้องดำเนินการติดตั้ง ทดสอบ และส่งมอบระบบพร้อมซอฟแวร์ทั้งหมดในโครงการตามขอบเขตการดำเนินโครงการ รวมทั้งจัดฝึกอบรมและส่งมอบเอกสารหรือคู่มือให้แล้วเสร็จ ภายใน 180 วัน นับถัดจากวันลงนามในสัญญา โดยมีระยะเวลาดำเนินงานและการส่งมอบงานแบ่งออกเป็น 3 งวดงาน ดังนี้

<u>งวดที่ 1:</u> ภายใน 30 วัน นับถัดจากวันลงนามในสัญญา โดยมีงานที่ต้องดำเนินการ ดังนี้

- แผนการดำเนินงานของโครงการ จำนวน 6 ชุด
- แผนการจัดเตรียมสถานที่การติดตั้งและทดสอบระบบคอมพิวเตอร์พร้อมอุปกรณ์ (Hardware Tools) จำนวน 6 ชุด

<u>งวดที่ 2:</u> ภายใน 150 วัน นับถัดจากวันลงนามในสัญญา โดยมีงานที่ต้องดำเนินการ ดังนี้

- รายงานการส่งมอบอุปกรณ์และส่งมอบ License ของซอฟแวร์ จำนวน 6 ชุด
- รายงานการติดตั้งอุปกรณ์และระบบงาน จำนวน 6 ชุด
- รายงานการทดสอบความถูกต้องและการยอมรับได้ของระบบงาน (Acceptance Test) จำนวน 6 ชุด
- แผนการฝึกอบรมที่ระบุวัน เวลา สถานที่ และครอบคลุมรายละเอียดตามข้อหัวข้อการฝึกอบรมในเอกสาร จำนวน 6 ชุด

งวดที่ 3: ภายใน 180 วัน นับถัดจากวันลงนามในสัญญา โดยมีงานที่ต้องดำเนินการ ดังนี้

- รายงานการฝึกอบรมเจ้าหน้าที่ตามแผนการฝึกอบรม จำนวน 6 ชุด พร้อมเอกสารคู่มือประกอบการฝึกอบรม และ CD ที่บรรจุเอกสารคู่มือประกอบการฝึกอบรมทุกหลักสูตร จำนวน 1 ชุด
- เอกสารหรือคู่มือปฏิบัติงานสำหรับผู้ใช้ (User Manual) คู่มือสำหรับการดูแลรักษาระบบงาน (System Maintenance Manual) และเอกสารต่าง ๆ ที่ได้ปรับปรุงแก้ไขเพิ่มเติมล่าสุด พร้อม Username และ Password สำหรับบริหารจัดการระดับ Administrator ทั้งในส่วนของฮาร์ดแวร์ ซอฟต์แวร์ และระบบงานคอมพิวเตอร์ทั้งหมดในโครงการ จำนวน 1 ชุด
- จัดทำบันทึกวิดีโอการฝึกอบรมเจ้าหน้าที่ ลงในแผ่น CD จำนวน 1 ชุด

10. เงื่อนไขการชำระเงิน

สศค. จะชำระเงินจ้าง โดยแบ่งออกเป็น 3 งวด ดังนี้

งวดที่ 1: เป็นจำนวนเงินในอัตราร้อยละ 10 ของวงเงินตามสัญญา ภายหลังที่ได้ทำการส่งมอบและได้รับการตรวจรับงานงวดที่ 1 เสร็จสิ้นสมบูรณ์

งวดที่ 2: เป็นจำนวนเงินในอัตราร้อยละ 50 ของวงเงินตามสัญญา ภายหลังที่ได้ทำการส่งมอบและได้รับการตรวจรับงานงวดที่ 2 เสร็จสิ้นสมบูรณ์

งวดที่ 3: เป็นจำนวนเงินในอัตราร้อยละ 40 ของวงเงินตามสัญญา ภายหลังที่ได้ทำการส่งมอบและได้รับการตรวจรับงานงวดที่ 3 เสร็จสิ้นสมบูรณ์

11. เงื่อนไขการปรับกรณีส่งมอบงานล่าช้า

กรณีที่ผู้ชนะการประกวดราคาไม่สามารถส่งมอบพัสดุได้ตามเงื่อนไขที่กำหนดไว้ในเอกสารนี้ ผู้ชนะการประกวดราคาจะต้องเสียค่าปรับให้ในอัตราร้อยละ 0.2 ของมูลค่าตามสัญญาจนกว่าจะได้รับพัสดุครบถ้วน

12. วงเงินในการจัดหา

เบิกจ่ายจากงบประมาณปี พ.ศ. 2565 วงเงินงบประมาณ 19,518,000 บาท (สิบเก้าล้านห้าแสนหนึ่งหมื่นแปดพันบาทถ้วน)

13. การรักษาความลับของข้อมูล

ผู้ชนะการประกวดราคาต้องรักษาข้อมูลที่เกี่ยวข้องกับโครงการหรือข้อมูลของ สศค. ไว้เป็นความลับตลอดไป และจะต้องไม่เปิดเผยข้อมูลดังกล่าวให้ผู้อื่นทราบโดยปราศจากความยินยอมเป็นลายลักษณ์อักษรของเจ้าของข้อมูลไม่ว่าโดยทางตรงหรือทางอ้อม และผู้ชนะการประกวดราคาจะดำเนินการตามขั้นตอนที่จำเป็นเพื่อหลีกเลี่ยงมิให้ข้อมูลถูกเปิดเผยและใช้ความระมัดระวังอย่างยิ่งเพื่อป้องกันบุคคลที่ไม่เกี่ยวข้องเข้าถึงข้อมูลนั้น หากผู้ชนะ

การประกวดราคาจงใจหรือประมาทเลินเล่อ กระทำหรืองดเว้นการกระทำใด ๆ ที่เป็นการเปิดเผยข้อมูลที่เกี่ยวข้องกับโครงการหรือข้อมูลของ สศค. อันก่อให้เกิดความเสียหาย ผู้ชนะการประกวดราคาต้องรับผิดชอบต่อ สศค. และถือว่าข้อพิจารณาของ สศค. ถือเป็นการสิ้นสุด จะร้องขอต่อไปไม่ได้

14. การรับประกันผลงานและการบำรุงรักษา

14.1 ผู้ชนะการประกวดราคาต้องรับประกันอุปกรณ์ทุกรายการที่เสนอซึ่งเป็นการรับประกันค่าแรง พร้อมอะไหล่ และบริการ ณ สถานที่ติดตั้ง (Onsite Service Warranty) โดยไม่คิดมูลค่าใด ๆ ทั้งสิ้น

14.2 การรับประกันระยะเวลา 1 ปี สำหรับทุกรายการในโครงการโดยเริ่มนับถัดจากวันที่คณะกรรมการตรวจรับพัสดุทำการตรวจรับเสร็จสิ้นสมบูรณ์แล้ว

14.3 เมื่อเกิดเหตุขัดข้อง สศค. สามารถแจ้งเหตุได้ตลอด 24 ชั่วโมง โดยช่องทางดังต่อไปนี้

- ติดต่อผ่าน E-mail
- ติดต่อผ่านโทรศัพท์สายด่วน (Hotline/Helpdesk/Call Center) หรือโทรศัพท์เคลื่อนที่
- ติดต่อผ่าน Instant Messaging

14.4 กรณีเกิดปัญหากับครุภัณฑ์คอมพิวเตอร์ในโครงการ ผู้ชนะการประกวดราคาต้องส่งเจ้าหน้าที่ที่มีความเชี่ยวชาญเพื่อจัดการแก้ไขปัญหาด้วยการปรับปรุงหรือเปลี่ยนอุปกรณ์ที่เกิดปัญหา ให้เสร็จเรียบร้อยภายใน 8 ชั่วโมง นับจากที่ได้รับแจ้งปัญหา และดำเนินการให้เสร็จเรียบร้อยไม่เกิน 24 ชั่วโมง

14.5 กรณีผู้ชนะการประกวดราคาไม่สามารถแก้ไข หรือซ่อมแซม หรือเปลี่ยนใหม่ ได้ภายใน 24 ชั่วโมง ผู้ชนะการประกวดราคาต้องนำเครื่องสำรองที่มีประสิทธิภาพทัดเทียมกันหรือดีกว่ามาใช้งานแทนไปจนกว่าจะแก้ไขหรือซ่อมแซมหรือเปลี่ยนใหม่ ให้แล้วเสร็จสมบูรณ์

14.6 คุณสมบัติของอะไหล่ ชิ้นส่วน หรืออุปกรณ์ใดๆ ที่ใช้ในการเปลี่ยนหรือทดแทนชั่วคราว

- กรณีเปลี่ยนอุปกรณ์ อุปกรณ์ที่นำมาเปลี่ยนต้องมีคุณสมบัติไม่ด้อยกว่าอุปกรณ์เดิมในทุกกรณี และสามารถใช้งานร่วมกับระบบเดิมได้เป็นอย่างดี โดยต้องเป็นอะไหล่จากเจ้าของผลิตภัณฑ์โดยตรง
- กรณีอุปกรณ์ทดแทนชั่วคราว อุปกรณ์ที่นำมาทดแทนเพื่อใช้งานชั่วคราว ต้องมีคุณสมบัติไม่ด้อยกว่าอุปกรณ์เดิมในทุกกรณี และสามารถใช้งานร่วมกับระบบเดิมได้โดยไม่ก่อให้เกิดปัญหาใด ๆ

14.7 เมื่อมีการตรวจสอบ/แก้ไขใด ๆ ผู้ชนะการประกวดราคาต้องส่งรายงานให้ สศค. ทุกครั้งภายใน 3 วันทำการนับจากวันที่ได้ดำเนินการแล้วเสร็จ โดยระบุวัน เวลา สถานที่ อาการ สาเหตุ การตรวจสอบ/แก้ไข และสถานภาพสุดท้ายของอุปกรณ์ และในกรณีที่เกิดความล่าช้าในการตรวจสอบแก้ไข ผู้ชนะการประกวดราคาจะต้องส่งรายงานความคืบหน้าให้ สศค. ทราบเป็นระยะจนกว่าจะดำเนินการแล้วเสร็จ

14.8 หากเกิดความเสียหายใด ๆ ซึ่งก่อให้เกิดความชำรุดบกพร่องหรือเกิดความสูญเสีย หรือความเสียหายแก่ทรัพย์สินของ สศค. อันเป็นผลสืบเนื่องมาจากการกระทำหรือละเว้นการกระทำของผู้ชนะการประกวดราคา ผู้ชนะการประกวดราคาต้องรับผิดชอบชดใช้ค่าเสียหายแก่ สศค. ตามจำนวนที่เสียหายจริงภายในระยะเวลาที่ สศค. กำหนด

14.9 การคิดค่าปรับ สศค. ยอมให้ระบบคอมพิวเตอร์ตามรายการที่กำหนดขัดข้องภายหลังที่คำนวณด้วยค่าตัวถ่วงแล้วได้ไม่เกินเดือนละ 24 ชั่วโมง ถ้าระบบคอมพิวเตอร์ขัดข้องเกินระยะเวลาดังกล่าว สศค. จะคิดค่าปรับในส่วนที่เกินในอัตราชั่วโมงละร้อยละ 0.035 ของราคาระบบคอมพิวเตอร์ทั้งหมดในโครงการ โดยพิจารณาจากบัญชีของ สศค. โดยมีเกณฑ์การคำนวณนับชั่วโมงและค่าตัวถ่วงเป็นดังนี้

ก. จำนวนชั่วโมงที่ขัดข้องในขณะใดขณะหนึ่งเท่ากับค่าสูงสุดของจำนวนชั่วโมงที่ขัดข้องในขณะนั้นของระบบคอมพิวเตอร์แต่ละระบบ คูณด้วยค่าตัวถ่วง

จำนวนชั่วโมง = ค่าสูงสุด (ชั่วโมงที่ขัดข้อง x ค่าตัวถ่วง)

เศษชั่วโมงนับเป็น 1 ชั่วโมง

ข. ค่าปรับ = 0.035% x (ผลรวมจำนวนชั่วโมง - 24) x ราคาระบบคอมพิวเตอร์ทั้งหมดในโครงการ

ค. กำหนดค่าตัวถ่วงของระบบคอมพิวเตอร์

ลำดับที่	รายการ	ค่าตัวถ่วง
1	อุปกรณ์วิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ (Security Incident Event Management: SIEM)	1
2	ระบบบริหารจัดการและตอบสนองต่อเหตุการณ์ภัยคุกคามทางคอมพิวเตอร์ (Security Orchestration, Automation and Response: SOAR)	1
3	ซอฟต์แวร์ตรวจจับและตอบสนองต่อภัยคุกคามทางไซเบอร์ (Endpoint Detection and Response: EDR)	1
4	ระบบตรวจจับและตอบสนองต่อระบบเครือข่ายคอมพิวเตอร์ (Network Detection and Response: NDR)	1
5	เครื่องคอมพิวเตอร์แม่ข่าย แบบ Hyperconverged	0.5
6	ชุดโปรแกรมระบบคอมพิวเตอร์เสมือนสำหรับเครื่องคอมพิวเตอร์แม่ข่าย	0.5
7	ชุดโปรแกรมบริหารจัดการระบบคอมพิวเตอร์เสมือน	0.5

15. การละเมิดลิขสิทธิ์หรือสิทธิบัตรเกี่ยวกับคอมพิวเตอร์

ในกรณีที่บุคคลภายนอกกล่าวอ้างหรือใช้สิทธิ์เรียกร้องใด ๆ ว่าการละเมิดสิทธิ์ หรือสิทธิบัตรเกี่ยวกับคอมพิวเตอร์และ/หรือ Software ที่เสนอ โดย สศค. มิได้แก้ไขหรือดัดแปลงไปจากเดิม ผู้ชนะการประกวดราคาจะต้องดำเนินการทั้งปวง

เพื่อให้การกล่าวอ้างหรือการเรียกร้องดังกล่าวระงับสิ้นไปโดยเร็ว หากผู้ชนะการประกวดราคามิอาจกระทำได้ และ สศค. ต้องรับผิดชดใช้ค่าเสียหายต่อบุคคลภายนอก เนื่องจากผลแห่งการละเมิดลิขสิทธิ์หรือสิทธิบัตรดังกล่าว ผู้ชนะการประกวดราคาต้องเป็นผู้ชำระค่าเสียหายและค่าใช้จ่ายรวมทั้งค่าฤชาธรรมเนียม และค่าทนายความแทน สศค. ทั้งนี้ สศค. จะแจ้งให้ผู้ชนะการประกวดราคาทราบเป็นลายลักษณ์อักษรเมื่อได้มีการกล่าวอ้างหรือใช้สิทธิ์เรียกร้องดังกล่าวโดยไม่ชักช้า

16. หน่วยงานที่รับผิดชอบดำเนินการ

ศูนย์เทคโนโลยีสารสนเทศ สำนักงานเศรษฐกิจการคลัง
โทรศัพท์ 0-2273-9020 ต่อ 3714 หรือ 3707
อีเมล์ itproject@fpo.go.th
