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 เพื่อจัดหาระบบรักษาความปลอดภัยสารสนเทศให้มีความทันสมัยตามเทคโนโลยีในปัจจุบันและให้รองรับกับปริมาณข้อมูล 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 หากมีการเปลี่ยนแปลงบุคลากรในภายหลังจากการชนะการประกวดราคาด้วยวิธีอิเล็กทรอนิกส์และในช่วงดำเนินงานโครงการจนตรวจรับงานงวดสุดท้ายแล้วเสร็จสมบูรณ์ 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

4. การเสนอราคา

ผู้ยื่นเสนอราคาต้องนำเสนอรายละเอียดเป็นตารางการเปรียบเทียบคุณสมบัติ ตามรูปแบบดังนี้

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

ผู้ยื่นเสนอราคาจะต้องเสนอกำหนดยืนราคาไม่น้อยกว่า 90 วันนับแต่วันที่ยืนยันราคาสุดท้าย โดยภายในกำหนดยืนราคาผู้ยื่นเสนอราคาหรือผู้มีสิทธิ์เสนอราคาจะต้องรับผิดชอบราคาที่ตนได้เสนอไว้ และจะถอนการเสนอราคามิได้

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

พรพร วรสิทธิ์

ลำดับที่	รายการ	จำนวน	หน่วย
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 หรือเสนออุปกรณ์ Storage ที่ทำ Compression หรือ Deduplication ได้

5.1.9 มีความสามารถในการสร้างความสัมพันธ์ (Correlation) ของข้อมูลเหตุการณ์ (Event) ได้เป็นอย่างน้อย

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 เช่น Firewall , Switch ,IPS เป็นต้น

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 มีสิทธิสำหรับผู้ดูแลระบบงานหลัก จำนวนไม่น้อยกว่า 2 สิทธิ (License) และอย่างน้อย 2 ผู้ใช้งาน (User) และสามารถเพิ่มเติมได้ในอนาคต

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

5.2.4 สามารถบริหารจัดการความปลอดภัย 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 สามารถกำหนดความสัมพันธ์ภายในกลุ่มของผู้ดูแลระบบ (Team Hierarchy) หรือสามารถทำ Shift Management ได้เป็นอย่างน้อย

5.2.7 สามารถใช้งานระบบ Playbook แบบ Drag and Drop ได้ โดยมีรูปแบบ OOB (Out-of-Box) Predefined Connector มาให้จำนวนไม่น้อยกว่า 300 การเชื่อมต่อ และรูปแบบการสั่งการแบบอัตโนมัติ

5.2.8 มีหน้าจอแสดงผล (Dashboard) ที่สามารถปรับแต่งค่าการแสดงผลสำหรับนักวิเคราะห์ระบบและผู้ดูแลระบบได้

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

5.2.10 สามารถทำการออกรายงานได้

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) และกำหนดเองได้

5.2.14 สามารถทำการสร้าง Playbook ได้อย่างน้อยดังนี้

1) Manual action and Task

2) การสร้างขั้นตอนในการตัดสินใจและอนุมัติ

3) การเรียกใช้งาน Playbook ที่ซ้อนกันได้

4) 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 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 โปรแกรมที่นำเสนอต้องมีระบบบริหารจัดการอยู่บน Cloud management (SaaS) และการเชื่อมต่อระหว่าง Agent กับ Cloud management ต้องมีการเข้ารหัสเพื่อความปลอดภัย

5.3.2 โปรแกรมต้องมีระบบบริหารจัดการแบบรวมศูนย์ (single console) โดยต้องบริหารจัดการ Policy ของ Endpoint ต่างๆ ได้อย่างน้อยดังนี้ Windows, Linux และ Mac

5.3.3 โปรแกรมที่นำเสนอต้องได้รับการยอมรับตามมาตรฐานสากล เช่น SOC 2, PCI DSS V3.2, CMMC, HIPAA, NIST SP 800-53 REV. 4, FFIEC, NSA-CIRA, CREST, AMTSO, GDPR, CSA-STAR เป็นต้น อย่างใดอย่างหนึ่งเป็นอย่างน้อย

5.3.4 โปรแกรมที่นำเสนอต้องสามารถทำการยืนยันตัวตนกับ ระบบ 2 Factor Authentication ได้

5.3.5 โปรแกรมสามารถติดตั้งได้กับระบบปฏิบัติการ ได้เป็นอย่างน้อย ดังต่อไปนี้

1) Windows

2) Windows Server

3) CentOS

4) Oracle Linux

5) Red Hat Enterprise Linux

6) Ubuntu

5.3.6 โปรแกรมที่นำเสนอต้องสามารถแสดงผลของภัยคุกคามที่เกิดขึ้นได้

5.3.7 โปรแกรมที่นำเสนอต้องสามารถป้องกันการ Exploit ไปยังช่องโหว่ (Vulnerability) เพื่อยึดเครื่อง (Compromised) ได้

5.3.8 โปรแกรมที่นำเสนอต้องสามารถป้องกัน Ransomware ในรูปแบบต่างๆ ได้

5.3.9 โปรแกรมที่นำเสนอต้องสามารถป้องกันการทำงานของ Registry ที่มีพฤติกรรมที่ต้องสงสัยได้ (Suspicious Registry Operations)

5.3.10 โปรแกรมที่นำเสนอต้องสามารถเปิดการทำงานในรูปแบบ Endpoint Detection and Response (EDR) เพื่อเก็บข้อมูลการใช้งาน (Activity) ของเครื่อง Endpoint ต่างๆ และนำมาวิเคราะห์หาภัยคุกคาม แบบ Realtime ได้

5.3.11 โปรแกรมที่นำเสนอต้องสามารถนำข้อมูลการแจ้งเตือนภัยคุกคาม (Alerts) มาแปลงให้อยู่ในรูปแบบ MITRE ATT&CK framework เพื่อง่ายต่อการทำความเข้าใจ

5.3.12 โปรแกรมที่นำเสนอต้องสามารถค้นหาข้อมูลการใช้งานภายในที่เกี่ยวข้องกับเครื่อง Windows และ Mac (Host Search) ได้

5.3.13 โปรแกรมที่นำเสนอต้องสามารถค้นหาข้อมูลการใช้งาน Hash (Hash Search) กับเครื่อง Windows และ Mac ได้

5.3.14 โปรแกรมที่นำเสนอต้องสามารถค้นหาข้อมูลการใช้งาน Username (User Search) กับเครื่อง Windows และ Mac ได้

5.3.15 เป็นซอฟต์แวร์ที่สามารถใช้ได้กับเครื่องคอมพิวเตอร์ และเครื่องคอมพิวเตอร์แม่ข่าย ได้ไม่น้อยกว่า 550 เครื่อง

5.3.16 สามารติดตั้งได้ทั้งแบบ On Cloud หรือ On Premise

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

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

5.4.2 ต้องมีความสามารถประมวลผลและวิเคราะห์ข้อมูลได้ในรูปแบบ On-Premise

5.4.3 ระบบที่เสนอต้องสามารถในการวิเคราะห์และตรวจจับภัยคุกคามขั้นสูงด้วยการใช้ Behavioral Techniques (Non-Signature-Based Detection) โดยการใช้ Machine Learning ในการตรวจวิเคราะห์ และต้องมีการใช้ Unsupervised Learning เป็นอย่างน้อย เพื่อสามารถตรวจจับ Network Traffic ที่ผิดปกติ (Anomaly Network Traffic) ได้

5.4.4 ระบบที่เสนอต้องมีความสามารถในการแสดงผลและสนับสนุนด้านการตอบสนองภัยคุกคามแบบ Manual Response หรือแบบ Automatic Response ได้

5.4.5 ต้องมีความสามารถ Correlate Security Events เพื่อให้ทราบว่าภัยคุกคามดังกล่าวมีความสัมพันธ์เชื่อมโยง โดยมี

5.4.5.1 แสดงผลความเชื่อมโยงระหว่างเครือข่าย Network Lateral Movement ได้

5.4.5.2 สามารถ Map Security Events กับ MITRE Framework หรือ Cyber Kill Chain เพื่อให้ทราบว่าภัยคุกคามดังกล่าวเป็นภัยคุกคามประเภทใด และอยู่ใน Attack Phase ใดได้

5.4.6 ต้องสามารถนำข้อมูลที่เป็น Network Packet มาแสดงผล และสามารถ Export PCAP เพื่อนำไปทำ Network Forensics ได้

5.4.7 ระบบรองรับการทำงานร่วมกับอุปกรณ์ด้านความมั่นคงปลอดภัย (Security Product) เช่น SIEM, Firewall, EDR ได้

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

5.5.1 เป็นเครื่องคอมพิวเตอร์แม่ข่ายที่ถูกออกแบบเป็น Hyperconverged โดยเฉพาะ มีหน่วยประมวลผลกลางชนิด Intel XEON Silver 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 มีสถาปัตยกรรมแบบ Scale-out และ Open architecture สามารถ share Data Store ให้ ESXi เครื่องอื่นได้

5.5.7 ระบบที่เสนอต้องสามารถทำการสำรองข้อมูลหรือมีซอฟต์แวร์สำหรับสำรองข้อมูล และกู้คืนข้อมูลได้ โดยมีคุณสมบัติ เช่น สามารถกำหนด Policy Backup, สามารถสำรองข้อมูล หรือกู้คืนข้อมูลแบบ File และ Full VM

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

5.5.9 มี Remote Management Port เพื่อช่วยในการจัดการ กับ Server จากระยะไกล หรือสามารถทำ Virtual Console รองรับการสั่งงานระยะไกล (Remote)

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 Channel, 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) ได้

5.7.2 สามารถติดตั้ง Patch และ Update สำหรับ Hypervisor Server ได้จากส่วนกลาง

5.7.3 สามารถเข้าถึงผ่าน Web Browser ได้

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

5.7.5 สามารถบริหารจัดการกับชุดระบบปฏิบัติการแม่ข่ายคอมพิวเตอร์เสมือนที่เสนอได้

6. การติดตั้งและทดสอบอุปกรณ์ในโครงการ

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

6.2 ในกรณีผลการทดสอบการทำงานของอุปกรณ์ในโครงการ ยังไม่สามารถทำงานได้อย่างถูกต้องครบถ้วนตามวัตถุประสงค์ของโครงการ 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

งวดที่ 2: 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 และครอบคลุมรายละเอียดตามข้อหัวข้อการฝึกอบรม ในเอกสาร จำนวน 6 ชุด

งวดที่ 3: ภายใน 180 วัน นับถัดจากวันลงนามในสัญญา โดยมีงานที่ต้องดำเนินการ ดังนี้

- รายงานการฝึกอบรมเจ้าหน้าที่ตามแผนการฝึกอบรม จำนวน 6 ชุด พร้อมเอกสารคู่มือประกอบการฝึกอบรม และยูเอสบีแฟลชไดรฟ์ที่บรรจุเอกสารคู่มือประกอบการฝึกอบรมทุกหลักสูตร 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 ลงในยูเอสบีแฟลชไดรฟ์ 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 หากผู้ชนะการประกวดราคาจงใจหรือประมาทเลินเล่อ 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 ระบบสามารถทำงานร่วมกับอุปกรณ์ด้านความมั่นคงปลอดภัย (Security Products) ของ สศค. และอุปกรณ์ที่จัดซื้อในโครงการนี้ได้

14.5 กรณีเกิดปัญหากับครุภัณฑ์คอมพิวเตอร์ในโครงการ ผู้ชนะการประกวดราคาต้องส่งเจ้าหน้าที่ที่มีความเชี่ยวชาญเพื่อจัดการแก้ไขปัญหาด้วยการปรับปรุงหรือเปลี่ยนอุปกรณ์ที่เกิดปัญหา ให้ดำเนินการภายใน 8 ชั่วโมง นับจากที่ได้รับแจ้งปัญหา และดำเนินการให้เสร็จเรียบร้อยไม่เกิน 24 ชั่วโมง

14.6 กรณีผู้ชนะการประกวดราคาไม่สามารถแก้ไข หรือซ่อมแซม หรือเปลี่ยนใหม่ ได้ภายใน 24 ชั่วโมง ผู้ชนะการประกวดราคาต้องนำเครื่องสำรองที่มีประสิทธิภาพทัดเทียมกันหรือดีกว่ามาใช้งานแทนไปจนกว่าจะแก้ไขหรือซ่อมแซมหรือเปลี่ยนใหม่ ให้แล้วเสร็จสมบูรณ์

14.7 คุณสมบัติของอะไหล่ ชิ้นส่วน หรืออุปกรณ์ใดๆ ที่ใช้ในการเปลี่ยนหรือทดแทนชั่วคราว

- กรณีเปลี่ยนอุปกรณ์ อุปกรณ์ที่นำมาเปลี่ยนต้องมีคุณสมบัติไม่ด้อยกว่าอุปกรณ์เดิมในทุกกรณี และสามารถใช้งานร่วมกับระบบเดิมได้เป็นอย่างดี โดยต้องเป็นอะไหล่จากเจ้าของผลิตภัณฑ์โดยตรง

- กรณีอุปกรณ์ทดแทนชั่วคราว อุปกรณ์ที่นำมาทดแทนเพื่อใช้งานชั่วคราว ต้องมีคุณสมบัติไม่ด้อยกว่าอุปกรณ์เดิมในทุกกรณี และสามารถใช้งานร่วมกับระบบเดิมได้โดยไม่ก่อให้เกิดปัญหาใด ๆ

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

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

14.10 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

ลำดับที่	รายการ	ค่าตัวถ่วง
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 ผู้ชนะการประกวดราคาจะต้องดำเนินการทั้งปวงเพื่อให้การกล่าวอ้างหรือการเรียกร้องดังกล่าวระงับสิ้นไปโดยเร็ว 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
