ขอบเขตของงาน
ซื้อระบบรักษาความมั่นคงปลอดภัยสารสนเทศ พร้อมติดตั้ง

1. ความเป็นมา

สำนักงานคณะกรรมการข้าราชการพลเรือน (สำนักงาน ก.พ.) ได้มีการใช้งานระบบรักษาความปลอดภัยทางเครือข่าย ที่สามารถป้องกันภัยคุกคามด้านเทคโนโลยีสารสนเทศ และลดความเสียหายกับข้อมูลสารสนเทศ โดยได้มีการใช้งานระบบตั้งแต่ปี พ.ศ. 2560 ประกอบกับในปีงบประมาณ พ.ศ. 2564 ได้ขยายความเร็วในการรับและส่งข้อมูล (Bandwidth) ของระบบเครือข่ายอินเทอร์เน็ต (Internet) เพื่อเพิ่มประสิทธิภาพในการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน การรับและส่งข้อมูลไปยังศูนย์ข้อมูลสำรอง (Disaster Recovery Site) และรองรับการให้บริการประชาชนและส่วนราชการได้รวดเร็วขึ้น แต่ทำให้ระบบรักษาความปลอดภัยทางเครือข่ายเดิมทำงานหนักขึ้น ดังนั้นเพื่อลดความเสี่ยงที่อาจเกิดขึ้นกับระบบ และเพิ่มประสิทธิภาพในการรักษาความปลอดภัยบนเครือข่ายของสำนักงาน ก.พ. จึงจำเป็นต้องจัดหาระบบรักษาความมั่นคงปลอดภัยสารสนเทศเพื่อทดแทนอุปกรณ์เดิม และเสริมการทำงานบนระบบเครือข่ายให้มีประสิทธิภาพ

ระบบรักษาความมั่นคงปลอดภัยสารสนเทศ พร้อมติดตั้ง ประกอบด้วย

1. อุปกรณ์รักษาความปลอดภัยเครือข่าย (Next Generation Firewall) จำนวน 2 เครื่อง
2. อุปกรณ์จัดเก็บข้อมูลและรายงานภัยคุกคามทางเครือข่าย จำนวน 1 เครื่อง

2. วัตถุประสงค์

2.1 เพื่อจัดหาอุปกรณ์ป้องกันภัยคุกคามเพื่อทดแทนอุปกรณ์ป้องกันภัยคุกคามทางระบบเครือข่ายที่มีการใช้งานมากกว่า 5 ปี

2.2 เพื่อเพิ่มประสิทธิภาพในการรักษาความปลอดภัยของระบบเครือข่าย และรองรับเชื่อมต่อที่รวดเร็วขึ้น ทั้งระบบเครือข่ายภายใน และระบบเครือข่ายภายนอก

2.3 เพื่อป้องกันการโจมตีระบบเครือข่ายของสำนักงาน ก.พ. และลดความเสี่ยงที่อาจเกิดขึ้นกับระบบสารสนเทศและฐานข้อมูลของสำนักงาน ก.พ.

3. คุณสมบัติของผู้ยื่นข้อเสนอ

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 เป็นนิติบุคคล ผู้มีอาชีพขายพัสดุที่ประกวดราคาซื้อด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่สำนักงาน ก.พ. ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์ความคุ้มกันเช่นว่านั้น

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

3.11 ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ “กิจการร่วมค้า” ต้องมีคุณสมบัติดังนี้

กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงฯ จะต้องมีการกำหนดสัดส่วนหน้าที่ และความรับผิดชอบในปริมาณงาน สิ่งของ หรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลักกิจการร่วมค้านั้นต้องใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

สำหรับข้อตกลงฯ ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมค้าหลัก ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน

3.12 ผู้ยื่นข้อเสนอต้องมีผลงานในการขายและติดตั้งระบบรักษาความมั่นคงปลอดภัยสารสนเทศประกอบด้วยอุปกรณ์รักษาความปลอดภัยเครือข่าย (Next Generation Firewall) ที่เป็นคู่สัญญาโดยตรงกับส่วนราชการหรือหน่วยงานของรัฐ อย่างน้อย 1 สัญญา/ผลงาน ที่มีวงเงินต่อสัญญาไม่น้อยกว่า 3,000,000.- บาท และเป็นผลงานที่ดำเนินการแล้วเสร็จและผ่านการตรวจรับเรียบร้อยแล้วภายในระยะเวลาไม่เกิน 5 ปี นับถึงวันยื่นข้อเสนอ โดยแนบหนังสือรับรองผลงานหรือสำเนาสัญญาที่แสดงรายละเอียดของพัสดุที่ขายมาพร้อมกับการยื่นข้อเสนอ ทั้งนี้ สำนักงาน ก.พ. ขอสงวนสิทธิ์ที่จะตรวจสอบข้อเท็จจริงโดยตรงจากหน่วยงานที่เป็นคู่สัญญาตามเอกสารที่เสนอ

3.13 ผู้ยื่นข้อเสนอต้องได้รับการแต่งตั้งให้เป็นตัวแทนจำหน่ายผลิตภัณฑ์ของอุปกรณ์ที่จัดซื้อจากบริษัทผู้ผลิต หรือเจ้าของผลิตภัณฑ์ หรือตัวแทนจำหน่ายผลิตภัณฑ์ในประเทศไทย หรือตัวแทนที่ได้รับการแต่งตั้งให้จำหน่ายผลิตภัณฑ์ในประเทศไทยในการยื่นประกวดราคาอิเล็กทรอนิกส์ครั้งนี้ โดยให้ยื่นแสดงเอกสารหลักฐาน

3.14 ผู้ยื่นข้อเสนอต้องเสนอรายชื่อทีมงานวิศวกรระบบ (Systems Engineer) ปฏิบัติงานออกแบบและติดตั้งอุปกรณ์ระบบรักษาความมั่นคงปลอดภัยสารสนเทศ โดยเป็นผู้ที่ได้รับการรับรองความรู้และทักษะด้านการติดตั้งระบบรักษาความมั่นคงปลอดภัยสารสนเทศจากเจ้าของผลิตภัณฑ์ ของผลิตภัณฑ์ที่เสนอ ดังนี้

1) The Fortinet Network Security Professional (NSE 4) หรือ

2) Palo Alto Networks Certified Network Security Administrator (PCNSA) หรือ

3) Check Point Certified Security Expert (CCSE)

โดยให้ยื่นแสดงเอกสารหลักฐาน

3.15 ผู้ยื่นข้อเสนอต้องมีเจ้าหน้าที่ด้านเทคนิคให้คำปรึกษาในการใช้งานอุปกรณ์ที่จัดซื้อ และเป็นพนักงานประจำของผู้ยื่นข้อเสนอมาแล้วไม่น้อยกว่า 1 ปี อย่างน้อย 1 คน โดยให้ยื่นแสดงเอกสารหลักฐาน

4. รายละเอียดคุณลักษณะเฉพาะ

รายละเอียดคุณลักษณะเฉพาะของระบบรักษาความมั่นคงปลอดภัยสารสนเทศ พร้อมติดตั้ง จำนวน 7 หน้า ตามเอกสารแนบ

5. การเสนอราคา

ผู้ยื่นข้อเสนอจะต้องเสนอกำหนดยืนราคา ไม่น้อยกว่า 120 วัน นับตั้งแต่วันเสนอราคา โดยภายในกำหนดยืนราคา ผู้ยื่นข้อเสนอต้องรับผิดชอบราคาที่ตนได้เสนอไว้ และจะถอนการเสนอราคามิได้

6. ระยะเวลาส่งมอบพัสดุ

ผู้ยื่นข้อเสนอจะต้องเสนอกำหนดเวลาส่งมอบระบบรักษาความมั่นคงปลอดภัยสารสนเทศ พร้อมติดตั้ง ไม่เกิน 120 วัน นับถัดจากวันลงนามในสัญญาซื้อขาย

7. การจ่ายเงิน

สำนักงาน ก.พ. กำหนดจ่ายเงินซึ่งได้รวมภาษีมูลค่าเพิ่ม ตลอดจนภาษีอากรอื่น ๆ และค่าใช้จ่ายทั้งปวงแล้ว ให้แก่ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกให้เป็นผู้ขาย โดยแบ่งออกเป็น 3 งวด ดังนี้

งวดที่ 1 เป็นจำนวนเงินในอัตราร้อยละ 15 ของสัญญาซื้อขาย เมื่อผู้ขายส่งมอบงานงวดที่ 1 ครบถ้วนถูกต้อง ทุกรายการ ให้แล้วเสร็จภายใน 45 วัน นับถัดจากวันลงนามในสัญญา และผ่านการตรวจรับจากคณะกรรมการตรวจรับพัสดุเรียบร้อยแล้ว

งวดที่ 2 เป็นจำนวนเงินในอัตราร้อยละ 60 ของสัญญาซื้อขาย เมื่อผู้ขายส่งมอบงานงวดที่ 2 ครบถ้วนถูกต้อง ทุกรายการ ให้แล้วเสร็จภายใน 100 วัน นับถัดจากวันลงนามในสัญญา และผ่านการตรวจรับจากคณะกรรมการตรวจรับพัสดุเรียบร้อยแล้ว

งวดที่ 3 เป็นจำนวนเงินในอัตราร้อยละ 25 ของสัญญาซื้อขาย เมื่อผู้ขายส่งมอบงานงวดที่ 3 ครบถ้วนถูกต้อง ทุกรายการ ให้แล้วเสร็จภายใน 120 วัน นับถัดจากวันลงนามในสัญญา และผ่านการตรวจรับจากคณะกรรมการตรวจรับพัสดุเรียบร้อยแล้ว

8. วงเงินในการจัดซื้อ

เงินงบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. 2566 วงเงิน 7,609,000.- บาท (เจ็ดล้านหกแสน-เก้าพันบาทถ้วน)

9. หลักเกณฑ์และสิทธิในการพิจารณา

9.1 ในการพิจารณาผลการยื่นข้อเสนอประกวดราคาอิเล็กทรอนิกส์ในครั้งนี้ สำนักงาน ก.พ. จะพิจารณาตัดสินโดยใช้หลักเกณฑ์ราคา และจะพิจารณาจากราคารวม

9.2 หากผู้ยื่นข้อเสนอซึ่งเป็นผู้ประกอบการ SMEs เสนอราคาสูงกว่าราคาต่ำสุดของผู้ยื่นข้อเสนอรายอื่นที่ไม่เกินร้อยละ 10 ให้หน่วยงานของรัฐจัดซื้อจัดจ้างจากผู้ประกอบการ SMEs ดังกล่าว โดยจัดเรียงลำดับผู้ยื่นข้อเสนอซึ่งเป็นผู้ประกอบการ SMEs ซึ่งเสนอราคาสูงกว่าราคาต่ำสุดของผู้ยื่นข้อเสนอรายอื่นไม่เกินร้อยละ 10 ที่จะเรียกมาทำสัญญาไม่เกิน 3 ราย

ผู้ยื่นข้อเสนอที่เป็นกิจการร่วมค้าที่จะได้สิทธิตามวรรคหนึ่ง ผู้เข้าร่วมค้าทุกรายจะต้องเป็นผู้ประกอบการ SMEs

9.3 หากผู้ยื่นข้อเสนอได้เสนอพัสดุที่ได้รับการรับรองและออกเครื่องหมายสินค้าที่ผลิตภายในประเทศไทย (Made in Thailand) จากสภาอุตสาหกรรมแห่งประเทศไทย เสนอราคาสูงกว่าราคาต่ำสุดของผู้เสนอราคารายอื่นไม่เกินร้อยละ 5 ให้จัดซื้อจัดจ้างจากผู้ยื่นข้อเสนอที่เสนอพัสดุที่ได้รับการรับรองและออกเครื่องหมายสินค้าที่ผลิตภายในประเทศไทย (Made in Thailand) จากสภาอุตสาหกรรมแห่งประเทศไทย

กรณีที่มีการเสนอราคาหลายรายการและกำหนดเงื่อนไขการพิจารณาราคารวม หากผู้ยื่นข้อเสนอได้เสนอพัสดุที่เป็นพัสดุที่ผลิตภายในประเทศ ที่ได้รับการรับรองและออกเครื่องหมายสินค้าที่ผลิตภายในประเทศไทย (Made in Thailand) จากสภาอุตสาหกรรมแห่งประเทศไทย มีสัดส่วนมูลค่าตั้งแต่ร้อยละ 60 ขึ้นไป ให้ได้แต้มต่อในการเสนอราคาตามวรรคหนึ่ง

อนึ่ง หากในการเสนอราคาครั้งนั้น ผู้ยื่นข้อเสนอรายใดมีคุณสมบัติทั้งข้อ 9.2 และข้อ 9.3 ให้ผู้เสนอราคารายนั้นได้แต้มต่อในการเสนอราคาสูงกว่าผู้ประกอบการรายอื่นไม่เกินร้อยละ 15

9.4 หากผู้ยื่นข้อเสนอซึ่งมิใช่ผู้ประกอบการ SMEs แต่เป็นบุคคลธรรมดาที่ถือสัญชาติไทยหรือนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยเสนอราคาสูงกว่าราคาต่ำสุดของผู้ยื่นข้อเสนอซึ่งเป็นบุคคลธรรมดาที่มิได้ถือสัญชาติไทยหรือนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายของต่างประเทศไม่เกินร้อยละ 3 ให้จัดซื้อจัดจ้างจากผู้ยื่นข้อเสนอซึ่งเป็นบุคคลธรรมดาที่ถือสัญชาติไทยหรือนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยดังกล่าว

ผู้ยื่นข้อเสนอที่เป็นกิจการร่วมค้าที่จะได้สิทธิตามวรรคหนึ่ง ผู้เข้าร่วมค้าทุกรายจะต้องเป็นบุคคลธรรมดาที่ถือสัญชาติไทยหรือนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย

10. อัตราค่าปรับ

ค่าปรับตามสัญญาซื้อขาย หรือข้อตกลงซื้อขายเป็นหนังสือ ให้คิดในอัตราร้อยละ 0.20 ของราคาค่าสิ่งของที่ยังไม่ได้รับมอบต่อวัน

11. การรับประกันความชำรุดบกพร่อง

11.1 ผู้ขายต้องจัดให้มีเจ้าหน้าที่ให้คำปรึกษาและตอบปัญหาด้วยภาษาไทยแก่สำนักงาน ก.พ. ทุกวันตลอด 24 ชั่วโมง และต้องดำเนินการบำรุงรักษาเชิงป้องกัน (Preventive Maintenance) ทุก 3 เดือน โดยตรวจสอบดูแลอุปกรณ์ที่เสนอ ให้อยู่ในสภาพใช้งานได้ดีอยู่เสมอตลอดระยะเวลารับประกัน รวมทั้งทำความสะอาดภายนอกอุปกรณ์ทุกชิ้นด้วยค่าใช้จ่ายของผู้ขาย โดยมีรายละเอียดงาน ดังนี้

- Update Firmware and patch (ถ้ามี)
- ตรวจสอบรายละเอียด Log ของระบบรักษาความมั่นคงปลอดภัยสารสนเทศ เพื่อวิเคราะห์ภัยคุกคาม และดำเนินการป้องกันไม่ให้เกิดภัยคุกคามที่ตรวจพบ
- ให้คำปรึกษาในการตรวจสอบระบบรักษาความมั่นคงปลอดภัยสารสนเทศ

11.2 ผู้ขายต้องรับประกันความชำรุดบกพร่องหรือขัดข้องของระบบรักษาความมั่นคงปลอดภัยสารสนเทศ เป็นระยะเวลาไม่น้อยกว่า 3 ปี แบบ On-Site Service นับถัดจากวันที่คณะกรรมการตรวจรับพัสดุได้ตรวจรับเสร็จสมบูรณ์ทั้งหมด ถ้าภายในระยะเวลาดังกล่าวระบบรักษาความมั่นคงปลอดภัยสารสนเทศชำรุดบกพร่องหรือขัดข้อง หรือใช้งานไม่ได้ทั้งหมดหรือแต่บางส่วน หรือเกิดความชำรุดบกพร่องหรือขัดข้องจากการติดตั้ง เว้นแต่ความชำรุดบกพร่องหรือขัดข้องดังกล่าวเกิดขึ้นจากความผิดของสำนักงาน ก.พ. ซึ่งไม่ได้เกิดขึ้นจากการใช้งานตามปกติ ผู้ขายจะต้องจัดการซ่อมแซมแก้ไขให้อยู่ในสภาพใช้การได้ดีดังเดิม โดยต้องเริ่มจัดการซ่อมแซมแก้ไขภายใน 2 วัน นับถัดจากวันที่ได้รับแจ้งจากสำนักงาน ก.พ. โดยไม่คิดค่าใช้จ่ายใดๆ จากสำนักงาน ก.พ. ทั้งสิ้น ถ้าผู้ขายไม่จัดการซ่อมแซมแก้ไขภายในกำหนดเวลาดังกล่าว สำนักงาน ก.พ. มีสิทธิที่จะทำการนั้นเอง หรือจ้างผู้อื่นทำการนั้นแทนผู้ขาย โดยผู้ขายต้องออกค่าใช้จ่ายเองทั้งสิ้นแทนสำนักงาน ก.พ.

11.3 ในกรณีที่ระบบรักษาความมั่นคงปลอดภัยสารสนเทศ พร้อมติดตั้ง ชำรุดบกพร่อง หรือใช้งานไม่ได้ ผู้ขายจะต้องทำการวิเคราะห์ หรือวินิจฉัยปัญหาภายใน 2 ชั่วโมงหลังจากได้รับแจ้งจากสำนักงาน ก.พ. โดยแจ้งกลับมายังเจ้าหน้าที่ผู้ดูแลระบบของสำนักงาน ก.พ. ทางโทรศัพท์หรือทางจดหมายอิเล็กทรอนิกส์ (E-Mail)

11.4 ผู้ขายมีหน้าที่บำรุงรักษาและซ่อมแซมแก้ไขระบบรักษาความมั่นคงปลอดภัยสารสนเทศให้อยู่ในสภาพใช้งานได้ดีอยู่เสมอตลอดระยะเวลาไม่น้อยกว่า 3 ปี แบบ On-Site Service ด้วยค่าใช้จ่ายของผู้ขาย โดยให้มีเวลาระบบรักษาความมั่นคงปลอดภัยสารสนเทศขัดข้องไม่เกินเดือนละ 48 ชั่วโมง มิฉะนั้นผู้ขายต้องยินยอมให้สำนักงาน ก.พ. คิดค่าปรับเป็นรายชั่วโมง ในอัตราร้อยละ 0.035 ของราคาระบบรักษาความมั่นคงปลอดภัยสารสนเทศในช่วงเวลาที่ไม่สามารถใช้ระบบรักษาความมั่นคงปลอดภัยสารสนเทศได้ในส่วนที่เกินกว่ากำหนดเวลาขัดข้องข้างต้น

12. ข้อสงวนสิทธิในการยื่นข้อเสนอ

เงินค่าพัสดุสำหรับการซื้อครั้งนี้ ได้มาจากเงินงบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. 2566

การลงนามในสัญญาจะกระทำได้ต่อเมื่อสำนักงาน ก.พ. ได้รับอนุมัติเงินค่าพัสดุจากงบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. 2566 แล้วเท่านั้น

13. สถานที่ติดต่อเพื่อแสดงความคิดเห็น

สามารถส่งข้อคิดเห็นหรือข้อเสนอแนะ วิจารณ์ เกี่ยวกับร่างขอบเขตของงานนี้ได้ที่

สถานที่ติดต่อ กลุ่มงานบริหารทรัพย์สิน สำนักงานเลขาธิการ สำนักงาน ก.พ. ถนนติวานนท์ ตำบลตลาดขวัญ อำเภอเมืองนนทบุรี จังหวัดนนทบุรี 11000

โทรศัพท์ 0 2547 1000 ต่อ 6276

โทรสาร 0 2547 1083

E-mail address: opm@ocsc.go.th

สาธารณชนที่ต้องการเสนอแนะ วิจารณ์ หรือมีความเห็น ต้องเปิดเผยตัว โดยระบุชื่อและที่อยู่ พร้อมหมายเลขโทรศัพท์ของผู้ให้ข้อเสนอแนะ วิจารณ์ หรือมีความเห็น

****

รายละเอียดคุณลักษณะเฉพาะ

ของระบบรักษาความมั่นคงปลอดภัยสารสนเทศ พร้อมติดตั้ง

1. ระบบรักษาความมั่นคงปลอดภัยสารสนเทศ พร้อมติดตั้ง จำนวน 1 ระบบ ประกอบด้วย

1.1 อุปกรณ์รักษาความปลอดภัยเครือข่าย (Next Generation Firewall) จำนวน 2 เครื่อง โดยแต่ละเครื่องมีคุณสมบัติ ดังนี้

1.1.1 เป็นอุปกรณ์รักษาความปลอดภัยเครือข่ายแบบ Next Generation Firewall

1.1.2 เป็นอุปกรณ์ Firewall ชนิด Next Generation Firewall แบบ Appliance สามารถทำงานร่วมกันในลักษณะ High Availability สามารถเลือกติดตั้งแบบ Active-Active และ Active-Standby หรือเทียบเท่า

1.1.3 มี Firewall Throughput ไม่น้อยกว่า 120 Gbps

1.1.4 รองรับ Concurrent Session หรือ Connection ได้ไม่น้อยกว่า 11,500,000 Sessions/ Connections หรือดีกว่า

1.1.5 รองรับ New Sessions/Sec หรือ New Connection/Sec ได้ไม่น้อยกว่า 600,000 Sessions/ Second หรือดีกว่า

1.1.6 มี IPsec VPN Throughput ไม่น้อยกว่า 40 Gbps

1.1.7 รองรับ Concurrent SSL VPN Users ไม่น้อยกว่า 6,000 Users

1.1.8 มี Threat Protection Throughput ไม่น้อยกว่า 9 Gbps โดยเปิดใช้งาน Function อย่างน้อยดังนี้ Firewall, IPS, Application control และ Malware protection

1.1.9 มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) อย่างน้อย ดังนี้

1) มีช่องเชื่อมต่อเครือระบบข่าย (Network Interface) แบบ 1 Gbps สำหรับหัวต่อสายแบบ RJ45 จำนวนไม่น้อยกว่า 16 ช่อง

2) มีช่องเชื่อมต่อเครือระบบข่าย (Network Interface) แบบ 1 Gbps สำหรับติดตั้ง Transceiver แบบ SFP (Small Form-Factor Pluggable) จำนวนไม่น้อยกว่า 4 ช่อง หรือดีกว่า

3) มีช่องเชื่อมต่อเครือระบบข่าย (Network Interface) แบบ 10 Gbps (SFP+) หรือดีกว่า จำนวนไม่น้อยกว่า 12 ช่อง พร้อม Transceiver Module แบบ 10G SR หรือดีกว่า จำนวนไม่น้อยกว่า 10 หน่วย

4) มีช่องเชื่อมต่อเครือระบบข่าย (Network Interface) แบบ 40GE (QSFP+) หรือดีกว่า จำนวนไม่น้อยกว่า 4 ช่อง

5) มีช่องเชื่อมต่อเครือระบบข่าย (Network Interface) สำหรับ Management แบบ 1 Gbps (RJ45) หรือดีกว่า จำนวนไม่น้อยกว่า 1 ช่อง

6) มีช่องเชื่อมต่อเครือระบบข่าย (Network Interface) สำหรับการตั้งค่า High Availability (HA) แบบ 10 Gbps (SFP+) หรือดีกว่า จำนวนไม่น้อยกว่า 2 ช่อง พร้อม Transceiver Module แบบ 10G SR จำนวนไม่น้อยกว่า 2 หน่วย

1.1.10 รองรับการทำ Virtual Firewall/Domain ได้อย่างน้อย 10 Virtual Systems/Domains และรองรับการขยายเป็นจำนวนไม่น้อยกว่า 200 Virtual Systems/Domains ได้

1.1.11 มี Power Supply จำนวน 2 หน่วย ทำงานร่วมกันแบบ Redundant Hot Swappable

1.1.12 อุปกรณ์ต้องได้การรับรองตามมาตรฐาน FCC และ UL ได้เป็นอย่างน้อย

1.1.13 สามารถทำ Routing Protocol แบบ OSPF, BGP และสามารถทำ NAT46 หรือ NAT64 หรือ IPv6 ได้เป็นอย่างน้อย

1.1.14 มีคุณสมบัติด้านความปลอดภัย ดังต่อไปนี้

1) Cloud-Based Sandboxing

2) Anti-Virus

3) IPS Signature

4) สามารถ Update Services ของระบบ Sandbox Cloud, Antivirus, IPS และ Signature ได้ตลอดระยะเวลาของการรับประกัน

1.1.15 สามารถทำหน้าที่ Proxy ทั้ง Explicit และ Transparent Proxy ได้ พร้อมสามารถทำ Proxy Chaining เพื่อส่งต่อ Proxy session ต่อไปยัง Proxy อื่นได้

1.1.16 มีคุณสมบัติในการป้องกันการโจมตีแบบ Denial of Service (DoS) สำหรับ IPv6 และ IPv4 และสามารถกำหนดเกณฑ์ (Threshold) ความผิดปกติของการจราจร (Traffic) ของชั้น Transport Layer ของ Open Systems Interconnection model (OSI model) ได้

1.1.17 มีคุณสมบัติ SD-WAN ที่สามารถควบคุม Application ใช้งานผ่าน WAN Link ตามค่า Service Level Agreement (SLA)

1.1.18 มี Dashboard แสดงสถานะการใช้งาน CPU และ Memory และ Session ในรูปแบบกราฟได้บนตัวอุปกรณ์ โดยสามารถเลือกแสดงผลย้อนหลังได้

1.1.19 สามารถเก็บและส่งรายละเอียด (Logging) และตรวจสอบการใช้งาน (Monitoring) ในรูปแบบ Syslog ได้

1.1.20 ผลิตภัณฑ์ที่เสนอมีระยะเวลาการรับประกันตัวอุปกรณ์ การสนับสนุนทางด้านการปรับปรุงระบบปฏิบัติการ ระบบรักษาความปลอดภัย และการสนับสนุนทางด้านเทคนิคไม่น้อยกว่า 3 ปี แบบ On-Site Service หลังจากผ่านการตรวจรับจากคณะกรรมการตรวจรับพัสดุของสำนักงาน ก.พ.

1.1.21 ผลิตภัณฑ์ที่เสนอต้องมีเครื่องหมายการค้าอยู่ในกลุ่ม Leader ของ Gartner Magic Quadrant for Networks Firewall ปี 2020 และ 2021 หรือ ปีล่าสุด

1.1.22 กรณีที่อุปกรณ์รักษาความปลอดภัยเครือข่าย (Next Generation Firewall) ไม่มีคุณสมบัติตามที่กำหนด ข้อ 1.1.14 และ 1.1.15 และ 1.1.18 สามารถเสนอระบบเพิ่มเพื่อให้มีคุณสมบัติตามที่กำหนด และเป็นผลิตภัณฑ์ที่มีประสิทธิภาพเหมาะสม และสามารถทำงานร่วมกับอุปกรณ์รักษาความปลอดภัยเครือข่าย (Next Generation Firewall) ที่ยื่นข้อเสนอ

1.2 อุปกรณ์จัดเก็บข้อมูลและรายงานภัยคุกคามทางเครือข่าย จำนวน 1 เครื่อง

1.2.1 เป็นอุปกรณ์ Hardware Appliance ที่สามารถเก็บรวบรวมเหตุการณ์ (Logs or Events) ที่เกิดขึ้นบนอุปกรณ์รักษาความปลอดภัยเครือข่าย (Next Generation Firewall) และมีเครื่องหมายการค้าเดียวกัน เพื่อให้สามารถทำงานร่วมกันได้อย่างมีประสิทธิภาพ

1.2.2 มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) 1 Gbps สำหรับหัวต่อสายแบบ RJ45 หรือดีกว่า จำนวนไม่น้อยกว่า 4 ช่อง

1.2.3 สามารถทำ RAID 1 ได้หรือดีกว่า

1.2.4 หน่วยจัดเก็บข้อมูล (Storage) มีขนาดความจุหลังทำ RAID 1 ไม่น้อยกว่า 3.5 TB

1.2.5 มีความสามารถในการจัดเก็บข้อมูลเพื่อวิเคราะห์ได้ไม่น้อยกว่า 2,000 Logs/Events per second และสามารถรองรับจำนวน log ได้ไม่น้อยกว่า 100 GB ต่อวัน

1.2.6 สามารถบริหารจัดการอุปกรณ์ผ่านโปรโตคอล HTTPS ผ่าน Web Browser หรือ GUI และโปรโตคอล SSH ได้

1.2.7 มีคุณสมบัติ Parse normalize และ Correlate log ข้อมูล log จากอุปกรณ์รักษาความปลอดภัยเครือข่าย (Next generation Firewall) และ SD-WAN หรืออุปกรณ์เพิ่มเติม เพื่อให้มีคุณสมบัติตามที่กำหนด

1.2.8 มี Dashboard และรายงานสรุปการใช้งานจากอุปกรณ์รักษาความปลอดภัยเครือข่าย (Next Generation Firewall) ได้อย่างน้อย ดังนี้

- Top sources
- Top destinations
- Top applications
- Top websites
- Top threats
- System events
- Resource usage

1.2.9 สามารถแสดงข้อมูล Log ประกอบด้วยข้อมูล Date, Time, Source IP, User, Destination IP และ Services ได้เป็นอย่างน้อย

1.2.10 มีรูปแบบรายงาน (Report templates) และสามารถแสดงรายงานในรูปแบบของ PDF และ CSV ได้

1.2.11 ได้รับการรับรองตามมาตรฐาน FCC และ UL

1.2.12 อุปกรณ์ที่เสนอต้องสามารถทำงานร่วมกับอุปกรณ์รักษาความปลอดภัยเครือข่าย (Next Generation Firewall) ได้อย่างมีประสิทธิภาพ

1.2.13 ผลิตภัณฑ์ที่เสนอมีระยะเวลาการรับประกันตัวอุปกรณ์ การสนับสนุนทางด้านการปรับปรุงระบบปฏิบัติการ ระบบรักษาความปลอดภัย และการสนับสนุนทางด้านเทคนิคไม่น้อยกว่า 3 ปี แบบ On-Site Service หลังจากผ่านการตรวจรับจากคณะกรรมการตรวจรับพัสดุของสำนักงาน ก.พ.

2. ขอบเขตการดำเนินงานและรายละเอียดการติดตั้ง

ผู้ขายต้องดำเนินการติดตั้งระบบรักษาความมั่นคงปลอดภัยสารสนเทศ พร้อมจัดทำเอกสารที่เกี่ยวข้อง ดังนี้

2.1 ดำเนินการจัดทำแผนดำเนินการโครงการ สำรวจสภาพแวดล้อมของศูนย์ข้อมูล (Data Center) ออกแบบและกำหนดนโยบาย (Policy) พร้อมนำเสนอและรายงานให้สำนักงาน ก.พ. พิจารณาอนุมัติการออกแบบและการกำหนดนโยบาย ให้ทราบถึงหลักการและที่มาของแนวคิดการออกแบบและการกำหนดนโยบายความปลอดภัยด้านสารสนเทศ

2.2 ดำเนินการติดตั้งระบบรักษาความมั่นคงปลอดภัยให้ทำงานร่วมกับระบบเครือข่าย และระบบต่าง ๆ ของสำนักงาน ก.พ. ตามหลักวิศวกรรม และหลักวิชาการ โดยต้องนำเสนอรูปแบบและวิธีการติดตั้งให้สำนักงาน ก.พ. พิจารณาอนุมัติก่อนเข้าดำเนินการ และในกรณีที่เกิดความเสียหายกับอุปกรณ์เดิมหรือสภาพแวดล้อมเดิมของสำนักงาน ก.พ. ผู้รับจ้างจะต้องรับผิดชอบค่าใช้จ่ายในการแก้ไขอุปกรณ์ให้สามารถกลับมาใช้งานได้เป็นปกติ

2.3 ผู้ขายต้องดำเนินการจัดหาและติดตั้งสายสัญญาณ สายไฟฟ้า และวัสดุอุปกรณ์ต่าง ๆ สำหรับใช้ในการติดตั้งระบบรักษาความมั่นคงปลอดภัยสารสนเทศให้มีประสิทธิภาพ ในกรณีที่จำเป็นต้องจัดหาวัสดุอุปกรณ์ในการติดตั้งเพิ่มเติมเพื่อให้เป็นไปตามข้อกำหนดของสัญญา ตามมาตรฐานความปลอดภัยตามหลักวิศวกรรม ตามหลักวิชาการ ผู้ขายจะต้องดำเนินการโดยไม่คิดค่าใช้จ่ายเพิ่มเติม

2.4 การดำเนินการติดตั้งระบบรักษาความมั่นคงปลอดภัยสารสนเทศ ต้องดำเนินการโดยทีมงานหรือพนักงานของผู้รับจ้างที่มีความรู้ความสามารถเกี่ยวกับการติดตั้งระบบรักษาความมั่นคงปลอดภัยสารสนเทศจากเจ้าของผลิตภัณฑ์ ของผลิตภัณฑ์ที่เสนอ ดังนี้

1) The Fortinet Network Security Professional (NSE 4) หรือ

2) Palo Alto Networks Certified Network Security Administrator (PCNSA) หรือ

3) Check Point Certified Security Expert (CCSE)

2.5 ผู้ขายต้องเคลื่อนย้ายระบบรักษาความมั่นคงปลอดภัยสารสนเทศเดิม และอุปกรณ์ต่าง ๆ ที่เกี่ยวข้อง ตามที่สำนักงาน ก.พ. กำหนด

2.6 การดำเนินการเพื่อเข้าพื้นที่สำหรับการปฏิบัติงานทั้งสิ้นตามสัญญา ต้องแจ้งให้สำนักงาน ก.พ. ทราบล่วงหน้าไม่น้อยกว่า 7 วัน

2.7 ผู้ขายต้องกำหนดและปรับแต่งค่า Configuration ของระบบรักษาความมั่นคงปลอดภัยสารสนเทศให้ทำงานได้อย่างมีประสิทธิภาพเหมาะสมกับอุปกรณ์และสภาพแวดล้อม ที่สำนักงาน ก.พ. ใช้งานอยู่

2.8 ผู้ขายต้องจัดทำคู่มือการใช้งาน และคู่มือบำรุงรักษาระบบต่าง ๆ เป็นเอกสารภาษาไทยที่สอดคล้องกับการตั้งค่าอุปกรณ์รักษาความปลอดภัยเครือข่าย (Next Generation Firewall) และอุปกรณ์จัดเก็บข้อมูลและรายงานภัยคุกคามทางเครือข่าย อ้างอิงจากเจ้าของผลิตภัณฑ์จำนวน 1 ชุด โดยแสดงรายละเอียดเป็นขั้นตอนที่สามารถทำความเข้าใจได้ง่าย

2.9 ผู้ขายต้องจัดทำคู่มือการตอบสนองภัยคุกคามและการโจมตีทางไซเบอร์ ตามความสามารถของระบบรักษาความมั่นคงปลอดภัยสารสนเทศที่จัดหา เป็นเอกสารภาษาไทย จำนวน 1 ชุด โดยแสดงรายละเอียดเป็นขั้นตอนที่สามารถทำความเข้าใจได้ง่าย

2.10 ผู้ขายต้องจัดอบรมถ่ายทอดความรู้ในการบริหารจัดการ และดูแลบำรุงรักษาระบบรักษาความมั่นคงปลอดภัยสารสนเทศ ให้แก่เจ้าหน้าที่ผู้ดูแลระบบสารสนเทศของสำนักงาน ก.พ. พร้อมทั้งจัดทำเอกสารประกอบการอบรมสำหรับผู้เข้าร่วมอบรม

2.11 ผู้ขายต้องจัดเจ้าหน้าที่ปฏิบัติงาน ณ สำนักงาน ก.พ. อย่างน้อย 1 คน ระยะเวลาไม่น้อยกว่า 10 วันทำการ เพื่อตรวจติดตามการกำหนดนโยบาย (Policy) ของระบบระบบรักษาความมั่นคงปลอดภัยสารสนเทศ และต้องสามารถแก้ไขปัญหาความขัดข้องของระบบฯ ได้ทุกระดับการขัดข้อง

2.12 ผู้ขายต้องรักษาความลับเกี่ยวกับการกำหนดนโยบายการรักษาความปลอดภัยระบบสารสนเทศของระบบรักษาความมั่นคงปลอดภัยสารสนเทศของสำนักงาน ก.พ.

3. การฝึกอบรม

ผู้ขายต้องการดำเนินการฝึกอบรมการใช้งานอุปกรณ์รักษาความปลอดภัยเครือข่าย (Next Generation Firewall) และอุปกรณ์จัดเก็บข้อมูลและรายงานภัยคุกคามทางเครือข่าย และความรู้พื้นฐานที่เกี่ยวข้องให้กับเจ้าหน้าที่สำนักงาน ก.พ. จำนวนไม่น้อยกว่า 3 คน โดยมีระยะเวลาในการฝึกอบรมรวมไม่น้อยกว่า 3 วัน โดยใช้สถานที่ของสำนักงาน ก.พ. เพื่อให้สามารถใช้งานและแก้ไขปัญหาเบื้องต้น พร้อมเอกสารคู่มือ มีรายละเอียดดังนี้

3.1 ความรู้พื้นฐานเกี่ยวกับเครือข่ายคอมพิวเตอร์และความปลอดภัยของระบบ (Basic Network & Security) ระยะเวลาไม่น้อยกว่า 1 วัน มีรายละเอียดหลักสูตร ดังนี้

- พื้นฐานสำคัญของการทำงานบนระบบเครือข่ายคอมพิวเตอร์ OSI Model และ TCP/IP Model
- ความรู้พื้นฐานทำความเข้าใจ TCP/IP , UDP Protocols และ Port Number
- ความรู้พื้นฐาน IPv4 และ IPv6
- การออกแบบ IPv4 Addressing และ Subnetting
- ตรวจสอบ และ แก้ไขปัญหา IPv4 Addressing และ Subnetting
- การตั้งค่าของอุปกรณ์เครือข่าย Router และ Switch

3.2 การอุปกรณ์รักษาความปลอดภัยเครือข่าย (Next Generation Firewall) และอุปกรณ์จัดเก็บข้อมูลและรายงานภัยคุกคามทางเครือข่าย ระยะเวลาไม่น้อยกว่า 2 วัน

- หลักการทำงานของอุปกรณ์รักษาความปลอดภัยเครือข่าย (Next Generation Firewall) และอุปกรณ์จัดเก็บข้อมูลและรายงานภัยคุกคามทางเครือข่าย
- หลักการติดตั้งอุปกรณ์รักษาความปลอดภัยเครือข่าย (Next Generation Firewall) และอุปกรณ์จัดเก็บข้อมูลและรายงานภัยคุกคามทางเครือข่าย

- หลักการตั้งค่าสำหรับการใช้งานและกำหนดนโยบายอุปกรณ์รักษาความปลอดภัยเครือข่าย (Next Generation Firewall) และอุปกรณ์จัดเก็บข้อมูลและรายงานภัยคุกคามทางเครือข่าย ดังนี้ Firewall, IPS, Antivirus, VPN, User Authentication, Log และ Report

- อธิบายการติดตั้งและการตั้งค่าระบบ ให้สำนักงาน ก.พ. ใช้งานตามหลักการ หรือหลักวิชาการที่เกี่ยวข้อง

- การแก้ไขปัญหาอุปกรณ์รักษาความปลอดภัยเครือข่าย (Next Generation Firewall) และอุปกรณ์จัดเก็บข้อมูลและรายงานภัยคุกคามทางเครือข่าย ดังนี้ Firewall, IPS, Antivirus, VPN, User Authentication, Log และ Report

- การบำรุงรักษาเชิงป้องกันอุปกรณ์รักษาความปลอดภัยเครือข่าย (Next Generation Firewall) และอุปกรณ์จัดเก็บข้อมูลและรายงานภัยคุกคามทางเครือข่าย

4. การส่งมอบและการชำระเงิน

ผู้ขายต้องส่งมอบระบบรักษาความมั่นคงปลอดภัยสารสนเทศ พร้อมติดตั้ง ภายใน 120 วัน นับถัดจากวันลงนามในสัญญาซื้อขาย โดยมีรายละเอียดการส่งมอบและการชำระเงิน ดังนี้

งวดงานที่	รายละเอียด	การชำระเงิน
1	แผนการติดตั้ง แผนการทดสอบระบบ แผนการจัดฝึกอบรม ร่างแบบการติดตั้งในรูปแบบเอกสาร จำนวน 2 ชุด และไฟล์เอกสารอิเล็กทรอนิกส์ที่อยู่ใน Flash drive จำนวน 1 ชุด ประกอบด้วย 1.1 แผนการดำเนินโครงการ 1.2 แผนการทดสอบระบบรักษาความมั่นคงปลอดภัยสารสนเทศ 1.3 แผนการคืน (Roll back) ระบบรักษาความมั่นคงปลอดภัยสารสนเทศ กรณีที่ไม่สามารถใช้งานได้ระหว่างการปรับเปลี่ยนจากระบบรักษาความมั่นคงปลอดภัยสารสนเทศเดิมไปยังระบบรักษาความมั่นคงปลอดภัยสารสนเทศที่จัดหา 1.4 แผนการบำรุงรักษาระบบรักษาความมั่นคงปลอดภัยสารสนเทศ (โดยข้อ 1.1 - 1.4 ต้องส่งมอบภายใน 15 วัน นับถัดจากวันที่ลงนามในสัญญา) 1.5 รายงานการสำรวจสภาพแวดล้อมของศูนย์ข้อมูล (Data Center) 1.6 รายงานโครงสร้างระบบเครือข่ายภายในและภายนอก 1.7 รายงานการเชื่อมโยงระบบเครือข่ายภายในและภายนอก 1.8 รายงานการเชื่อมโยงระบบรักษาความปลอดภัยของสำนักงาน ก.พ. (โดยข้อ 1.5 - 1.8 ต้องส่งมอบภายใน 30 วัน นับถัดจากวันที่ลงนามในสัญญา)	ร้อยละ 15

งวดงานที่	รายละเอียด	การชำระเงิน
	1.9 รายงานการออกแบบและกำหนดนโยบาย (Policy) ระบบรักษาความมั่นคงปลอดภัยสารสนเทศ อ้างอิงตามหลักวิชาการ ข้อกำหนดด้านมาตรฐานความปลอดภัย มาตรฐานการติดตั้ง และมาตรฐานสากลอื่นๆ ที่เกี่ยวข้อง 1.10 รายงานการออกแบบและติดตั้งระบบรักษาความมั่นคงปลอดภัยสารสนเทศ กับระบบเครือข่าย ระบบเครื่องแม่ข่าย ระบบสำรองข้อมูล และระบบจัดเก็บข้อมูล ระบบสารสนเทศทั้งภายนอก ภายใน และระบบเครือข่ายที่เกี่ยวข้องกับระบบเครือข่ายของสำนักงาน ก.พ. (โดยข้อ 1.9 - 1.10 ต้องส่งมอบภายใน 45 วัน นับถัดจากวันที่ลงนามในสัญญา) (ส่งมอบงานงวดที่ 1 ภายใน 45 วัน นับถัดจากวันลงนามในสัญญา)	
2	รายงานการติดตั้ง รายงานการตั้งค่า ในรูปแบบเอกสาร จำนวน 2 ชุด และไฟล์เอกสารอิเล็กทรอนิกส์ที่อยู่ใน Flash drive จำนวน 1 ชุด ประกอบด้วย 2.1 รายงานการติดตั้งระบบรักษาความมั่นคงปลอดภัยสารสนเทศ 2.2 รายงานการตั้งค่าอุปกรณ์รักษาความปลอดภัยเครือข่าย (Next Generation Firewall) และอุปกรณ์จัดเก็บข้อมูลและรายงานภัยคุกคามทางเครือข่าย (ส่งมอบงานงวดที่ 2 ภายใน 100 วัน นับถัดจากวันลงนามในสัญญา)	ร้อยละ 60
3	รายงานผลการทดสอบการทำงาน รายงานฝึกอบรม คู่มือการใช้งาน คู่มือบำรุงรักษา ในรูปแบบเอกสาร จำนวน 2 ชุด และไฟล์เอกสารอิเล็กทรอนิกส์ที่อยู่ใน Flash drive จำนวน 1 ชุด ประกอบด้วย 3.1 รายงานผลการทดสอบการทำงานของอุปกรณ์รักษาความปลอดภัยเครือข่าย (Next Generation Firewall) และอุปกรณ์จัดเก็บข้อมูลและรายงานภัยคุกคามทางเครือข่าย 3.2 รายงานการฝึกอบรม 3.3 คู่มือภาษาไทยเกี่ยวกับการใช้งานตามการตั้งค่าการใช้งานของอุปกรณ์รักษาความปลอดภัยเครือข่าย (Next Generation Firewall) และอุปกรณ์จัดเก็บข้อมูลและรายงานภัยคุกคามทางเครือข่าย 3.4 คู่มือภาษาไทยเกี่ยวกับการบำรุงรักษาเชิงป้องกันของอุปกรณ์รักษาความปลอดภัยเครือข่าย (Next Generation Firewall) และอุปกรณ์จัดเก็บข้อมูลและรายงานภัยคุกคามทางเครือข่าย พร้อมรายละเอียดการบำรุงรักษาเชิงป้องกัน (Checklist) ตามมาตรฐานของเจ้าของผลิตภัณฑ์ (ส่งมอบงานงวดที่ 3 ภายใน 120 วัน นับถัดจากวันลงนามในสัญญา)	ร้อยละ 25
