ขอบเขตของงาน (Terms of Reference: TOR)
รายการเช่าระบบแสดงตัวตนในการเข้าถึงอินเทอร์เน็ต (Authentication)

1. ความเป็นมา

ด้วยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 กำหนดให้ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ โดยให้สามารถระบุตัวผู้ใช้บริการ นับตั้งแต่เริ่มใช้บริการ และต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวัน นับตั้งแต่การใช้บริการสิ้นสุดลง ปัจจุบันการเข้าใช้ระบบอินเทอร์เน็ตยังไม่มีการแสดงตัวตนของผู้บริการซึ่งไม่เป็นไปตามมาตรา 26 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 ในนิยามของ “ผู้ใช้บริการ” หมายความว่า (4) ในการเก็บข้อมูลจราจร นั้น ต้องสามารถระบุรายละเอียดผู้ใช้บริการเป็นรายบุคคลได้ (Identification and Authentication) เช่น ลักษณะการใช้บริการ Proxy Server, Network Address Translation (NAT) หรือ Proxy Cache หรือ Cache Engine หรือบริการ Free Internet หรือ บริการ 1222 หรือ Wi-Fi Hotspot ต้องสามารถระบุตัวตนของผู้ใช้บริการเป็นรายบุคคลได้จริง ดังนั้น เพื่อให้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 สำนักงานปลัดกระทรวงศึกษาธิการจึงต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์เนื่องจากเป็นผู้ให้บริการอินเทอร์เน็ต จึงได้จัดทำโครงการเช่าระบบแสดงตัวตนในการเข้าถึงอินเทอร์เน็ต (Authentication) เพื่อให้สามารถระบุตัวผู้ใช้บริการได้

2. วัตถุประสงค์

เพื่อจัดเช่าระบบเพื่อแสดงตัวตนในการเข้าถึงอินเทอร์เน็ต (Authentication) ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

3. คุณสมบัติของผู้เสนอราคา

3.1 ผู้เสนอราคาต้องเป็นผู้มีประสบการณ์ในการบำรุงรักษาหรือติดตั้งอุปกรณ์เครือข่ายคอมพิวเตอร์ จำนวนไม่น้อยกว่า 1 ผลงาน โดยผลงานดังกล่าวต้องเป็นผลงานที่เสร็จเรียบร้อยแล้วเป็นเวลาไม่เกิน 3 ปี นับถึงวันยื่นเอกสาร โดยมีสำเนาสัญญาหรือหนังสือรับรองผลงานกับหน่วยงานราชการ หน่วยงานของรัฐ รัฐวิสาหกิจ หรือหน่วยงานภาคเอกชนในประเทศไทยที่น่าเชื่อถือ เพื่อประกอบการพิจารณามายื่นพร้อมกับเอกสารเพื่อประกอบการพิจารณา

3.2 ผู้รับจ้างต้องได้รับการแต่งตั้งให้เป็นตัวแทนจำหน่ายจากผู้ผลิตหรือตัวแทนจำหน่ายในประเทศไทยตามข้อ 4.1 สำหรับโครงการนี้ พร้อมยื่นเอกสารประกอบในวันที่ยื่นเสนอราคา

3.3 ผู้เสนอราคาต้องมีผู้เชี่ยวชาญอย่างน้อย 1 คน ที่ผ่านการอบรมและรับรอง (Certified) ด้าน Firewall Administrator และระบบตรวจสอบสถานะเครือข่าย PRTG Monitoring Expert เป็นอย่างน้อย โดยทำหน้าที่ปรับแต่งค่ากำหนดค่าอุปกรณ์รักษาความปลอดภัย (Firewall) และระบบตรวจสอบสถานะเครือข่ายตามความต้องการของผู้ว่าจ้าง โดยผู้เสนอราคาจะต้องทำการยื่นเอกสารประวัติบุคลากร และเอกสารผ่านการอบรมและรับรอง (Certified) พร้อมยื่นเอกสารประกอบในวันที่ยื่นเสนอราคา

3.4 ผู้เสนอราคาต้องมีผู้เชี่ยวชาญอย่างน้อย 1 คน ที่ผ่านการอบรมและรับรอง (Certified) ในหลักสูตร CCIE เป็นอย่างน้อย ทำหน้าที่ในการให้คำปรึกษาและปรับแต่งค่าอุปกรณ์เครือข่ายเดิมของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงศึกษาธิการ ให้สามารถใช้งานได้กับอุปกรณ์ที่เสนอในโครงการได้อย่างมีประสิทธิภาพ โดยผู้เสนอราคาจะต้องทำการยื่นเอกสารประวัติบุคลากร และเอกสารผ่านการอบรมและรับรอง (Certified) พร้อมยื่นเอกสารประกอบในวันที่ยื่นเสนอราคา

3.5 ผู้เสนอราคาต้องขึ้นทะเบียนผู้ค้ากับภาครัฐ

4. รายละเอียดขอบเขตของงาน

4.1 อุปกรณ์รักษาความปลอดภัย จำนวน 1 ชุด โดยมีคุณสมบัติดังต่อไปนี้

4.1.1 เป็นอุปกรณ์รักษาความปลอดภัยไฟล์วอล์แบบ Appliance ที่มี Network Module Slots อย่างน้อย 1 Slot และ สามารถติดตั้งใน Rack ขนาด 19 นิ้วได้

4.1.2 สามารถทำการแสดงตัวตน (User Authentication) ร่วมกับระบบ LDAP , Microsoft Active Directory , Radius และ TACACS+ ได้เป็นอย่างน้อย

4.1.3 มีระบบป้องการโจมตี แบบ Anti-Evasion Technologies และสามารถทำการ Custom Fingerprinting ได้เป็นอย่างน้อย

4.1.4 ไม่จำกัดจำนวนผู้ใช้งาน ✓

4.1.5 มี Firewall Throughput ขนาดไม่น้อยกว่า 60 Gbps และสามารถรองรับ Concurrent Connections ได้ไม่น้อยกว่า 12,000,000 Connections

4.1.6 มี Inspection Throughput สำหรับการตรวจสอบ Traffic ขนาดไม่น้อยกว่า 6 Gbps

4.1.7 มีอินเตอร์เฟส แบบ Copper Ethernet 10/100/1000 หรือดีกว่า ไม่น้อยกว่า 8 พอร์ต

4.1.8 มี Interface 10 Gigabit Ethernet แบบ SFP+ จำนวนไม่น้อยกว่า 2 พอร์ต

4.1.9 สามารถใช้งานได้บนเครือข่าย IPv4 และ IPv6 ได้

4.1.10 สามารถป้องกันการบุกรุก Deep Inspection หรือ IPS Mode ได้

4.1.11 สามารถทำ Automatic Anti-Spoofing ให้อัตโนมัติ

4.1.12 รองรับการทำงานในลักษณะของ High Availability (HA) หรือ Clustering Firewall แบบ Active-Active ได้ และรองรับการขยาย Cluster Node ไม่น้อยกว่า 16 Node ได้ในอนาคต

4.1.13 สามารถทำ Load Balance Link หรือ Multi-Link ISP แบบ Active/Active Link ได้ไม่น้อยกว่า 6 ISP-Link โดยสามารถทำ Multi-Link ในลักษณะการหา Link ที่ดีที่สุดแบบ Round Trip time ได้เป็นอย่างน้อย และสามารถทำ Server Load Balancing ได้

4.1.14 สามารถทำ Application Control ได้

4.1.15 สามารถทำ VLAN tagging ได้ไม่จำกัด

4.1.16 มีระบบบริหารจัดการแบบส่วนกลาง (Centralize Management) จำนวน 1 ระบบ โดยมีคุณสมบัติอย่างน้อยดังนี้

4.1.16.1 เป็นซอฟต์แวร์ที่สามารถติดตั้งได้บนระบบปฏิบัติการ Windows และ Linux ได้แบบ GUI ที่ทำหน้าที่ในการบริหารจัดการ และจัดเก็บ Traffic Log ของอุปกรณ์รักษาความปลอดภัยและแสดงตัวตนที่เสนอในโครงการได้ โดยผู้เสนอจะต้องเสนอเครื่องแม่ข่ายพร้อมติดตั้งระบบซอฟต์แวร์บริหารจัดการแบบส่วนกลางที่เสนอในโครงการด้วย

4.1.16.2 ไม่จำกัดจำนวนผู้ใช้งาน

4.1.16.3 สามารถทำ Policy Comparison, Policy Validation และ Policy Snapshots ได้ เพื่อง่ายต่อการตรวจสอบความถูกต้องของ Policy ก่อนการ Deploy Policies จริง เพื่อป้องกันความผิดพลาดในการใช้งานได้ พร้อมทั้งสามารถสร้าง Policy แบบ Jump Rule ได้เพื่อเพิ่มประสิทธิภาพการทำงานของอุปกรณ์ให้ดียิ่งขึ้น

4.1.16.4 สามารถสร้าง Policy ได้ไม่จำกัด

4.1.16.5 สามารถแสดงแผนภาพสถานะของอุปกรณ์ในลักษณะ Geo-locations, Networks Diagrams, Real-Time System Status และ Top-Rate Statistics ได้เป็นอย่างน้อย

4.1.16.6 สามารถทำการ Customize Dashboard เช่นทำการเพิ่มข้อมูลในส่วนของ ข้อมูล Real-Time System Status และ Top-Rate Statistics ได้ และสามารถตั้ง Threshold เพื่อแจ้งเตือนเมื่อค่าเกินที่กำหนดได้

4.1.16.7 สามารถ Filtering Log ด้วยการ Drag and Dropping ข้อมูล Log จาก Fields ได้ และสามารถสร้าง Rule จาก Log ที่แสดงได้

4.1.16.8 สามารถทำการแสดง Log ในรูปแบบแผนภาพการโจมตี (Log Visualization) เช่น แสดงภาพ Attack Analysis , Network Application and Client Executable Usage ได้ และสามารถทำ Log Aggregations ได้

4.1.16.9 สามารถทำการตรวจสอบการใช้งาน Connections ที่เกิดขึ้นบนอุปกรณ์รักษาความปลอดภัยและแสดงตัวตนที่เสนอได้ โดยสามารถแสดงข้อมูล IP ต้นทาง, IP ปลายทาง, Services ที่ใช้งาน, สถานะ Connection State เช่น TCP Established หรือ TCP Closed ของการเชื่อมต่อได้เป็นอย่างน้อย

4.1.16.10 มีระบบการทำ Fail-Safe ทั้งในส่วนของ Policy Upload และ Remote Upgrade Firmware เพื่อป้องกันความผิดพลาดในกรณีที่มีการ Upload ข้อมูลที่ไม่สมบูรณ์ไปอุปกรณ์

4.1.16.11 สามารถกำหนดเงื่อนไขการแจ้งเตือน (Alert Policy)ได้ โดยสามารถ ส่ง Alert หรือ Notify ผ่าน Email, SNMP trap และ Custom Scripts ได้เป็นอย่างน้อย

4.1.16.12 มีระบบ Incident Management เพื่อช่วยผู้ดูแลระบบสามารถติดตามและแก้ไขปัญหาได้ง่าย

4.1.16.13 รองรับการตรวจสอบและติดตามการทำงานของอุปกรณ์อื่น ๆ ได้ เช่น Router หรือ Switch เป็นต้น และสามารถทำการรับข้อมูลจากอุปกรณ์อื่น ๆ เช่น ข้อมูล Log, Netflow มาทำการวิเคราะห์ร่วมกันกับอุปกรณ์ที่เสนอได้

4.1.16.14 สามารถทำการส่งข้อมูล Log ในรูปแบบ Syslog ออกไปยังระบบ Central Log ได้

4.2 ระบบแสดงตัวตน (Authentication) จำนวน 1 ระบบ โดยมีคุณสมบัติดังต่อไปนี้

4.2.1 สามารถทำงานร่วมกับอุปกรณ์รักษาความปลอดภัยและแสดงตัวตน ที่เสนอได้

4.2.2 สามารถทำการยืนยันตัวบุคคล (Authentication) ได้ผ่าน Radius และ LDAP ได้

4.2.3 สามารถติดตั้งได้บนระบบปฏิบัติการ Linux ได้เป็นอย่างน้อย

4.2.4 สามารถทำการเชื่อมโยงหรือส่งข้อมูล Log ของ Radius ไปยังระบบปฏิบัติการ Linux ระบบ Central Log ด้วยรูปแบบของ Syslog ได้

4.2.5 สามารถบริหารจัดการได้ผ่าน Web Interface และ Command Line เป็นอย่างน้อย

4.2.6 สามารถดูสถิติการใช้งานภาพรวมของระบบ แบบ GUI Dashboard ได้

4.3 ระบบลงทะเบียนผู้ใช้ (Self Registration) จำนวน 1 ระบบ โดยมีคุณสมบัติดังต่อไปนี้

4.3.1 สามารถติดตั้งได้บนระบบปฏิบัติการ Linux ได้เป็นอย่างน้อย

4.3.2 สามารถทำการลงทะเบียนผู้ใช้งานโดยสามารถกรอกรายละเอียดข้อมูลสำหรับลงทะเบียน เช่น หมายเลขบัตรประชาชน, ชื่อ, นามสกุล, Email, หมายเลขโทรศัพท์มือถือ ได้เป็นอย่างน้อย

4.3.3 สามารถบริหารจัดการได้ผ่าน Web Interface ได้เป็นอย่างน้อย

4.3.4 มีระบบในการทำ Forget Password หรือ Reset Password ในกรณีผู้ลงทะเบียนมีการลืม Password ได้

4.3.5 ผู้ใช้สามารถเปลี่ยนรหัสผ่าน (Password) ได้

4.3.6 สามารถทำการค้นหา, แก้ไข และลบ ผู้ใช้งานที่ต้องการออกจากระบบได้

4.3.7 สามารถทำงานร่วมกันกับระบบแสดงตัวตนที่เสนอในโครงการได้

4.4 ผู้รับจ้างต้องทำการติดตั้งอุปกรณ์รักษาความปลอดภัย ระบบแสดงตัวตน พร้อมระบบลงทะเบียนผู้ใช้ให้สามารถทำงานร่วมกันได้

4.5 ทำการปรับแต่ง Security Policies ให้มีความเหมาะสมกับกลุ่มของผู้ใช้งาน

4.6 ทำการปรับแต่งในส่วนของ Web Captive Portal Login ของอุปกรณ์รักษาความปลอดภัยและยืนยันตัวตน ที่เสนอในโครงการให้สามารถแสดงข้อมูล ตามรายละเอียดอย่างน้อยดังนี้

4.6.1 User Name หรือหมายเลขบัตรประชาชน สำหรับใช้ในการ Login เข้าระบบ

4.6.2 Password หรือ รหัสผ่าน

4.6.3 แสดงข้อมูลที่จำเป็นเช่น คู่มือการใช้งาน และ Link ข้อมูลข่าวสารที่จำเป็นสำหรับระบบ

4.6.4 สามารถแสดงข้อความรายละเอียดสิทธิความรับผิดชอบสำหรับการใช้งานระบบ หรือ Disclaimer Message เพื่อให้ผู้ใช้งานกดปุ่มยืนยันก่อนการใช้งานระบบได้

4.7 ผู้รับจ้างมีหน้าที่ตรวจสอบอุปกรณ์และระบบเพื่อแสดงตัวตนในการเข้าถึงอินเทอร์เน็ต ให้อยู่ในสภาพพร้อมใช้งาน ให้สามารถใช้งานได้ตลอดอายุสัญญาเช่านี้ อย่างน้อยเดือนละ 1 ครั้ง

4.8 กรณีระบบเพื่อแสดงตัวตนในการเข้าถึงอินเทอร์เน็ต ชำรุดบกพร่องใช้งานไม่ได้ทั้งหมดหรือแต่บางส่วน หรือความชำรุดบกพร่องอันเกิดจากการใช้งาน ผู้รับจ้างต้องจัดให้มีช่างที่มีความรู้ความชำนาญ มาจัดการซ่อมแซมแก้ไขให้อยู่ในสภาพใช้งานได้ดีตามปกติภายใน 6 ชั่วโมง นับแต่เวลาที่ได้รับแจ้งจากผู้ว่าจ้าง

หากระบบเพื่อแสดงตัวตนในการเข้าถึงอินเทอร์เน็ต ไม่สามารถแก้ไขให้ใช้งานได้ ผู้รับจ้างจะต้องแจ้งให้ผู้ว่าจ้างทราบเป็นลายลักษณ์อักษร ภายใน 24 ชั่วโมง และผู้รับจ้างจะต้องจัดหาระบบเพื่อแสดงตัวตนในการเข้าถึงอินเทอร์เน็ต มาทดแทนโดยระบบที่ทดแทนต้องมีคุณสมบัติเท่ากันหรือสูงกว่าเดิม ภายใน 3 วันทำการ โดยไม่คิดค่าใช้จ่ายเพิ่มเติม หากผู้รับจ้างไม่สามารถจัดหาระบบให้ผู้ว่าจ้างได้ภายในระยะที่กำหนดผู้รับจ้างยินยอมให้ผู้ว่าจ้างปรับเป็นรายวันในอัตราร้อยละ 0.10 ตามระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 ข้อ 162 โดยคิดตามเวลาทำการปกติและเศษของวันคิดเป็น 1 วัน

กรณีผู้รับจ้างไม่สามารถปฏิบัติตามข้อสัญญาได้ ผู้ว่าจ้างขอสงวนสิทธิ์ที่จะติดต่อบริษัทอื่น ๆ เพื่อมาซ่อมแซมระบบเพื่อแสดงตัวตนในการเข้าถึงอินเทอร์เน็ต ให้สามารถใช้งานได้ดังเดิม โดยค่าใช้จ่ายจะต้องคิดกับผู้รับจ้างทั้งหมด

4.9 ผู้รับจ้างจะต้องจัดอบรมการใช้งานระบบแสดงตัวตนในการเข้าถึงอินเทอร์เน็ต ให้แก่บุคลากรของหน่วยงานจำนวนไม่น้อยกว่า 5 คน และไม่น้อยกว่า 1 วัน โดยผู้รับจ้างเป็นผู้ออกค่าใช้จ่ายทั้งหมด ภายใน 30 วันหลังจากการลงนามในสัญญา

5. ระยะเวลาดำเนินการ

จำนวน 10 เดือน

6. ระยะเวลาส่งมอบงาน

ผู้รับจ้างจะต้องส่งมอบรายงานผลการดำเนินการดูแล ซ่อมแซม แก้ไขและผลการตรวจสอบอุปกรณ์และระบบเพื่อแสดงตัวตนในการเข้าถึงอินเทอร์เน็ต (Authentication) และข้อมูลสถิติการใช้งานของอุปกรณ์ให้ผู้รับผิดชอบทราบอย่างน้อยเดือนละ 1 ครั้ง ตลอดอายุสัญญานี้ เป็นรายงานประจำเดือน ภายในวันที่ 7 ของเดือนถัดไป ยกเว้นเดือนสุดท้ายของการเช่า ผู้รับจ้างต้องส่งมอบภายในวันที่ 30 กันยายน 2564

7. วงเงินในการจัดหา

วงเงินงบประมาณ 1,249,000 บาท (หนึ่งล้านสองแสนสี่หมื่นเก้าพันบาทถ้วน) เดือนละ 124,900 บาท (หนึ่งแสนสองหมื่นสี่พันเก้าร้อยบาทถ้วน)

8. ผู้รับผิดชอบโครงการ

กลุ่มดาต้าเซ็นเตอร์และเครือข่าย ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป. ศธ.

9. เงื่อนไขอื่น ๆ

ผู้รับจ้างต้องจัดทำแผนการดำเนินงานพร้อมติดตั้งระบบเพื่อแสดงตัวตนในการเข้าถึงอินเทอร์เน็ต (Authentication) ภายใน 15 วันหลังจากทำการเซ็นสัญญากับผู้ว่าจ้าง

10. กำหนดหลักเกณฑ์การพิจารณาคัดเลือกด้วยราคารวม