ข้อกำหนด และขอบเขตของงาน
โครงการจัดซื้อสิทธิ์การใช้งานซอฟต์แวร์ป้องกันการโจมตีของเครื่องคอมพิวเตอร์ปลายทาง
(Endpoint Protection)

---

1. หลักการและเหตุผล

กองระบบและบริหารข้อมูลเชิงยุทธศาสตร์การอุดมศึกษาวิทยาศาสตร์ วิจัยและนวัตกรรม (กรข.) สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม (สป.อว.) ภารกิจหลักในการสนับสนุนการดำเนินงานด้านเทคโนโลยีสารสนเทศของ สป.อว. ทั้งด้านอุดมศึกษา และด้านวิทยาศาสตร์และนวัตกรรม ซึ่งมีการพัฒนาระบบโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ เพื่อรองรับการปฏิบัติงาน และประสานงานแลกเปลี่ยนข้อมูลผ่านระบบเครือข่ายคอมพิวเตอร์ทั้งภายในและภายนอกองค์กร ตามนโยบายและยุทธศาสตร์ด้านเทคโนโลยีสารสนเทศและการสื่อสารของประเทศให้สามารถใช้งานได้ตลอดเวลา รวมถึงมีความมั่นคงปลอดภัยในการใช้งานนั้น

ปัจจุบัน กรข. ได้มีการใช้งานซอฟต์แวร์ป้องกันการโจมตีของเครื่องคอมพิวเตอร์ปลายทาง (Endpoint Protection) ที่ได้ดำเนินการจัดซื้อในปีงบประมาณ ๒๕๖๗ มีสิทธิ์การใช้งานจำนวน ๕๐๐ สิทธิ์ เป็นระยะเวลา ๒ ปี โดยจะสามารถใช้งานได้ถึงเดือน ธันวาคม พ.ศ. ๒๕๖๙ แต่เนื่องด้วยซอฟต์แวร์ดังกล่าวไม่เพียงพอต่อจำนวนเครื่องคอมพิวเตอร์ลูกข่าย และเครื่องคอมพิวเตอร์แม่ข่ายของ สป.อว. ที่มีประมาณ ๑,๑๐๐ เครื่อง อาจส่งผลให้มีความเสี่ยงที่องค์กร ไม่สามารถตรวจจับและป้องกันการโจมตีของไวรัส มัลแวร์ และภัยคุกคามต่างๆ ได้อย่างทันท่วงที (Real-time)

กรข. จึงจำเป็นต้องจัดซื้อสิทธิ์การใช้งานซอฟต์แวร์ป้องกันการโจมตีของเครื่องคอมพิวเตอร์ปลายทาง (Endpoint Protection) เพิ่มเติม จำนวน ๖๐๐ สิทธิ์การใช้งาน เพื่อให้ครอบคลุมเครื่องคอมพิวเตอร์ของ สป.อว. ทั้งนี้ เพื่อป้องกันเครื่องคอมพิวเตอร์จากไวรัส มัลแวร์ การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และส่งเสริมให้บุคลากรของ สป.อว. สามารถใช้งานเครื่องคอมพิวเตอร์ได้อย่างปลอดภัยและมีประสิทธิภาพ

2. วัตถุประสงค์

2.1 เพื่อจัดหาสิทธิ์การใช้งานซอฟต์แวร์รักษาความปลอดภัยบนเครื่องคอมพิวเตอร์เพิ่มเติมมาใช้ในองค์กรให้เกิดประสิทธิภาพ

2.2 เพื่อเป็นการสร้างความเชื่อมั่นด้านการรักษาความปลอดภัยสำหรับการใช้งานเครื่องคอมพิวเตอร์ปลายทางของ สป.อว.

2.3 เพื่อป้องกันทรัพยากรข้อมูลสารสนเทศที่สำคัญขององค์กร และลดความเสี่ยงในการถูกโจรกรรมข้อมูลจากภายนอกองค์กร

3. **คุณสมบัติผู้ยื่นข้อเสนอ**

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 ผู้มีอาชีพรับจ้างงานที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่ สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่ รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละสิทธิ์และความคุ้มกันเช่นว่านั้น

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

3.11 ผู้ยื่นข้อเสนอต้องเป็นตัวแทนที่ได้รับการแต่งตั้งอย่างเป็นทางการ ให้มีสิทธิ์ในการจำหน่ายและบริการหลังการขายจากบริษัทผู้ผลิต หรือสาขาผู้ผลิตในประเทศไทย หรือตัวแทนจำหน่ายอย่างเป็นทางการในประเทศไทยสำหรับโครงการนี้ โดยแนบเอกสารดังกล่าวในวันยื่นข้อเสนอด้วย

4. รายละเอียดคุณลักษณะเฉพาะด้านเทคนิค

สิทธิ์การใช้งานซอฟต์แวร์ป้องกันการโจมตีของเครื่องคอมพิวเตอร์ปลายทาง (Endpoint Protection) จำนวน 600 ลิขสิทธิ์

4.1 เป็นสิทธิ์การใช้งานซอฟต์แวร์ประเภท Next-Generation Antivirus และสามารถทำ Endpoint Detection & Response Solutions (EDR) ได้ใน Agent เดียว

4.2 ซอฟต์แวร์ (agent) ที่ติดตั้งใน Windows, Windows Server, Linux และ MacOS จะต้องเป็นผลิตภัณฑ์ที่มีเครื่องหมายการค้าเดียวกันในทุกระบบปฏิบัติการที่ติดตั้ง

4.3 มีระบบบริหารจัดการอยู่แบบ Cloud management (SaaS) และการเชื่อมต่อระหว่าง Agent กับ Cloud management ต้องมีการเข้ารหัสแบบ TLS-encrypted เพื่อความปลอดภัย

4.4 สามารถตรวจจับ Malware โดยไม่อาศัย signature และไม่ต้องทำการ update signature บนเครื่องลูกข่าย

4.5 สามารถป้องกัน Malware และ การโจมตีที่ไม่เกิดจากมัลแวร์ (Malware-free attack) ด้วยเทคโนโลยี Machine learning และ Indicator of Attack (IOA) ได้เป็นอย่างน้อย

4.6 สามารถป้องกัน Known and Unknown malware, Adware และ potentially unwanted programs (PUPs) ด้วยเทคโนโลยี Machine learning

4.7 สามารถทำการตัดการเชื่อมต่อระบบเครือข่าย (Network Containment) ของเครื่องคอมพิวเตอร์ที่มีการติดตั้ง Agent ผ่านระบบบริหารจัดการส่วนกลาง (Centralize Management)

4.8 สามารถติดตั้งซอฟต์แวร์ป้องกันการโจมตีของเครื่องคอมพิวเตอร์ลูกข่ายผ่านทาง Active Directory (AD) ได้สำหรับเครื่องคอมพิวเตอร์ที่ทำงานบนระบบปฏิบัติการ Windows

4.9 สามารถนำข้อมูลการแจ้งเตือนภัยคุกคาม (Alerts) มาแปลงให้อยู่ในรูปแบบ MITRE ATT&CK framework เพื่อง่ายต่อการทำความเข้าใจ

4.10 สามารถป้องกันผู้ใช้งานที่ไม่มีสิทธิ์หรือมัลแวร์ที่พยายามถอนการติดตั้ง Agent หรือ Disable Agent ของเครื่องคอมพิวเตอร์ลูกข่ายได้

4.11 สามารถแสดงผลของภัยคุกคามที่เกิดขึ้นออกมาเป็นรูปภาพ Process Tree, Process Table และ Process Activity ได้

4.12 มี Dashboard ที่ Monitor Incidents ของบริการค้นหาภัยคุกคามเชิงรุก (Threat Hunting service) อย่างน้อยดังนี้

- Total hunting leads requiring investigation
- Hunting leads by host type
- Hunting leads by resolution

4.13 สามารถสร้าง custom hash เพื่อทำการ Detect, Blocklist และ Allow list ได้

4.14 สามารถกำหนดการแจ้งเตือนตาม Priority Score ได้เป็นอย่างน้อย

4.15 สามารถเชื่อมต่อกับไปยังเครื่องปลายทาง (Real Time Response) เพื่อทำการ run command ต่างๆ ได้อย่างน้อยดังนี้

- List running processes and kill processes
- Show network connections
- Navigate the file system, get or delete files
- Upload files
- Remotely restart or shut down a host
- Manage and run custom scripts or executables (powershell, zsh, bash)

4.16 สามารถเปิดการทำงานในรูปแบบ Endpoint Detection and Response (EDR) เพื่อเก็บข้อมูลการใช้งาน (Activity) ของเครื่อง Endpoint ต่างๆ และนำมาวิเคราะห์หาภัยคุกคาม แบบ Realtime ได้

4.17 สามารถป้องกันการ Exploit ไปยังช่องโหว่ (Vulnerability) เพื่อป้องกันการยึดเครื่อง (Compromised) ได้อย่างน้อยดังนี้

- Forced Address Space Layout Randomization
- Forced Data Execution Protection
- Null Page Allocation
- Heap Spray Preallocation
- SEH Overwrite Protection

4.18 สามารถป้องกัน Ransomware ในรูปแบบต่างๆ ได้อย่างน้อยดังนี้

- ป้องกันการลบ volume shadow copy
- ป้องกันการเข้ารหัสไฟล์ (File Encryption)
- ป้องกันไม่ให้ ransomware เข้าไป Access File System
- ป้องกันการลบ Volume Shadow Copy
- ป้องกัน ransomware ประเภท Cryptowall
- ป้องกัน ransomware ประเภท Locky

4.19 สามารถป้องกันการทำงานของ Registry ที่มีพฤติกรรมที่ต้องสงสัยได้ (Suspicious Registry Operations)

4.20 สามารถเก็บข้อมูลภายในระบบปฏิบัติการ (kernel-mode) ได้ไม่น้อยกว่า 400 Raw events เพื่อนำมาย้อนรอยภัยคุกคามที่เกิดขึ้น (Incident)

4.21 สามารถสร้าง custom IOA เพื่อตรวจจับพฤติกรรมที่ผิดปกติ (Malicious behaviors) หรือต้องการตรวจจับพฤติกรรมการทำงานที่องค์กรต้องการเฝ้าระวังได้อย่างน้อยดังนี้

- Process Creation
- File Creation
- Network Connection (IPv4, IPv6)
- Domain Name

4.22 สามารถค้นหาข้อมูลการใช้งานภายในที่เกี่ยวข้อง (Host Search) ได้อย่างน้อยดังนี้

- Host info
- External network connections
- Map of external network connections
- Detection history
- Local and External Ips
- User Logon Activities
- Unique Executables Written
- Unique Injected Threads
- Unique DLL Injections
- Java injected Threads
- Command History

4.23 สามารถค้นหาข้อมูลการใช้งาน Hash (Hash Search) ได้อย่างน้อยดังนี้

- PE file info
- Detect History
- Unresolved Detects
- Process Executions

4.24 สามารถค้นหาข้อมูลการใช้งาน Username (User Search) ได้อย่างน้อยดังนี้

- User Logon Activities
- Detect History
- Unresolved Detects
- Process Executions
- Admin tool usage

4.25 โปรแกรมที่ติดตั้งในเครื่อง Endpoint ต้องใช้งาน CPU ไม่เกิน 5% และต้องสามารถติดตั้งใช้งานได้เต็มประสิทธิภาพโดยไม่มีความจำเป็นต้อง reboot (no reboot)

4.26 สามารถทำการยืนยันตัวตนกับระบบ 2 Factor Authentication ได้ หรือดีกว่า

4.27 สามารถ Upgrade Machine learning และ Indicator of Attack (IOA) โดยแยกจากการ Update patch ของ Operating System เพื่อให้สามารถทำการ Update ได้อย่างอิสระ และไม่จำเป็นต้อง reboot (no reboot)

4.28 สามารถกำหนด Policy ตามกลุ่มของเครื่อง (Host Groups) ได้

4.29 มีบริการในการค้นหาภัยคุกคามเชิงรุก (Threat Hunting service) โดยผู้เชี่ยวชาญ (Human Analysis) แบบ 24/7 ครอบคลุมทุกเครื่องคอมพิวเตอร์ที่ติดตั้ง Agent Software โดยจะต้องเป็นบริการจากบริษัทที่มีเครื่องหมายการค้าเดียวกันโปรแกรมที่นำเสนอ เพื่อให้มีประสิทธิภาพในการรับมือภัยคุกคาม

4.30 มีบริการแจ้งเตือน Incident จากผู้เชี่ยวชาญด้านการทำ Threat hunting โดยการแจ้งเตือน Incident ที่ตรวจพบผ่านทาง email notification เป็นอย่างน้อย

4.31 ซอฟต์แวร์ที่นำเสนอต้องใช้งานร่วมกับซอฟต์แวร์ป้องกันการโจมตีของเครื่องคอมพิวเตอร์ปลายทาง (Endpoint Protection) เดิม ของ สป.อว. ได้ ภายใต้ระบบบริหารจัดการส่วนกลาง (Centralize Management) เดียวกัน

5. ขอบเขตการดำเนินงาน

5.1 ผู้ยื่นข้อเสนอดำเนินการติดตั้งโปรแกรมหรือซอฟต์แวร์ต่างๆ ที่ได้นำเสนอในโครงการนี้ ให้สามารถใช้งานได้ และตรงตามคุณสมบัติที่ระบุไว้ข้างต้น

5.2 ในระหว่างการติดตั้งซอฟต์แวร์ที่นำเสนอภายในโครงการนี้ จะต้องไม่มีผลกระทบต่อการทำงานของระบบงานต่างๆ หรือก่อให้เกิดความเสียหายแก่ สป.อว. ทั้งนี้ หากเกิดผลกระทบหรือความเสียหาย ผู้รับจ้างต้องเป็นผู้ดำเนินการแก้ไขให้สามารถใช้งานได้ตามปกติ และรับผิดชอบค่าใช้จ่ายที่เกิดขึ้นทั้งหมด

5.3 ดำเนินการจัดทำคู่มือการติดตั้ง (Configuration) และคู่มือการใช้งานซอฟต์แวร์ พร้อมรูปประกอบอย่างละเอียด ให้กับ สป.อว.

6. การปฏิบัติตามนโยบายด้าน ICT ของ สป.อว.

ผู้รับจ้างหรือเจ้าหน้าที่ของผู้รับจ้างจะต้องปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ของ สป.อว. และขั้นตอนปฏิบัติต่างๆ ตามนโยบาย ISO 27001:2022 รวมถึงคำสั่ง และวิธีปฏิบัติที่เกี่ยวข้องอย่างเคร่งครัด

7. การปกปิดความลับทางด้านข้อมูล (Non-disclosure agreement)

ผู้รับจ้างหรือเจ้าหน้าที่ของผู้รับจ้างจะต้องดำเนินการลงนามการปกปิดความลับทางด้านข้อมูล (Non-disclosure agreement) ให้กับสำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม สำหรับโครงการนี้ เพื่อเป็นการรักษาความลับทางด้านข้อมูลไม่ให้รั่วไหลสู่สาธารณะโดยไม่ได้รับอนุญาต

8. การอบรม

ผู้ยื่นข้อเสนอต้องจัดอบรมการใช้งาน และการแก้ปัญหาเบื้องต้นของซอฟต์แวร์ที่นำเสนอให้กับผู้ดูแลระบบ สป.อว. จำนวนไม่น้อยกว่า 5 คน ณ สป.อว. โดยผู้ยื่นข้อเสนอต้องเป็นผู้รับผิดชอบค่าใช้จ่ายทั้งหมด ในการจัดหาเอกสารประกอบการอบรมแต่ละหลักสูตรให้กับ สป.อว.

9. ระยะเวลาการส่งมอบ

9.1 ผู้เสนอราคาต้องดำเนินการภายในระยะเวลา 90 วัน นับถัดจากวันที่ลงนามในสัญญา

9.2 เสนอราคาต้องจัดส่งเอกสารสิทธิ์การใช้งาน (License) ในโครงการนี้ทั้งหมด ในรูปแบบของเอกสารและ Electronic File จำนวนอย่างน้อย 3 ชุดให้กับ สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม (สป.อว.)

10. หลักเกณฑ์การพิจารณา

เกณฑ์การพิจารณาผู้ชนะการเสนอราคา ใช้เกณฑ์ราคาและพิจารณาจากราคารวม

11. ระยะเวลาการรับประกัน

11.1. มีสิทธิ์การใช้งานและการรับประกันผลิตภัณฑ์ซอฟต์แวร์ที่นำเสนอในโครงการนี้ทั้งหมดเป็นระยะเวลาไม่น้อยกว่า 1 ปี นับถัดจากวันที่คณะกรรมการตรวจรับพัสดุได้ดำเนินการตรวจรับเป็นที่เรียบร้อยแล้ว ในกรณีที่เกิดปัญหาเมื่อได้รับแจ้งปัญหาทาง E-mail หรือทางโทรศัพท์ ผู้เสนอราคาต้องให้คำปรึกษา แก้ไขปัญหาเบื้องต้นทางโทรศัพท์ ซึ่งต้องถือปฏิบัติในระยะเวลาประกัน

11.2. ผู้เสนอราคาต้องเป็นผู้ประสานงานหลักในการแก้ไขปัญหา กรณีที่มีการแจ้งปัญหาการใช้งาน ไปยังบริษัทเจ้าของผลิตภัณฑ์ที่นำเสนอในโครงการนี้ กรณีหากมีค่าใช้จ่ายเกิดขึ้นทางผู้เสนอราคาต้องเป็นผู้รับผิดชอบค่าใช้จ่ายทั้งหมด ซึ่งต้องถือปฏิบัติในระยะเวลาการรับประกัน

12. การจ่ายเงิน

ผู้ว่าจ้างจะชำระเงินเต็มจำนวนมูลค่า เมื่อผู้ขายได้ส่งมอบงานและสิทธิ์การใช้งานซอฟต์แวร์ในโครงการนี้ทั้งหมดแล้วเสร็จ และคณะกรรมการได้ตรวจรับเรียบร้อยแล้ว

13. ค่าปรับ

หากผู้ขายไม่สามารถส่งมอบครุภัณฑ์ให้แล้วเสร็จตามเวลาที่กำหนดไว้ ผู้ขายจะต้องชำระค่าปรับให้แก่ทาง สป.อว. เป็นรายวันอัตราร้อยละ 0.10 (ศูนย์จุดหนึ่งศูนย์) ของราคาสิ่งของที่ยังไม่ได้รับมอบ

14. กำหนดยืนราคา 90 วัน

15. สถานที่ส่งมอบพัสดุ

สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม
เลขที่ 75/47 ถนนพระรามที่ 6 แขวงทุ่งพญาไท เขตราชเทวี กรุงเทพมหานคร
โทร. 0 2333 3778 โทรสาร 0 2333 3884

16. งบประมาณ

วงเงินงบประมาณ 1,020,000 บาท (หนึ่งล้านสองหมื่นบาทถ้วน)

(นายพฤทธิ์ แกะกระโทก)
นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ
ผู้กำหนดคุณลักษณะเฉพาะ

(นายจิรายุ ชัยมีบุญ)
นักวิชาการคอมพิวเตอร์ชำนาญการ
ผู้กำหนดคุณลักษณะเฉพาะ

(นางสาวศุภกร สาระวงศ์)
เจ้าหน้าที่ระบบงานคอมพิวเตอร์
ผู้กำหนดคุณลักษณะเฉพาะ