แบบ บก.๐๖

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและรายละเอียดค่าใช้จ่าย
การจัดซื้อจัดจ้างที่ไม่ใช่งานก่อสร้าง

๑. ชื่อโครงการ จัดซื้อระบบซอฟต์แวร์ป้องกันโปรแกรมประสงค์ร้าย จำนวน ๑ ระบบ

๒. หน่วยงานเจ้าของโครงการ กรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ

๓. วงเงินงบประมาณที่ได้รับจัดสรร ๒,๕๐๐,๐๐๐ บาท (สองล้านห้าแสนบาทถ้วน)

๔. วันที่กำหนดราคากลาง (ราคาอ้างอิง) ณ วันที่ ๒๕ พ.ย.๖๖

เป็นเงิน ๒,๕๐๐,๐๐๐ บาท ราคา/หน่วย (ถ้ามี) บาท

๕. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)

๕.๑ บริษัท ซีเคียวร์ เซอร์ฟ จำกัด

๕.๒ บริษัท เน็ตเวิร์ค อินฟราสตรัคเจอร์ จำกัด

๕.๓ บริษัท อีเทอร์นิตี้ จำกัด

๕.๔ บริษัท ทีซีเอ็ม เทคโนโลยี จำกัด

๖. รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง) ทุกคน

๖.๑ น.อ.ระวิ พงษ์สุวรรณ

๖.๒ น.อ.อิศรพันธุ์ สายโสภา

๖.๓ น.ท.จตุพร ศรีกลชาญ

๖.๔ ร.ท.ธนาสิน นารีแก้ว

น.อ. ประธานกรรมการ

รายละเอียดคุณลักษณะเฉพาะ
การซื้อระบบซอฟต์แวร์ป้องกันโปรแกรมประสงค์ร้าย

๑. ความเป็นมา

กรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือเป็นหน่วยเทคนิคของกองทัพเรือ มีหน้าที่ความรับผิดชอบพัสดุสายสื่อสารและเทคโนโลยีสารสนเทศ และเป็นหน่วยรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับระบบงานสารสนเทศและระบบเครือข่ายกองทัพเรือ โดยที่ผ่านมาได้จัดหาโปรแกรมแอนตี้ไวรัส (Antivirus Program) ติดตั้งให้กับเครื่องคอมพิวเตอร์สำนักงานและเครื่องคอมพิวเตอร์แม่ข่ายภายในกองทัพเรือ เพื่อใช้เป็นเครื่องมือสำหรับการป้องกันและรักษาความปลอดภัยจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้น ส่งผลให้ระบบเครือข่ายคอมพิวเตอร์ได้รับการปกป้องหากตรวจพบสิ่งผิดปกติ รวมถึงวิเคราะห์หาสาเหตุที่แท้จริง (Root cause) ทำให้สามารถลดความเสียหายหรือผลกระทบจากภัยคุกคามไซเบอร์ที่เกิดขึ้นกับระบบงานสารสนเทศกองทัพเรือได้ ดังนั้นจึงจำเป็นต้องจัดหาโปรแกรมแอนตี้ไวรัส เพื่อเสริมสร้างขีดความสามารถด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับเครื่องคอมพิวเตอร์สำนักงานและเครื่องคอมพิวเตอร์แม่ข่ายของกองทัพเรือ ให้สามารถทำงานได้อย่างต่อเนื่องและมีประสิทธิภาพยิ่งขึ้น ซึ่งตามแผนการจัดซื้อจัดจ้างประจำปีงบประมาณ พ.ศ.๒๕๖๗ ให้กรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ จัดหาระบบซอฟต์แวร์ป้องกันโปรแกรมประสงค์ร้าย จำนวน ๑ ระบบ

๒. วัตถุประสงค์

๑.๑ เพื่อเสริมสร้างขีดความสามารถด้านการรักษาความปลอดภัยสำหรับอุปกรณ์คอมพิวเตอร์ที่เชื่อมต่อกับระบบสารสนเทศของกองทัพเรือ ให้มีความปลอดภัยจากโปรแกรมประสงค์ร้ายประเภทต่าง ๆ

๑.๒ เพื่อให้สามารถใช้งานระบบสารสนเทศของกองทัพเรือ ได้อย่างต่อเนื่องและมีประสิทธิภาพ

๓. คุณลักษณะทั่วไป

๓.๑ เป็นโปรแกรมสำหรับการป้องกัน ค้นหา ทำลายหรือหยุดยั้งการบุกรุกหรือโจมตีจากโปรแกรมประสงค์ร้ายในรูปแบบต่าง ๆ จำนวน ๑ ระบบ ซึ่งประกอบด้วยรายการดังนี้

๓.๑.๑ ระบบซอฟต์แวร์ป้องกันโปรแกรมประสงค์ร้าย จำนวน ๖,๐๐๐ สิทธิ์การใช้งาน

๓.๑.๒ ซอฟต์แวร์บริหารจัดการระบบซอฟต์แวร์ป้องกันโปรแกรมประสงค์ร้าย จำนวน ๑ Account

๓.๒ ติดตั้งสิทธิ์การใช้งานระบบซอฟต์แวร์ป้องกันโปรแกรมประสงค์ร้าย จำนวนรวม ๖,๐๐๐ สิทธิ์การใช้งาน ไว้บนเครื่องคอมพิวเตอร์แม่ข่ายของกองทัพเรือตามจุดติดตั้งที่ทางราชการกำหนด

๓.๓ ติดตั้งซอฟต์แวร์บริหารจัดการระบบซอฟต์แวร์ป้องกันโปรแกรมประสงค์ร้าย จำนวน ๑ Account

๓.๔ ฝึกอบรมการใช้งาน

๔. คุณลักษณะเฉพาะ

๔.๑ ระบบซอฟต์แวร์ป้องกันโปรแกรมประสงค์ร้าย จำนวน ๖,๐๐๐ สิทธิ์การใช้งาน มีคุณลักษณะอย่างน้อยดังนี้

๔.๑.๑ เป็นซอฟต์แวร์ที่มีคุณสมบัติป้องกันโปรแกรมประสงค์ร้าย ที่สามารถรองรับการติดตั้งโปรแกรมผ่านโปรแกรมบริหารจัดการจากส่วนกลาง (Network Discovery) หรือติดตั้งเองโดยใช้ไฟล์ติดตั้ง

๔.๑.๒ เป็นซอฟต์แวร์ที่สามารถติดตั้งได้บนระบบปฏิบัติการ ดังต่อไปนี้

๔.๑.๒.๑ ระบบปฏิบัติการสำหรับเครื่องแม่ข่าย ตั้งแต่ Windows Server 2008 R2 ขึ้นไป

๔.๑.๒.๒ ระบบปฏิบัติการสำหรับเครื่องลูกข่าย ตั้งแต่ Windows7 SP1 ขึ้นไป โดยสามารถติดตั้งในแบบ 32 bit หรือ 64 bit ได้

๔.๑.๒.๓ ระบบปฏิบัติการ Linux เช่น Ubuntu หรือ CentOS

๔.๑.๓ ในส่วนของการป้องกันโปรแกรมประสงค์ร้าย ต้องมีขีดความสามารถขั้นต่ำ ดังนี้

๔.๑.๓.๑ สามารถทำการตรวจจับโปรแกรมประสงค์ร้าย ได้แก่ ไวรัส, โทรจัน, Worm, Rootkit , Phishing , Adware, Keylogger ได้เป็นอย่างน้อย

๔.๑.๓.๒ มีฟังก์ชันในการเฝ้าระวังการทำงานของ Ransomware เพื่อป้องกันไม่ให้สร้างความเสียหายกับเครื่องคอมพิวเตอร์ได้ (Ransomware Vaccine)

๔.๑.๓.๓ สามารถกำหนดนโยบายการรักษาความปลอดภัย เพื่อนำไปใช้โดยผู้ใช้ปลายทางไม่สามารถยกเลิกหรือแก้ไขนโยบายได้เอง

๔.๑.๓.๔ สามารถสั่งสแกน/อัพเดททันทีหรือกำหนดช่วงเวลาการ สแกน/อัพเดท ได้จาก Management Console พร้อมทั้งสามารถสั่งปิดเครื่องภายหลังจากการสแกนได้

๔.๑.๓.๕ ผู้ดูแลระบบ สามารถเลือกที่จะทำการลบไฟล์ที่ต้องสงสัยว่าเป็นไวรัส หรือสามารถกักกันไฟล์ (Quarantine) ที่ต้องสงสัยได้

๔.๑.๓.๖ ต้องสามารถกำหนดพาสเวิร์ด (Password) ในการป้องกันการรถอนการติดตั้งโปรแกรมได้

๔.๑.๓.๗ สามารถอัพเดทฐานข้อมูลแอนตี้ไวรัส ผ่านทาง Web Management Console ได้หรืออัพเดทผ่านทางเครื่องที่อยู่ในระบบเครือข่ายที่อยู่ในโดเมน (Domain) เดียวกันได้ โดยสามารถเลือกกำหนด ได้เพียงช่องทางเดียวหรือได้ทั้งสองช่องทาง

๔.๑.๓.๘ สามารถกำหนดให้เครื่องลูกข่ายทำหน้าที่รับข้อมูลการอัพเดทจากทาง Management Console และเครื่องดังกล่าวสามารถกระจายข้อมูลการ Update ต่อไปยังเครื่องลูกข่ายอื่น ๆ ได้

๔.๑.๓.๙ สามารถทำการคืนไฟล์ (Restore) ที่ถูกกักกัน (Quarantine) กลับไปยังตำแหน่งเดิมได้ โดยผ่านทาง Management Console หรือผ่านทางเครื่องลูกข่าย หรือกำหนดโฟลเดอร์ปลายทางที่ต้องการใหม่ได้ รวมทั้งทำการ Add exclusion เพื่อยกเว้นการสแกนไฟล์นั้นในแบบอัตโนมัติ ไปยัง Policies ที่กำหนดไว้ได้

๔.๑.๓.๑๐ สามารถกำหนดการอัพเดทตามช่วงเวลาได้

๔.๑.๓.๑๑ สามารถกำหนดการเข้าถึงเว็บไซต์ /โปรแกรม ว่าอนุญาต/ไม่อนุญาต ให้เข้าใช้งานได้

๔.๑.๓.๑๒ สามารถบล็อก (Block) เว็บหลอกลวง หรือเว็บที่อาจเป็นอันตรายได้ (Anti-Phishing)

๔.๑.๓.๑๓ สามารถตรวจจับและถอนโปรแกรมแอนตี้ไวรัสที่ใช้งานอยู่ก่อนการติดตั้งใหม่ได้

๔.๑.๓.๑๔ สามารถอนุญาตให้ใช้งานหรือไม่ให้ใช้งานอุปกรณ์ต่อพ่วงจำพวก External storage, Internal storage, Bluetooth, Network adaptor, Imaging device ได้

๔.๑.๓.๑๕ มีการแสดงผล Incidents ที่แสดง Timeline และ Events Record เพื่อดูกิจกรรมที่ต้องสงสัยในแบบเรียลไทม์ พร้อมทั้งหลักฐานที่ถูกทำการวิเคราะห์ ด้วยเทคโนโลยีแบบ Threat Analysis

๔.๑.๓.๑๖ มีเทคโนโลยีการทำงานแบบ EDR (Endpoint Detection and Response) เพื่อทำงานร่วมกับระบบป้องกันไวรัสหรือ EPP (Endpoint Protection Platform) ได้ทั้งระบบปฏิบัติการ Windows, MacOS และ Linux

๔.๑.๓.๑๗ มี EDR Sensor ที่ทำงานร่วมกับกับซอฟต์แวร์ป้องกันไวรัสที่ใช้งานอยู่แบบ Single Agent โดยไม่ต้องทำการติดตั้งใหม่ รวมทั้งบริหารจัดการแบบรวมศูนย์โดยไม่แยกการบริหารจัดการ

๔.๑.๓.๑๘ สามารถป้องกันการโจมตีประเภท Fileless attacks และ Script-based attacks ได้

๔.๒ ซอฟต์แวร์บริหารจัดการระบบซอฟต์แวร์ป้องกันโปรแกรมประสงค์ร้าย มีคุณลักษณะขั้นต่ำ ดังนี้

๔.๒.๑ ระบบสามารถควบคุมและบริหารจัดการจากส่วนกลางแบบ Cloud Console หรือสามารถติดตั้งบนระบบปฏิบัติการ Microsoft Windows หรือ VMWare ESX ได้

๔.๒.๒ สามารถบริหารจัดการความปลอดภัยบนเครื่องคอมพิวเตอร์ลูกข่ายในด้าน Anti-Malware, Firewall, Intrusion Detection และ Device Control เป็นอย่างน้อยในซอฟต์แวร์ตัวเดียว

๔.๒.๓ สามารถทำการปรับปรุง Malware Signature แบบ Incremental ได้

๔.๒.๔ สามารถกำหนดให้เครื่องคอมพิวเตอร์ลูกข่ายทำการดาวน์โหลดไฟล์ Malware Signature จากเครื่องคอมพิวเตอร์ลูกข่ายแทนการดาวน์โหลดจากเครื่องคอมพิวเตอร์แม่ข่ายได้

๔.๒.๕ สามารถบริหารจัดการไฟล์ที่ถูกกักกัน (Quarantine) โดยซอฟต์แวร์ป้องกันโปรแกรมไม่พึงประสงค์ที่ติดตั้งบนเครื่องคอมพิวเตอร์ลูกข่าย ได้จากส่วนกลาง

๔.๒.๖ สามารถตรวจสอบซอฟต์แวร์ที่ติดตั้งบนเครื่องลูกข่ายที่มีช่องโหว่หรือไม่ได้ทำการอัพเดทได้

๔.๒.๗ สามารถเตือนผู้ดูแลระบบด้วยการส่งจดหมายอิเล็กทรอนิกส์ พร้อมกับสร้างรายงานการทำงานและสถานะของซอฟต์แวร์ป้องกันโปรแกรมประสงค์ร้าย ในรูปแบบ PDF ได้

๔.๒.๘ สามารถควบคุมการตั้งค่าการใช้งานของเครื่องคอมพิวเตอร์ลูกข่าย ผ่านซอฟต์แวร์ป้องกันโปรแกรมประสงค์ร้ายที่ติดตั้งบนเครื่องคอมพิวเตอร์ได้

๔.๒.๙ สามารถรายงานผลการสำรวจโปรแกรมที่ติดตั้งบนเครื่องคอมพิวเตอร์ลูกข่ายที่มีช่องโหว่ และภาพรวมความเสี่ยงที่จะเกิดภัยคุกคามทั้งระบบได้ (Risk Management)

๕. การติดตั้งและการฝึกอบรม

๕.๑ การติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่าย

๕.๑.๑ ติดตั้งสิทธิ์การใช้งานระบบซอฟต์แวร์ป้องกันโปรแกรมประสงค์ร้าย จำนวนรวม ๖,๐๐๐ สิทธิ์การใช้งาน บนเครื่องคอมพิวเตอร์แม่ข่ายของกองทัพเรือที่ทางราชการจัดเตรียมไว้ เพื่อทำหน้าที่เป็น Relay Server สำหรับการอัพเดตฐานข้อมูลไวรัส โดยแยกเป็นพื้นที่ต่าง ๆ ดังนี้ ๑.) ศูนย์ข้อมูลกลาง จว.กรุงเทพฯ จำนวน ๒,๘๐๐ สิทธิ์การใช้งาน ๒.) ชุมสายโทรศัพท์ฐานทัพเรือสัตหีบ จว.ชลบุรี จำนวน ๒,๐๐๐ สิทธิ์การใช้งาน ๓.) ชุมสายโทรศัพท์ ทัพเรือภาคที่ ๒ จว.สงขลา จำนวน ๔๐๐ สิทธิ์การใช้งาน ๔.) ชุมสายโทรศัพท์ ทัพเรือภาคที่ ๓ จว.ภูเก็ต จำนวน ๔๐๐ สิทธิ์การใช้งาน ๕.) ห้องแผนกสื่อสารและสารสนเทศ รพ.สมเด็จพระปิ่นเกล้า กรมแพทย์ทหารเรือ จว.กรุงเทพ จำนวน ๔๐๐ สิทธิ์การใช้งาน

๕.๑.๒ ติดตั้งซอฟต์แวร์บริหารจัดการระบบซอฟต์แวร์ป้องกันโปรแกรมประสงค์ร้าย บนระบบคลาวด์ (Cloud) จำนวน ๑ Account สำหรับการบริหารจัดการเครื่อง Relay Server โดยให้เครื่อง Relay Server ที่ศูนย์ข้อมูลกลาง เป็นเครื่องคอมพิวเตอร์แม่ข่ายหลัก สำหรับการบริหารจัดการ

๕.๒ การติดตั้งบนเครื่องคอมพิวเตอร์สำนักงานอัตโนมัติ

ผู้ขายต้องกำหนดให้ผู้ใช้งานดาวน์โหลด Software Agent เพื่อการติดตั้งจากเครื่องคอมพิวเตอร์แม่ข่ายตามพื้นที่ที่กำหนด

๕.๓ การฝึกอบรม

ผู้ขายต้องจัดอบรมเกี่ยวกับการติดตั้งระบบ การใช้งานและการแก้ไขปัญหา ให้แก่เจ้าหน้าที่กองทัพเรือ จำนวน ๑๕ นาย ระยะเวลา ๒ วัน โดยผู้ขายต้องจัดเตรียมอุปกรณ์ เครื่องมือและเอกสารประกอบการอบรม และเป็นผู้รับผิดชอบค่าใช้จ่ายทั้งสิ้น

๖. กำหนดส่งมอบและการตรวจรับพัสดุ

๖.๑ กำหนดเวลาส่งมอบพัสดุพร้อมติดตั้งตามสถานที่ ที่ทางราชการกำหนด ไม่เกิน ๖๐ วัน นับถัดจากวันลงนามในสัญญาซื้อขาย หรือนับถัดจากวันสิ้นสุดอายุการใช้งานตามสัญญาที่มีอยู่เดิม หากสิ้นสุดสัญญาที่มีอยู่เดิมก่อนวันทำสัญญา ให้นับถัดจากวันลงนามในสัญญากับทางราชการ หรือเมื่อได้รับแจ้งจากทางราชการ

๖.๒ ผู้ขายต้องจัดเจ้าหน้าที่ร่วมกับเจ้าหน้าที่ของกองทัพเรือ ในการติดตั้งและการถอดถอนระบบซอฟต์แวร์ป้องกันโปรแกรมประสงค์ร้ายเดิมบนเครื่องคอมพิวเตอร์แม่ข่ายของกองทัพเรือ ในพื้นที่ ๑.) ศูนย์ข้อมูลกลาง จว.กรุงเทพฯ ๒.) ชุมสายโทรศัพท์ฐานทัพเรือสัตหีบ จว.ชลบุรี ๓.) ชุมสายโทรศัพท์ ทัพเรือภาคที่ ๒ จว.สงขลา

๔.) ชุมสายโทรศัพท์ ทัพเรือภาคที่ ๓ จว.ภูเก็ต ๕.) ห้องแผนกสื่อสารและสารสนเทศ รพ.สมเด็จพระปิ่นเกล้า กรมแพทย์ทหารเรือ จว.กรุงเทพ รวมถึงดำเนินการทดสอบให้สามารถใช้งานได้อย่างต่อเนื่อง

๖.๓ ผู้ขายต้องส่งมอบโปรแกรมติดตั้งพร้อมเอกสารคู่มือการใช้งานที่เป็นภาษาไทย ในรูปแบบ Flash Drive จำนวน ๑๐ ชุด

๖.๔ กำหนดตรวจรับตามสถานที่ติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย ตามข้อ ๕.๑.๑ และในขั้นตอนการตรวจรับผู้ขายต้องส่งมอบหนังสือรับรอง(ฉบับจริง) จากผู้ผลิตหรือผู้ผลิตสาขาประเทศไทยโดยตรงหรือตัวแทนจำหน่ายในประเทศไทยที่ได้รับการแต่งตั้งจากผู้ผลิตอย่างถูกต้องว่าผลิตภัณฑ์ที่เสนอขายเป็นของแท้ ของใหม่ ไม่เคยใช้งานมาก่อนหรือปรับปรุงสภาพขึ้นมาใหม่หรือดัดแปลงสภาพมาและยังอยู่ในสายการผลิต

๗. การจ่ายเงิน

กรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ จะจ่ายค่าสิ่งของซึ่งได้รวมภาษีมูลค่าเพิ่ม ภาษีอากรอื่น ๆ และค่าใช้จ่ายทั้งปวงแล้ว ให้แก่ผู้ขายเมื่อผู้ขายได้ส่งมอบสิ่งของได้ครบถ้วนตามสัญญาซื้อขายหรือข้อตกลงเป็นหนังสือ และคณะกรรมการตรวจรับพัสดุได้ตรวจรับมอบสิ่งของไว้เรียบร้อยแล้ว

๘. การรับประกันความชำรุดบกพร่อง

๘.๑ ผู้ขายต้องมีการรับประกันระบบซอฟต์แวร์ป้องกันโปรแกรมประสงค์ร้ายพร้อมซอฟต์แวร์บริหารจัดการเป็นระยะเวลาไม่น้อยกว่า ๑ ปี นับถัดจากวันที่กรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ ได้รับมอบสิ่งของโดยต้องรีบจัดการซ่อมแซมแก้ไขให้ใช้การได้ดีดังเดิม ภายใน ๒ วัน นับถัดจากวันที่ได้รับแจ้งความชำรุดบกพร่อง

๘.๒ ผู้ขายต้องจัดให้มีการตรวจสอบบำรุงรักษาและปรับปรุงการทำงานของระบบซอฟต์แวร์ป้องกันโปรแกรมประสงค์ร้าย และซอฟต์แวร์บริหารจัดการฯ ตามวงรอบ จำนวน ๑ ครั้ง/ไตรมาส รวม ๔ ครั้ง พร้อมทั้งทำรายงานสรุปการบำรุงรักษาผลิตภัณฑ์ให้ทางราชการทราบทุกครั้งเมื่อดำเนินการแล้วเสร็จ

๘.๓ ผู้ขายต้องพร้อมให้คำปรึกษาและแนะนำขั้นตอนการใช้งานและการแก้ไขปัญหาข้อขัดข้อง เมื่อมีการร้องขอจากทางราชการ

๘.๔ ผู้ขายต้องพร้อมให้บริการในช่วงวันและเวลาราชการ (จันทร์ - ศุกร์ และ ๐๘๓๐ – ๑๖๓๐) และต้องจัดส่งเจ้าหน้าที่เข้ามาทำการตรวจสอบแก้ไขปัญหาข้อขัดข้องใน ๔ ชั่วโมง หลังจากที่ได้รับแจ้ง และต้องซ่อมแซมแก้ไขให้สามารถใช้ราชการได้ดังเดิม ภายใน ๔๘ ชั่วโมง

๙. อัตราค่าปรับ

ค่าปรับตามแบบสัญญาซื้อขายหรือข้อตกลงซื้อขายเป็นหนังสือ ให้คิดในอัตราร้อยละ ๐.๒๐ ของราคารวมตามสัญญา ฯ นับถัดจากวันครบกำหนดตามสัญญา ฯ จนถึงวันที่ผู้ขายได้นำสิ่งของมาส่งมอบและนำไปติดตั้งให้แก่ทางราชการจนถูกต้องครบถ้วน

๑๐. หลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอ

การพิจารณาคัดเลือกข้อเสนอในการจัดซื้อจัดจ้างครั้งนี้ กรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือจะพิจารณาตัดสินโดยใช้หลักเกณฑ์ราคา

๑๑. คุณสมบัติของผู้ยื่นข้อเสนอ

ผู้ยื่นข้อเสนอต้องได้รับการแต่งตั้งให้เป็นตัวแทนจำหน่ายจากผู้ผลิตหรือตัวแทนจำหน่ายในประเทศไทย โดยให้ยื่นขณะเข้าเสนอราคา

๑๒. หลักฐานการยื่นข้อเสนอ

๑๒.๑ เอกสารแสดงตราอักษร รุ่น บริษัท ประเทศผู้ผลิต และคุณลักษณะเฉพาะของพัสดุที่เสนอขายที่ตรงกับคุณลักษณะเฉพาะของพัสดุตามข้อ ๔ พร้อมทั้งทำเครื่องหมายระบุให้ชัดเจน

๑๒.๒ หนังสือแต่งตั้งจากผู้ผลิต หรือตัวแทนจำหน่ายภายในประเทศ

๑๒.๓ ผู้ยื่นข้อเสนอต้องทำการรับรองเอกสารทุกแผ่นทุกหน้า

๑๓. การเสนอราคา

๑๓.๑ ราคาที่เสนอเป็นราคารวมทั้งสิ้น ซึ่งรวมภาษีมูลค่าเพิ่ม ภาษีอากรอื่น ๆ และค่าใช้จ่ายทั้งปวงแล้วจนกระทั่งส่งมอบพัสดุให้ ณ สถานที่ทางราชการกำหนดไว้ ตามข้อ ๕.๑

๑๓.๒ ราคาที่เสนอจะต้องเสนอกำหนดยืนราคา ไม่น้อยกว่า ๙๐ วัน ตั้งแต่วันเสนอราคา โดยภายในกำหนดยืนราคา ผู้ยื่นข้อเสนอต้องรับผิดชอบราคาที่ตนได้เสนอไว้และจะถอนการเสนอราคามิได้

๑๔. เงื่อนไขและข้อกำหนดอื่น ๆ

๑๔.๑ ผู้เสนอราคาแสดงรายการราคา (Price Breakdown) โดยให้ทราบถึงราคาของรายการต่าง ๆ ที่นำเสนอ

๑๔.๒ ผู้เสนอราคาต้องจัดทำรายการเปรียบเทียบเป็นรายข้อ (Statement of Compliance) ที่แสดงการเปรียบเทียบรายละเอียดของผลิตภัณฑ์ที่เสนอขายกับรายละเอียดคุณลักษณะเฉพาะที่ทางราชการกำหนด โดยต้องระบุตราอักษร ยี่ห้อแบบ-รุ่น ของผลิตภัณฑ์ที่เสนอขาย รวมทั้งทำเครื่องหมายบ่งบอกในแคตตาล็อกหรือเอกสารที่เกี่ยวข้องให้ชัดเจน ในกรณีที่คุณลักษณะเฉพาะที่ทางราชการกำหนดไม่ปรากฏในเอกสารคุณลักษณะเฉพาะของพัสดุ ผู้ขายจะต้องมีหนังสือรับรองจากบริษัทผู้ผลิต หรือผู้แทนจำหน่าย เพื่อรับรองว่ามีคุณลักษณะเฉพาะตามที่ทางราชการกำหนด และต้องแนบเอกสารดังกล่าวมาพร้อมกับใบเสนอราคา

น.อ. ประธานกรรมการ
(ระวิ พงษ์สุวรรณ)

น.อ. กรรมการ
(อิศรพันธุ์ สายโสภา)

น.ท. กรรมการ
(จตุพร ศรีกลชาญ)

ร.ท. กรรมการและเลขานุการ
(ธนาสิน นารีแก้ว)