แบบ บก.06

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและรายละเอียดค่าใช้จ่าย
การจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง

1. ชื่อโครงการ ซื้อสิทธิ์การป้องกันการโจมตีเครือข่ายในปริมาณสูง
2. หน่วยงานเจ้าของโครงการ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
3. วงเงินงบประมาณที่ได้รับจัดสรร 1,700,000 บาท
4. วันที่กำหนดราคากลาง (ราคาอ้างอิง) ณ วันที่ 24 พ.ย. 68 เป็นเงิน 1,700,000 บาท
5. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)
   - 5.1 บริษัท ทีซีเอ็ม เทคโนโลยี จำกัด
   - 5.2 บริษัท อินเตอร์เนชั่นแนล เน็ตเวิร์ค ซิสเต็ม จำกัด (มหาชน)
   - 5.3 บริษัท สตรีม ไอ.ที. คอนซัลติ้ง
6. รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง) ทุกคน
   - 6.1 นายพรพรหม ประภากิตติกุล
   - 6.2 นายบุญเนา ทิพย์มณี
   - 6.3 นายปานเพชร ศรีเนตร์

ETDA	ข้อกำหนดรายละเอียดคุณลักษณะเฉพาะ (Terms of Reference :TOR)		จำนวน	๘ หน้า
	เรื่อง	ซื้อสิทธิ์การป้องกันการโจมตีเครือข่ายในปริมาณสูง		
	จัดทำโดย	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์	วันที่จัดทำ	พ.ย. ๖๘

๑. <u>ความเป็นมา</u>

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) มีความมุ่งมั่นในการส่งเสริมและสนับสนุนการใช้เทคโนโลยีเพื่อเพิ่มประสิทธิภาพการทำงานและสนับสนุนโครงการต่าง ๆ ตามพันธกิจขององค์กร โดยมีการประยุกต์ใช้ระบบสารสนเทศ เพื่อภารกิจที่สำคัญหลายประการ เช่น ระบบสารสนเทศเพื่อสนับสนุนการควบคุมดูแลการประกอบธุรกิจบริการแพลตฟอร์มดิจิทัล และด้วยปัจจุบันภัยคุกคามทางไซเบอร์ทั้งการโจมตีทำให้ระบบสารสนเทศไม่พร้อมใช้งานเพื่อหวังผลประโยชน์ การโจมตีเชิงลึกเพื่อเข้าควบคุมระบบและเพื่อเข้าถึงข้อมูลสำคัญขององค์กรหรือผู้มีส่วนเกี่ยวข้อง ยิ่งทวีความรุนแรง และยังคงมีเป้าหมายมุ่งตรงต่อระบบสารสนเทศที่สำคัญของหน่วยงานของรัฐเป็นสำคัญ

เนื่องจากสิทธิการป้องกันการโจมตีเครือข่ายในปริมาณสูง เดิมที่ สพธอ. ได้ใช้งานอยู่จะหมดอายุ เพื่อเป็นการเตรียมความพร้อมต่อการโจมตีที่อาจเกิดขึ้นอย่างมีนัยะต่อการให้บริการสารสนเทศของ สพธอ. จึงมีความประสงค์ซื้อสิทธิ์การป้องกันการโจมตีเครือข่ายในปริมาณสูงในผลิตภัณฑ์ คลาวด์แฟร์ (Cloudflare) ซึ่งเป็นผลิตภัณฑ์เดิม ที่ สพธอ.ได้ใช้งานอยู่ เพื่อความต่อเนื่องในการให้บริการสำคัญในการป้องกันการโจมตีระบบสารสนเทศ และสนับสนุนด้านการเฝ้าระวังภัยคุกคามไซเบอร์ ทำให้เกิดความมั่นคงปลอดภัย และความน่าเชื่อถือต่อการให้บริการสู่สาธารณะ

๒. <u>วัตถุประสงค์</u>

เพื่อจัดซื้อซื้อสิทธิ์การป้องกันการโจมตีเครือข่ายในปริมาณสูง

๓. <u>คุณสมบัติผู้เสนอราคา</u>

๓.๑ มีความสามารถตามกฎหมาย

๓.๒ ไม่เป็นบุคคลล้มละลาย

๓.๓ ไม่อยู่ระหว่างเลิกกิจการ

๓.๔ ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราวเนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

๓.๕ ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

๓.๖ มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

๓.๗ เป็นบุคคลธรรมดาหรือนิติบุคคลผู้มีอาชีพขายพัสดุที่ประกวดราคาซื้อด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

๓.๘ ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่ สพธอ. ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

๓.๙ ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

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

๓.๑๑ ต้องยื่นรายการแสดงการเปรียบเทียบรายละเอียดคุณลักษณะเฉพาะที่ สพธอ. ต้องการ กับรายละเอียดคุณลักษณะเฉพาะที่เสนอว่าตรงกันหรือไม่ โดยหลักฐานที่แสดงต้องเป็นตัวอย่างหรือข้อมูลจริงที่สอดคล้องตามรายละเอียดคุณลักษณะเฉพาะ หากรายละเอียดคุณลักษณะเฉพาะในเอกสารขัดแย้งกันเอง สพธอ. ขอสงวนสิทธิ์ที่จะพิจารณาในส่วนที่เป็นประโยชน์สูงสุดแก่ สพธอ.

๓.๑๒ ต้องยื่นหนังสือต้นฉบับที่มีเนื้อหาระบุการแต่งตั้งให้เป็นตัวแทนจำหน่ายและสนับสนุนการให้บริการซ่อมแซมแก้ไข จากเจ้าของผลิตภัณฑ์ หรือสาขาประจำประเทศไทยของเจ้าของผลิตภัณฑ์ตามข้อ ๔.๑

๔. <u>รายละเอียดคุณลักษณะเฉพาะ</u>

๔.๑ บริการระบบป้องกันการโจมตีเครือข่ายปริมาณสูง DDoS แบบคลาวด์ อย่างน้อยอยู่ใน Leader in the 2022 "Gartner Magic Quadrant for WAAP" ปี ๒๕๖๕ รองรับการใช้งานไม่น้อยกว่า ๔ โดเมน ตามที่ สพธอ. กำหนด มีระยะเวลาการใช้งานอย่างน้อย ๑ ปี โดยมีคุณลักษณะดังนี้

๔.๑.๑. ความสามารถในการป้องกันการโจมตีประเภท DDoS ของแต่ละเว็บไซต์ ดังนี้

(๑) เป็นรูปแบบการให้บริการที่ออกแบบมาสำหรับป้องกันการโจมตีแบบ DDoS ที่สามารถป้องการการโจมตีเว็บไซต์ แอปพลิเคชัน โดยให้บริการป้องกันการโจมตีแบบไม่จำกัดจำนวนครั้ง และไม่มีข้อจำกัดในการรับปริมาณการโจมตีที่เกิดขึ้น

(๒) ต้องสามารถป้องกันการโจมตีในลักษณะ DDoS ในลักษณะ Volumetric และในระดับแอปพลิเคชัน ครอบคลุมทั้งในระดับโพรโตคอล Layer 3 (Network layer), Layer 4 (Transport layer) และ Layer 7 (Application layer)

(๓) ต้องสามารถตั้งค่าการบล็อคการเข้าใช้งานทั้งในรูปแบบ Blacklisting และ การอนุญาตให้เข้าถึงเฉพาะ Whitelisting โดยใช้ข้อมูลที่กำหนดโดยผู้ใช้งานดังต่อไปนี้ได้เป็นอย่างน้อย

- IP Address
- IP Range (Network Address)
- Autonomous System Number (ASN)
- Geolocation

(๔) ต้องรองรับการทำงานในโหมด Reverse proxy โดยให้บริการเป็นตามโปรโตคอล SSL/TLS เวอร์ชัน 1.3 เป็นอย่างน้อยโดยรองรับการติดตั้งและบริหารจัดการกุญแจลับ (Private Key) ผ่านระบบได้

(๕) ต้องรองรับการเชื่อมต่อกับเซิร์ฟเวอร์เว็บไซต์ต้นทาง (Upstream server) ของหน่วยงานทั้งแบบ Plain , Outdated Protocol (TLS 1.0), และ Unverified Certificate (Self signed, Expired cert)

(๖) ต้องสามารถออกใบรับรอง SSL ให้เว็บไซต์ทั้งหมดที่ตั้งค่าไว้ได้ จากผู้ให้บริการที่ได้รับความเชื่อถือจากเว็บเบราว์เซอร์อย่างน้อย Chrome Firefox Edge Safari (บน Desktop และ Mobile) โดยไม่มีค่าใช้จ่ายเพิ่มเติม

(๗) ต้องสามารถรองรับการติดตั้งและบริหารจัดการใบรับรอง SSL จากภายนอกได้อย่างน้อย ๔ ใบรับรองในลักษณะ Wildcard

(๘) ต้องสามารถตั้งค่าจำกัดการเชื่อมต่อของบริการ (Rate Limit) ตามวัตถุประสงค์ของการป้องกัน โดยต้องสามารถดำเนินการตามปัจจัยได้ดังต่อไปนี้ได้เป็นอย่างน้อย

- Connection
- Client certificate
- Source IP Address
- URL

(๙) ต้องสามารถตั้งค่ากลไกการตอบสนองต่อการใช้งานในกรณีที่ผิดปกติ อย่างน้อยด้วยเทคนิค JavaScript challenge

(๑๐) ต้องสามารถป้องกันการโจมตีผ่านทาง PoP (Point of Presence) ที่มีอยู่ทั่วโลกอย่างน้อยในทวีปเอเชีย (ที่ไม่ใช่ประเทศไทย) ทวีปอเมริกาเหนือ ทวีปยุโรป โดยมี Throughput รวมไม่น้อยกว่า ๑๐ Tbps (ก่อนป้องกัน) และสามารถส่งต่อ Traffic ที่ปกติรวมได้ไม่น้อยกว่า ๔ TB ต่อเดือน ภายใต้ Peak traffic ไม่เกิน 1 Gbps ซึ่งแต่ละ PoP ต้องมีความสามารถในการป้องกันการโจมตี DDoS การป้องกันการโจมตีด้วย WAF และการให้บริการในลักษณะ CDN ได้

(๑๑) ต้องสามารถสร้าง Static html content ผ่าน Html editor แยกแต่ละเว็บไซต์ สำหรับกรณีที่เว็บไซต์ปลายทางไม่สามารถเข้าใช้งานได้ หรือเป็นเงื่อนไขพิเศษที่กำหนดขึ้นจากกิจกรรม Health Check โดยมีอัตราการเรียกใช้งานเว็บไซต์ จำนวนรวมไม่เกิน ๑๐๐,๐๐๐,๐๐๐ ครั้งต่อเดือน และเป็นกลไกที่ทำงานแยกจากเซิร์ฟเวอร์เว็บไซต์ของหน่วยงาน ซึ่งเป็นการตั้งค่าที่ไม่ต้องติดตั้งระบบใดเพิ่มเติม (Serverless)

(๑๒) ต้องสามารถทำ Content Caching ของเว็บไซต์ โดยมีคุณสมบัติดังต่อไปนี้

- ต้องวิเคราะห์การเก็บ Cache โดยอย่างน้อยมีข้อมูลการแสดงผลที่แสดงให้เห็นการถึงเปรียบเทียบประสิทธิภาพในแต่ละช่วงเวลา รวมถึงข้อมูลสถิติเวลาการตอบรับ (Response time) ได้เอง เพื่อนำมาปรับปรุงการตั้งค่าที่เกี่ยวข้อง

- ต้องทำการ Purge Cache ทั้งหมดได้ในทันที หรือทำการ Custom Purge เฉพาะ URL, Host name และ Tag ได้ โดยต้องสามารถใช้ API ในการอัพเดท Cache เมื่อมีการอัพเดท Content ได้
- ต้องลดขนาด บีบอัด ของไฟล์รูปภาพ โดยรองรับทั้งแบบ Lossy Lossless และ WebP

(๑๓) ต้องสามารถตรวจจับความเสี่ยงจากการเข้าใช้งานของ IP ที่อาจเป็นอันตราย (IP Reputation)

(๑๔) ต้องสามารถให้บริการ Authoritative DNS services และรองรับการทำ DNSSEC โดยไม่จำกัดจำนวน DNS Zone

(๑๕) ต้องสามารถรองรับการทำ Global Load Balancing โดยสามารถตั้งค่ากลไกการทำงานได้อย่างน้อยดังนี้

- Failover
- Geolocation

(๑๖) ต้องสามารถวิเคราะห์รูปแบบการใช้งานแบบสถิติย้อนหลัง หรือ ณ ปัจจุบัน เพื่อให้สามารถพิจารณาถึงรูปแบบการเรียกใช้งานที่มีปริมาณสูงอย่างผิดปกติ โดยกำหนดปัจจัยที่สามารถวิเคราะห์ได้ดังนี้

- URL
- Date time (Range)
- Domain
- Source IP address

๔.๑.๒. ความสามารถในการป้องกันการโจมตีเว็บไซต์ ดังนี้

(๑) เป็นรูปแบบการให้บริการที่ออกแบบมาสำหรับป้องกันการโจมตีเว็บไซต์แบบผ่านกลไกของ Web Application Firewall (WAF) ได้แบบไม่จำนวนครั้งของการป้องกัน รวมถึงอย่างน้อยต้องสามารถกำหนดเงื่อนไขที่เชื่อมโยงกับข้อมูลดังต่อไปนี้ได้

- URL
- HTTP POST data
- HTTP header รวมถึง Parameter ของคำสั่ง HTTP

(๒) ต้องสามารถให้บริการ Reverse web proxy รองรับการทำงานผ่านโปรโตคอล IPv4 และ IPv6 และสามารถเชื่อมไปหาเว็บไซต์ที่ต้องการป้องกันได้

(๓) ต้องสามารถตั้งค่าจำกัดการเชื่อมต่อของเว็บไซต์ (Rate Limit) อย่างน้อยตาม URL โดยสามารถกำหนดการป้องกันในแต่ละเว็บไซต์แยกกันได้ ไม่น้อยกว่า ๑๐๐ เงื่อนไขต่อเว็บไซต์

(๔) ต้องสามารถป้องกันการโจมตีเว็บไซต์ตามประเภทของ OWASP (Open Web Application Security Project) TOP ๑๐ เวอร์ชันที่ สพธอ. กำหนด

(๕) ต้องสามารถทำ Health Check กับเว็บไซต์ โดยสามารถกำหนดปัจจัยในการตรวจสอบได้อย่างน้อยดังนี้

- URL
- HTTP Response Code
- HTTP Method
- HTTP Response Data

(๖) ต้องสามารถสืบค้น และแสดงผลรายงานในลักษณะ Dashboard สำหรับการเฝ้าระวังการใช้งานเว็บไซต์ที่อาจผิดปกติ หรือการโจมตีของเว็บไซต์ โดยสามารถแสดงรายงานอย่างน้อยดังต่อไปนี้

- ปริมาณการเรียกเว็บไซต์
- ปริมาณการเรียกเว็บไซต์ผ่านแคช
- ปริมาณการบล็อคการโจมตี
- ปริมาณภัยคุกคามที่พบ

(๗) ต้องสามารถทำการทดสอบเงื่อนไขในการป้องกันก่อนมีการปรับปรุงให้การตั้งค่ามีผล

(๘) ต้องสามารถทำการตรวจสอบการออกใบรับรอง SSL โดยใช้กลไก Certificate Transparency และสามารถแจ้งเตือนเมื่อมีผู้ทำการออกใบรับรองภายใต้ชื่อ Domain เดียวกับที่ตั้งค่าป้องกันไว้ได้

(๙) ต้องสามารถจำแนกผู้ใช้งาน (Unique visitor) ที่มีการเชื่อมต่อเครือข่ายลักษณะ NAT Network เพื่อให้สามารถพิจารณาจำนวนของผู้ใช้งานทั้งหมดได้

๔.๑.๓. ต้องมีฟังก์ชันหรือความสามารถในการบริหารจัดการระบบ ดังนี้

(๑) การสร้างบัญชีผู้ใช้งานย่อยได้ไม่จำกัด

(๒) การกำหนดสิทธิเข้าใช้งานระบบ โดยรองรับการใช้งาน Two-Factor Authentication

(๓) การเพิ่ม แก้ไข และลบเว็บไซต์ที่ตั้งค่าตามข้อ ๔.๑.๑ และ ๔.๑.๒ ผ่านทางหน้าบริหารจัดการที่เป็นเว็บไซต์ และผ่าน API ได้

(๔) การสืบค้น และแสดงผลรายงานในลักษณะ Dashboard แบบ Near Real-time (ไม่เกิน ๕ นาที) สำหรับการเฝ้าระวังการใช้งานเว็บไซต์ที่อาจผิดปกติ หรือการโจมตีของเว็บไซต์ โดยประกอบด้วยข้อมูลที่นำมาจัดทำรายงานอย่างน้อยตามรายการดังต่อไปนี้

- URL
- Domain
- Source IP address
- Unique visitor
- Visitor's user agent
- Visitor's country
- Status code

- Attack type (หากพบประเภทหรือลักษณะการโจมตี) โดยต้องมีการแจกแจงชื่อประเภทให้ชัดเจน เช่น Synflood, Blacklist IP Reputation

(๕) การจัดเก็บบันทึกการใช้งาน (Access log) และเชื่อมต่อ Raw log ไปยังระบบภายนอกผ่าน API ของเจ้าของผลิตภัณฑ์ โดยต้องสามารถส่งต่อข้อมูลอย่างน้อย ดังนี้

- Source IP address
- Destination IP address
- Source port
- Destination port
- URL
- Domain
- Attack type (หากพบประเภทหรือลักษณะการโจมตี) โดยต้องมีการแจกแจงชื่อประเภทให้ชัดเจน เช่น Synflood, Blacklist IP Reputation

๔.๒ ผู้เสนอราคาต้องจัดเตรียมเจ้าหน้าที่ผู้เชี่ยวชาญจำนวนอย่างน้อย ๑ คน หรือเพียงพอต่อการดำเนินการในแต่ละข้อ ซึ่งต้องจัดเตรียมช่องทางในการติดต่อ ในลักษณะ ๒๔ ชั่วโมง ๗ วัน นับถัดจากวันลงนามสัญญา ถึงวันครบกำหนดส่งมอบงานงวดสุดท้าย โดยมีคุณสมบัติและหน้าที่ดังต่อไปนี้

๔.๒.๑ ได้รับใบรับรองการบริหารจัดการระบบป้องกันการโจมตีเครือข่ายปริมาณสูง DDoS ตามข้อ ๔.๑ จากเจ้าของผลิตภัณฑ์

๔.๒.๒ ดำเนินการตั้งค่าระบบให้รองรับการป้องกันการโจมตีเว็บไซต์ตามที่ สพธอ. กำหนด ทั้งในมิติของการติดตั้งใหม่ หรือการปรับปรุงการตั้งค่ามาจากบริการอื่นๆ พร้อมจัดทำรายงานผลการตั้งค่าแยกตามเว็บไซต์ โดยต้องเสนอรูปแบบของรายงานเพื่อขอความเห็นชอบจาก สพธอ. ก่อน อย่างน้อยครอบคลุมขั้นตอนดังต่อไปนี้

(๑) การเรียนรู้รูปแบบการใช้งานของเว็บไซต์ด้วยกลไกอัตโนมัติ

(๒) การตั้งค่าการป้องกันการโจมตีประเภท DDoS และการโจมตีเว็บไซต์ในรูปแบบอื่นด้วยกลไกของ Web Application Firewall (WAF)

(๓) การตรวจวิเคราะห์การโจมตี ปรับปรุงการตั้งค่า

(๔) การปรับปรุงข้อมูลในรายงานผลการตั้งค่าฯ ให้มีความทันสมัย และถูกต้องอยู่เสมอเมื่อมีการปรับปรุงการตั้งค่า หรือที่เกี่ยวข้อง

(๕) การตั้งค่าเดิมและการปรับปรุงการตั้งค่าเพื่อการติดตั้งใหม่ (หากมี)

๔.๒.๓. ประสานเพื่อตั้งค่าและแก้ไขตามที่ สพธอ. ร้องขอ โดยใช้ช่องทางที่ สพธอ. กำหนด ซึ่งต้องมีการตอบกลับผลการตั้งค่า และแก้ไขหรือให้คำแนะนำ ภายใน ๑ ชั่วโมงหลังจากเมื่อมีการร้องขอ

๔.๒.๔. ให้คำปรึกษา และการดำเนินการในการบริหารจัดการระบบป้องกันการโจมตีเครือข่ายปริมาณสูง DDoS ตามข้อ ๔.๑ แก่ สพธอ.

๔.๓ ผู้เสนอราคาต้องจัดทำคู่มือสำหรับผู้ดูแลระบบของระบบที่นำเสนอในข้อ ๔.๑ ทั้งมิติการติดตั้งตั้งค่าและการเลือกแนวทางการป้องกัน ขณะที่โดยโจมตี โดยเนื้อหาต้องได้รับการอนุมัติความครอบคลุมและความเหมาะสมจาก สพธอ.

๔.๔ ผู้เสนอราคาต้องจัดหาหลักสูตรฝึกอบรมเพื่อพัฒนาศักยภาพสำหรับการยกระดับการบริหารจัดการบริหารจัดการระบบป้องกันการโจมตีเครือข่ายปริมาณสูง DDoS สำหรับเจ้าหน้าที่ สพธอ. พร้อมการสอบวัดระดับสำหรับประกาศนียบัตรวิชาชีพด้านความมั่นคงปลอดภัยสารสนเทศ โดยเป็นการดำเนินการจัดหาหลักสูตรและสอบในลักษณะ On-Site หรือตามที่ สพธอ. กำหนดมีรายการและรายละเอียดดังต่อไปนี้

๔.๔.๑ เอกสารยืนยันสิทธิสำหรับการเข้าอบรมหลักสูตรอบรมที่ได้รับการรับรองจากเจ้าของผลิตภัณฑ์โดยตรง พร้อมสิทธิสำหรับให้เจ้าหน้าที่ สพธอ. สอบเพื่อขอใบรับรองการบริหารจัดการระบบป้องกันการโจมตีเครือข่ายปริมาณสูง DDoS จากเจ้าของผลิตภัณฑ์ตามข้อ ๔.๑ จำนวนไม่น้อยกว่า ๔ คน มีอายุการใช้งานสิทธิอย่างน้อยไม่ต่ำกว่า ๑๕๐ วันนับถัดจากวันที่ส่งมอบงวดที่ ๒

๔.๔.๒ เอกสารยืนยันสิทธิสำหรับเข้ารับการอบรมหลักสูตรประกาศนียบัตรวิชาชีพด้านการความมั่นคงปลอดภัยสารสนเทศ Certified Cloud Security Professional (CCSP) ซึ่งสอนโดยหน่วยงานที่อยู่ในรายการตาม ISC2 Official Cybersecurity Training Partners พร้อมสิทธิการลงทะเบียนสอบประกาศนียบัตรดังกล่าว ให้แก่เจ้าหน้าที่ สพธอ. จำนวนไม่น้อยกว่า ๒ คน มีอายุการใช้งานสิทธิอย่างน้อยไม่ต่ำกว่า ๑๕๐ วันนับถัดจากวันที่ส่งมอบงวดที่ ๒

๕. กำหนดยืนราคา

ผู้ยื่นข้อเสนอจะต้องเสนอกำหนดยืนราคาไม่น้อยกว่า ๙๐ (เก้าสิบ) วัน นับแต่วันที่เสนอราคาโดยภายในกำหนดยืนราคาสุดท้าย ผู้ยื่นข้อเสนอหรือผู้มีสิทธิเสนอราคาจะต้องรับผิดชอบราคาที่ตนได้เสนอไว้และจะถอนการเสนอราคามิได้

๖. สถานที่ส่งมอบ

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา (อาคารซี) ชั้น ๔ เลขที่ ๑๒๐ หมู่ที่ ๓ ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐

๗. วงเงินในการจัดหา

วงเงินงบประมาณ ๑,๗๐๐,๐๐๐ บาท (หนึ่งล้านเจ็ดแสนบาทถ้วน)

ราคากลาง เป็นจำนวนเงิน ๑,๗๐๐,๐๐๐ บาท (หนึ่งล้านเจ็ดแสนบาทถ้วน)

๘. สิ่งส่งมอบและกำหนดเวลาการส่งมอบ

ผู้ขายจะต้องส่งมอบพัสดุตามรายละเอียดคุณลักษณะเฉพาะข้อ ๔ โดยแบ่งกำหนดระยะเวลาการส่งมอบพัสดุเป็นจำนวน ๒ (สอง) งวด ดังนี้

๘.๑ งวดที่ ๑ ดำเนินการส่งมอบตามรายละเอียดคุณลักษณะเฉพาะตามข้อ ๔.๑ และ ๔.๒ ภายใน ๒๐ (ยี่สิบ) วัน นับถัดจากวันที่ลงนามสัญญา

๘.๒ งวดที่ ๒ ดำเนินการส่งมอบตามรายละเอียดคุณลักษณะเฉพาะตามข้อ ๔.๓ และ ๔.๔ ภายใน ๖๐ (หกสิบ) วัน นับถัดจากวันที่ลงนามสัญญา

๙. เงื่อนไขการจ่ายเงิน

สพธอ. จะจ่ายเงินค่าพัสดุให้กับผู้ขาย โดยแบ่งเป็น ๒ (สอง) งวด ดังนี้

งวดที่ ๑ อัตราร้อยละ ๘๐ (แปดสิบ) ของค่าพัสดุ เมื่อผู้ขายได้ส่งมอบพัสดุ ดำเนินการและส่งมอบงานตามสิ่งส่งมอบในข้อ ๘.๑ และคณะกรรมการตรวจรับได้ตรวจรับพัสดุครบถ้วนถูกต้องแล้ว

งวดที่ ๒ อัตราร้อยละ ๒๐ (ยี่สิบ) ของค่าพัสดุ เมื่อผู้ขายได้ส่งมอบพัสดุ ดำเนินการและส่งมอบงานตามสิ่งส่งมอบในข้อ ๘.๒ และคณะกรรมการตรวจรับได้ตรวจรับพัสดุครบถ้วนถูกต้องแล้ว

๑๐. อัตราค่าปรับ

เมื่อครบกำหนดส่งมอบพัสดุตามที่กำหนดไว้ ถ้าผู้ขายไม่ส่งมอบพัสดุตามที่ตกลงซื้อให้แก่ สพธอ. ส่งมอบล่าช้า หรือส่งมอบพัสดุไม่ถูกต้อง ไม่ครบจำนวน หรือไม่เป็นไปตามที่ตกลงกันไว้ ผู้ขายจะต้องชำระค่าปรับให้ สพธอ. เป็นรายวันในอัตราร้อยละ ๐.๒๐ (ศูนย์จุดสองศูนย์) ของมูลค่าพัสดุ นับถัดจากวันที่ครบกำหนดตามสัญญาจนถึงวันที่ผู้ขายได้ส่งมอบพัสดุให้แก่ สพธอ. จนถูกต้องครบถ้วน

การคิดค่าปรับในกรณีพัสดุที่ตกลงซื้อขายประกอบกันเป็นชุด แต่ผู้ขายส่งมอบเพียงบางส่วน หรือขาดส่วนประกอบส่วนหนึ่งส่วนใดไป ทำให้ไม่สามารถใช้การได้โดยสมบูรณ์ ให้ถือว่ายังไม่ได้ส่งมอบพัสดุนั้นเลย และให้คิดค่าปรับจากราคาพัสดุเต็มทั้งชุด

๑๑. หลักเกณฑ์การพิจารณา

ใช้เกณฑ์ราคาในการพิจารณา