- ร่าง -

รายละเอียดคุณลักษณะเฉพาะของครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ สำหรับโครงการปรับปรุงประสิทธิภาพระบบรักษาความมั่นคงปลอดภัยสารสนเทศ ด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding)

---

๑. ความเป็นมา

สำนักงานคณะกรรมการข้าราชการพลเรือน ได้รับจัดสรรเงินงบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. ๒๕๖๐ งบลงทุน เพื่อจัดซื้อครุภัณฑ์คอมพิวเตอร์และอุปกรณ์สำหรับโครงการปรับปรุงประสิทธิภาพระบบรักษาความมั่นคงปลอดภัยสารสนเทศ จำนวน ๓ ระบบ

๒. วัตถุประสงค์

เพื่อจัดหาครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ ดังนี้

๒.๑ เพื่อทดแทนอุปกรณ์ป้องกันการโจมตีระบบเครือข่าย Firewall และ IPS ที่มีอายุการใช้งานมากกว่า ๗ ปีขึ้นไป

๒.๒ เพื่อให้สำนักงานมีระบบป้องกันการโจมตีระบบเครือข่ายที่มีประสิทธิภาพ ลดความเสี่ยงที่อาจจะเกิดขึ้นกับเครื่องคอมพิวเตอร์แม่ข่ายและระบบต่าง ๆ

๓. คุณสมบัติของผู้มีสิทธิเสนอราคา

๓.๑ เป็นนิติบุคคลผู้มีอาชีพขายพัสดุที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

๓.๒ ไม่เป็นผู้ที่ถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานของทางราชการและได้แจ้งเวียนชื่อแล้ว หรือไม่เป็นผู้ที่ได้รับผลของการสั่งให้นิติบุคคลหรือบุคคลอื่นเป็นผู้ทิ้งงานตามระเบียบของทางราชการ

๓.๓ ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้เสนอราคารายอื่นที่เข้ายื่นข้อเสนอให้แก่สำนักงานคณะกรรมการข้าราชการพลเรือน ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรม ในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

๓.๔ ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้เสนอราคาได้มีคำสั่งให้สละสิทธิ์ความคุ้มกันเช่นว่านั้น

๓.๕ ไม่เป็นผู้ที่ถูกประเมินสิทธิผู้เสนอราคาในสถานะที่ห้ามเข้าเสนอราคาและห้ามทำสัญญาตามที่ กวพ. กำหนด

๓.๖ นิติบุคคลที่จะเข้าเป็นคู่สัญญาต้องไม่อยู่ในฐานะเป็นผู้ไม่แสดงบัญชีรายรับรายจ่าย หรือแสดงบัญชีรายรับรายจ่ายไม่ถูกต้องครบถ้วนในสาระสำคัญ

๓.๗ นิติบุคคลที่จะเข้าเป็นคู่สัญญากับหน่วยงานภาครัฐ ซึ่งได้ดำเนินการจัดซื้อจัดจ้างด้วยระบบอิเล็กทรอนิกส์ (e-Government Procurement : e-GP) ต้องลงทะเบียนในระบบอิเล็กทรอนิกส์ของกรมบัญชีกลาง ที่เว็บไซต์ศูนย์ข้อมูลจัดซื้อจัดจ้างภาครัฐ

๓.๘ คู่สัญญาต้องรับและจ่ายเงินผ่านบัญชีธนาคาร เว้นแต่ การจ่ายเงินแต่ละครั้ง ซึ่งมีมูลค่าไม่เกินสามหมื่นบาท คู่สัญญาอาจจ่ายเป็นเงินสดก็ได้

๔. รายการพัสดุ

ลำดับที่	รายการ	จำนวน
๑.	ระบบป้องกันการโจมตีเครือข่าย (Firewall)	๑ ระบบ
๒.	ระบบป้องกันไวรัสทางเครือข่าย	๑ ระบบ
๓.	ซอฟท์แวร์ป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์แม่ข่าย	๑ ระบบ

รายละเอียดคุณลักษณะเฉพาะของครุภัณฑ์คอมพิวเตอร์และอุปกรณ์สำหรับโครงการปรับปรุงประสิทธิภาพระบบรักษาความมั่นคงปลอดภัยสารสนเทศ จำนวน ๕ หน้า ตามเอกสารแนบ ๑

๕. ระยะเวลาดำเนินการ

กำหนดระยะเวลาดำเนินการ ภายใน ๑๒๐ วัน นับถัดจากวันลงนามในสัญญา

๖. ระยะเวลาส่งมอบพัสดุ

ส่งมอบพัสดุให้แก่สำนักงานคณะกรรมการข้าราชการพลเรือน ภายใน ๑๒๐ วัน นับถัดจากวันลงนามในสัญญา

๗. การจ่ายเงิน

การเบิกจ่ายเงินงวดเดียว เมื่อผู้ขายส่งมอบพัสดุ ครบถ้วน ถูกต้อง ทุกรายการ และผ่านการตรวจรับจากคณะกรรมการตรวจรับพัสดุเรียบร้อยแล้ว

๘. วงเงินในการจัดซื้อ

เงินงบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. ๒๕๖๐ วงเงิน ๖,๔๐๐,๐๐๐.- บาท (หกล้านสี่แสนบาทถ้วน)

๙. ราคากลางในการจัดซื้อ

เป็นเงินจำนวน ๖,๒๑๒,๔๒๐.- บาท (หกล้านสองแสนหนึ่งหมื่นสองพันสี่ร้อยยี่สิบบาทถ้วน) รายละเอียดตามเอกสารแนบ ๒

๑๐. หลักเกณฑ์และสิทธิในการพิจารณา

ในการพิจารณาผลการยื่นข้อเสนอประกวดราคาอิเล็กทรอนิกส์ครั้งนี้ สำนักงาน-คณะกรรมการข้าราชการพลเรือนจะพิจารณาตัดสินโดยใช้หลักเกณฑ์ราคา และจะพิจารณาจากราคารวม

๑๑. สถานที่ติดต่อเพื่อขอทราบข้อมูลเพิ่มเติม และส่งข้อเสนอแนะ วิจารณ์ หรือแสดงความคิดเห็น

สามารถส่งข้อคิดเห็นหรือข้อเสนอแนะ วิจารณ์ เกี่ยวกับร่างขอบเขตของงานนี้ได้ที่

สถานที่ติดต่อ กลุ่มงานบริหารทรัพย์สิน สำนักงานเลขาธิการ สำนักงาน-คณะกรรมการข้าราชการพลเรือน ถนนติวานนท์ ตำบลตลาดขวัญ อำเภอเมืองนนทบุรี จังหวัดนนทบุรี ๑๑๐๐๐

โทรศัพท์ ๐ ๒๕๔๗ ๑๐๑๘

โทรสาร ๐ ๒๕๔๗ ๑๐๘๓

เว็บไซต์ www.ocsc.go.th (E-mail address : opm@ocsc.go.th)

สาธารณชนที่ต้องการเสนอแนะ วิจารณ์ หรือมีความเห็น ต้องเปิดเผยชื่อและที่อยู่ของผู้ให้ข้อเสนอแนะ วิจารณ์ หรือมีความเห็นด้วย

รายละเอียดคุณลักษณะเฉพาะของครุภัณฑ์คอมพิวเตอร์และอุปกรณ์สำหรับโครงการ ปรับปรุงประสิทธิภาพระบบรักษาความมั่นคงปลอดภัยสารสนเทศ

1. ระบบป้องกันการโจมตีเครือข่าย (Firewall) จำนวน 1 ระบบ

เป็นอุปกรณ์แบบ Hardware Appliance ที่เป็น Next Generation Firewall จำนวน 2 ชุด โดยแต่ละชุดมีคุณสมบัติ ดังนี้

1.1 สามารถตรวจจับและควบคุม Application, User และ Content โดยเฉพาะเจาะจงได้

1.2 สามารถรองรับ Throughput ของระบบ Firewall และระบบการป้องกันภัยคุกคามทางเครือข่าย โดยทำงานพร้อมกัน จำนวนไม่น้อยกว่า 1 Gbps

1.3 สามารถรองรับ Throughput ของ IPSec VPN จำนวนไม่น้อยกว่า 500 Mbps

1.4 สามารถทำ VLANs tagging จำนวนอย่างน้อย 500 VLANs ได้

1.5 สามารถทำ Link Aggregation ตามมาตรฐาน 802.3ad ได้

1.6 มี Ethernet port แบบ 10/100/1000 จำนวนไม่น้อยกว่า 8 Ports

1.7 มี Interface แบบ 10/100/1000 สำหรับบริหารจัดการโดยเฉพาะ จำนวน 1 Port

1.8 มีพอร์ต Serial Console จำนวน 1 Port

1.9 สามารถจัดการระบบด้วยวิธีการต่างๆ ได้ดังนี้

1.9.1 SSH

1.9.2 Web Graphic User Interface

1.9.3 Command Line Interface หรือ โปรแกรมบริหารจัดการ

1.10 มี Storage ขนาดไม่น้อยกว่า 120 GB

1.11 สามารถตรวจสอบและกำหนด Policy การใช้งานในระดับ Application (Application Control) เช่น Application ประเภท Web 2.0, Social Networking, IM, P2P, Voice, Video และ File Sharing ได้ โดย Application ต่างๆ ต้องมีการจัดแบ่งตาม Category, Tag และระดับความเสี่ยง (Risk Level) ของ Application

1.12 สามารถจัดการ Policy การใช้บริการผ่านอุปกรณ์ โดยสามารถระบุจากข้อมูลเครือข่าย เช่น IP, Port หรือ Protocol ได้

1.13 สามารถกำหนด Security Policy ตาม User, User Group และอุปกรณ์ โดย Integrate เข้ากับ Active Directory ได้

1.14 มีระบบการกรอง URL (URL Filtering) ที่สามารถติดตาม ควบคุมการเข้าถึงเว็บไซต์ ได้ตาม Category และสามารถกำหนด Black list และ White list ได้

1.15 มีระบบตรวจจับพฤติกรรมเพื่อระบุ Malware และ Zero-day Malware

1.16 มีระบบป้องกันภัยคุกคาม (Threat Prevention) หรือระบบป้องกันการโจมตีและการบุกรุกเครือข่าย โดยมีคุณสมบัติ ดังนี้

1.16.1 สามารถป้องกันการบุกรุกแบบ Vulnerability Exploit

1.16.2 สามารถป้องกันเทคนิคการหลบซ่อนการโจมตีแบบ IP Defragmentation และ TCP Stream Segmentation

1.16.3 สามารถป้องกันเครือข่าย และสามารถตรวจจับ Overflow, Trojan และ Spyware

1.16.4 สามารถตรวจจับ และป้องกัน Virus บนโปรโตคอล HTTP, FTP, POP3 และ SMTP

1.16.5 สามารถตรวจจับ และป้องกัน Virus ที่ฝังตัวมากับ PDF, HTML และ Java script

1.16.6 สามารถตรวจจับ File ที่ต้องสงสัยว่าอาจจะเป็น Malware บนโปรโตคอล HTTP, FTP, POP3 และ SMTP ได้

1.17 สามารถส่ง Logs ไปยังอุปกรณ์จัดเก็บ Logs หรือ สามารถทำงานร่วมกับระบบภายนอกเพื่อรับส่งข้อมูล

1.18 สามารถสร้างรายงานที่ปรับแต่งได้ ตามประเภทของข้อมูลที่ต้องการแสดง ชนิดของการแสดงผล เช่น กราฟแท่ง กราฟวงกลม และออกรายงานตามความต้องการ ในรูปแบบ CSV หรือ PDF หรือ HTML และสามารถกำหนดให้ออกรายงาน พร้อมส่งผ่านระบบอีเมล์ไปยังผู้ที่เกี่ยวข้องได้โดยอัตโนมัติ

1.19 มีระบบการแสดงผลแบบ Dashboard ที่สามารถปรับแต่งได้

1.20 มีระบบจัดการคุณภาพการให้บริการ (Quality of Service) โดยสามารถกำหนด Policy เพื่อจัดการ Bandwidth ของ Traffic โดยระบุขอบเขตสูงสุด และลำดับความสำคัญ (Priority) ของ Traffic ได้

1.21 สามารถทำงานในลักษณะ High Availability ในรูปแบบ Active-Active และ Active-Passive ได้

1.22 สามารถใช้งาน Routing แบบ Dynamic Routing ได้แก่ OSPF, BGP, และ RIP v1 หรือ RIP v2 ได้

1.23 สามารถใช้งานตามมาตรฐาน IPv6 ได้

1.24 ผลิตภัณฑ์ที่เสนอต้องได้รับการรับรองมาตรฐาน ICSA

1.25 ผลิตภัณฑ์ที่เสนอต้องอยู่ในกลุ่ม Leader หรือ Challengers ของผลิตภัณฑ์ประเภท Enterprise Network Firewall ปี 2016 ของ Gartner

1.26 ผลิตภัณฑ์ที่เสนอต้องได้รับรองมาตรฐานด้านการแผ่กระจายของแม่เหล็กไฟฟ้า FCC และได้รับมาตรฐานด้านความปลอดภัย UL หรือ CE

1.27 ผลิตภัณฑ์ที่เสนอต้องสามารถติดตั้งบน Rack 19 นิ้วได้

2. ระบบป้องกันไวรัสทางเครือข่าย จำนวน 1 ระบบ โดยมีคุณสมบัติ ดังนี้

2.1 เป็นอุปกรณ์แบบ Hardware Appliance ที่ทำหน้าที่ตรวจจับ ค้นหา แจ้งเตือน และรายงานอันตรายจากภัยต่างๆ (Threats) ในระบบเครือข่ายให้กับผู้ดูแลระบบได้แบบ Real-Time

2.2 สามารถตรวจเนื้อหา การเชื่อมต่อ และพฤติกรรมที่ไม่ปลอดภัย หรือการโจมตีระบบได้

2.3 มี Interface แบบ Ethernet 10/100/1000 ไม่ต่ำกว่า 4 Ports

/ 2.4 สามารถรองรับ Throughput ได้ไม่น้อยกว่า 1 Gbps

2.5 มี Storage ขนาดไม่น้อยกว่า 500 GB จำนวน 2 หน่วย

/ 2.6 มีหน่วยความจำ (Memory) ไม่น้อยกว่า 16 GB

2.7 มี Power Supply จำนวน 2 หน่วย โดยทำงานแบบ Redundant Power Supply

2.8 สามารถรับข้อมูล Traffic ด้วยวิธี Mirror Port ได้ และรองรับการตรวจหาข้อมูล Traffic ได้จากโปรโตคอล SMTP, POP3, HTTP, DNS และ CIFS หรือ SMB ได้ และสามารถตรวจค้นการใช้งานโปรแกรม เช่น Instant Messaging, P2P file sharing และ Streaming media ได้

2.9 สามารถตรวจจับ และค้นหาการโจมตี แบบ APT (Advanced Persistent Threats), Zero-day Malware และการโจมตีโดยใช้ Document Exploits หรือ Exploit kit tool ได้

2.10 สามารถตรวจสอบไฟล์ที่ต้องสงสัย และวิเคราะห์พฤติกรรมของไฟล์ โดยใช้ระบบ Virtual Analyzer โดยไม่ส่งตัวอย่างไฟล์ที่ต้องสงสัยไปยังภายนอกระบบเครือข่าย และสามารถกำหนดข้อบังคับ (Rule) เพื่อเลือกไฟล์ที่ต้องสงสัยในการส่งไปยังระบบ Virtual Analyzer

2.11 สามารถสร้างระบบ Custom Virtual Analyzer บนระบบปฏิบัติการ Windows XP, Windows 7, Windows 8, Windows 10, Windows Server 2003, Window Server 2008, Window Server 2012 และรองรับไฟล์ที่มีขนาดใหญ่กว่า 40 Mb ได้ เพื่อเพิ่มความปลอดภัยให้ระบบมากยิ่งขึ้น

2.12 สามารถเรียกดูรายงาน Top Malware-Infected Hosts, Top Suspicious Behavior Detected และทำการปรับแต่งหน้าจอ (Custom Dashboard) ได้

2.13 สามารถสร้างรายงาน (Report) ได้ทั้งแบบ On-Demand และ Scheduled ในรูปแบบ PDF

2.14 สามารถค้นหา Logs แบบกำหนดเงื่อนไข เช่น ชนิดของการตรวจสอบ (Detection Type), IP Address, Mac Address และค้นหา Logs แบบกำหนดเวลาได้ และสามารถส่ง Logs ในรูปแบบ CEF และ LEEF ได้

2.15 สามารถตรวจจับ และค้นหาภัยคุกคาม ประเภท Bots, Trojan, Worm และ Key loggers ได้

2.16 สามารถบริหารจัดการอุปกรณ์ผ่าน Web Browser เช่น Internet Explorer และ Firefox ได้

2.17 สามารถกำหนดสิทธิของผู้ดูแลระบบในระดับที่แตกต่างกันได้ (Role-based Administration)

2.18 มีระบบบริหารจัดการแบบรวมศูนย์ (Centralized Management) ทั้งระบบ Antivirus และระบบ APT

2.19 ผลิตภัณฑ์ที่เสนอต้องอยู่ในกลุ่ม Leader ของผลิตภัณฑ์ประเภท Endpoint Protection Platforms ปี 2016 ของ Gartner

3. ซอฟต์แวร์ป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์แม่ข่าย จำนวน 1 ระบบ โดยมีคุณสมบัติ ดังนี้

3.1 สามารถใช้งานกับเครื่องคอมพิวเตอร์แม่ข่ายเสมือน (VM) จำนวนไม่น้อยกว่า 50 เครื่อง

3.2 สามารถทำงานบนระบบปฏิบัติการ Windows และ Linux ได้

3.3 สามารถทำงานแบบ Agent based สำหรับ VMWare ESXi และ Microsot Hyper-V

3.4 สามารถเลือกการสแกน Malware ได้ ดังนี้

3.4.1 Full Scan

3.4.2 Quick Scan

3.4.3 Real-Time Scan

3.5 สามารถป้องกันช่องโหว่ของระบบปฏิบัติการโดยไม่ต้องติดตั้ง Patches บนระบบปฏิบัติการเสมือน เพื่อป้องกันปัญหาที่อาจเกิดขึ้นจากการ Patches โดยที่ยังไม่ได้ทำการทดสอบกับการใช้งานจริง และต้องสามารถแจ้งเตือนถึงช่องโหว่ใหม่ที่เกิดขึ้นได้

3.6 สามารถป้องกันการโจมตีที่มีเป้าหมายจากช่องโหว่ของโปรแกรมประเภท Web Application ได้ เช่น SQL injection, Cross-site Script และสามารถป้องกันอันตรายประเภท Zero-day Attacks และ Exploits ประเภทต่างๆ ได้

3.7 สามารถป้องกันการเข้าใช้งาน Web Site ที่อันตรายหรือ Web Site ที่ไม่อนุญาตให้เข้าถึงได้ และกำหนดระดับการป้องกันได้ด้วยเทคโนโลยี Web Reputation กับระบบ Cloud ของเจ้าของผลิตภัณฑ์ได้

3.8 สามารถควบคุมการเข้าถึง Application ต่างๆ ในระดับ Network ได้

3.9 สามารถบริหารจัดการระบบทั้งหมดได้จากส่วนกลางผ่าน Web Browser และมีระบบบริหารจัดการสำหรับ Virtualization แบบ Private Cloud และ Public Cloud เช่น vCloud และ AWS หรือ Microsoft Azure โดยอยู่ภายใต้ Server เครื่องเดียวกันได้

3.10 สามารถทำ Recommend Scan ของ IPS Policy ได้แบบอัตโนมัติ

3.11 สามารถตรวจสอบ Malware และป้องกันภัยคุกคามจากช่องโหว่ของระบบปฏิบัติการและโปรแกรม ดังนี้

3.11.1 Anti-Malware Solution Platform (AMSP)

3.11.2 Smart Scan

3.11.3 Web Reputation

3.11.4 Virtual Patching

3.11.5 Intrusion Prevention

3.12 สามารถควบคุมการรับส่งข้อมูล Traffic เพื่อทำการตรวจสอบความผิดปกติ และการฝ่าฝืนนโยบายการใช้งาน และสามารถทำ Stateful Firewall เพื่อวิเคราะห์ Packet สำหรับโปรโตคอล TCP, UDP และ ICMP ได้

3.13 สามารถสร้างรายงานในรูปแบบของ PDF และ RTF ได้ และสามารถป้องกันการเปิดรายงานโดยการเข้ารหัสด้วย Password ได้

3.14 สามารถกำหนดสิทธิในการเข้าใช้งาน (Role-based) ของแต่ละ Users ได้

3.15 สามารถแจ้งเตือนผ่าน Email, Syslog และ SNMP ได้

3.16 สามารถตรวจสอบความถูกต้องของข้อมูล (Data Integrity) ของระบบปฏิบัติการ เช่น การแก้ไข File, Directory, Registry Key และ Installed Software ได้

3.17 มี Agent ที่สามารถติดตั้งบนระบบปฏิบัติการ Microsoft Windows เพื่อทำการตรวจสอบความปลอดภัยบน Microsoft Windows Event ได้

3.18 ผลิตภัณฑ์ที่เสนอต้องได้รับการรับรองมาตรฐานด้านความปลอดภัย Common Criteria EAL 4+

<u>เงื่อนไขทั่วไป/การดำเนินการ</u>

1. ผู้ขายต้องทำการฝึกอบรม และจัดทำเอกสารประกอบการฝึกอบรม ประกอบด้วย
   1.1 การใช้งานระบบป้องกันการโจมตีเครือข่าย (Firewall)
   1.2 การใช้งานระบบป้องกันไวรัสทางเครือข่าย
   1.3 การใช้งานซอฟต์แวร์ป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์แม่ข่าย

โดยมีระยะเวลาในการอบรม รวมไม่น้อยกว่า 2 วัน โดยใช้สถานที่ของสำนักงานคณะกรรมการข้าราชการพลเรือน ให้กับเจ้าหน้าที่ จำนวนไม่น้อยกว่า 5 คน

2. ผู้ขายจะต้องดำเนินการติดตั้งระบบฯ และจัดทำรายงานการติดตั้งระบบฯ ที่ส่งมอบ
3. ผู้ขายจะต้องรับผิดชอบค่าใช้จ่ายในการบำรุงรักษาระบบฯ และ License ที่เกิดขึ้น เป็นระยะเวลาไม่น้อยกว่า 3 ปี

<u>การรับประกันความชำรุดบกพร่อง</u>

ผู้ขายจะต้องรับประกันความชำรุดบกพร่อง หรือขัดข้องของครุภัณฑ์ที่ซื้อขายที่เกิดขึ้นภายในระยะเวลาไม่น้อยกว่า 3 ปี นับถัดจากวันที่ผ่านการตรวจรับจากคณะกรรมการตรวจรับพัสดุ โดยภายในระยะเวลาดังกล่าว หากเกิดความชำรุดบกพร่อง หรือขัดข้องอันเนื่องมาจากการใช้งานตามปกติ ผู้ขายจะต้องจัดการซ่อมแซมแก้ไขให้อยู่ในสภาพใช้การได้ดีดังเดิมภายใน 3 วันทำการนับถัดจากวันที่ได้รับแจ้งจากสำนักงานคณะกรรมการข้าราชการพลเรือน

<u>การส่งมอบงาน</u>

ผู้ขายต้องส่งมอบครุภัณฑ์คอมพิวเตอร์และอุปกรณ์สำหรับโครงการปรับปรุงประสิทธิภาพระบบรักษาความมั่นคงปลอดภัยสารสนเทศพร้อมติดตั้ง และจัดอบรมให้แล้วเสร็จ ภายใน 120 วัน นับถัดจากวันลงนามในสัญญา โดยผู้ขายต้องดำเนินการติดตั้ง และจัดส่งรายงาน ดังนี้

1. รายงานการอบรมและคู่มือการใช้งาน จำนวน 5 ชุด
2. รายงานการติดตั้งระบบฯ จำนวน 5 ชุด

<u>การชำระเงิน</u>

สำนักงานคณะกรรมการข้าราชการพลเรือน จะชำระเงินทั้งหมด เมื่อผู้ขายดำเนินการส่งมอบครุภัณฑ์คอมพิวเตอร์และอุปกรณ์สำหรับโครงการปรับปรุงประสิทธิภาพระบบรักษาความมั่นคงปลอดภัยสารสนเทศพร้อมติดตั้ง และผ่านการตรวจรับจากคณะกรรมการตรวจรับพัสดุแล้ว

เอกสารแนบ ๒

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและราคากลาง (ราคาอ้างอิง)

ในการจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง

1. ชื่อโครงการ ครุภัณฑ์คอมพิวเตอร์และอุปกรณ์สำหรับโครงการปรับปรุงประสิทธิภาพระบบรักษาความมั่นคงปลอดภัยสารสนเทศ /หน่วยงานเจ้าของโครงการ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงาน ก.พ.

2. วงเงินงบประมาณที่ได้รับจัดสรร 6,400,000.- บาท

3. วันที่กำหนดราคากลาง (ราคาอ้างอิง) 28 ธันวาคม ๒๕๕๙

เป็นเงิน 6,212,420.-บาท

รายการ	จำนวน	ราคาต่อหน่วย (บาท)	ราคารวม (บาท)
1. ระบบป้องกันการโจมตีเครือข่าย (Firewall)	1 ระบบ	3,002,420.-	3,002,420.-
2. ระบบป้องกันไวรัสทางเครือข่าย	1 ระบบ	1,605,000.-	1,605,000.-
3. ซอฟต์แวร์ป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์ในเครือข่าย	1 ระบบ	1,605,000.-	1,605,000.-

4. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)

ใช้เกณฑ์ราคารวมต่ำสุด จากการสืบราคาจากบริษัทผู้ขาย จำนวน 3 ราย ได้แก่

4.1 บริษัท เคมิท กรุ๊ป จำกัด

4.2 บริษัท แอ็ดวานซ์ อินฟอร์เมชั่น เทคโนโลยี จำกัด (มหาชน)

4.3 บริษัท คอม เทรดดิ้ง จำกัด

5. รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง)

5.1 นายบวร มีโต นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ .....

5.2 นางสาวพิมลพรรณ หอมรสสุคนธ์ นักวิชาการคอมพิวเตอร์ชำนาญการ .....

5.3 นายวรเชษฐ์ จันทร์บุญนาค นักวิชาการคอมพิวเตอร์ชำนาญการ .....

28/12/59

(นางสุกัญญา ธนะเสวี)

ผอ.ศสส.