กองทุนบำเหน็จบำนาญข้าราชการ

ขอบเขตของงาน (Terms of Reference : TOR)

การซื้อระบบรักษาความปลอดภัย Firewall และระบบศูนย์กลางบริหารจัดการระบบรักษาความปลอดภัย Firewall และพร้อมติดตั้ง

---

1. หลักการและเหตุผล

กองทุนบำเหน็จบำนาญข้าราชการ (กบข.) ได้ติดตั้งใช้งานระบบรักษาความปลอดภัย Firewall หลัก และ Firewall สำรองทำงานคู่กันแบบ High Availability หรือ HA ภายในศูนย์คอมพิวเตอร์ของ กบข. เพื่อทำหน้าที่ป้องกันและรักษาความมั่นคงปลอดภัยให้แก่ระบบสารสนเทศของ กบข.อย่างต่อเนื่องจนถึงปัจจุบัน

เนื่องจากขณะนี้ระบบรักษาความปลอดภัย Firewall ดังกล่าวจะสิ้นสุดการสนับสนุนด้าน Software ที่ติดตั้งบนระบบรักษาความปลอดภัย Firewall จากเจ้าของผลิตภัณฑ์ เพื่อความพร้อมใช้งานอย่างต่อเนื่อง กบข. เห็นควรดำเนินการจัดซื้อระบบรักษาความปลอดภัย Firewall หลัก และ Firewall สำรอง โดยมีการออกแบบสถาปัตถยกรรมโครงสร้างพื้นฐานรักษาความปลอดภัย Firewall ใหม่ให้มีการแยกและช่วยกันทำงานระหว่างเครือข่ายภายนอก (Internet Zone) จำนวน 2 ชุดและเครือข่ายภายใน (Internal Zone) จำนวน 2 ชุดพร้อมมีระบบศูนย์กลางบริหารจัดการระบบรักษาความปลอดภัย Firewall และพร้อมติดตั้ง โดยมีระยะเวลาดำเนินการและส่งมอบงานไม่เกิน 90 วัน นับแต่วันที่ลงนามสัญญา และมีระยะเวลารับประกันและการบำรุงรักษาเป็นเวลาไม่น้อยกว่า 1 ปี

2. วัตถุประสงค์

เพื่อจัดซื้อระบบรักษาความปลอดภัย Firewall หลัก และ Firewall สำรอง โดยมีการออกแบบสถาปัตถยกรรมโครงสร้างพื้นฐานรักษาความปลอดภัย Firewall ใหม่ให้มีการแยกและช่วยกันทำงานระหว่างเครือข่ายภายนอก (Internet Zone) จำนวน 2 ชุดและเครือข่ายภายใน (Internal Zone) จำนวน 2 ชุดพร้อมมีระบบศูนย์กลางบริหารจัดการระบบรักษาความปลอดภัย Firewallและพร้อมติดตั้ง ทดแทนระบบฯ เดิม และมีระยะเวลารับประกันและการบำรุงรักษาเป็นเวลาไม่น้อยกว่า 1 ปี

3. คุณสมบัติผู้ยื่นข้อเสนอ

3.1 ผู้ยื่นข้อเสนอต้องมีคุณสมบัติตามมาตรฐานที่ระบบการจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic GovernmentProcurement : e-GP) กำหนด

4. รายการรายละเอียดพัสดุ

4.1 จัดซื้อระบบรักษาความปลอดภัย Firewall หลัก และ Firewall สำรอง โดยมีการออกแบบสถาปัตถยกรรมโครงสร้างพื้นฐานรักษาความปลอดภัย Firewall ใหม่ให้มีการแยกและช่วยกันทำงานระหว่างเครือข่ายภายนอก (Internet Zone) จำนวน 2 ชุดและเครือข่ายภายใน (Internal Zone) จำนวน 2 ชุด พร้อมมีระบบศูนย์กลางบริหารจัดการระบบรักษาความปลอดภัย Firewallและพร้อมติดตั้ง โดยมีรายละเอียดดังนี้

4.1.1 อุปกรณ์ระบบรักษาความปลอดภัย Firewall สำหรับ Internet Zone จำนวน 2 หน่วย ซึ่งแต่ละหน่วยมีคุณลักษณะดังนี้

4.1.1.1 เป็นอุปกรณ์ Firewall ชนิด Next Generation Firewall แบบ Hardware Appliance

4.1.1.2 มี Firewall Throughput ไม่น้อยกว่า 70 Gbps หรือ NGFW Throughput ไม่น้อยกว่า 18 Gbps

4.1.1.3 รองรับ Concurrent Session ไม่น้อยกว่า 8,000,000 Sessions และ New Sessions/Sec ได้อย่างน้อย 290,000 Sessions/Sec

4.1.1.4 มี IPsec VPN หรือ SSL VPN Throughput ไม่น้อยกว่า 17 Gbps และรองรับ Concurrent SSL VPN Users ได้อย่างน้อย 1,000 Users

4.1.1.5 ระบบที่เสนอสามารถทำ 2 Factor Authentication (2FA) ในการใช้งาน VPN ได้ในลักษณะ Mobile Token โดยมีลิขสิทธิ์การใช้งานได้ไม่น้อยกว่า 300 licenses หรือเสนอระบบเพิ่มเติมเพื่อให้มีคุณสมบัติตามที่ระบุ

4.1.1.6 สามารถบริหารจัดการ SSL Inspection Throughput หรืออื่นๆที่เกี่ยวข้อง

4.1.1.7 มี Threat Protection Throughput ไม่น้อยกว่า 7 Gbps (เปิดใช้งาน Firewall, IPS, Application control และ Malware protection)

4.1.1.8 สามารถทำ Virtual Firewall (Virtual Domain) ได้อย่างน้อย 10 Virtual Domain

4.1.1.9 รองรับการควบคุม Application ใช้งานผ่าน WAN link ตามค่า SLA ที่กำหนดจาก Latency, Jitter, Packet loss ได้เป็นอย่างน้อย และรองรับการทำ Fail-over link ได้แบบอัตโนมัติ หรือรองรับการทำ Link Load Balance

4.1.1.10 สามารถป้องกันภัยคุกคามขั้นสูง (Advance Threat Protection) โดยส่งไฟล์ต้องสงสัยไปตรวจสอบกับระบบ Cloud-based Sandbox ที่ให้บริการโดยเจ้าของผลิตภัณฑ์ และได้รับการอัพเดท Dynamic signature ตลอดระยะเวลารับประกัน

4.1.1.11 สามารถป้องกันการโจมตีผ่านช่องโหว่ของระบบต่างๆ จาก IPS signature, Protocol anomaly detection และมีระบบ Rate-based DOS protection ป้องกัน TCP Syn flood, Port scan, ICMP sweep ได้เป็นอย่างน้อย

4.1.1.12 สามารถควบคุมการใช้งานเว็บไซต์ (Web Filtering) ตามประเภทของเว็บไซต์ (Web Categories) ได้ไม่น้อยกว่า 80 ประเภท และสามารถกำหนดประเภทเองได้ (Local Categories)

4.1.1.13 สามารถตรวจจับ (scan) และป้องกัน Virus ผ่านการใช้งานทาง Web, Mail และ FTP ได้เป็นอย่างน้อย

4.1.1.14 สามารถทำ Routing Protocol แบบ OSPF, BGP และสามารถทำ NAT46, NAT64, IPv4, IPv6 ได้เป็นอย่างน้อย

4.1.1.15 มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) อย่างน้อย ดังนี้

- แบบ GE RJ45 ไม่น้อยกว่า 10 พอร์ต
- แบบ GE SFP ไม่น้อยกว่า 8 ช่อง พร้อมเสนอ Transceiver มาพร้อม แบบ SX ไม่น้อยกว่า 4 หน่วย
- แบบ 10G SFP+ ไม่น้อยกว่า 8 ช่อง พร้อมเสนอ Transceiver แบบ SR มาพร้อม ไม่น้อยกว่า 4 หน่วย
- รองรับการมี 40GE QSFP+ ได้ไม่น้อยกว่า 2 ช่อง ได้ในอนาคต

4.1.1.16 มี network interface สำหรับ Management และ HA อย่างละ 1 port เป็นอย่างน้อย

4.1.1.17 มี Power Supply แบบ Dual Power Supply และเป็นแบบ Hot Swappable

4.1.1.18 สามารถทำ DNS Filtering หรือ DNS Security

4.1.1.19 สามารถพิสูจน์ตัวตน (Authentication) ผู้ใช้งานได้ โดยรองรับฐานข้อมูลผู้ใช้แบบ Local, LDAP, RADIUS, TACACS+

4.1.1.20 มีคุณสมบัติ DLP เพื่อตรวจจับไฟล์ และข้อมูลสำคัญ โดยกำหนดเงื่อนไขแบบ File Type, File Size, Regular Expression ได้เป็นอย่างน้อย

4.1.1.21 สามารถในการทำ High Availability (HA) ระหว่างคู่ของอุปกรณ์ที่เสนอในโครงการได้ โดยรองรับทั้งแบบ Active-Active และ Active-Passive

4.1.1.22 อุปกรณ์สามารถ Update IPS Service, Web Filtering Service, Sandbox Cloud Service, AntiSpam Service และ Signature ได้ตลอดระยะเวลาของการรับประกัน

4.1.1.23 ผลิตภัณฑ์ที่เสนอ ต้องอยู่ในกลุ่ม Recommended จาก NSS Labs ด้าน Next Generation Firewall (NGFW) ปี 2019 หรือปัจจุบัน

4.1.1.24 ผลิตภัณฑ์ที่เสนอ ต้องอยู่ในกลุ่ม Leader ของ Gartner Magic Quadrant for Enterprise Network Firewalls ปี 2019 หรือปัจจุบัน

4.1.1.25 อุปกรณ์ต้องได้รับรองมาตรฐาน FCC, VCCI, CE เป็นอย่างน้อย

4.1.2 อุปกรณ์ระบบรักษาความปลอดภัย Firewall สำหรับ Internal Zone จำนวน 2 หน่วย ซึ่งแต่ละหน่วยมีคุณลักษณะดังนี้

4.1.2.1 เป็นอุปกรณ์ Firewall ชนิด Next Generation Firewall แบบ Hardware Appliance

4.1.2.2 มี Firewall Throughput ไม่น้อยกว่า 150 Gbps หรือ NGFW Throughput ไม่น้อยกว่า 45 Gbps

4.1.2.3 รองรับ Concurrent Session ไม่น้อยกว่า 11,000,000 Sessions และ New Sessions/Sec ได้อย่างน้อย 430,000 Sessions/Sec

4.1.2.4 มี IPsec VPN หรือ SSL VPN Throughput ไม่น้อยกว่า 20 Gbps และรองรับ Concurrent SSL VPN Users ได้อย่างน้อย 1,000 Users

4.1.2.5 รองรับการทำ SSL Inspection Throughput

4.1.2.6 มี Threat Protection Throughput ไม่น้อยกว่า 10 Gbps (เปิดใช้งาน Firewall, IPS, Application control และ Malware protection)

4.1.2.7 สามารถทำ Virtual Firewall (Virtual Domain) ได้อย่างน้อย 10 Virtual Domain

4.1.2.8 รองรับการควบคุม Application ใช้งานผ่าน WAN link ตามค่า SLA ที่กำหนดจาก Latency, Jitter, Packet loss ได้เป็นอย่างน้อย และสามารถทำ Fail-over link ได้แบบอัตโนมัติ หรือมีความสามารถทำ Link Load Balance

4.1.2.9 สามารถป้องกันภัยคุกคามขั้นสูง (Advance Threat Protection) โดยส่งไฟล์ต้องสงสัยไปตรวจสอบกับระบบ Cloud-based Sandbox ที่ให้บริการโดยเจ้าของผลิตภัณฑ์ และได้รับการอัพเดท Dynamic signature ตลอดระยะเวลารับประกัน

4.1.2.10 สามารถป้องกันการโจมตีผ่านช่องโหว่ของระบบต่างๆ จาก IPS signature, Protocol anomaly detection และมีระบบ Rate-based DOS protection ป้องกัน TCP Syn flood, Port scan, ICMP sweep ได้เป็นอย่างน้อย

4.1.2.11 สามารถตรวจจับ (scan) และป้องกัน Virus ผ่านการใช้งานทาง Web, Mail และ FTP ได้เป็นอย่างน้อย

4.1.2.12 สามารถทำ Routing Protocol แบบ OSPF, BGP และสามารถทำ NAT46, NAT64,IPv4, IPv6 ได้เป็นอย่างน้อย

4.1.2.13 มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) อย่างน้อย ดังนี้

- แบบ GE RJ45 ไม่น้อยกว่า 12 พอร์ต
- แบบ 10G SFP+ ไม่น้อยกว่า 12 ช่อง พร้อมเสนอ Transceiver แบบ SR มาพร้อมไม่น้อยกว่า 6 หน่วย
- แบบ 40GE QSFP+ ได้ไม่น้อยกว่า 4 ช่อง พร้อมเสนอ Transceiver มาพร้อมไม่น้อยกว่า 2 หน่วย

4.1.2.14 มี network interface สำหรับ Management และ HA อย่างละ 1 port เป็นอย่างน้อย

4.1.2.15 มี Power Supply แบบ Dual Power Supply และเป็นแบบ Hot Swappable

4.1.2.16 สามารถทำ DNS Filtering หรือ DNS Security

4.1.2.17 สามารถพิสูจน์ตัวตน (Authentication) ผู้ใช้งานได้ โดยรองรับฐานข้อมูลผู้ใช้แบบ Local, LDAP, RADIUS, TACACS+

4.1.2.18 มีคุณสมบัติ DLP เพื่อตรวจจับไฟล์ และข้อมูลสำคัญ โดยกำหนดเงื่อนไขแบบ File Type, File Size, Regular Expression ได้เป็นอย่างน้อย หรือเทียบเท่า หรือดีกว่า

4.1.2.19 สามารถในการทำ High Availability (HA) ระหว่างคู่ของอุปกรณ์ที่เสนอในโครงการได้ โดยรองรับทั้งแบบ Active-Active และ Active-Passive

4.1.2.20 อุปกรณ์สามารถ Update IPS Service, Sandbox Cloud Service, AntiSpam Service และ Signature ได้ตลอดระยะเวลาของการรับประกัน

4.1.2.21 ผลิตภัณฑ์ที่เสนอ ต้องอยู่ในกลุ่ม Recommended จาก NSS Labs ด้าน Next Generation Firewall (NGFW) ปี 2019 หรือปัจจุบัน

4.1.2.22 ผลิตภัณฑ์ที่เสนอ ต้องอยู่ในกลุ่ม Leader ของ Gartner Magic Quadrant for Enterprise Network Firewalls ปี 2019 หรือปัจจุบัน

4.1.2.23 อุปกรณ์ต้องได้รับรองมาตรฐาน FCC, VCCI, CE เป็นอย่างน้อย

4.1.3 ระบบศูนย์กลางบริหารจัดการระบบรักษาความปลอดภัย Firewall จำนวน 1 ชุด ที่มีคุณลักษณะเฉพาะอย่างน้อยดังนี้

4.1.3.1 เป็น Virtual Appliance ที่สามารถบริหารจัดการอุปกรณ์รักษาความปลอดภัยเครือข่ายทั้ง 4 ชุดที่เสนอในโครงการนี้ได้ และอยู่ภายใต้เครื่องหมายการค้าเดียวกันกับอุปกรณ์ NGFW ที่เสนอทั้งหมดได้

4.1.3.2 สามารถติดตั้งบน Hypervisor ได้แก่ VMware ESX/ESXi, Microsoft Hyper-V, KVM, Nutanix AHV, Amazon Web Services (AWS), Microsoft Azure, ได้เป็นอย่างน้อย

4.1.3.3 รองรับการมี Storage สำหรับออกรายงานได้ไม่น้อยกว่า 6 TB

4.1.3.4 สามารถบริหารจัดการอุปกรณ์รักษาความปลอดภัยเครือข่าย (NGFW), Virtual Appliance, และ Virtual Domain/Firewall/System จำนวนรวมไม่น้อยกว่า 10 อุปกรณ์/ระบบ

4.1.3.5 สามารถบริหารจัดการ Policies, Objects และ VPN ให้กับอุปกรณ์ NGFW ได้เป็นอย่างน้อย

4.1.3.6 สามารถ Update Software/Firmware และ Securities Signature ให้กับอุปกรณ์ที่ถูกบริหารได้

4.1.3.7 มีคุณสมบัติ RESTful API เพื่อปรับการตั้งค่าอุปกรณ์ไฟล์วอล เช่น policy และ object ได้เป็นอย่างน้อย

4.1.3.8 สามารถแสดง Physical Topology หรือ Logical Topology ได้เป็นอย่างน้อย หรือมีคุณความสามารถเทียบเท่า หรือดีกว่า

4.1.3.9 สามารถกำหนดสิทธิให้กับผู้ดูแลระบบ ที่จะเข้ามาใช้งานอุปกรณ์บริหารจัดการสำหรับอุปกรณ์รักษาความปลอดภัยเครือข่ายได้ (Role-based Administration)

4.1.3.10 สามารถบริหารจัดการผ่านโปรโตคอล HTTPS และ SSH ได้เป็นอย่างน้อย

4.1.3.11 มีคุณสมบัติออกรายงานอย่างน้อยดังต่อไปนี้

- มีอัตราความสามารถรับจำนวน log ได้ไม่น้อยกว่า 11 GB ต่อวันเป็นอย่างน้อย

- สามารถทำการสำรองข้อมูล Log ไปยังอุปกรณ์จัดเก็บข้อมูลภายนอก เช่น External Storage หรือ FTP/SFTP Server เป็นต้นได้

- มี Dashboard ที่สรุปข้อมูล Top sources, Top destinations, Top applications, Top websites, Top threats, System events และ Resource usage ได้เป็นอย่างน้อย

- สามารถแสดงข้อมูล Log เช่น Date, Time, Source IP, User, Destination IP และ Services ได้เป็นอย่างน้อย

- มีรูปแบบรายงาน (Report templates) มาให้ไม่น้อยกว่า 30 รูปแบบ และสามารถ custom รายงาน และสามารถแสดงรายงานในรูปแบบของ PDF, HTML และ CSV ได้เป็นอย่างน้อย

4.1.4 ผู้เสนอราคาต้องเสนออุปกรณ์เชื่อมต่อระบบเครือข่าย (Cisco SFP-10G-SR = 10GBASE-SR SFP+ Transceiver Module) พร้อมสาย Fiber Optic Patch Cord Cable หรืออุปกรณ์อื่นๆที่เกี่ยวข้องติดตั้งบนอุปกรณ์ Switch Cisco N5K-C5548UP-FA ของ กบข. จำนวน 12 ชุด พร้อมดำเนินการเชื่อมต่อกับอุปกรณ์ Firewall ที่นำเสนอ

4.2 ผู้ขายต้องจัดหาลิขสิทธิ์การใช้งานทั้งหมดของ Hardware/Software ที่ถูกต้องตามกฎหมายสำหรับติดตั้งใช้งานในระบบรักษาความปลอดภัย Firewall ของ กบข.

4.3 การติดตั้งระบบรักษาความปลอดภัย Firewall มีขอบเขตงานอย่างน้อยดังนี้

4.3.1 บริหารโครงการ (Project Management) พร้อมจัดตั้งทีมงานเพื่อรับผิดชอบดูแลในส่วนต่างๆ ของโครงการนี้ ให้แล้วเสร็จภายในระยะเวลาที่กำหนด โดยต้องประชุมหารือกับ กบข. เพื่อสรุปรายละเอียดการออกแบบสถาปัตยกรรม การทำงานและแผนงานตามวันและเวลาที่ กบข. กำหนด และต้องจัดทำและส่งมอบแผนงาน (Project Plan) พร้อมรายละเอียดในการดำเนินงานทั้งหมดให้ผู้ว่าจ้าง

4.3.2 ติดตั้งระบบรักษาความปลอดภัย Firewall และระบบศูนย์กลางบริหารจัดการระบบรักษาความปลอดภัย Firewall และระบบอื่น ๆ ของ กบข. ที่เกี่ยวข้องเพื่อให้มีประสิทธิภาพตามที่ออกแบบและตกลงไว้กับทาง กบข.

4.3.3 กำหนดและปรับแต่งค่า Configuration ระบบรักษาความปลอดภัย Firewall และระบบศูนย์กลางบริหารจัดการระบบรักษาความปลอดภัย Firewall ให้สามารถจัดส่งข้อมูลจราจร Event Log ไปยังอุปกรณ์ Centralize Log Server ของ กบข. ได้

4.3.4 ตรวจสอบการทำงานระบบรักษาความปลอดภัย Firewall และระบบศูนย์กลางบริหารจัดการระบบรักษาความปลอดภัย Firewall หลังจากที่ทำการติดตั้งตามช่วงเวลาที่กำหนด เพื่อติดตามเฝ้าดูการทำงานของระบบให้เป็นไปตามข้อกำหนดในเอกสาร TOR

4.3.5 กำหนดและปรับแต่งค่า Configuration ของระบบรักษาความปลอดภัย Firewall และระบบศูนย์กลางบริหารจัดการระบบรักษาความปลอดภัย Firewall ให้ทำงานได้อย่างมีประสิทธิภาพเหมาะสมกับสภาพแวดล้อมของ กบข.

4.3.6 จัดทำคู่มือการติดตั้งระบบรักษาความปลอดภัย Firewall และระบบศูนย์กลางบริหารจัดการระบบรักษาความปลอดภัย Firewall รวมทั้งคู่มือการใช้งานและคู่มือบำรุงรักษาระบบต่าง ๆ เป็นเอกสารภาษาไทย จำนวน 1 ชุด ส่งมอบให้แก่ กบข. โดยแสดงรายละเอียดเป็นขั้นตอนที่สามารถทำความเข้าใจได้ง่าย

4.3.7 จัดอบรมถ่ายทอดความรู้ในการบริหารจัดการและดูแลบำรุงรักษาระบบรักษาความปลอดภัย Firewall และระบบศูนย์กลางบริหารจัดการระบบรักษาความปลอดภัย Firewall ให้แก่เจ้าหน้าที่ผู้ดูแลระบบสารสนเทศของ กบข. พร้อมทั้งจัดทำเอกสารประกอบการอบรมสำหรับผู้เข้าร่วมอบรม

4.3.8 ผู้ขายต้องดำเนินการถอดถอนระบบรักษาความปลอดภัย Firewall ของ กบข. เดิมพร้อมติดตั้งระบบรักษาความปลอดภัย Firewall ใหม่โดยดำเนินการย้ายคุณลักษณะค่า Configuration และข้อมูลอื่น ๆ ที่เกี่ยวข้องของระบบรักษาความปลอดภัย Firewall เดิมไปยังระบบรักษาความปลอดภัย Firewall ที่ติดตั้งใหม่ให้ถูกต้องครบถ้วนหรือ หากมีการออกแบบสถาปัตยกรรมใหม่จากข้อ 4.3.1 เพื่อให้มีประสิทธิภาพให้ดำเนินการตามที่ออกแบบและตกลงไว้กับทาง กบข. โดยมีแผนหรือวิธีการถอดถอนและแผนสำรองย้อนกลับเมื่อเกิดปัญหาในการเปลี่ยนระบบรักษาความปลอดภัย Firewall และการติดตั้งจะต้องใช้งานร่วมกับโครงสร้างพื้นฐานปัจจุบัน และกำหนดระยะเวลาในการ Monitor และจูนค่า Configuration เพื่อไม่ก่อให้เกิดผลกระทบกับการใช้งานปัจจุบัน

4.4 การรับประกันมีรายละเอียดดังนี้

4.4.1 การรับประกันคุณภาพหลังการติดตั้งสำหรับระบบรักษาความปลอดภัย Firewall และระบบศูนย์กลางบริหารจัดการระบบรักษาความปลอดภัย Firewall และสิทธิ์การใช้งาน Hardware/Software รวมถึงการบำรุงรักษาให้ระบบฯพร้อมใช้งานไม่น้อยกว่า 1 ปี โดยไม่มีค่าใช้จ่ายใด ๆ เพิ่มเติมตลอดระยะเวลาสัญญา นับแต่วันที่ กบข. ตรวจรับมอบพัสดุ

4.4.2 ผู้ขายต้องดูแลบำรุงรักษาระบบรักษาความปลอดภัย Firewall และระบบศูนย์กลางบริหารจัดการระบบรักษาความปลอดภัย Firewall ตามรายละเอียดในข้อ 4.1 ให้อยู่ในสภาพที่พร้อมใช้งานได้เป็นอย่างดีและมีประสิทธิภาพอยู่เสมอ ทุกวันตลอด 24 ชั่วโมง ตลอดระยะเวลาสัญญา

4.4.3 ผู้ขายต้องจัดให้มีเจ้าหน้าที่ประจำเป็นผู้มีความชำนาญเพื่อดำเนินการบำรุงรักษาเชิงป้องกัน (Preventive Maintenance) ระบบรักษาความปลอดภัย Firewall และระบบศูนย์กลางบริหารจัดการระบบรักษาความปลอดภัย Firewall ณ สำนักงานของ กบข. (On-site) โดยดำเนินการตรวจสอบสภาพการทำงานและบำรุงรักษาระบบฯ ของ กบข. ให้อยู่ในสภาพที่พร้อมใช้งานได้เป็นอย่างดีและมีประสิทธิภาพอยู่เสมอ อย่างน้อย 3 เดือนต่อ 1 ครั้ง หรือไม่น้อยกว่า 4 ครั้งต่อปี และอัพเกรด Version ซอฟท์แวร์ที่เกี่ยวข้องอย่างน้อยทุก 6 เดือน (ถ้ามี) หรือแล้วแต่ตกลงตลอดระยะเวลาสัญญา

4.4.4 การให้บริการบำรุงรักษาระบบรักษาความปลอดภัย Firewall และระบบศูนย์กลางบริหารจัดการระบบรักษาความปลอดภัย Firewall ของ กบข. และ/หรือการอัพเกรด Version ซอฟท์แวร์ที่เกี่ยวข้อง ในแต่ละครั้ง ผู้ขายต้องจัดทำและส่งมอบรายงานผลการดำเนินงานและการให้บริการ (Service Report) และ Logbook/Check list ของงานที่ดำเนินการ ในรูปแบบเอกสารรายงานจำนวน 1 ชุด ให้กับ กบข. ภายใน 15 วัน นับแต่วันที่ได้ดำเนินงานในแต่ละครั้งแล้วเสร็จ

4.4.5 ในกรณีที่ระบบรักษาความปลอดภัย Firewall และระบบศูนย์กลางบริหารจัดการระบบรักษาความปลอดภัย Firewall ไม่สามารถใช้งานได้ตามปกติ ผู้ขายต้องดำเนินการตรวจสอบ ซ่อมแซมแก้ไขเพื่อให้ระบบฯสามารถใช้งานได้ดีตามปกติและอย่างมีประสิทธิภาพดังเดิม โดยสำนักงานไม่ต้องเสียค่าใช้จ่ายใด ๆ เพิ่มเติมตลอดระยะเวลาสัญญา โดยมีเงื่อนไขการให้บริการขั้นต่ำดังต่อไปนี้

(1) ในกรณีระบบฯ ชำรุดเสียหายหรือไม่สามารถใช้งานได้ตามปกติ หากตรวจสอบพบว่าเกิดจากผลิตภัณฑ์ไม่ว่าจะเกิดบนระบบรักษาความปลอดภัย Firewall และระบบศูนย์กลางบริหารจัดการระบบรักษาความปลอดภัย Firewall ผลิตภัณฑ์ หรือเกิดจากความผิดพลาดของผู้ขายที่ทำให้ระบบฯ เสียหายก็ตาม ผู้ขายจะเป็นผู้รับผิดชอบเองทั้งหมด

(2) ในกรณีที่เหตุขัดข้องของระบบรักษาความปลอดภัย Firewall และระบบศูนย์กลางบริหารจัดการระบบรักษาความปลอดภัย Firewall เกิดจาก Bugs ของ Software ที่ติดตั้งใช้งานอยู่กับระบบฯ ผู้ขายต้อง Upgrade Software ที่เป็น Version ใหม่ เพื่อแก้ไขปัญหาที่เกิดขึ้น และเพื่อให้ระบบฯ สามารถใช้งานได้ตามปกติ ทั้งนี้ ในการ Upgrade Software ที่เป็น Version ใหม่ดังกล่าว ผู้ขายจะต้องเสนอแนวทางดำเนินการและวิเคราะห์ผลกระทบที่อาจเกิดขึ้นเสนอให้ กบข. พิจารณาให้ความเห็นชอบเสียก่อนเริ่มดำเนินการทุกครั้ง

(3) ในกรณีเจ้าของผลิตภัณฑ์ได้ออกโปรแกรมมาแก้ไขช่องโหว่หรือจุดบกพร่อง (Security Patch) ผู้ขายจะต้องดำเนินการ Upgrade Security Patch ให้แล้วเสร็จและสามารถใช้งานได้อย่างสมบูรณ์โดยมิชักช้า ทั้งนี้ ในการ Upgrade Security Patch ดังกล่าว ผู้ขายจะต้องเสนอแนวทางดำเนินการและวิเคราะห์ผลกระทบที่อาจเกิดขึ้นเสนอให้ กบข. พิจารณาให้ความเห็นชอบเสียก่อนเริ่มดำเนินการทุกครั้ง

(4) กบข. สามารถขอรับคำปรึกษาด้านเทคนิคผ่านทาง e-mail หรือโทรศัพท์ได้โดยไม่จำกัดจำนวนครั้งตลอด 24 ชั่วโมงทุกวัน ตลอดระยะเวลาสัญญา

(5) ในกรณีระบบรักษาความปลอดภัย Firewall และระบบศูนย์กลางบริหารจัดการระบบรักษาความปลอดภัย Firewallของ กบข. ไม่พร้อมใช้งานตามปกติ ผู้ขายต้องสนับสนุนความพร้อมใช้งานโดย กบข. สามารถเรียกใช้บริการบำรุงรักษา ทุกวันตลอด 24 ชั่วโมง โดยไม่ต้องเสียค่าใช้จ่ายใดๆ เพิ่มเติมตลอดระยะเวลาสัญญา รวมทั้งสามารถแจ้งปัญหาทาง e-mail หรือโทรศัพท์ ให้ผู้ขายรับทราบ และผู้ขายต้องตอบกลับภายใน 1 ชั่วโมง นับตั้งแต่เวลาที่ได้รับแจ้งจาก กบข. กรณีผู้ขายพิจารณาเหตุขัดข้องที่เกิดขึ้นดังกล่าวหากสามารถแก้ปัญหาแบบการเข้าถึงระยะไกล (Remote) ได้ ผู้ขายต้องแก้ไขให้ระบบฯ ของ กบข. พร้อมใช้งานได้ตามปกติ ภายใน 4 (สี่) ชั่วโมง นับตั้งแต่เวลาที่ได้รับแจ้งจาก กบข.

(6) หากผู้ขายพิจารณาแล้วว่าไม่สามารถแก้ปัญหาแบบการเข้าถึงระยะไกล (Remote) ได้ ผู้ขายต้องเข้ามาตรวจสอบและให้บริการภายในพื้นที่ติดตั้ง ณ สำนักงานของ กบข. (on site services) ภายในระยะเวลา 4 (สี่) ชั่วโมง นับตั้งแต่เวลาที่ได้รับแจ้งจาก กบข. โดยผู้ขายจะต้องรายงานปัญหาความชำรุดบกพร่องของระบบรักษาความปลอดภัย Firewall และระบบศูนย์กลางบริหารจัดการระบบรักษาความปลอดภัย Firewall ของ กบข. ที่เกิดขึ้นและเสนอแนวทางการแก้ไขปัญหาความชำรุดบกพร่องของระบบฯ ให้ กบข. พิจารณาภายใต้ข้อกำหนดดังต่อไปนี้

(ก) ในกรณีที่ระบบฯ ของ กบข. ชำรุดเสียหายไม่สามารถใช้งานได้ทั้งหมดหรือไม่สามารถใช้งานได้ในส่วนที่สำคัญต่อ กบข. ผู้ขายจะต้องดำเนินการซ่อมแซมแก้ไข เพื่อให้ระบบฯ ของ กบข. อยู่ในสภาพใช้งานได้ตามปกติ ภายในระยะเวลา 8 ชั่วโมง นับแต่เวลาที่ได้รับแจ้งจาก กบข. หรือภายในระยะเวลาอื่นใดที่ กบข. กำหนดให้ตามความเหมาะสม

(ข) ในกรณีที่ระบบฯ ของ กบข. ชำรุดเสียหายไม่สามารถใช้งานได้ในส่วนที่ไม่สำคัญต่อ กบข. ผู้ขายต้องเสนอระยะเวลาการแก้ไขความชำรุดบกพร่องจนแล้วเสร็จให้ กบข. พิจารณาให้ความเห็นชอบ ซึ่งผู้ขายจะต้องดำเนินการตามแผนงานดังกล่าวให้แล้วเสร็จโดยไม่ชักช้า

4.4.6 ผู้ขายต้องส่งรายงานปัญหาที่เกิดขึ้น รวมถึงวิธีการและขั้นตอนการแก้ไขปัญหาที่เกิดขึ้นโดยละเอียด ในรูปแบบของเอกสารและ File ข้อมูล แก่ กบข. ภายใน 3 วันทำการโดยรายละเอียดของรายงานอย่างน้อยต้องประกอบด้วย วัน เดือน ปี ที่เกิดปัญหา, รายละเอียดและการวิเคราะห์สาเหตุของปัญหาที่เกิดขึ้น , วิธีการแก้ไขปัญหา, แนวทางการป้องกันปัญหา เป็นต้น

4.4.7 กบข. จะถือเอาเวลาที่ผู้ขายได้รับแจ้งจากพนักงานหรือตัวแทนของกบข. ส่ง e-mail หรือโทรศัพท์แจ้งเหตุฉุกเฉินหรือระบบไม่พร้อมใช้งานเป็นเวลาเริ่มต้น เพื่อใช้ในการคำนวณระยะเวลาตามข้อตกลงระดับการให้บริการ (Service Level Agreement) ที่กำหนดไว้

4.4.8 ผู้ขายต้องจัดให้มีเจ้าหน้าที่ประจำที่มีความสามารถในการรับแจ้งปัญหา ตลอดจนการแก้ไขปัญหารวมทั้งให้บริการปรึกษาปัญหาการใช้ระบบรักษาความปลอดภัย Firewall และระบบศูนย์กลางบริหารจัดการระบบรักษาความปลอดภัย Firewall แบบทุกวันตลอด 24 ชั่วโมง ตลอดระยะเวลาสัญญา

5. หลักฐานการยื่นข้อเสนอ

ผู้ยื่นข้อเสนอจะต้องเสนอเอกสารหลักฐานยื่นมาพร้อมการเสนอราคา โดยแยกเป็น 2 ส่วน คือ

5.1 ส่วนที่ 1 อย่างน้อยต้องมีเอกสารดังต่อไปนี้

(1) ในกรณีผู้ยื่นข้อเสนอเป็นนิติบุคคล

(ก) ห้างหุ้นส่วนสามัญหรือห้างหุ้นส่วนจำกัด ให้ยื่นสำเนาหนังสือรับรองการจดทะเบียนนิติบุคคล (ระยะเวลาไม่เกิน 90 วัน) บัญชีรายชื่อหุ้นส่วนผู้จัดการ ผู้มีอำนาจควบคุม (ถ้ามี) พร้อมรับรองสำเนาถูกต้อง

(ข) บริษัทจำกัดหรือบริษัทมหาชนจำกัด ให้ยื่นสำเนาหนังสือรับรองการจดทะเบียนนิติบุคคล (ระยะเวลาไม่เกิน 90 วัน) หนังสือบริคณห์สนธิ บัญชีรายชื่อกรรมการผู้จัดการ ผู้มีอำนาจควบคุม(ถ้ามี) บัญชีผู้ถือหุ้นรายใหญ่ (ถ้ามี) พร้อมรับรองสำเนาถูกต้อง

(2) ในกรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดาหรือคณะบุคคลที่ไม่ใช่นิติบุคคลให้ยื่นสำเนาบัตรประจำตัวประชาชนของผู้นั้น สำเนาข้อตกลงที่แสดงถึงการเข้าเป็นหุ้นส่วน (ถ้ามี) สำเนาบัตรประจำตัวประชาชนของผู้เป็นหุ้นส่วน หรือสำเนาหนังสือเดินทางของผู้เป็นหุ้นส่วนที่มิได้ถือสัญชาติไทย พร้อมทั้งรับรองสำเนาถูกต้อง

(3) ในกรณีผู้ยื่นข้อเสนอเป็นผู้ยื่นข้อเสนอร่วมกันในฐานะเป็นผู้ร่วมค้า ให้ยื่นสำเนาสัญญาของการเข้าร่วมค้า และเอกสารตามที่ระบุไว้ใน (1) หรือ (2) ของผู้ร่วมค้า แล้วแต่กรณี

(4) เอกสารเพิ่มเติมอื่น ๆ ได้แก่ สำเนาใบทะเบียนพาณิชย์ สำเนาทะเบียนภาษีมูลค่าเพิ่ม พร้อมทั้งรับรองสำเนาถูกต้อง

5.2 ส่วนที่ 2 อย่างน้อยต้องมีเอกสารดังต่อไปนี้

(1) ในกรณีที่ผู้ยื่นข้อเสนอมอบอำนาจให้บุคคลอื่นกระทำการแทนให้แนบหนังสือมอบอำนาจซึ่งปิดอากรแสตมป์ตามกฎหมาย จะต้องระบุในหนังสือมอบอำนาจให้ชัดเจนว่ามีอำนาจในการเสนอราคาแทนหรือทำการในเรื่องใด โดยมีหลักฐานแสดงตัวตนของผู้มอบอำนาจและผู้รับมอบอำนาจ (แนบสำเนาบัตรประจำตัวประชาชนผู้มอบอำนาจและผู้รับมอบอำนาจพร้อมรับรองสำเนาถูกต้อง) ทั้งนี้ หากผู้รับมอบอำนาจเป็นบุคคลธรรมดาต้องเป็นผู้ที่บรรลุนิติภาวะตามกฎหมายแล้วเท่านั้น

(2) แคตตาล็อกและ/หรือแบบรูปรายการรายละเอียดคุณลักษณะเฉพาะ (ถ้ามี)

(3) ผู้ยื่นข้อเสนอต้องจัดทำตารางเปรียบเทียบคุณสมบัติของผู้ยื่นข้อเสนอ รายละเอียดคุณลักษณะเฉพาะ และการรับประกัน (ถ้ามี) ตาม TOR นี้ กับข้อเสนอของผู้ยื่นข้อเสนอ ซึ่งคุณลักษณะเฉพาะจะต้องระบุหัวข้อให้ถูกต้องตรงกันกับเอกสารหรือแคตตาล็อกที่เสนอโดยให้จัดทำในรูปแบบดังต่อไปนี้

ลำดับ	ข้อกำหนดตาม TOR	ความสอดคล้อง	รายละเอียดข้อเสนอ	เอกสารอ้างอิง
	▪ คัดลอกคุณสมบัติของผู้ยื่นข้อเสนอ ▪ คัดลอกข้อกำหนดรายละเอียดคุณลักษณะเฉพาะของพัสดุตามที่กำหนดใน TOR ▪ คัดลอกการรับประกัน	▪ ตรงหรือดีกว่าข้อกำหนดตาม TOR	▪ ระบุคุณสมบัติผู้ยื่นข้อเสนอ ▪ ระบุรายการและรายละเอียดคุณลักษณะเฉพาะของพัสดุที่เสนอมาให้พิจารณา ▪ ระบุรายละเอียดการรับประกันพัสดุที่เสนอมาให้พิจารณา	▪ ระบุเลขหน้าของเอกสารอ้างอิงหรือแคตตาล็อก

(6) จากข้อ 4.1.1,4.1.2 และ 4.1.3 ผู้เสนอราคาต้องมีหนังสือแต่งตั้งการเป็นตัวแทนจำหน่ายจากบริษัทเจ้าของผลิตภัณฑ์ที่มีสาขาในประเทศไทยโดยตรง และมีเอกสารรับรองว่าอุปกรณ์ที่เสนอเป็นอุปกรณ์ใหม่ ไม่เคยถูกใช้งานมาก่อน และยังอยู่ในสายการผลิต

6. การเสนอราคา

6.1 ผู้ยื่นข้อเสนอต้องยื่นข้อเสนอและเสนอราคาโดยไม่มีเงื่อนไขใด ๆ ทั้งสิ้น

6.2 ราคาที่เสนอจะต้องเป็นราคาที่รวมภาษีมูลค่าเพิ่มและภาษีอื่น (ถ้ามี) รวมค่าใช้จ่ายทั้งปวงไว้ด้วยแล้ว

6.3 ผู้ยื่นข้อเสนอต้องยืนราคาเป็นเวลาไม่น้อยกว่า 90 วัน นับตั้งแต่วันที่เสนอราคา โดยภายในกำหนดยืนราคา ผู้ยื่นข้อเสนอจะต้องรับผิดชอบราคาที่ตนเสนอไว้ และถอนการเสนอราคามิได้

6.4 ผู้ยื่นข้อเสนอจะต้องดำเนินการส่งมอบพัสดุไม่เกิน 90 วัน นับถัดจากวันลงนามในสัญญาหรือวันที่ได้รับหนังสือแจ้งจาก กบข. ให้ส่งมอบพัสดุ

6.5 กรณีงานจัดซื้อที่ประกอบด้วยพัสดุหลายประเภทในโครงการเดียวกัน ผู้เสนอราคาต้องแยกราคาต่อหน่วยของพัสดุแต่ละประเภท (**cost breakdown)** ให้ชัดเจน (ถ้ามี)

7. **หลักเกณฑ์และสิทธิในการพิจารณา**

7.1 การพิจารณาผลการยื่นข้อเสนอครั้งนี้ กบข. จะพิจารณาตัดสินโดยใช้หลักเกณฑ์คะแนนรวมด้านคุณภาพและด้านราคาสูงที่สุด (Price Performance) ในการพิจารณาผู้ชนะการยื่นข้อเสนอ กบข. จะพิจารณาโดยให้คะแนนตามปัจจัยหลักและน้ำหนักที่กำหนด ดังต่อไปนี้

1. ราคาที่ยื่นข้อเสนอ (price) กำหนดน้ำหนักเท่ากับร้อยละ 40
2. ข้อเสนอด้านเทคนิค กำหนดน้ำหนักเท่ากับร้อยละ 60

โดยแบ่งหัวข้อการพิจารณาออกเป็น 4 หัวข้อย่อย ดังนี้

1) ความน่าเชื่อถือ ผลงาน และความมั่นคงของผู้ยื่นข้อเสนอ (5 คะแนน)

- เอกสารรายละเอียดของผู้ยื่นข้อเสนอ (Company Profile)
- เอกสารแสดง ผลงาน ที่สอดคล้องกับขอบเขตการดำเนินงานตาม TOR นี้

2) ภาพรวมด้านการออกแบบ (ผลิตภัณฑ์) รายละเอียดระบบรักษาความปลอดภัย Firewall และระบบศูนย์กลางบริหารจัดการระบบรักษาความปลอดภัย Firewall (20 คะแนน)

- เอกสารแสดงสถาปัตยกรรมของระบบฯ ที่นำเสนอ
- เอกสารแสดงรายงานผลการวิจัยเชิงคุณภาพหรือความมั่นคง ของผลิตภัณฑ์ในตลาดปลอดภัย รวมทั้งทิศทาง พัฒนาการของเทคโนโลยี และผู้มีส่วนร่วมกับผลิตภัณฑ์ที่นำเสนอ

3) รูปแบบ ด้านการออกแบบ (ผู้เสนอราคาออกแบบให้สอดคล้องกับโครงสร้างพื้นฐานของ กบข.) แผนงานการติดตั้งสำหรับ กบข. (20 คะแนน)

- เอกสารการบริหารโครงการติดตั้งระบบฯ
- เอกสารแสดงแผนผัง Network Diagram ที่จะออกแบบให้ กบข.
- รายละเอียดการจัดเตรียมเจ้าหน้าที่ตามตำแหน่งหน้าที่ของผู้ติดตั้งระบบฯเพื่อดำเนินการตามแผนงาน
- รายละเอียดเจ้าหน้าที่ประจำผู้มีความชำนาญ ประวัติการศึกษาและประกาศนียบัตรของผู้ติดตั้งระบบฯบอกถึงระดับของความรู้และประสบการณ์ที่เกี่ยวข้อง

4) รายละเอียดการบริการและความพร้อมให้บริการ (Service Availability) (10 คะแนน)

- เอกสารรายละเอียดบริการแจ้งเหตุขัดข้องระบบฯ
- เอกสารที่แสดงถึงการกำหนดข้อตกลงความพร้อมให้บริการ (Service Availability)
- รายละเอียดการจัดเตรียมเจ้าหน้าที่ตามตำแหน่งหน้าที่ของผู้ให้บริการบำรุงรักษาเพื่อดำเนินการตามแผนงาน
- รายละเอียดเจ้าหน้าที่ผู้ให้บริการบำรุงรักษาประจำ ผู้มีความชำนาญ ประวัติการศึกษาและประกาศนียบัตร บอกถึงระดับของความรู้และประสบการณ์ที่เกี่ยวข้อง

5) พิจารณาราคาสิทธิ์การใช้งาน Hardware/Software และบริการบำรุงรักษาหลังหมดระยะเวลารับประกัน (5 คะแนน)

- เอกสารใบเสนอราคา สิทธิ์การใช้งาน Hardware/Software และบริการบำรุงรักษาหลังหมดระยะเวลารับประกัน

8. การทำสัญญาซื้อขาย

ผู้ชนะการคัดเลือกจะต้องทำสัญญาซื้อขายตามแบบที่ กบข. กำหนด ภายใน 15 วัน นัดถัดจากวันที่ได้รับแจ้ง และจะต้องวางหลักประกันสัญญาเป็นเงินเท่ากับร้อยละ 5 ของราคาค่าสิ่งของที่ซื้อ

9. ค่าจ้างและการจ่ายเงิน

กบข. จะจ่ายค่าสิ่งของซึ่งได้รวมภาษีมูลค่าเพิ่ม ภาษีอากรอื่น และค่าใช้จ่ายทั้งปวงให้แก่ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกให้เป็นผู้ขายภายใน 30 วัน เมื่อผู้ขายได้ส่งมอบสิ่งของและ กบข. ได้ตรวจรับมอบสิ่งของไว้เรียบร้อยแล้ว ตามรายการรายละเอียดพัสดุข้อ 4.1 ถึง 4.2 ดำเนินการติดตั้งได้ครบถ้วนตามรายการรายละเอียดพัสดุข้อ 4.3 พร้อมทั้ง กบข. ได้รับหนังสือเรียกเก็บเงินจากผู้ขายและผู้ขายจะต้องทำข้อมูล

เปรียบเทียบสิ่งของที่ส่งมอบกับสิ่งของตามที่สัญญากำหนดว่าส่งมอบได้ครบถ้วนหรือไม่ โดยให้จัดทำในรูปแบบดังต่อไปนี้

ลำดับ	ข้อกำหนดตาม TOR	ความสอดคล้อง	รายละเอียดข้อเสนอ	เอกสารอ้างอิง
	▪ คัดลอกข้อกำหนดของพัสดุที่ต้องส่งมอบตาม TOR	▪ ตรงตามข้อกำหนดของ TOR หรือดีกว่า	▪ ระบุรายละเอียดของพัสดุที่เสนอส่งมอบ	▪ ระบุเลขหน้าของเอกสารอ้างอิง

10. อัตราค่าปรับ

ค่าปรับตามสัญญาซื้อขายหรือข้อตกลงจ้างเป็นหนังสือให้คิดในอัตราร้อยละ 0.20 ของราคาค่าสิ่งของที่ยังไม่ได้รับมอบต่อวัน

11. การรับประกันความชำรุดบกพร่อง

ผู้ชนะการคัดเลือกจะต้องรับประกันความชำรุดบกพร่องของงานที่เกิดขึ้นเป็นระยะเวลาไม่น้อยกว่า 1 ปี ถ้าหากปรากฏว่ามีความชำรุดบกพร่องของงานที่ส่งมอบเกิดขึ้น ต้องรีบจัดการซ่อมแซมแก้ไขให้ใช้การได้ดีดังเดิมภายใน 1 วัน นับถัดจากวันที่ได้รับแจ้งความชำรุดบกพร่อง

ผู้ขายมีหน้าที่บำรุงรักษาและซ่อมแซมแก้ไขระบบรักษาความปลอดภัย Firewall และระบบศูนย์กลางบริหารจัดการระบบรักษาความปลอดภัย Firewall ให้อยู่ในสภาพใช้งานได้ดีอยู่เสมอตลอดระยะเวลาดังกล่าวในวรรคหนึ่งด้วยค่าใช้จ่ายของผู้ขาย โดยให้มีเวลาระบบรักษาความปลอดภัย Firewall และระบบศูนย์กลางบริหารจัดการระบบรักษาความปลอดภัย Firewall ขัดข้องรวมตามเกณฑ์การคำนวณเวลาขัดข้องไม่เกินร้อยละ 5 (ห้า) ของเวลาใช้งานทั้งหมดของระบบรักษาความปลอดภัย Firewall และระบบศูนย์กลางบริหารจัดการระบบรักษาความปลอดภัย Firewall ของเดือนนั้น มิฉะนั้นผู้ขายต้องยอมให้ผู้จ้างคิดค่าปรับเป็นรายชั่วโมงในอัตราร้อยละ 0.035 ของค่าจัดซื้อ ระบบรักษาความปลอดภัย Firewall และระบบศูนย์กลางบริหารจัดการระบบรักษาความปลอดภัย Firewall และพร้อมติดตั้ง ทั้งหมดตามสัญญานี้ ในช่วงเวลาที่ไม่สามารถใช้ระบบรักษาความปลอดภัย Firewall และระบบศูนย์กลางบริหารจัดการระบบรักษาความปลอดภัย Firewall ได้ในส่วนที่เกินกว่ากำหนดเวลาขัดข้องข้างต้น

เกณฑ์การคำนวณเวลาขัดข้องของระบบรักษาความปลอดภัย Firewall และระบบศูนย์กลางบริหารจัดการระบบรักษาความปลอดภัย Firewall ตามวรรคสอง ให้เป็นดังนี้

- กรณีที่ระบบรักษาความปลอดภัย Firewall และระบบศูนย์กลางบริหารจัดการระบบรักษาความปลอดภัย Firewall เกิดขัดข้องของระบบฯพร้อมกันหลายหน่วย ให้นับเวลาขัดข้องของหน่วยที่มีตัวถ่วงมากที่สุดเพียงหน่วยเดียว

- กรณีความเสียหายอันสืบเนื่องมาจากความขัดข้องของระบบรักษาความปลอดภัย Firewall และระบบศูนย์กลางบริหารจัดการระบบรักษาความปลอดภัย Firewall แตกต่างกัน เวลาที่ใช้ในการคำนวณค่าปรับจะเท่ากับเวลาขัดข้องของระบบฯหน่วยนั้นคูณด้วยตัวถ่วงซึ่งกำหนดตัวถ่วงน้ำหนักมีค่า = 1

12. วงเงินในการจัดซื้อ

วงเงินในการจัดซื้อครั้งนี้เป็นเงิน 7,000,000 บาท (เจ็ดล้านบาทถ้วน) ซึ่งรวมภาษีมูลค่าเพิ่ม ภาษีอากรอื่น และค่าใช้จ่ายทั้งปวงด้วยแล้ว

13. ข้อสงวนสิทธิ์ในการยื่นข้อเสนอและอื่น ๆ

ผู้ยื่นข้อเสนอซึ่ง กบข. ได้คัดเลือกแล้ว ไม่ไปทำสัญญาหรือข้อตกลงซื้อเป็นหนังสือภายในเวลาที่กำหนด กบข. จะริบหลักประกันการยื่นข้อเสนอ (ถ้ามี) หรือเรียกร้องจากผู้ออกหนังสือค้ำประกันการยื่นเสนอราคาทันที และอาจพิจารณาเรียกร้องให้ชดใช้ความเสียหายอื่น (ถ้ามี) รวมทั้งจะพิจารณาให้เป็นผู้ทิ้งงานตามระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ

14. มาตรการป้องกันการทุจริตและประพฤติมิชอบ

ด้วย กบข. มีนโยบายต่อต้านการทุจริตและประพฤติมิชอบที่บั่นทอนเศรษฐกิจและสังคมของประเทศ กบข. ไม่ยอมรับการทุจริตและประพฤติมิชอบทุกรูปแบบ (Zero Tolerance) ไม่ว่าจะเป็นการกระทำโดยบุคลากรของ กบข. หรือบริษัทในเครือของ กบข. หรือบุคคลที่เกี่ยวข้องกับกิจการของ กบข. ซึ่งรวมถึงคู่ค้าของ กบข. ทุกราย นอกจากนี้ กบข. ยังยึดมั่นในการดำเนินธุรกิจอย่างมีจริยธรรม จรรยาบรรณ และรับผิดชอบต่อสังคมและผู้มีส่วนได้เสียทุกกลุ่มด้วย

กบข. จึงขอความร่วมมือจากผู้ยื่นข้อเสนอ หากพบเห็นการกระทำของบุคลากรของ กบข. หรือบริษัทในเครือของ กบข. หรือบุคคลที่เกี่ยวข้องกับกิจการของ กบข. หรือคู่ค้าของ กบข. รายใดที่มีการกระทำเข้าข่ายทุจริต ติดสินบน หรือเรียกรับเงิน ทรัพย์สินหรือประโยชน์อื่นใดที่ไม่เหมาะสม ไม่ว่าในรูปแบบใด ขอให้แจ้งโดยตรงไปยังบุคคลและที่อยู่ดังต่อไปนี้

“ประธานอนุกรรมการตรวจสอบ
ฝ่ายตรวจสอบภายใน กองทุนบำเหน็จบำนาญข้าราชการ
เลขที่ 990 อาคารอับดุลราฮิม เพลส ถนนพระราม 4
แขวงสีลม เขตบางรัก กรุงเทพมหานคร 10500”

15. ผู้จัดทำขอบเขตของงาน (Terms of Reference : TOR)

1. นายวัชรพงศ์ ชัยกิจ
