Phần 2. YÊU CẦU VỀ KỸ THUẬT

Chương V. YÊU CẦU VỀ KỸ THUẬT

Mục 1. Yêu cầu về kỹ thuật

1.1. Giới thiệu chung về dự toán mua sắm, gói thầu

a) giới thiệu chung:

- Tên dự toán: Cập nhật các phần mềm bảo mật;
- Tên gói thầu: Cập nhật các phần mềm bảo mật;
- Chủ Đầu tư: Cục Công nghệ thông tin - Bộ Tư pháp;
- Địa điểm thực hiện: Cục Công nghệ thông tin - Bộ Tư pháp, số 60 Trần Phú, phường Ba Đình, thành phố Hà Nội.
- Nguồn vốn: Ngân sách nhà nước;
- Hình thức lựa chọn nhà thầu: Đấu thầu rộng rãi qua mạng trong nước;
- Phương thức lựa chọn nhà thầu: Một giai đoạn một túi hồ sơ;
- Thời gian bắt đầu tổ chức lựa chọn nhà thầu: Quý II/2026;
- Thời gian tổ chức lựa chọn nhà thầu: 30 ngày;
- Loại hợp đồng: Trọn gói;
- Thời gian thực hiện gói thầu: 15 ngày

b) Mục tiêu:

Cập nhật phần mềm bảo mật cho các các thiết bị, giải pháp tại Trung tâm dữ liệu điện tử của Bộ Tư pháp nhằm hoạt động liên tục, thông suốt, đảm bảo an toàn an ninh thông tin.

1.2. Yêu cầu về kỹ thuật

a) Yêu cầu chung về kỹ thuật:

- Hàng hóa đảm bảo chất lượng, chính hãng có nguồn gốc xuất xứ rõ ràng;
- Hàng hóa hợp pháp và được lưu hành hợp pháp tại Việt Nam;
- Đơn vị cung cấp hoàn toàn chịu trách nhiệm về mọi thiệt hại phát sinh do việc khiếu nại của bên thứ ba về việc vi phạm bản quyền sở hữu trí tuệ liên quan đến hàng hóa mà đơn vị đã cung cấp;
- Tuân thủ các quy định về tiêu chuẩn hiện hành tại quốc gia hoặc vùng lãnh thổ mà hàng hóa có xuất xứ.

b) Yêu cầu về kỹ thuật cụ thể:

Stt	Danh mục hàng hóa	Yêu cầu kỹ thuật tối thiểu
1	**Gia hạn bản quyền Phần mềm quét virus quản lý tập trung cho máy trạm và máy chủ vật lý với số lượng 800 users**	
1.1	License phần mềm BCY Endpoint Security (12 tháng)	- Khả năng phát hiện và phòng chống mã độc: + Phát hiện theo hành vi (Heuristic analysis) + Công nghệ phân tích tự động

Stt	Danh mục hàng hóa	Yêu cầu kỹ thuật tối thiểu
		+ Phát hiện dựa trên Machine Learning & Big Data + Nhận diện theo mẫu (Signature-based) - Khả năng phòng chống tấn công nâng cao: + Chống tấn công bắc cầu (Anti-Bridging) + Ngăn chặn khai thác lỗ hổng (Exploit Prevention) + Bảo vệ email khỏi mã độc + Lọc và kiểm soát truy cập web + Chống phishing + Chống mã hóa dữ liệu (Ransomware protection) + Phòng chống APT - Kiểm soát thiết bị và người dùng: + Kiểm soát thiết bị ngoại vi + Kiểm soát ứng dụng + Kiểm soát theo chính sách nhóm - Quản lý tập trung và vận hành: + Quản lý tập trung + Tự động cập nhật cơ sở dữ liệu + Triển khai nhanh (1-click install) vào 1 file cài đặt standalone + Kiểm soát toàn bộ chức năng của phần mềm Endpoint Client tại máy trạm - Khả năng tích hợp hệ thống: + Tích hợp SIEM + Tích hợp AD/LDAP - Giám sát và báo cáo: + Giám sát trạng thái Endpoint + Giám sát tình hình virus toàn hệ thống + Chức năng báo cáo thống kê tình hình virus cho người quản trị, người dùng + Xuất báo cáo theo định dạng PDF, HTML
2	**Giải pháp bảo đảm an toàn thông tin cho hệ thống thư điện tử Pineapp Mailsecure (Cyfox Mailsecure) cho 2000 users (12 tháng)**	
2.1	Pineapp Mailsecure (Cyfox Mailsecure) cho 2000 users	- Hỗ trợ tối thiểu các tính năng: + Phát hiện & Ngăn chặn Email Phishing + Chống giả mạo (Anti-Spoofing) + Xác thực email (Email Messaging Authentication) + Quản lý lưu lượng email (Email traffic) + Hỗ trợ LDAP (LDAP Support)
3	**Gia hạn bảo hành thiết bị tường lửa Check Point - GÓI NGFW (Next**	

Stt	Danh mục hàng hóa	Yêu cầu kỹ thuật tối thiểu
	Generation Firewall)	
3.1	Thiết bị tường lửa vùng mạng internet: Check Point 6700 – Base. (Thời gian gia hạn bảo hành 12 tháng). Serial Number: 2223BA5517 & 2223BA5520	- Hardware Maintenance: Renewal Co-Standard Support for 6700 Base Appliance with SandBlast subscription package for 1 year (Số lượng: 02) - Hardware Maintenance: Renewal Co-Standard Support for 4 Port 10GBase-F SFP+ interface card for 6000, 7000, 16000, 26000 and 28000 series. Requires an additional 10GBase SFP+ transceiver (Số lượng: 02) - Hardware Maintenance: Renewal Co-Standard Support for Replacement AC Power Supply for 6600/6700/6900 series appliances (Số lượng: 02) - Hardware Maintenance: Renewal Co-Standard Support for SFP+ transceiver for 10G fiber Ports - short range (10GBase-SR) (Số lượng: 08) - Software Subscription: Next Generation Firewall Package for additional 1 year for 6700 Base Appliance (Số lượng: 02) **Tính năng :** - Kiểm soát ứng dụng (Application Control) : Hỗ trợ nhận diện và kiểm soát ít nhất 10,000 ứng dụng có sẵn - Tính năng phòng chống xâm nhập (IPS) : + Có tính năng phòng chống xâm nhập (IPS) với khả năng phát hiện ngăn chặn thực thi các lỗ hổng đã biết, DNS Tunneling, DoS… + Phương thức phát hiện: Vulnerability and exploit signatures, Protocol validation, Anomaly detection, behavioral analysis + Có khả năng phát hiện tấn công tấn công theo mức độ, tấn công từ chối dịch vụ DoS, tấn công điểm yếu ứng dụng, tấn công điểm yếu hệ điều hành - Tính năng kiểm soát nội dung : + Cho phép thiết lập chính sách kiểm soát việc upload/download dựa trên loại nội dung và định dạng dữ liệu. - Tính năng Site-to-site VPN : + Hỗ trợ triển khai Site-to-Site VPN với các mô hình Star, Mesh. + Hỗ trợ định tuyến lưu lượng VPN thông qua Domain Based VPN và Route Based VPN + Hỗ trợ khả năng tìm đường đi tối ưu cho lưu lượng VPN

Stt	Danh mục hàng hóa	Yêu cầu kỹ thuật tối thiểu
		+ Hỗ trợ khả năng lựa chọn các cổng kết nối được dùng cho VPN kết nối tới nội bộ và bên ngoài. + Khả năng chia sẻ tải để phân phối đồng đều lưu lượng VPN - Tính năng SSL VPN: Hỗ trợ tính năng SSL VPN - Chính sách kiểm soát người dùng (User-based Policy) : + Khả năng tích hợp với Microsoft AD, LDAP, RADIUS + Cho phép thiết lập chính sách trên thông tin định danh người dùng, hoặc nhóm người dùng - Tính năng giải mã hoá : + Hỗ trợ HTTPS Inspection, với TLS 1.3, theo chiều outbound, inbound, và chia sẻ dữ liệu đã giải mã các thiết bị khác. Hỗ trợ HTTPS Inspection trên các cổng không theo tiêu chuẩn. + Có menu riêng để cấu hình chính sách giải mã HTTPS, độc lập với cấu hình chính sách kiểm soát truy cập. - Tính sẵn sàng cao : Hỗ trợ các cơ chế hoạt động: +Active/Active L2, Active/Passive L2 and L3 + Cluster, VRRP - Các tính năng định tuyến Unicas và Multicast : + Hỗ trợ các giao thức định tuyến động: OSPFv2 and v3, BGP, RIP + Static routes, Multicast routes + Policy-based routing + PIM-SM, PIM-SSM, PIM-DM, IGMP v2, and v3 - Sao lưu dự phòng: Hỗ trợ cơ chế Backup cấu hình và Snapshot toàn bộ hệ thống giúp tối ưu vận hành
3.2	Thiết bị tường lửa vùng mạng trung tâm: Check Point 6600 – Plus (Thời gian gia hạn bảo hành 12 tháng). Serial Number: 2245BA2260 & 2245BA245	- Hardware Maintenance: Renewal Co-Standard Support for 6600 Plus appliance with SandBlast subscription package for 1 year (Số lượng: 02) - Software Subscription: Next Generation Firewall Package for additional 1 year for 6600 PLUS Appliance (Số lượng: 02) Tính năng : - Kiểm soát ứng dụng (Application Control): Hỗ trợ nhận diện và kiểm soát ít nhất 10,000 ứng dụng có sẵn - Tính năng phòng chống xâm nhập (IPS):

Stt	Danh mục hàng hóa	Yêu cầu kỹ thuật tối thiểu
		+ Có tính năng phòng chống xâm nhập (IPS) với khả năng phát hiện ngăn chặn thực thi các lỗ hổng đã biết, DNS Tunneling, DoS… + Phương thức phát hiện: Vulnerability and exploit signatures, Protocol validation, Anomaly detection, behavioral analysis + Có khả năng phát hiện tấn công tấn công theo mức độ, tấn công từ chối dịch vụ DoS, tấn công điểm yếu ứng dụng, tấn công điểm yếu hệ điều hành - Tính năng kiểm soát nội dung : + Cho phép thiết lập chính sách kiểm soát việc upload/download dựa trên loại nội dung và định dạng dữ liệu. - Tính năng Site-to-site VPN : + Hỗ trợ triển khai Site-to-Site VPN với các mô hình Star, Mesh. + Hỗ trợ định tuyến lưu lượng VPN thông qua Domain Based VPN và Route Based VPN + Hỗ trợ khả năng tìm đường đi tối ưu cho lưu lượng VPN + Hỗ trợ khả năng lựa chọn các cổng kết nối được dùng cho VPN kết nối tới nội bộ và bên ngoài. + Khả năng chia sẻ tải để phân phối đồng đều lưu lượng VPN - Tính năng SSL VPN: Hỗ trợ tính năng SSL VPN - Chính sách kiểm soát người dùng (User-based Policy): + Khả năng tích hợp với Microsoft AD, LDAP, RADIUS + Cho phép thiết lập chính sách trên thông tin định danh người dùng, hoặc nhóm người dùng - Tính năng giải mã hoá : + Hỗ trợ HTTPS Inspection, với TLS 1.3, theo chiều outbound, inbound, và chia sẻ dữ liệu đã giải mã các thiết bị khác. Hỗ trợ HTTPS Inspection trên các cổng không theo tiêu chuẩn. + Có menu riêng để cấu hình chính sách giải mã HTTPS, độc lập với cấu hình chính sách kiểm soát truy cập. - Tính sẵn sàng cao : Hỗ trợ các cơ chế hoạt động: +Active/Active L2, Active/Passive L2 and L3 + Cluster, VRRP

Stt	Danh mục hàng hóa	Yêu cầu kỹ thuật tối thiểu
		- Các tính năng định tuyến Unicas và Multicast : + Hỗ trợ các giao thức định tuyến động: OSPFv2 and v3, BGP, RIP + Static routes, Multicast routes + Policy-based routing + PIM-SM, PIM-SSM, PIM-DM, IGMP v2, and v3 - Sao lưu dự phòng: Hỗ trợ cơ chế Backup cấu hình và Snapshot toàn bộ hệ thống giúp tối ưu vận hành
4	**Thiết bị tường lửa ứng dụng: Imperva X2520 Web Application Firewall**	
4.1	Gia hạn bảo hành thiết bị Imperva X2520 Web Application Firewall (thời gian gia hạn bảo hành 12 tháng). Serial number: 2245BA0126	- Hardware Maintenance: X2520 Web Application Firewall, Annual Enhanced Support (Số lượng: 01) - Hardware Maintenance SSL Accelerator Card - Mid Capacity for X2520/X4520/ X6520, Annual Enhanced Support (Số lượng: 01) - Hardware Maintenance: 10 Gigabit Ethernet Network Interface Card - PCIE- Dual SR Fiber Bypass for X2520 / X4520 / X6520 /X8520 / X10K2, Annual Enhanced Support (Số lượng: 01) - Software Subscription VM150 Management Server Virtual Appliance, Annual Enhanced Subscription (Số lượng: 01) **Tính năng:** + Cho phép quản trị thông qua giao diện Web User Interface, API + Cho phép cấu hình cảnh báo qua email + Cho phép thực hiện tạo báo cáo có khả năng tùy chỉnh nội dung theo nhu cầu, có sẵn các báo cáo mẫu và có thể trích xuất dưới dạng PDF, CSV + Cho phép tạo và phần quyền người dùng theo vai trò + Cho phép đăng xuất tài khoản của người dùng và ngắt hiệu lực của tài khoản đăng nhập vào trang quản trị hệ thống + Cho phép xuất log ra hệ thống SIEM bằng syslog + Cho phép ẩn các dữ liệu ví dụ như số tài khoản, mã PIN, mật khẩu,… trong phần nhật ký log để tránh lộ lọt thông tin. + Phần mềm quản trị cài đặt được trên các môi trường Vmware

1.3. Các yêu cầu khác:

1.3.1. Yêu cầu về triển khai cung cấp hàng hóa:

- Tích hợp với hệ thống bảo mật, đảm bảo không ảnh hưởng hoạt động hệ thống hiện có của Chủ đầu tư;

- Trong quá trình thực hiện cài đặt cung cấp hàng hóa, nhà thầu phải đảm bảo dữ liệu an toàn, nguyên vẹn;

- Đối với các phần mềm (License) cung cấp phải là phiên bản thương mại mới nhất tính đến thời điểm dự thầu hoặc tương thích với các hệ thống sẵn có của Chủ đầu tư. Đồng thời trong quá trình cung cấp hàng hóa, nhà thầu phải cập nhật miễn phí các bản vá lỗi và các phiên bản nâng cấp nhỏ từ nhà sản xuất nếu có

- Nhà thầu cử cán bộ kỹ thuật thực hiện cập nhật phần mềm bảo mật cho các trang thiết bị và giải pháp đảm bảo an toàn thông tin

- Trong suốt thời gian cung cấp hàng hóa, nhà thầu phải cam kết bố trí nhân sự hỗ trợ kỹ thuật từ xa 24 giờ/ngày + 7 ngày/tuần trong thời gian thực hiện hợp đồng và phải đảm bảo đưa ra phương án xử lý sự cố trong vòng 01 giờ kể từ khi nhận được yêu cầu của đơn vị sử dụng vào bất kỳ thời điểm nào;

- Địa điểm triển khai cập nhật các phần mềm bảo mật và hỗ trợ kỹ thuật: Cục Công nghệ thông tin - Bộ Tư pháp, số 60 Trần Phú, phường Ba Đình, thành phố Hà Nội;

- Hình thức sở hữu: bản quyền phải được đăng ký dưới tên của đơn vị sử dụng do Chủ đầu tư yêu cầu;

- Nhà thầu phải cam kết đáp ứng các yêu cầu về đảm bảo an toàn thông tin theo: Luật An toàn thông tin mạng số 86/2015/QH13; Nghị định 85/2016/NĐ-CP ngày 01/07/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ; Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 Quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/07/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

- Trong trường hợp trúng thầu, nhà thầu phải cung cấp Giấy phép hoặc Giấy ủy quyền bán hàng của nhà sản xuất, đại lý phân phối hoặc Giấy chứng nhận quan hệ đối tác hoặc tài liệu khác có giá trị tương đương nhằm chứng minh nhà thầu được ủy quyền hợp lệ của nhà sản xuất, đại lý phân phối để cung cấp hàng hóa.

1.3.2. Yêu cầu về bảo đảm chất lượng hàng hóa:

Stt	Nội dung	Yêu cầu
1	Biện pháp tổ chức cung cấp hàng hóa	Nhà thầu có biện pháp tổ chức cung cấp hàng hóa cụ thể (thuyết minh chi tiết) khả thi và đảm bảo không làm ảnh hưởng hoạt động hệ thống CNTT của Chủ đầu tư, bao gồm đầy đủ nội dung: + Tổ chức nhân sự, + Phương án cung cấp, + Bảo hành hỗ trợ kỹ thuật, đầu mối hỗ trợ 24x7 cụ thể (email, điện thoại)
2	Biện pháp bảo đảm chất	Nhà thầu có biện pháp bảo đảm chất lượng hàng hóa cụ thể (thuyết minh chi tiết) phù hợp, bao gồm

Stt	Nội dung	Yêu cầu
	lượng dịch vụ	Quy trình cung cấp, Kiểm tra thử nghiệm

1.3.3. Yêu cầu về bảo hành, hỗ trợ kỹ thuật:

- Nội dung bảo hành, hỗ trợ kỹ thuật:

+ Bảo hành, Hỗ trợ kỹ thuật 24x7 trong suốt thời gian cung cấp dịch vụ;

+ Bảo hành, hỗ trợ kỹ thuật hàng hóa theo tiêu chuẩn quy định của Nhà sản xuất;

+ Địa điểm Bảo hành, hỗ trợ kỹ thuật: Tại vị trí khách hàng.

- Hỗ trợ an toàn bảo mật: Có giải pháp hỗ trợ an toàn bảo mật cụ thể (thuyết minh chi tiết) phù hợp hệ thống mạng CNTT của Chủ đầu tư, bao gồm:

+ Đảm bảo an toàn bảo mật cho hệ thống mạng CNTT.

+ Hỗ trợ quản trị, xử lý trực tiếp tại địa điểm của Chủ đầu tư.

Mục 2. Bản vẽ

Không có.

Mục 3. Kiểm tra và thử nghiệm

Các kiểm tra và thử nghiệm cần tiến hành gồm có:

- Kiểm tra hàng hóa về số lượng, chất lượng.
- Kiểm tra tính năng hàng hóa
- Các kiểm tra khác theo yêu cầu Chủ đầu tư.