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

- Tên gói thầu: Mua sắm bản quyền, thiết bị và triển khai dịch vụ mạng bảo mật cho các đơn vị của Cục DTNN

- Phạm vi gói thầu:

(1) Nhiệm vụ: Trang bị bổ sung giải pháp bảo mật tại Cục DTNN đáp ứng yêu cầu về an toàn thông tin

- Thời gian thực hiện: Năm 2025-2026

- Đặc điểm, quy mô:

+ Trang bị thiết bị chống tấn công DDoS chuyên dụng: 01 bộ, bảo hành chính hãng 03 năm, kèm dịch vụ triển khai cài đặt tại đơn vị sử dụng.

+ Trang bị bản quyền phần mềm tẩy xóa dữ liệu: 01 bộ, bảo hành chính hãng 03 năm.

(2) Nhiệm vụ: Gia hạn bản quyền cập nhật Antivirus tại các đơn vị và dịch vụ hỗ trợ chính hãng giai đoạn 2025 – 2027

- Thời gian thực hiện: Năm 2025-2027

- Đặc điểm, quy mô: Gia hạn bản quyền cập nhật Antivirus tại các đơn vị và dịch vụ hỗ trợ chính hãng, gồm:

+ 1.300 license,trong đó:150 máy chủ, 1.150 máy trạm và máy tính xách tay.

+ Dịch vụ hỗ trợ kỹ thuật chính hãng.

+ Thời gian cập nhật: 02 năm (24 tháng liên tục)

(3) Nhiệm vụ: Gia hạn bản quyền phần mềm bảo mật hệ thống ảo hóa và dịch vụ hỗ trợ chính hãng giai đoạn 2025 – 2027.

- Thời gian thực hiện: Năm 2025-2027

- Đặc điểm, quy mô: Gia hạn bản quyền phần mềm bảo mật hệ thống ảo hoá và hỗ trợ chính hãng gồm:

+ Bản quyền phần mềm bảo mật hệ thống ảo hóa cho 26 CPU vật lý

+ Dịch vụ hỗ trợ kỹ thuật chính hãng.

+ Thời gian cập nhật: 02 năm (24 tháng liên tục)

(4) Nhiệm vụ: Thay thế giải pháp mạng, bảo mật tại Cục DTNN.

- Thời gian thực hiện: Năm 2025-2026

- Đặc điểm, quy mô:

+ Thay thế thiết bị tường lửa mạng lõi: 02 bộ, bảo hành chính hãng 03 năm, kèm dịch vụ triển khai cài đặt, lắp đặt tại đơn vị sử dụng.

+ Thay thế thiết bị cân bằng tải tích hợp tính năng WAF: 01 bộ, bảo hành chính hãng 03 năm, kèm dịch vụ triển khai cài đặt, lắp đặt tại đơn vị sử dụng.

(5) Nhiệm vụ: Bảo hành mở rộng và bản quyền phần mềm cho các thiết bị mạng, bảo mật của Cục DTNN.

- Thời gian thực hiện: Năm 2025

- Đặc điểm, quy mô:

+ Bảo hành mở rộng và license cho các thiết bị phòng chống tấn công APT trang bị năm 2018 thời gian 03 năm: *(1) 01 x thiết bị phòng chống tấn công APT qua đường Internet; (2) 01 x thiết bị chống tấn công APT qua đường email; (3) 01 x Thiết bị quản trị tập trung các thiết bị APT.*

+ Bảo hành mở rộng cho thiết bị Switch và Firewall tại các Chi cục DTNN trang bị năm 2018 thời gian 03 năm: *(1) 15 x Bảo hành mở rộng thiết bị chuyển mạch Juniper Ex2300-24T chính hãng; (2) 15 x Bảo hành mở rộng thiết bị Firewall Juniper SRX340 chính hãng.*

+ Bảo hành mở rộng và bản quyền phần mềm chi thiết bị Switch và Firewall tại các điểm kho trang bị năm 2019: *(1) 40 x Bảo hành mở rộng thiết bị chuyển mạch Juniper EX2300-24T chính hãng; (2) 42 x Bảo hành mở rộng và bản quyền phần mềm bảo mật cho thiết bị Firewall SRX300 chính hãng.*

(6) Nhiệm vụ: Bảo hành mở rộng thiết bị mạng, bảo mật tại Cục DTNN.

- Thời gian thực hiện: Năm 2025-2026

- Đặc điểm, quy mô: Bảo hành mở rộng và bản quyền phần mềm cho cho các thiết bị mạng, bảo mật tại Cục DTNN trang bị đưa vào sử dụng năm 2020 và 2019 để đảm bảo hoạt động an toàn thông tin, kết nối truy cập Internet, WAN, LAN của Cục DTNN, gồm:

+ Bảo hành mở rộng và license cho thiết bị Firewall cho vùng Internet (Juniper SRX 1500) tại Cục DTNN thời gian 03 năm: 02 thiết bị;

+ Bảo hành mở rộng và license cho thiết bị Firewall WAN (Juniper SRX 1500) tại Cục DTNN thời gian 03 năm: 02 thiết bị;

+ Bảo hành mở rộng thiết bị chuyển mạch Core (Juniper QFX10002-36Q) thời gian 03 năm: 01 thiết bị;

+ Bảo hành mở rộng thiết bị chuyển mạch cho máy chủ dịch vụ hạ tầng, Intranet (Juniper EX3400-48T) thời gian 03 năm: 02 thiết bị;

+ Bảo hành mở rộng thiết bị chuyển mạch cho vùng LAN (Juniper EX2300) thời gian 03 năm: 04 thiết bị.

- Địa điểm thực hiện: các đơn vị của Cục Dự trữ Nhà nước

1.2. Yêu cầu về kỹ thuật

1.2.1 Yêu cầu kỹ thuật chung

Tại E-HSDT, nhà thầu cam kết thực hiện các nội dung sau:

a. Chất lượng hàng hóa

Hàng hóa cung cấp phải là hàng hóa chính hãng, mới 100%, sản xuất từ năm 2025 trở về sau, được nhập khẩu đồng bộ nếu là hàng hóa sản xuất ở nước ngoài.

b. Tính hợp lệ của hàng hóa

Nhà thầu có cam kết khi bàn giao hàng hóa cho Chủ đầu tư, nhà thầu sẽ cung cấp các tài liệu chứng minh tính hợp lệ của hàng hóa:

+ Bản gốc hoặc Bản sao công chứng/chứng thực cho Giấy chứng nhận xuất xứ (CO) và Giấy chứng nhận chất lượng (CQ) đối với thiết bị nhập khẩu.

+ Bản gốc hoặc Bản sao công chứng/chứng thực cho Giấy chứng nhận xuất xưởng/Giấy chứng nhận chất lượng đối với thiết bị sản xuất tại Việt Nam.

c. Hiệu lực của hàng hóa

- Hàng hóa chào thầu là dòng sản phẩm nhà sản xuất chưa có kế hoạch ngừng cung cấp trên thị trường (End-of-sale) và không phải dòng sản phẩm đã dừng sản xuất (End-of-life).

- Tài liệu chứng minh: Nhà thầu có văn bản cam kết sẽ chuyển cho Chủ đầu tư văn bản của hãng sản xuất (hoặc đại diện hợp pháp của Hãng sản xuất tại Việt Nam) xác nhận về tính hiệu lực của hàng hóa trước khi được trao hợp đồng. Trường hợp nhà thầu không chuyển được cho Chủ đầu tư văn bản của hãng sản xuất (hoặc đại diện hợp pháp của Hãng sản xuất tại Việt Nam) xác nhận về tính hiệu lực của hàng hóa, Chủ đầu tư sẽ mời nhà thầu xếp hạng tiếp theo vào hoàn thiện hợp đồng

d. Yêu cầu về an toàn thông tin

Nhà thầu có trách nhiệm cam kết tuân thủ các quy định an toàn bảo mật trong quá trình triển khai:

+ Cam kết đảm bảo an toàn, bảo mật và tính riêng từ về thông tin, dữ liệu của Chủ đầu tư; tuân thủ quy định của pháp luật hiện hành. Mọi thông tin, dữ liệu thu thập, tạo ra hoặc xử lý trong quá trình thực hiện hợp đồng thuộc quyền sở hữu của Chủ đầu tư. Nhà thầu có trách nhiệm bảo đảm an ninh, an toàn thông tin, chuyển giao đầy đủ cho Chủ đầu tư các thông tin, dữ liệu khi kết thúc hợp đồng.

+ Các nội dung thực hiện có khả năng ảnh hưởng đến hiệu năng của hệ thống hoặc gây gián đoạn dịch vụ của người dùng hoặc hệ thống thông tin phải thực hiện ngoài giờ.

1.2.2 Yêu cầu kỹ thuật chi tiết

a. Tính năng, thông số kỹ thuật:

(1) Yêu cầu hạng mục "Bảo hành mở rộng và bản quyền phần mềm cho các thiết bị mạng, bảo mật của Cục DTNN"

STT	Hạng mục	Yêu cầu kỹ thuật	Số lượng	Đơn vị tính
1	Bảo hành mở rộng và license cho các thiết bị phòng chống tấn công APT trang bị năm 2018			
1.1	Thiết bị phòng chống tấn công APT qua đường Internet		1	Thiết bị
	Mở rộng bảo hành và cập nhật các mối đe dọa, mẫu malware từ chính hãng cho thiết bị Fireeye NX2550			
		Bản quyền có hiệu năng: 250 Mbps		
		Cập nhật các mối đe dọa, mẫu malware		
		Mô tả các dòng Malware trong báo cáo		

		Cung cấp các thuộc tính trong các cảnh báo với các tác nhân đe dọa		
		Phân tích các lỗ hổng và chuỗi các ảnh hưởng liên quan trong các cảnh báo		
		Bảo hành thay thế thiết bị khi thiết bị có lỗi xảy ra theo chính sách của Hãng		
	Thời gian duy trì:	03 năm kể từ ngày bàn giao, nghiệm thu đưa vào sử dụng		
1.2	Thiết bị chống tấn công APT qua đường email		1	Thiết bị
	Mở rộng bảo hành và cập nhật các mối đe dọa, mẫu malware từ chính hãng cho thiết bị Fireeye EX3500 cho 1.300 người dùng			
		Bản quyền cho phép tối thiểu 1300 người dùng (user mailbox)		
		Cập nhật các mối đe dọa, mẫu malware		
		Mô tả các dòng Malware trong báo cáo		
		Cung cấp các thuộc tính trong các cảnh báo với các tác nhân đe dọa		
		Phân tích các lỗ hổng và chuỗi các ảnh hưởng liên quan trong các cảnh báo		
		Bảo hành thay thế thiết bị khi thiết bị có lỗi xảy ra theo chính sách của Hãng		
	Thời gian duy trì:	03 năm kể từ ngày bàn giao, nghiệm thu đưa vào sử dụng		
1.3	Thiết bị quản trị tập trung các thiết bị APT		1	Thiết bị
	Mở rộng bảo hành thiết bị Fireeye CM4500			
		Bảo hành thay thế thiết bị khi thiết bị có lỗi xảy ra theo chính sách của Hãng		
	Thời gian duy trì:	03 năm kể từ ngày bàn giao, nghiệm thu đưa vào sử dụng		
2	Bảo hành mở rộng cho thiết bị Switch và Firewall tại	Bảo hành mở rộng cho thiết bị Switch và Firewall tại các		

	các Chi Cục DTNN trang bị năm 2018	Chi Cục DTNN trang bị năm 2018		
2.1	Bảo hành mở rộng thiết bị chuyển mạch Juniper Ex2300-24T chính hãng		15	Thiết bị
	Mở rộng bảo hành từ chính hãng cho thiết bị Juniper Ex2300-24T			
		Có khả năng truy cập vào các bản phát hành phần mềm OS khi chúng được phát hành		
		Thay thế thiết bị khi thiết bị có lỗi xảy ra theo chính sách của Hãng		
		Có khả năng truy cập vào hệ thống hỗ trợ chính hãng 24/7		
	Thời gian duy trì:	03 năm kể từ ngày bàn giao, nghiệm thu đưa vào sử dụng		
2.2	Bảo hành mở rộng thiết tị Firewall Juniper SRX340 chính hãng		15	Thiết bị
	Mở rộng bảo hành từ chính hãng cho thiết bị Juniper SRX340			
		Có khả năng truy cập vào các bản phát hành phần mềm OS khi chúng được phát hành		
		Thay thế thiết bị khi thiết bị có lỗi xảy ra theo chính sách của Hãng		
		Có khả năng truy cập vào hệ thống hỗ trợ chính hãng 24/7.		
	Thời gian duy trì:	03 năm kể từ ngày bàn giao, nghiệm thu đưa vào sử dụng		
3	Bảo hành mở rộng và bản quyền phần mềm cho thiết bị Switch và Firewall tại các điểm kho trang bị năm 2019			
3.1	Bảo hành mở rộng thiết bị chuyển mạch Juniper EX2300-24T chính hãng		40	Thiết bị
	Mở rộng bảo hành từ chính hãng cho thiết bị Juniper Ex2300-24T			
		Có khả năng truy cập vào các bản phát hành phần mềm OS khi chúng được phát hành		
		Thay thế thiết bị khi thiết bị có lỗi xảy ra theo chính sách của Hãng		
		Có khả năng truy cập vào hệ thống hỗ trợ chính hãng 24/7.		

	Thời gian duy trì:	03 năm kể từ ngày bàn giao, nghiệm thu đưa vào sử dụng		
3.2	Bảo hành mở rộng và bản quyền phần mềm bảo mật cho thiết bị Firewall SRX300 chính hãng		42	Thiết bị
	Mở rộng bảo hành và bản quyền phần mềm từ chính hãng cho thiết bị Juniper SRX300			
		Có khả năng truy cập vào các bản phát hành phần mềm OS khi chúng được phát hành		
		Thay thế thiết bị khi thiết bị có lỗi xảy ra theo chính sách của Hãng		
		Có khả năng truy cập vào hệ thống hỗ trợ chính hãng 24/7.		
		Bản quyền: IDP *(Intrusion Detection and Prevention)* /IPS *(Intrusion Prevention Signature)*		
	Thời gian duy trì:	03 năm kể từ ngày bàn giao, nghiệm thu đưa vào sử dụng		

(2) Yêu cầu hạng mục "Trang bị bổ sung giải pháp bảo mật tại Cục DTNN đáp ứng yêu cầu về an toàn thông tin"

TT	Hạng mục	Yêu cầu kỹ thuật tối thiểu	Số lượng	Đơn vị tính
I	**Thiết bị chống tấn công DDoS**		**1**	**Bộ**
	Năng lực throughput (Clean Traffic) có khả năng mở rộng lên đến:	30 Gbps		
	Khả năng ngăn chặn lưu lượng DDoS (mpps):	38Mpps		
	Độ trễ (Latency):	80 micro giây		
	Cổng mạng (protection Interface/Inspection port):	04 cổng quang 10GE kèm tranceiver		
	Cổng quản trị:	02 x 1GbE		
	Hỗ trợ công nghệ phi trạng thái (Stateless)	Stateless packet processing		
	Hợ trợ ngăn chặn các loại tấn công:	volumetric, TCP-state exhaustion và application-layer		
	Bảo vệ DDoS (DDoS Protection)	TCP/UDP/HTTP(S) flood attacks, botnet protection, hacktivist protection, host behavioral protection, anti-spoofing, payload expression-		

		based filtering, blacklists/whitelists, multiple protections for HTTP, DNS and SIP, TCP connection limiting, fragmentation attacks, connection attacks		
	Chế độ hoạt động (Operation Mode):	inline active; inline inactive (reporting, no blocking); SPAN port monitor		
	Tính năng khác:	Hỗ trợ khả năng giải mã SSL/TLS (SSL/TLS decryption)		
		Tích hợp bypass (fail-open/ fail close) bằng phần cứng		
		Hỗ trợ truyền tải các gói tin với kích thước lớn lên đến 9000 bytes (cấu hình MTU hoặc tính năng Jumbo Frame)		
	Quản trị (Management)	SNMP		
		CLI; Web UI; HTTPS		
	Thông báo:	SNMP trap, Syslog; email		
	Nguồn điện	Nguồn AC 220-240V		
		02 nguồn dự phòng		
	Bảo hành	Bảo hành chính hãng thiết bị 36 tháng tại đơn vị sử dụng		
	Bản quyền	+ Bản quyền năng lực xử lý (Clean traffic throughput License): 1Gbps; hỗ trợ khả năng nâng cấp bản quyền lên tới 30 Gbps + Bản quyền cập nhập cơ sở dữ liệu chống tấn công DDoS trong 36 tháng		
II	**Bản quyền phần mềm tẩy xoá dữ liệu vĩnh viễn**		**1**	**Gói bản quyền**
	Có nền tảng quản lý tập trung:	Tính năng quản trị tập trung cho phép nhà quản trị tạo lập chính sách, quy trình phục vụ tẩy xóa dữ liệu cho đơn vị. Cho phép quản lý quy trình xóa đồng thời nhiều thiết bị và hiển thị trạng thái của tất cả các thiết bị được kết nối. Sử dụng để lưu trữ license, báo cáo tẩy xóa, Truy xuất báo cáo tẩy xóa theo nhiều tiêu chí khác nhau dưới định dạng PDF/CSV/XML		

		- Tính năng thực hiện tẩy xóa dữ liệu trên các thiết bị từ xa		
		- Tính năng tẩy xóa dữ liệu file hoặc thư mục theo các chính sách được đặt ra theo lịch trình		
		- Tính năng tẩy xóa dữ liệu được chọn (File, folder) trên các máy tính đang hoạt động		
		- Tính năng tẩy xóa dữ liệu trên các loại tủ đĩa lưu trữ khi chúng đang được kết nối đến máy chủ. Cho phép tái sử dụng dung lượng lưu trữ trên tủ đĩa ngay sau khi tẩy xóa, không cần phải cấu hình lại hệ thống tủ đĩa		
	Tính năng phần mềm:	- Tính năng tẩy xóa dữ liệu trên các máy ảo: Tích hợp với các nền tảng ảo hóa như VMWare cho phép người quản trị có thể xóa sách máy ảo theo yêu cầu, đồng thời hoạt động trong suốt với người dùng. Xóa toàn bộ các tệp tin liên quan khi xóa máy ảo như tệp cấu hình máy ảo, tệp ổ đĩa ảo, các tệp ảnh chụp hệ thống snapshot		
		- Tính năng tẩy xóa dữ liệu trên các ổ đĩa cứng (bao gồm cả SSD) của máy tính, máy chủ, tủ đĩa lưu trữ		
		- Tính năng tẩy xóa dữ liệu trên ổ đĩa cứng ảo		
		- Tính năng tẩy xóa thiết bị lưu trữ gắn ngoài như USB/Flash/SD Card		
		- Tính năng tự động xóa theo mục đích của người sử dụng để ngăn ngừa rò rỉ thông tin nhạy cảm		
		- Tính năng xóa tất cả các loại tệp khỏi các chương trình như Microsoft Excel, Word và PowerPoint		
		- Hỗ trợ xóa các loại ổ đĩa, kể các ổ đĩa được kết nối với IDE, SATA SCSI, Fibre Channel hoặc iSCSI		

		Phần mềm tẩy xóa dữ liệu cho PC, Laptop, Server, thiết bị di động, USB, SAN/Storage		
		Dữ liệu bị xóa không có khả năng phục hồi (có chứng nhận từ một trong các tổ chức quốc tế có uy tín như Common Criteria, NATO, NIST, PCI DSS, NCSC, BSI…)		
	Bản quyền	- Bản quyền phần mềm cho tối đa 500 thiết bị/năm - Thời gian sử dụng bản quyền là 03 năm từ ngày nghiệm thu bàn giao hàng hóa		

(3) Yêu cầu hạng mục "Thay thế giải pháp mạng, bảo mật tại Cục DTNN"

TT	Hạng mục	Yêu cầu kỹ thuật tối thiểu	Số lượng	Đơn vị tính
I	**Thay thế thiết bị tường lửa mạng lõi**		**02**	**Bộ**
	Chassis	Thiết kế dạng 19 inches, rack mountable		
	Năng lực thiết bị			
		Thông lượng firewall: 77 Gbps		
		Thông lượng Next-generation firewall: 59 Gbps		
		Thông lượng Application Control hoặc Application Security hoặc tương đương: 68 Gbps		
		Số lượng kết nối mới trên giây (Connections per second): 540.000		
		Số lượng kết nối đồng thời (Concurrent session): 9.800.000		
		Thông lượng IPSec vpn: 34 Gbps		
	Giao diện kết nối			
		Cổng 10 Gigabit Ethernet SFP+: 8 cổng, kèm tranceiver Multimode cùng hãng với thiết bị tường lửa		
		Cổng HA/SYNC: tối thiểu 2 cổng 10GbE, kèm sẵn tranceiver Multimode		
	Tính năng thiết bị			
		Thiết bị phải có sẵn tính năng kiểm soát an ninh đồng thời cho		

		các ứng dụng có Port động: FTP, DNS, PPTP, SIP, H.323, RTSP		
		Có sẵn tính năng Network address translation		
		Hỗ trợ tích hợp tính năng bảo mật: Antivirus, Antispam, URL/web filtering, IPS		
		Hỗ trợ tính năng điều khiển và ưu tiên traffic dựa trên thông tin của ứng dụng		
		Thiết bị phải có sẵn tính năng SSL Proxy/SSL Inspection		
		Có sẵn bản quyền tính năng IPS, AppSecure hoặc tương đương tối thiểu 3 năm		
	Các tính năng lớp 3			
		Hỗ trợ các giao thức IPv4, RIP, OSPF, BGP, Static route		
		Hỗ trợ Equal cost multipath (ECMP)		
		Hỗ trợ Policy-based routing/Policy-based forwarding		
		Support IPv6		
	Tính năng QoS	Hỗ trợ DiffServ		
	Công cụ quản trị			
		CLI: telnet/ssh		
		Hỗ trợ SNMP		
		Web: htttp/https		
	Tính sẵn sàng			
		Active/Active và Active/Passisve		
		Đồng bộ cấu hình		
		Đồng bộ phiên kết nối cho Firewall và VPN		
	Nguồn điện	Nguồn AC 220-240V		
		Full Power Supply Redundant, Mô đun nguồn AC		
	Bảo hành thiết bị	Bảo hành chính hãng thiết bị 36 tháng tại đơn vị sử dụng, kể từ ngày bàn giao, nghiệm thu đưa vào sử dụng		
II	**Thay thế thiết bị cân bằng tải tích hợp tính năng WAF**		**01**	**Bộ**
	Kiểu dáng	Thiết kế dạng 19 inches, rack mountable		
	Năng lực thiết bị			
	- Cổng kết nối:	4 x 25G/10G SFP+ ports, bao gồm transceiver		

	- Lưu ttrữ:	480 GB		
	- Thông lượng L4:	25 Gbps		
	- Thông lượng L7:	17 Gbps		
	- Số L7 requests trong 1 giây:	500.000		
	- Hardware Offload SSL bulk encryption hoặc SSL Throughput:	10 Gbps		
	- SSL TPS:	10.000		
	- Compression hoặc Compression Thoughput:	15 Gbps		
	- Tính năng cân bằng tải			
		+ Thuật toán: Round Robin, Least Connection, Dynamic Ratio, Fastest hoặc các thuật toán tương đương.		
		+ Hỗ trợ các cơ chế giám sát và khả năng kết hợp nhiều cơ chế giám sát theo (Địa chỉ IP, dịch vụ) cho phép kiểm tra trạng thái của ứng dụng dựa trên nhiều yếu tố đồng thời		
		+ Hỗ trợ tăng tốc SSL trên phần cứng để giúp giảm tải xử lý SSL trên máy chủ (SSL Offload)		
		+ SSL Forward Proxy, SSL Session Re-use, hỗ trợ chuẩn mã hóa TLS 1.3		
		+ Phòng chống tấn công Web ở Layer 7 (slowloris, slowpost, HTTP GET Flood, Recursive GET Flood (Web Scraping), Dirt Jumper (HTTP Flood) hoặc tương đương.		
		+ Hỗ trợ RFC2385 TCP-MD5 để bảo vệ TCP Traffic		
		+ Cung cấp khả năng lập trình scripting cho phép phân tích, xử lý và phát hiện dựa trên thành phần của lưu lượng trong mạng.		
	- Tính năng tường lửa ứng dụng:			
		+ Chống tấn công theo mẫu đã biết (signatures) và được cập nhật thường xuyên.		
		+ Có chức năng chống lại các tấn công dịch vụ Web, tấn công		

		nhằm vào các ứng dụng XML hoặc Web Service.		
		+ Có chức năng kiểm tra, giám sát phiên giao dịch của người dùng (session/user tracking); có cơ chế kiểm tra, bảo vệ, phát hiện và ngăn chặn các hình thức tấn công chiếm phiên làm việc (session hijacking).		
		+ Có chức năng tự động yêu cầu xác thực challenge-response (như CAPTCHA) để ngăn chặn các công cụ duyệt web tự động.		
		+ Có chức năng phát hiện và ngăn chặn, giảm thiểu mức độ ảnh hưởng của các hình thức tấn công từ chối dịch vụ lớp ứng dụng (Layer-7 DoS attack) tối thiểu các hình thức: SQL Injection; OS Command injection; XPath Injection; Brute-force; Remote File Inclusion (RFI); Cross-Site Scripting (XSS); Cross-Site Request Forgery (CSRF).		
	Tính sẵn sàng	- Tính sẵn sàng: Active-Active/ Active – Standby		
	Nguồn điện	02 nguồn AC		
	Bảo hành thiết bị	Bảo hành chính hãng thiết bị 36 tháng tại đơn vị sử dụng, kể từ ngày bàn giao, nghiệm thu đưa vào sử dụng		
	Bản quyền	Bản quyền cập nhập signature trong 36 tháng		

(4) Yêu cầu hạng mục "Gia hạn bản quyền cập nhật Antivirus tại các đơn vị và dịch vụ hỗ trợ kỹ thuật chính hãng giai đoạn 2025-2027"

STT	Hạng mục	Yêu cầu kỹ thuật
1	**Phần mềm phòng chống Virus cho máy chủ và máy trạm**	
1.1	**Phần mềm phòng chống Virus**	
	- Quét virus trong:	Bộ nhớ, file, thư mục, file nén, thiết bị lưu trữ ngoài.
	- Chế độ quét:	- Quét thủ công (manual scan);
		- Quét theo lịch (Schedule scan).
	- Cho phép bật/tắt chế độ rà quét theo thời gian thực	Có

	- Cho phép thiết lập các tùy chọn đối với chế độ rà quét theo yêu cầu bao gồm:	Chọn kiểu rà quét, nhập đường dẫn đến thư mục cần ra quét, chọn hành động được áp dụng tự động khi phát hiện có mã độc trong quá trình rà quét, lên lịch rà quét
	- Cơ chế bảo vệ	Diệt (protect/prevent/anti): virus, Trojan, Spyware, Adware, Rootkit.
		Bảo vệ theo thời gian thực (real-time protection hoặc tương đương).
		Bảo vệ truy cập web
		Chủ động phòng vệ (hoặc Proactive Protection/Proactive defence).
		Tính năng phòng chống virus mã hóa Ransomware
		Phòng chống tấn công mạng Network attack
		Chống khai thác chủ động ngăn chặn các cuộc tấn công zero-day được thực hiện thông qua các hoạt động khai thác ngụy trang
		Tự động bảo vệ phần mềm bảo mật khỏi bị vô hiệu hóa hoặc thay đổi bởi những kẻ tấn công trên điểm cuối.
		Lớp bảo vệ tiên tiến, phân tích tự động và chuyên sâu các tệp đáng ngờ mà chưa được ký bởi tính năng antimalware.
	- Cập nhật mẫu virus	Cập nhật tự động mẫu virus cho server, máy trạm
		Đặt lịch cập nhật tự động cho endpoint từ server
		Cập nhật manual cho Server và endpoint cho toàn hệ thống
	Hỗ trợ hệ điều hành cài đặt	- Cài đặt được trên Window Server, Linux - Cài đặt được trên Windows 7/8/10/11 (32, 64 bit)
	Giao diện phần mềm phòng chống mã độc cài trên máy chủ, máy trạm	- Hỗ trợ ngôn ngữ Tiếng Việt
1.2	**Yêu cầu về bản quyền sử dụng**	
a)	Thời gian bản quyền sử dụng cập nhật, nâng cấp phiên bản	02 năm
b)	Số lượng bản quyền	- Bản quyền sử dụng cho 150 máy chủ - Bản quyền sử dụng cho 1.150 máy trạm - Dịch vụ hỗ trợ trực tiếp chính hãng
2	**Thành phần quản lý tập trung cho phần mềm phóng chống Virus**	
	- Tính năng quản lý	+ Tự động cập nhật mẫu Virus

		+ Cập nhật từ máy chủ quản lý tập trung mẫu Virus cho các Client: Tự động hoặc manual
		Quản lý thông tin trên toàn hệ thống + Tên máy, địa chỉ IP + Phiên bản phần mềm phòng chống Virus + Tình trạng kết nối của phần mềm phòng chống Virus với thành phần quản lý tập trung + Báo cáo thống kê, số lượng, loại Virus phát hiện được, kết quả xử lý trên từng máy tính,
		+ Đặt lịch quét định kỳ thống nhất cho một nhóm hoặc tất cả máy tính trong hệ thống
		+ Ra lệnh từ xa cho một nhóm hoặc tất cả máy tính trong hệ thống thực hiện quét virus
	Cho phép tìm kiếm dữ liệu log bằng từ khóa để xem lại	Cho phép tìm kiếm dữ liệu log bằng từ khóa để xem lại
	Log chức năng phát hiện và ngăn chặn mã độc	- AV cho phép ghi log tất cả các sự kiện về mã độc phát hiện được trong các quá trình rà quét thủ công hoặc tự động. - AV cho phép ghi log chức năng phát hiện và ngăn chặn mã độc có các trường thông tin sau: + Thời gian sinh log (bao gồm năm, tháng, ngày, giờ, phút và giây). + Đường dẫn đến vị trí mã độc phát hiện được. + Mô tả của mã độc phát hiện được. + Phân loại của mã độc phát hiện được.
	Định dạng log	AV cho phép chuẩn hóa log theo tối thiểu 01 định dạng được định nghĩa trước để truyền dữ liệu log cho các phần mềm quản lý, phân tích, điều tra log
	Cho phép hiển thị các kết quả rà quét, các thống kê về tình hình phát hiện và xử lý mã độc trên thiết bị được bảo vệ;	Cho phép hiển thị các báo cáo kết quả rà quét, các thống kê về tình hình phát hiện và xử lý mã độc trên thiết bị được bảo vệ;
	- Hỗ trợ hệ điều hành cài đặt	Đối với thành phần quản lý tập trung là phần mềm, yêu cầu cài đặt được trên Windows Server/ Linux hoặc máy ảo trên các nền tảng ảo hóa VMware, Citrix, Microsoft, Linux, Nutanix
	Giao diện thành phần quản trị tập trung	Hỗ trợ giao diện tiếng Việt

5) Yêu cầu hạng mục "Gia hạn bản quyền phần mềm bảo mật hệ thống ảo hoá và dịch vụ hỗ trợ chính hãng giai đoạn 2025-2027"

STT	Hạng mục	Yêu cầu kỹ thuật
1	**Gia hạn bản quyền phần mềm bảo mật hệ thống ảo hóa**	
1.1	**Yêu cầu phần mềm**	
	- Cơ chế bảo vệ	Diệt (protect/prevent/anti): virus, Trojan, Spyware, Adware, Rootkit.
		Bảo vệ theo thời gian thực (real-time protection hoặc tương đương).
		Chủ động phòng vệ (hoặc Proactive Protection/Proactive defence).
		Tính năng phòng chống virus mã hóa Ransomware
		Phòng chống tấn công mạng Network attack
		Chống khai thác chủ động ngăn chặn các cuộc tấn công zero-day được thực hiện thông qua các hoạt động khai thác ngụy trang
		Tự động bảo vệ phần mềm bảo mật khỏi bị vô hiệu hóa hoặc thay đổi bởi những kẻ tấn công trên điểm cuối.
		Tính năng bảo vệ cao cấp
		Lớp bảo vệ tiên tiến, phân tích tự động và chuyên sâu các tệp đáng ngờ mà chưa được ký bởi tính năng antimalware.
	Bảo vệ bộ nhớ trong	Bảo vệ bộ nhớ trong chống virus chiếm quyền cho máy chủ Citrix Xenserver
	Tích hợp với VMware Vshield	Bộ quét tương thích với Vshield
	Hỗ trợ triển khai máy chủ quét tập trung cho môi trường VMWare vShield	Hỗ trợ triển khai máy chủ quét tập trung cho môi trường VMWare vShield
	Hỗ trợ triển khai máy chủ quét tập trung cho môi trường VMWare NSX	Hỗ trợ triển khai máy chủ quét tập trung cho môi trường VMWare NSX
	Hỗ trợ triển khai máy chủ quét tập trung cho nhiều môi trường ảo hóa	Hỗ trợ triển khai máy chủ quét tập trung cho nhiều môi trường ảo hóa
	Bảo vệ chống virus cho môi trường ảo với dạng phần mềm không cần phải cài đặt	Bảo vệ chống virus cho môi trường ảo với dạng phần mềm không cần phải cài đặt
	Hỗ trợ nhiều kiểu quét	Hỗ trợ quét nhanh, quét toàn bộ (full scan), quet theo yêu cầu (customer scan), quét bộ nhớ, quét mạng
	Máy quét đơn phải có khả năng	Chứa cơ sở dữ liệu virus, Cung cấp bảo vệ toàn bộ, được cập nhật, Cung cấp quét tối ưu

	Quản lý và cài đặt từ xa	- Máy quét ảo phải có khả năng tùy chỉnh trước khi cài
		- Management Console phải được báo cáo mô đun antivirus có được kích hoạt hay không trên từng VM
	Tương thích với các hệ thống ảo hóa	XenServer
		Citrix XenApp and XenDesktop 7.18, 7.17, 7.16, 7.15 LTSR, 7.6 LTSR
		Citrix VDI-in-a-Box 5.x
		Microsoft Hyper-V Server 2008 R2, 2012, 2012 R2, 2016, 2019 or Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019 (including Hyper-V Hypervisor)
		Red Hat Enterprise Virtualization 3.0 (including KVM Hypervisor)
		Nutanix Prism with AOS 5.5, 5.10, 5.15
		ESXi 5.5 or later for each server
		vCenter Server 5.5 or later
		VMware NSX-T Manager
	Tương thích với máy chủ hệ thống quản trị hiện tại	Phần mềm triển khai phải tương thích, tích hợp hoàn toàn với hệ thống máy chủ quản trị Virus Bitdefender GravityZone tại Cục DTNN, không cài đặt thêm máy chủ quản trị.
	- Giao diện phần mềm phòng chống mã độc	- Hỗ trợ ngôn ngữ Tiếng Việt
1.2	**Yêu cầu về bản quyền sử dụng**	
a)	Thời gian bản quyền sử dụng cập nhật, nâng cấp phiên bản	02 năm
b)	Số lượng bản quyền	Bản quyền sử dụng cho hệ thống máy chủ ảo hóa đáp ứng 26 CPU vật lý

(6) Yêu cầu hạng mục "Bảo hành mở rộng thiết bị mạng, bảo mật tại Cục DTNN"

STT	Hạng mục	Yêu cầu kỹ thuật	Số lượng	Đơn vị tính
1	Bảo hành mở rộng và license cho thiết bị Firewall cho vùng Internet tại Cục DTNN		2	Thiết bị
	Mở rộng bảo hành từ chính hãng cho thiết bị Juniper SRX1500			
		Có khả năng truy cập vào các bản phát hành phần mềm OS khi chúng được phát hành		
		Thay thế thiết bị khi thiết bị có lỗi xảy ra theo chính sách của Hãng		

		Có khả năng truy cập vào hệ thống hỗ trợ chính hãng 24/7.		
		Bản quyền: IDP *(Intrusion Detection and Prevention)* /IPS *(Intrusion Prevention Signature)*		
	Thời gian duy trì:	03 năm kể từ ngày bàn giao, nghiệm thu đưa vào sử dụng		
2	Bảo hành mở rộng và license cho thiết bị Firewall cho vùng WAN tại Cục DTNN		2	Thiết bị
	Mở rộng bảo hành từ chính hãng cho thiết bị Juniper SRX1500			
		Có khả năng truy cập vào các bản phát hành phần mềm OS khi chúng được phát hành		
		Thay thế thiết bị khi thiết bị có lỗi xảy ra theo chính sách của Hãng		
		Có khả năng truy cập vào hệ thống hỗ trợ chính hãng 24/7.		
	Thời gian duy trì:	03 năm kể từ ngày bàn giao, nghiệm thu đưa vào sử dụng		
3	Bảo hành mở rộng thiết bị chuyển mạch Core		1	Thiết bị
	Mở rộng bảo hành từ chính hãng cho thiết bị Juniper QFX10002			
		Có khả năng truy cập vào hệ thống hỗ trợ chính hãng 24/7		
		Có khả năng truy cập vào các bản phát hành phần mềm OS khi chúng được phát hành		
		Thay thế thiết bị khi thiết bị có lỗi xảy ra theo chính sách của Hãng		
	Dịch vụ hỗ trợ cho license	Có khả năng hỗ trợ chính hãng 24/7 cho các license của thiết bị QFX10002		

	Thời gian duy trì:	03 năm kể từ ngày bàn giao, nghiệm thu đưa vào sử dụng		
4	Bảo hành mở rộng thiết bị chuyển mạch cho máy chủ dịch vụ hạ tầng Intranet (3 năm)		2	Thiết bị
	Mở rộng bảo hành từ chính hãng cho thiết bị chuyển mạch Juniper EX3400-48T			
		Có khả năng truy cập vào các bản phát hành phần mềm OS khi chúng được phát hành		
		Thay thế thiết bị khi thiết bị có lỗi xảy ra theo chính sách của Hãng		
		Có khả năng truy cập vào hệ thống hỗ trợ chính hãng 24/7.		
	Thời gian duy trì:	03 năm kể từ ngày bàn giao, nghiệm thu đưa vào sử dụng		
5	Bảo hành mở rộng thiết bị chuyển mạch cho LAN (3 năm)		4	Thiết bị
	Mở rộng bảo hành từ chính hãng cho thiết bị chuyển mạch Juniper EX2300-48T			
		Có khả năng truy cập vào các bản phát hành phần mềm OS khi chúng được phát hành		
		Thay thế thiết bị khi thiết bị có lỗi xảy ra theo chính sách của Hãng		
		Có khả năng truy cập vào hệ thống hỗ trợ chính hãng 24/7.		
	Thời gian duy trì:	03 năm kể từ ngày bàn giao, nghiệm thu đưa vào sử dụng		

Ghi chú

Tất cả nội dung yêu cầu liên quan đến tên riêng của thông số kỹ thuật, thương hiệu, ký mã hiệu, nhãn hiệu, model, nguồn gốc xuất xứ (nếu có) trong E-HSMT chỉ mang tính tham khảo cho nhà thầu nhằm thuận lợi hơn trong quá trình đề xuất sản phẩm cho gói thầu, không phải là tiêu chuẩn đánh giá kỹ thuật của E-HSMT. Nhà thầu không bắt buộc

phải chào theo yêu cầu về tên riêng của thông số kỹ thuật, thương hiệu, ký mã hiệu, nhãn hiệu, model, nguồn gốc xuất xứ (nếu có) trừ các hạng mục liên quan đến hạng mục: (1) Bảo hành mở rộng và bản quyền phần mềm cho các thiết bị mạng, bảo mật của Cục DTNN; (2) Gia hạn bản quyền cập nhật Antivirus tại các đơn vị và dịch vụ hỗ trợ kỹ thuật chính hãng giai đoạn 2025-2027; (3) Gia hạn bản quyền phần mềm bảo mật hệ thống ảo hoá và dịch vụ hỗ trợ chính hãng giai đoạn 2025-2027; (4) Bảo hành mở rộng thiết bị mạng, bảo mật tại Cục DTNN.

Trong quá trình chuẩn bị E-HSDT, nhà thầu có thể tổ chức khảo sát trực tiếp hệ thống để làm rõ tính tương thích của các hàng hóa và các yêu cầu kỹ thuật khác trong phạm vi gói thầu. Nhà thầu tự chịu trách nhiệm tìm hiểu mọi thông tin cần thiết để lập E-HSDT và thực hiện hợp đồng. Toàn bộ chi phí khảo sát do nhà thầu tự chi trả.

Nhà thầu phải nộp kèm Tài liệu kỹ thuật chính hãng (datasheet/catalogue) đối với sản phẩm chào thầu.

Ngoài bản đề xuất thiết bị/sản phẩm chào hàng. Nhà thầu phải soạn bảng so sánh về kỹ thuật để chứng minh hàng hóa do nhà thầu chào tuân thủ với các yêu cầu đó theo mẫu cung cấp bên dưới. Trong bảng tuyền bố đáp ứng phải nêu rõ mức độ đáp ứng các yêu cầu của E-HSMT (bao gồm từng khoản mục, đặc tính kỹ thuật chi tiết quy định tại bản trên của từng hàng mục chào thầu). Nhà thầu chỉ được phép sử dụng các từ ngữ sau: "Đáp ứng", "Không đáp ứng" để trả lời về tính đáp ứng theo yêu cầu của E-HSMT. Tất cả các đáp ứng yêu cầu kỹ thuật đều phải được giải thích cụ thể, tham chiếu rõ ràng đến từng dòng/từng trang của tài liệu kỹ thuật.

Bảng So sánh

Hạng mục số	**Tên hàng hóa**	**Thông số kỹ thuật và các tiêu chuẩn của hàng hóa trong E-HSMT**	**Thông số kỹ thuật và các tiêu chuẩn của hàng hóa chào trong E-HSDT**	**Hồ sơ tham chiếu**	**Tính đáp ứng của hàng hóa**
(1)	*(2)*	*(3)*	*(4)*	*(5)*	*(6)*

Ghi chú:

- Nội dung ở các cột (1), (2), (3) phải được lập tương ứng với nội dung của Bảng Thông số kỹ thuật và các tiêu chuẩn

- Cách thức trình bày nội dung ở cột (5) như sau: "Tên tài liêu" – "Phần, Chương, Mục, bảng (nếu có)" – "trang" - "dòng"

- Nội dung ở cột (6) chỉ được ghi "Đáp ứng" hoặc "Không đáp ứng"

b. Yêu cầu dịch vụ liên quan

(1) Thực hiện, tiến độ các công việc liên quan dịch vụ triển khai như sau:

- Xây dựng tài liệu kế hoạch cài đặt, tích hợp các hệ thống;

- Di chuyển hệ thống từ thiết bị cũ sang hệ thống thiết bị mới;

- Kiểm tra và thử nghiệm hệ thống;

- Xây dựng tài liệu cầu hình và vận hành.

- Phối hợp với Chủ đầu tư xây dựng và thuyết minh phương án bảo đảm an toàn thông tin mạng, hồ sơ cấp độ an toàn thông tin đối với hạng mục triển khai.

Chi tiết về các công việc sẽ thực hiện trong gói thầu được trao đổi, hoàn thiện trong quá trình triển khai Hợp đồng và triển khai gói thầu

(2) Nội dung công việc hỗ trợ kỹ thuật thực hiện đối phần mềm gia hạn bản quyền Antivirus:

- Rà soát, cài đặt, cập nhật phần mềm endpoint và phần mềm quản lý endpoint theo phiên bản mới nhất (hoặc theo khuyến nghị của hãng sản xuất) tại thời điểm triển khai.

- Nâng cấp phiên bản theo khuyến nghị, chính sách của hãng hoặc khi có yêu cầu

- Định kỳ 6 tháng 1 lần thực hiện việc kiểm tra, rà soát cấu hình hệ thống Endpoint Security trong phạm vi triển khai

- Hỗ trợ xử lý các vấn đề về virus, malware trên máy chủ, máy trạm khi có yêu cầu của Cục DTNN (24x7)

- Hỗ trợ kết xuất thông tin về mã độc theo yêu cầu của Bộ quản lý chuyên ngành về CNTT

- Hỗ trợ lấy mẫu mã độc các trường hợp nghi ngờ nhiễm mã độc mà hệ thống Endpoint không/chưa phát hiện được, gửi đến nhà sản xuất/đơn vị hỗ trợ của nhà sản xuất để phần tích, cập nhật phiên bản dữ liễu (nếu cần thiết) cho hệ thống quản lý endpoint và endpoiny do nhà sản xuất phát hành

- Trong trường hợp hệ thống Endpoint Security bị lỗi: Đơn vị triển khai có trách nhiệm xử lý khắc phục lỗi (bao gồm cả cài đặt lại nếu không thể khắc phục lỗi trên hệ thống hiện tại)

(3) Nội dung công việc hỗ trợ kỹ thuật thực hiện đối phần mềm gia hạn bản quyền bảo mật hệ thống ảo hóa:

- Rà soát, cài đặt, cập nhật phần mềm bảo mật hệ thống ảo hoá theo phiên bản mới nhất (hoặc theo khuyến nghị của hãng sản xuất) tại thời điểm triển khai

- Nâng cấp phiên bản theo khuyến nghị, chính sách của hãng hoặc khi có yêu cầu.

- Định kỳ 6 tháng 1 lần thực hiện việc kiểm tra, rà soát cấu hình hệ thống bảo mật hệ thống ảo hoá trong phạm vi triển khai

- Hỗ trợ xử lý các vấn đề về virus, malware trên máy chủ khi có yêu cầu của Cục DTNN (24x7)

- Hỗ trợ kết xuất thông tin về mã độc theo yêu cầu của Bộ quản lý chuyên ngành về CNTT.

- Hỗ trợ lấy mẫu mã độc các trường hợp nghi ngờ nhiễm mã độc mà hệ thống Endpoint không/chưa phát hiện được, gửi đến nhà sản xuất/đơn vị hỗ trợ của nhà sản xuất để phần tích, cập nhật phiên bản dữ liễu (nếu cần thiết) cho hệ thống quản lý endpoint và endpoiny do nhà sản xuất phát hành

- Trong trường hợp hệ thống bảo mật hệ thống ảo hoá bị lỗi: Đơn vị triển khai có

trách nhiệm xử lý khắc phục lỗi (bao gồm cả cài đặt lại nếu không thể khắc phục lỗi trên hệ thống hiện tại)

1.3. Các yêu cầu khác

1.3.1. Giải pháp kỹ thuật; biện pháp tổ chức cung cấp, triển khai các nội dung có liên quan và phương án bố trí nhân sự triển khai dịch vụ

Trong E-HSDT, Nhà thầu trình bày kỹ thuật; biện pháp tổ chức cung cấp, triển khai các nội dung có liên quan và phương án bố trí nhân sự triển khai dịch vụ đảm bảo tính hợp lý, hiệu quả đáp ứng các yêu cầu cơ bản như sau:

- Có biện pháp tổ chức cung cấp, triển khai các nội dung có liên quan đầy đủ, hợp lý đáp ứng theo phạm vi cung cấp của E-HSMT

- Có thuyết minh biện pháp tổ chức, giải pháp kỹ thuật bao gồm sơ đồ bố trí nhân sự đáp ứng đầy đủ các yêu cầu tại Mục 1.2 – Yêu cầu về kỹ thuật

1.3.2. Bảo hành, hỗ trợ kỹ thuật

Nhà thầu phải có cam kết về các phương án bảo hành, hỗ trợ kỹ thuật và phương án đảm bảo chất lượng dịch vụ trong thời gian bảo hành đáp ứng các yêu cầu sau:

- Thời gian bảo hành đối với thiết bị chống tấn công DDos, phần mềm tẩy xoá dữ liệu vĩnh viễn, thiết bị tường lửa mạng lõi, thiết bị cân bằng tải tích hợp tính năng WAF đáp ứng tối thiểu 3 năm bắt đầu kể từ ngày hai bên ký Biên bản nghiệm thu sản phẩm, hạng mục công việc thuộc hợp đồng.

- Đối với phần cứng thiết bị: Tất cả các thành phần thuộc thiết bị do nhà thầu cung cấp sẽ được hưởng chính sách bảo hành chính hãng đầy đủ từ hãng sản xuất

- Cung cấp văn bản của hãng sản xuất thiết bị/phần mềm xác nhận về việc hãng cung cấp dịch vụ bảo hành/bản quyền cho các thiết bị/phần mềm thuộc phạm vi mua sắm

- Hỗ trợ kỹ thuật trong thời gian bảo hành:

+ Hỗ trợ kỹ thuật 24x7: 24h liên tục trong trong ngày và 07 ngày trong tuần bảo gồm cả ngày nghỉ lễ (online/call/remote support)

+ Khi có yêu cầu xử lý sự cố phần cứng, nhà thầu phải cử kỹ thuật viên đến địa điểm đặt thiết bị của Chủ đầu tư trong vòng tối đa 04 giờ (04h) kể từ khi tiếp nhận yêu cầu.

+ Cung cấp dịch vụ thay thế linh kiện hỏng/hư lỗi theo chính sách bảo hành chính hãng của hãng sản xuất

+ Bảo hành tại chỗ khi thiết bị (hoặc cấu phần thiết bị) bị lỗi/hỏng bằng thiết bị (hoặc cấu phần thiết bị) mới chính hãng sản xuất có tính năng và tiêu chuẩn kỹ thuật tương đương hoặc cao hơn so với thiết bị được bảo hành

+ Trong trưởng hợp thiết bị (hoặc cấu phần thiết bị) lỗi/hỏng phải mang về hãng bảo hành, nhà thầu phải thực hiện việc bố trí thiết bị (hoặc cấu phần thiết bị) tạm thời thay thế để bảo hệ thống hoạt động bình thường. Thiết bị (hoặc cấu phần thiết bị) tạm thời này phải là sản phẩm chính hãng, có tính năng và tiêu chuẩn tương đương hoặc cao hơn thiết bị lỗi.

+ Thời gian hoàn thành sửa chữa, thay thế thiết bị: Trong vòng 72 giờ kể từ khi nhận thông báo hoặc kể từ thời điểm 2 bên xác định thiết bị phải bảo hành.

+ Phối hợp thực hiện cập nhật Firmware/nâng cấp phiên bản cho thiết bị bạo hành hoặc phối hợp kiểm tra phần cứng thiết bị khi có yêu cầu

+ Nhà thầu chịu trách nhiệm khắc phục 100% các sự cố kỹ thuật (nếu có) trong thời gian bảo hành, đảm bảo thiết bị hoạt động ổn định, liên tục.

+ Nhà thầu phải cung cấp đầu mối liên lạc (thông tin đầu mối bao gồm số điện thoại, email) để chủ đầu tư liên hệ khi cần hỗ trợ kỹ thuật hoặc có sự cố. Nếu có bất kỳ thay đổi nào về đầu mối liên hệ của nhà thầu trong thời gian bảo hành phải thông báo cho Chủ đầu tư bằng văn bản.

+ Toàn bộ chi phí liên quan đến hỗ trợ kỹ thuật, bảo hành, thay thế linh kiện và cập nhật phần mềm sẽ do nhà thầu chịu trách nhiệm và không phát sinh thêm chi phí đối với Chủ đầu tư.

- Phương án đảm bảo chất lượng dịch vụ: Nhà thầu trình bày cụ thể chi tiết về quy trình, cách thức để đảm bảo chất lượng các dịch vụ bảo hành, hỗ trợ kỹ thuật theo yêu cầu trên.

1.3.3. Mức độ đáp ứng các yêu cầu về cung cấp vật tư, thiết bị thay thế và các dịch vụ liên quan khác

a. Nhà thầu phải có cam kết cung cấp linh kiện, thiết bị thay thế cho toàn bộ thành phần chính của thiết bị (RAM, HDD/SSD, nguồn, card mạng…) đáp ứng các yêu cầu tối thiểu sau:

- Linh kiện, thiết bị cung cấp là chính hãng, mới 100% tương thích hoàn toàn với thiết bị gốc và không ảnh hưởng đến bảo hành chính hãng, được nhập khẩu hoặc phân phối bởi đại lý ủy quyền chính thức tại Việt Nam

- Nhà thầu cam kết cung cấp xác nhận bằng văn bản từ Hãng sản xuất hoặc Nhà phân phối được ủy quyền của hãng sản xuất về thời gian hỗ trợ linh kiện, thiết bị thay thế (EOSL/EOL roadmap) trước thời điểm ký hợp đồng

b. Nhà thầu phải có cam kết thực hiện việc di chuyển (migration) hệ thống thiết bị cũ sang hệ thống thiết bị mới, đáp ứng các yêu cầu tối thiểu sau:

- Lập kế hoạch di chuyển (migration) chi tiết, gồm:

+ Các bước di chuyển thiết bị

+ Thời gian chuyển đổi (ít ảnh hưởng vận hành)

+ Phân tích rủi ro và phương án khôi phục (rollback)

- Đảm bảo tính tương thích hệ thống:

+ Kiểm tra thiết bị mới có thể tương thích với mô hình hiện tại.

+ Cập nhật các gói phần mềm/phụ thuộc cần thiết trước khi chuyển đổi

- Đảm bảo toàn vẹn dữ liệu:

+ Thực hiện backup đầy đủ cấu hình của thiết bị trước khi di chuyển

- Thử nghiệm và nghiệm thu:

+ Kiểm tra các ứng dụng, dịch vụ sau khi di chuyển

- Đảm bảo an toàn thông tin:

+ Cấu hình bảo mật, phân quyền người dùng

+ Cập nhật bản vá bảo mật mới nhất trước khi đưa hệ thống vào vận hành

c. Nhà thầu phải có cam kết cung cấp dịch vụ kiểm tra và thử nghiệm đáp ứng các yêu cầu nêu tại Mục 3. Kiểm tra và thử nghiệm tại Chương V của E-HSMT

1.3.4 Yêu cầu về điều khoản thương mại

- Nhà thầu phải có cam kết: Giá dự thầu do nhà thầu đề xuất phải là giá trọn gói, đã bao gồm toàn bộ thuế, phí, chi phí vận chuyển, lắp đặt, cài đặt, bảo hành, đào tạo chuyển giao công nghệ và các chi phí liên quan khác để thực hiện đầy đủ nội dung theo yêu cầu của Chủ đầu tư.

- Nhà thầu cam kết sẽ chấp thuận hoàn toàn các điều kiện thương mại đã được nêu tại E-HSMT. Ngoài ra cam kết chấp thuận hoàn toàn quy chế xử phạt hợp đồng, cụ thể như sau:

+ Phạt 1%/tuần chậm so với tiến độ chi tiết đã được đề xuất tại E-HSDT, không quá 8% giá trị phần nghĩa vụ hợp đồng bị vi phạm

+ Phạt 3%/tuần chậm so với tổng tiến độ thực hiện gói thầu đã được đề xuất tại E-HSDT, không quá 8% giá trị phần nghĩa vụ hợp đồng bị vi phạm

+ Trường hợp Nhà thầu chậm tiến độ quá 3 tuần so với tiến độ chi tiết hoặc tổng tiến độ đã được phê duyệt mà không được sự chấp thuận của chủ đầu tư bằng văn bản; Chủ đầu tư có quyền chấm dứt hợp đồng ngay lập tức mà không cần thông báo trước, trừ trường hợp bất khả kháng. Đồng thời, Nhà thầu phải chịu các chế tài theo quy định của hợp đồng. Giá trị phạt hợp đồng sẽ được khấu trừ trực tiếp vào giá trị khối lượng Nhà thầu đã thực hiện. Trường hợp Nhà thầu chưa thực hiện bất kỳ khối lượng nào (không có giá trị để khấu trừ), Chủ đầu tư có quyền tịch thu toàn bộ giá trị bảo đảm thực hiện hợp đồng.

1.3.5. Thời gian giao hàng, tiến độ cung cấp

- Nhà thầu có bảng tiến độ chi tiết thể hiện từng nội dung theo phạm vi cung cấp từ lúc ký hợp đồng đến khi nghiệm thu, bàn giao, thanh lý hợp đồng.

- Đối với các hạng mục gia hạn bản quyền và bảo hành mở rộng *(Bảo hành mở rộng và license cho thiết bị Firewall cho vùng Internet (Juniper SRX 1500) tại Cục DTNN; Bảo hành mở rộng và license cho thiết bị Firewall WAN (Juniper SRX 1500) tại Cục DTNN; Bảo hành mở rộng và license cho thiết bị Firewall cho vùng Internet tại Cục DTNN; Bảo hành mở rộng và license cho thiết bị Firewall cho vùng WAN tại Cục DTNN; Bảo hành mở rộng thiết bị chuyển mạch Core; Bảo hành mở rộng thiết bị chuyển mạch cho máy chủ dịch vụ hạ tầng Intranet; Bảo hành mở rộng thiết bị chuyển mạch Core (Juniper QFX10002-36Q); Bảo hành mở rộng thiết bị chuyển mạch cho máy chủ dịch vụ hạ tầng, Intranet (Juniper EX3400-48T); Bảo hành mở rộng và license cho các thiết bị phòng chống tấn công APT trang bị năm 2018),* nhà thầu phải đáp ứng tiến độ như sau:

+ Thời gian bàn giao bản quyền (nếu có), chứng nhận gia hạn bảo hành của hãng

sản xuất không quá 45 ngày kể từ ngày ký hợp đồng.

+ Thời gian hoàn thành dịch vụ có liên quan để bàn giao, nghiệm thu đưa vào sử dụng không quá 45 ngày kể từ ngày hợp đồng có hiệu lực

+ Thời gian cập nhận bản quyền phần mềm thiết bị (nếu có), bảo hành mở rộng: 36 tháng kể từ ngày ký nghiệm thu, đưa vào sử dụng

- Đối với các hạng mục gia hạn bản quyền và dịch vụ hỗ trợ kỹ thuật chính hãng (*Gia hạn bản quyền cập nhật Antivirus tại các đơn vị và dịch vụ hỗ trợ chính hãng giai đoạn 2025-2027; Gia hạn bản quyền phần mềm bảo mật hệ thống ảo hoà và dịch vụ hỗ trợ chính hãng giai đoạn 2025-2027),* nhà thầu phải đáp ứng tiến độ như sau:

+ Thời gian bàn giao bản quyền, dịch vụ hỗ trợ kỹ thuật chính hãng không quá 30 ngày kể từ ngày hợp đồng có hiệu lực.

+ Thời gian hoàn thành triển khai dịch vụ "Triển khai cài đặt, cập nhật phần mềm cho các đơn vị của Cục DTNN" để bàn giao, nghiệm thu đưa vào sử dụng không quá 45 ngày kể từ ngày hợp đồng có hiệu lực

+ Thời gian bản quyền cập nhật, dịch vụ hỗ trợ chính hãng: 2 năm kể từ ngày ký nghiệm thu, đưa vào sử dụng

- Đối với các hạng mục trang bị bổ sung giải pháp bảo mật tại Cục DTNN *(bao gồm: thiết bị chống tấn công DdoS, bản quyền phần mềm tẩy xoá dữ liệu vĩnh viễn, thiết bị tường lửa mạng lõi, thiết bị cân bằng tải tích hợp tính năng WAF):*

+ Thời gian bàn giao thiết bị để thực hiện kiểm tra trước khi triển khai dịch vụ không quá 120 ngày kể từ ngày ký hợp đồng đối với thiết bị *chống tấn công DdoS, bản quyền phần mềm tẩy xoá dữ liệu vĩnh viễn, thiết bị tường lửa mạng lõi với thiết bị cân bằng tải tích hợp tính năng WAF.*

+ Thời gian hoàn thành triển khai dịch vụ để bàn giao, nghiệm thu đưa vào sử dụng không quá 150 ngày kể từ ngày hợp đồng có hiệu lực

+ Thời gian bảo hành, cập nhật bản quyền (nếu có): 36 tháng tại đơn vị sử dụng

1.3.6. Đào tạo chuyển giao công nghệ

- Mục đích: Chuyển giao công nghệ cung cấp cho các học viên những kiến thức về quản lý, sử dụng, quản trị, vận hành toàn bộ thiết bị/giải pháp

- Đối tượng: Cán bộ quản trị/vận hành hệ thống

- Nội dung hướng dẫn sử dụng cho từng hạng mục theo phạm vi cung cấp đáp ứng yêu cầu:

+ Có thuyết minh rõ nội dung đào tạo và hướng dẫn quản trị on-job có đầy đủ tiêu chí: nội dung, đối tượng, thời gian;

+ Tài liệu triển khai, quản trị cho mỗi hệ thống do nhà thầu cung cấp, đảm bảo đủ các nội dung về hướng dẫn cài đặt, cấu hình, vận hành.

1.3.7 Uy tín nhà thầu

a. Uy tín của nhà thầu thông qua việc thực hiện các hợp đồng tương tự trước đây.

Nhà thầu cam kết đầy đủ nội dung sau trong E-HSDT:

- Nhà thầu không có hợp đồng tương tự chậm tiến độ hoặc bỏ dở do lỗi của nhà

thầu.

- Nhà thầu không có hợp đồng không thực hiện các cam kết về bảo hành, bảo trì, dịch vụ sau bán hàng.

b. Uy tín của nhà thầu về việc đảm bảo tình trạng pháp lý lành mạnh khi tham dự gói thầu

Có cam kết nội dung sau trong HSDT:

- Nhà thầu, Đại diện pháp luật của nhà thầu, các nhân sự tham gia thực hiện gói thầu không đang trong tình trạng thụ lý điều tra, khởi tố hoặc tranh chấp, kiện tụng mà thời gian xử lý tranh chấp kiện tụng nằm trong thời gian dự kiến thực hiện gói thầu

- Cam kết mọi cá nhân được giao nhiệm vụ liên hệ, nhiệm vụ thực hiện các công việc thuộc gói thầu đều có lý lịch tư pháp rõ ràng, không có tiền án tiền sự và nhà thầu sẵn sàng cung cấp lý lịch tư pháp đầy đủ nếu chủ đầu tư có yêu cầu.

- Nhà thầu hoàn thành đầy đủ nghĩa vụ theo quy định của pháp luật trong việc sử dụng lao động (Sử dụng nhân sự trong độ tuổi lao động theo quy định, có ký hợp đồng lao động trong trường hợp phải ký hợp đồng lao động và hoàn tất các nghĩa vụ trả lương, thù lao, đóng bảo hiểm bắt buộc và các chế độ khác đầy đủ và đúng thời hạn theo quy định của Pháp luật…)

- Nhà thầu có cam kết không có các hành vi vi phạm qui định về mua, bán trái phép hóa đơn, gian lận thuế hoặc trốn thuế theo quy định của pháp luật trong 3 năm gần nhất.

- Nhà thầu có cam kết tuân thủ các quy định của pháp luật về trụ sở chính và địa điểm kinh doanh theo quy định của pháp luật.

- Cam kết tuân thủ trách nhiệm đền bù đối với mọi thiệt hại đối với Chủ đầu tư và các bên liên quan gây ra do lỗi của Nhà thầu trong quá trình thực hiện gói thầu.

c. Uy tín của nhà thầu trong quá trình tham gia hoạt động đấu thầu

- Cam kết không bị kết luận vi phạm quy định về đấu thầu ở bất kỳ gói thầu nào trong vòng 3 năm gần nhất trước thời điểm đóng thầu;

- Cam kết không đang bị bất kỳ Chủ đầu tư, Chủ đầu tư nào cấm tham gia hoạt động đấu thầu trong vòng 3 năm gần nhất trước thời điểm đóng thầu; (Trường hợp các kết luận công khai trên hệ thống mạng đấu thầu quốc gia chưa kịp xử lý đính chính trước thời điểm dự thầu nhà thầu có thể cung cấp xác nhận đính chính của đơn vị Chủ đầu tư có kết luận vi phạm để chứng minh)

d. Uy tín của nhà thầu trong việc sử dụng các tài liệu thông tin trong hồ sơ dự thầu

Nhà thầu có cam kết các nội dung sau:

- Cam kết các thông tin kê khai và các tài liệu đính kèm trong hồ sơ dự thầu là chính xác và trung thực, nhà thầu đã xác minh tính chính xác và chân thực của thông tin, tài liệu trước khi dự thầu và sẵn sàng cung cấp thông tin, tài liệu chứng minh tính xác thực theo yêu cầu của Chủ đầu tư.

- Cam kết có đầy đủ bản gốc của các tài liệu đính kèm hồ sơ dự thầu và các tài liệu chứng minh nội dung thông tin kê khai tại E-HSDT, sẵn sàng cung cấp đối chiếu nếu có

yêu cầu của Chủ đầu tư.

Mục 2. Bản vẽ

Không có bản vẽ

Mục 3. Kiểm tra và thử nghiệm

3.1. Yêu cầu chung về kiểm tra và thử nghiệm

- Nhà thầu có trách nhiệm tổ chức kiểm tra và thử nghiệm các nội dung có liên quan trong gói thầu để đảm bảo đáp ứng đầy đủ các yêu cầu kỹ thuật nêu tại Mục 1.2.2. của Chương này

- Nhà thầu phải cung cấp các công cụ, thiết bị kiểm tra (nếu cần thiết) và tài liệu hướng dẫn cần thiết để thực hiện kiểm tra và thử nghiệm

- Kết quả kiểm tra và thử nghiệm phải được lập thành biên bản, có chữ ký xác nhận của đại diện Chủ đầu tư và Nhà thầu.

- Nhà thầu chịu toàn bộ chi phí liên quan đến kiểm tra va thử nghiệm, bao gồm chi phí nhân sự, thiết bị và chi phí phát sinh khác như thuê đơn vị có chức năng để kiểm tra, đánh giá chất lượng hàng hóa trước khi bàn giao khi có yêu cầu của chủ đầu tư (trong trường hợp có nghi ngờ về chất lượng hàng hóa).

3.2. Nội dung kiểm tra và thử nghiệm

3.2.1. Kiểm tra hàng hóa trước khi thi công

- Trước khi tổ chức kiểm tra hàng hóa, Nhà thầu có văn bản thông báo kế hoạch giao hàng để Chủ đầu tư bố trí nhân sự kiểm tra hàng hóa. Tại thời điểm kiểm tra hàng hóa, hai Bên sẽ thực hiện kiểm tra sơ bộ thông số kỹ thuật các hàng hóa do Nhà thầu cung cấp gồm chủng loại, số lượng, xuất xứ…, nếu hàng hóa đáp ứng yêu cầu thì cán bộ kỹ thuật hai Bên sẽ tiến hành ký Biên bản kiểm tra hàng hóa.

- Nếu các hàng hóa không đạt yêu cầu sẽ dược trả lại cho Nhà thầu và nhà thầu phải có trách nhiệm bổ sung hoặc thay thế hàng hóa mới chịu phạt chậm thực hiện hợp đồng nếu hàng hóa bổ sung hoặc thay thế không đảm bảo tiến độ hợp đồng yêu cầu.

- Nội dung kiểm tra hàng hóa là thiết bị phần cứng:

+ Kiểm tra về số lượng và chủng loại

+ Kiểm tra về chất lượng và xuất xứ

+ Kiểm tra các thông số phần cứng để xác minh đáp ứng yêu cầu của hợp đồng

- Nội dung kiểm tra hàng hóa là phần mềm thương mại:

+ Kiểm tra về số lượng và chủng loại

+ Kiểm tra tính năng phần mềm

3.2.2. Lắp đặt, cài đặt, hàng hóa

Trong vòng 15 ngày sau khi hợp đồng có hiệu lực, cán bộ kỹ thuật của Nhà thầu có trách nhiệm thực hiện khảo sát yêu cầu lắp đặt thiết bị và lập phương án tổ chức triển khai, kịch bản nghiệm thu các thiết bị, phần mềm trong phạm vi gói thầu.

Việc lắp đặt, cài đặt hàng hóa chỉ được thực hiện khi phương án triển khai được đại diện lãnh đạo của Chủ đầu tư thông qua. Công việc này phải được thực hiện bởi các nhân sự có đầy đủ năng lực cho việc triển khai.

3.2.3. Kiểm tra đánh giá bảo mật trước khi đưa vào vận hành:

- Rá soát kiểm tra lỗ thổng bảo mật các thiết bị và phần mềm trong phạm vị gói thầu: Tiêu chuẩn đành giá; Lên kịch bản, các phướng án đánh giá; thu thập thông tin; Phân tích, nhận dạng điểm yếu; Báo cáo

- Kiểm tra tiêu chuẩn cấu hình an toàn thiết bị

- Báo cáo kiểm tra đánh giá an toàn thông tin là một phần của Biên bản nghiệm thu bàn giao hàng hóa của hợp đồng

3.3. Quy trình kiểm tra và thử nghiệm

- Lập kế hoạch kiểm tra và thử nghiệm: Nhà thầu phải lập kế hoạch chi tiết, bao gồm các bước thực hiện, thời gian, nhân sự tham gia và các công cụ sử dụng. Kế hoạch này phải trình cho Chủ đầu tư trước khi thực hiện.

- Thực hiện kiểm tra va thử nghiệm

+ Nhà thầu thực hiện kiểm tra và thử nghiệm theo kế hoạch đã được phê duyệt

+ Đại diện Chủ đầu tư có quyền giám sát toàn bộ quá trình

Kết quả kiểm tra thử nghiệm: Sau khi hoàn thành, hai bên ký xác nhận các biên bản theo yêu cầu của hợp đồng

Xử lý sự cố: Nếu phát hiện hàng hóa hoặc dịch vụ không đạt yêu cầu, Nhà thầu phải khắc phục trong thời gian tối đa 03 ngày làm việc kể từ khi nhận được thông báo từ Chủ đầu tư. Sau khi khắc phục, Nhà thầu tổ chức kiểm tra và thử nghiệm lại. Chủ đầu tư có quyền chấm dựt hợp đồng nếu Nhà thầu không khắc phục được sự cố sau quá 03 lần kiểm tra, thử nghiệm không đáp ứng yêu cầu.