BỘ CÔNG AN **CỤC CẢNH SÁT PCCC VÀ CNCH**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 1425 /PCCC&CNCH-P1	*Hà Nội, ngày 15 tháng 5 năm 2025*

Kính gửi: .....

.....

Cục Cảnh sát phòng cháy, chữa cháy và cứu nạn, cứu hộ (PCCC và CNCH) dự kiến thuê dịch vụ di chuyển máy chủ (có bảng kê chi tiết các nội dung công việc gửi kèm theo).

Nếu Công ty có khả năng cung cấp dịch vụ, đề nghị cung cấp bản chào giá của dịch vụ cho Cục Cảnh sát PCCC và CNCH.

Hồ sơ chào giá của Công ty đề nghị gửi về Cục Cảnh sát PCCC và CNCH, thời hạn: Chậm nhất là ngày 20/5/2025; địa chỉ: Số 01 Vũ Hữu, Nhân Chính, Thanh Xuân, Hà Nội./.

Nơi nhận:
- Như trên;
- Đ/c Cục trưởng (để báo cáo);
- Lưu: VT, P1.

KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

Đại tá Hoàng Ngọc Huynh

THÔNG SỐ NỘI DUNG DỊCH VỤ CUNG CẤP

(Kèm theo Văn bản số /PCCC&CNCH-P1 ngày /05/2025)

Stt	Nội dung công việc
1	**Kiểm tra, đánh giá, đề xuất và dịch chuyển và cấu hình hệ thống vật lý**
1.1	Đánh giá hiện trạng hạ tầng mạng và máy chủ vật lý, đánh giá tuổi thọ thiết bị, kiểm tra nhật ký lỗi phần cứng 5 máy chủ vật lý
1.2	Đánh giá hiện trạng hạ tầng mạng và máy chủ vật lý, đánh giá tuổi thọ thiết bị, kiểm tra nhật ký lỗi phần cứng 1 tường lửa và 2 bộ chuyển mạch
1.3	Đánh giá hiện trạng dịch vụ và hệ điều hành, phương án ảo hóa đang được cung cấp trên 05 máy chủ vật lý
1.4	Khảo sát đánh giá hiện trạng mô hình mạng 1 tường lửa và 2 bộ chuyển mạch
1.5	Khảo sát và ghi nhận nhu cầu nâng cấp hoặc cải thiện, để đáp ứng khối lượng công việc
1.6	Viết báo cáo hiện trạng phần cứng và phần mềm
1.7	Lập kế hoạch cải tạo hoặc mở rộng hạ tầng mạng, đảm bảo tính tương thích của hệ thống mới và tối ưu hóa hiệu suất và phù hợp với nhu cầu sử dụng
1.8	Lên kế hoạch tác động phần mềm, bao gồm tắt các dịch vụ, tắt thiết bị vật lý, vận chuyển, kiểm thử, tái triển khai lại hệ thống mới
1.9	Kiểm tra, khảo sát và đánh giá hạ tầng, thực hiện đo đạc và kiểm tra tốc độ, độ trễ mạng của khu vực mới
1.10	Đảm bảo hệ thống mạng đáp ứng các tiêu chuẩn kỹ thuật và phù hợp với quy định về an toàn thông tin
1.1	Tháo rời, vận chuyển, triển khai lại hệ thống máy chủ vật lý, 1 tường lửa và 2 bộ chuyển mạch từ Viettel IDC Hòa Lạc đến Trung tâm dữ liệu Bộ Công an (80 Trần Quốc Hoàn, Cầu Giấy, TP. Hà Nội), tài liệu hóa, kiểm tra lỗi vật lý qua nhật ký, thực hiện báo cáo bằng văn bản.
2	**Cấu hình thiết bị tường lửa, switch. Router và thiết bị quản lý Wi-Fi tập trung**
2.1	Khảo sát và đề xuất mô hình tường lửa phù hợp với quy mô và nhu cầu bảo mật của hệ thống mới dựa trên thực tế sử dụng, bao gồm quá trình tuning
2.2	Cài đặt tường lửa tại vị trí chiến lược trong hệ thống mạng để kiểm soát luồng dữ liệu ra/vào
2.3	Xây dựng và triển khai các chính sách kiểm soát truy cập (Access Control Policies) để ngăn chặn các truy cập không hợp lệ từ bên ngoài và hạn chế truy cập vào các tài nguyên quan trọng chỉ dành cho các đối tượng được cấp quyền
2.4	Cấu hình cơ chế phát hiện và ngăn chặn xâm nhập (Intrusion Detection and Prevention System - IDPS) để nhận diện và xử lý kịp thời các mối đe dọa dựa trên thực tế sử dụng, bao gồm quá trình tuning

2.5	Triển khai mã hóa dữ liệu khi truyền qua mạng để bảo mật thông tin dựa trên thực tế sử dụng, bao gồm quá trình tuning
2.6	Thiết lập các chính sách lọc web (Web Filtering) để chặn truy cập vào các trang web độc hại hoặc không phù hợp dựa trên thực tế sử dụng, bao gồm quá trình tuning
2.7	Áp dụng chính sách giám sát lưu lượng mạng để nhận diện các hành vi bất thường và tối ưu hóa sử dụng băng thông dựa trên thực tế sử dụng, bao gồm quá trình tuning
2.8	Cấu hình hệ thống tự động thông báo khi phát hiện các sự kiện bảo mật nghiêm trọng dựa trên thực tế sử dụng, bao gồm quá trình tuning
2.9	Sử dụng phần mềm chuyên dụng để quét và phát hiện các phần mềm độc hại trên toàn bộ hệ thống 5 máy chủ vật lý
2.10	Loại bỏ các mã độc, phần mềm không hợp lệ và khôi phục hệ thống bị ảnh hưởng
2.11	Cấu hình các chính sách bảo mật cho máy tính và hệ thống mạng (mật khẩu mạnh, giới hạn truy cập, mã hóa dữ liệu)
2.12	Tài liệu hóa quy trình vận hành và hướng dẫn đào tạo nhân sự bàn giao của khách hàng về nhận thức và tuân thủ các quy tắc an toàn thông tin
2.13	Quy hoạch các lớp mạng riêng cho dịch vụ, vùng quản lý thiết bị (Out of band management), vùng quản trị (VPN điều khiển từ xa, log tập trung) để cách ly các chức năng hệ thống, chống lây nhiễm chéo mã độc trong nội bộ dựa trên thực tế sử dụng, bao gồm quá trình tuning
2.14	Thiết lập cơ chế chống DDoS L4 dựa trên thực tế sử dụng, bao gồm quá trình tuning
2.15	Thiết lập chính sách lọc nội dung độc hại trên môi trường mạng dựa trên thực tế sử dụng, bao gồm quá trình tuning
2.16	Chi phí vận chuyển, vật tư triển khai bao gồm dây mạng, hạt mạng và phụ phí phát sinh