THỦ TƯỚNG CHÍNH PHỦ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 1017/QĐ-TTg	*Hà Nội, ngày 14 tháng 8 năm 2018*

VĂN PHÒNG UBND TỈNH TÂY NINH
ĐẾN Số: 2997
Ngày: 21/8/18
Chuyển: ...
- KGVX (bản)
- KSTTHC (bản)
- TTCBTH (bản)

QUYẾT ĐỊNH

Phê duyệt Đề án giám sát an toàn thông tin mạng đối với hệ thống, dịch vụ công nghệ thông tin phục vụ Chính phủ điện tử đến năm 2020, định hướng đến năm 2025

THỦ TƯỚNG CHÍNH PHỦ

Căn cứ Luật Tổ chức Chính phủ ngày 19 tháng 6 năm 2015;

Căn cứ Luật Công nghệ thông tin ngày 29 tháng 6 năm 2006;

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 2017 của Thủ tướng Chính phủ ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;

Căn cứ Nghị quyết 36a/NQ-CP ngày 14 tháng 10 năm 2015 của Chính phủ về Chính phủ điện tử;

Xét đề nghị của Bộ trưởng Bộ Thông tin và Truyền thông,

QUYẾT ĐỊNH:

Điều 1. Phê duyệt Đề án giám sát an toàn thông tin mạng đối với hệ thống, dịch vụ công nghệ thông tin phục vụ Chính phủ điện tử đến năm 2020, định hướng đến 2025 (sau đây gọi tắt là Đề án) với các nội dung chủ yếu sau:

I. MỤC TIÊU CỦA ĐỀ ÁN

1. Định hướng đến năm 2025

a) Mở rộng phạm vi, nâng cao năng lực giám sát an toàn mạng, an toàn hệ thống thông tin (gọi chung là giám sát an toàn thông tin mạng) cho Trung tâm giám sát an toàn thông tin mạng quốc gia tại Trung tâm ứng cứu khẩn cấp

máy tính Việt Nam (VNCERT) và các bộ, cơ quan ngang bộ, tỉnh, thành phố trực thuộc Trung ương, các nhà cung cấp dịch vụ hạ tầng mạng Internet (viết tắt là nhà mạng ISP) để tăng cường khả năng phát hiện sớm, cảnh báo kịp thời, chính xác về các sự kiện, sự cố, dấu hiệu, hành vi, mã độc xâm phạm, nguy cơ, điểm yếu, lỗ hổng có khả năng gây mất an toàn thông tin mạng đối với các hệ thống thông tin, dịch vụ công nghệ thông tin phục vụ Chính phủ điện tử (sau đây viết tắt là hệ thống thông tin phục vụ Chính phủ điện tử).

b) Nâng cao tính hệ thống, đồng bộ và chuẩn hóa công tác giám sát an toàn thông tin mạng cho hệ thống thông tin phục vụ Chính phủ điện tử trên phạm vi cả nước; tăng cường hiệu quả, khả năng phát hiện, ứng phó tấn công, sự cố an toàn thông tin mạng, hướng tới xây dựng hệ thống thông tin phục vụ Chính phủ điện tử bền vững.

c) Thiết lập được mạng lưới hệ thống giám sát an toàn thông tin mạng trên toàn quốc, đảm bảo liên kết, liên thông, phối hợp chặt chẽ, hiệu quả giữa giám sát tập trung của Trung tâm giám sát an toàn thông tin mạng quốc gia, giám sát của các nhà mạng ISP và giám sát cơ sở của chủ quản các hệ thống thông tin.

d) Phát triển được đội ngũ chuyên gia phục vụ giám sát an toàn thông tin mạng chuyên nghiệp và kỷ luật.

2. Mục tiêu cụ thể

a) Nâng cấp, mở rộng hệ thống giám sát an toàn thông tin mạng tại VNCERT thành Trung tâm giám sát an toàn thông tin mạng quốc gia nhằm nâng cao hiệu quả kết nối, thu thập, phân tích dữ liệu tập trung phục vụ giám sát an toàn thông tin cho hệ thống thông tin phục vụ Chính phủ điện tử tại các bộ, ngành, địa phương.

b) Tăng cường năng lực hệ thống quan trắc, giám sát cơ sở; áp dụng thống nhất chuẩn kết nối trao đổi thông tin giữa Trung tâm giám sát an toàn thông tin mạng quốc gia và các hệ thống quan trắc, giám sát cơ sở để giám sát an toàn thông tin mạng cho hệ thống thông tin phục vụ Chính phủ điện tử tại các bộ, ngành, địa phương.

c) Đảm bảo hệ thống giám sát an toàn thông tin mạng được thường xuyên cập nhật, nâng cấp để nâng cao khả năng chủ động, ứng phó tấn công mạng và đáp ứng kịp thời với sự thay đổi liên tục của công nghệ.

d) Đảm bảo đầy đủ điều kiện, kỹ thuật, mặt bằng để thiết lập các thiết bị quan trắc cơ sở trên hệ thống mạng Internet của các nhà mạng ISP kết nối với Trung tâm giám sát an toàn thông tin mạng quốc gia. Tăng cường giám sát an toàn thông tin mạng cho các hệ thống, dịch vụ hạ tầng mạng do nhà mạng ISP cung cấp có liên quan đến hệ thống thông tin phục vụ Chính phủ điện tử.

đ) Nâng cao năng lực và phát triển đội ngũ chuyên gia phục vụ giám sát an toàn thông tin mạng cho hệ thống thông tin phục vụ Chính phủ điện tử thông qua đào tạo, huấn luyện, bồi dưỡng kỹ năng, kỹ thuật và nghiệp vụ. Tăng cường chia sẻ thông tin, phối kết hợp giữa các đơn vị tham gia bảo đảm an toàn thông tin mạng cho hệ thống thông tin phục vụ Chính phủ điện tử nói riêng và cho các hạ tầng thông tin quan trọng của quốc gia nói chung.

II. NHIỆM VỤ VÀ GIẢI PHÁP

1. Xây dựng, hoàn thiện thể chế, tạo cơ sở pháp lý đầy đủ trong triển khai giám sát an toàn thông tin mạng đối với hệ thống, dịch vụ công nghệ thông tin phục vụ Chính phủ điện tử

a) Xây dựng, ban hành các cơ chế, chính sách, quy định, hướng dẫn về giám sát an toàn thông tin mạng, đảm bảo việc triển khai đồng bộ giữa Bộ Thông tin và Truyền thông, các bộ, ngành, địa phương, các nhà mạng ISP và tổ chức có liên quan; xây dựng các tiêu chuẩn, quy chuẩn, tài liệu kỹ thuật về giám sát, bảo đảm an toàn thông tin mạng, văn bản hướng dẫn phục vụ đầu tư hệ thống quan trắc, giám sát cơ sở và triển khai giám sát an toàn thông tin mạng cho hệ thống thông tin phục vụ Chính phủ điện tử.

b) Áp dụng phương thức giám sát trực tiếp và giám sát gián tiếp, theo hướng dẫn của Bộ Thông tin và Truyền thông và Cơ quan điều phối quốc gia VNCERT.

c) Triển khai đồng bộ các hệ thống kỹ thuật phục vụ giám sát an toàn thông tin mạng cho hệ thống thông tin phục vụ Chính phủ điện tử, bao gồm: Trung tâm giám sát an toàn thông tin mạng quốc gia đặt tại VNCERT; các hệ thống quan trắc và giám sát cơ sở đặt tại các bộ, ngành, địa phương; hệ thống quan trắc và giám sát tại nhà mạng ISP, trên quan điểm tận dụng tối đa các trang thiết bị hiện có kết hợp đầu tư mới, nâng cấp, bổ sung đảm bảo tính liên thông, đồng bộ và diện phủ.

d) Xây dựng, ban hành và triển khai áp dụng các tiêu chuẩn, giải pháp kỹ thuật đảm bảo việc trao đổi thông tin, kết nối, liên thông giữa hệ thống giám sát an toàn thông tin mạng quốc gia với hệ thống quan trắc, giám sát cơ sở tại các bộ, ngành, địa phương được liên tục, ổn định và hiệu quả.

đ) Xây dựng, ban hành các cơ chế, chính sách, định mức tài chính và các điều kiện cần thiết đảm bảo nguồn lực và hiệu quả công tác giám sát an toàn thông tin mạng cho hệ thống thông tin phục vụ Chính phủ điện tử.

e) Xây dựng, trình Thủ tướng Chính phủ phê duyệt quy định chế độ ưu đãi và cơ chế tài chính đặc thù cho nhân lực giám sát an toàn thông tin mạng, Trung tâm giám sát an toàn mạng quốc gia, bộ phận quản lý, vận hành hệ thống quan trắc, giám sát cơ sở nhằm xây dựng, phát triển nguồn nhân lực phục vụ giám sát, điều phối, ứng cứu, bảo đảm an toàn thông tin mạng cho Chính phủ điện tử và cơ quan nhà nước.

2. Nâng cao năng lực Trung tâm giám sát an toàn thông tin mạng quốc gia phục vụ Chính phủ điện tử

a) Đầu tư mở rộng, nâng cấp và bổ sung nguồn lực vận hành Trung tâm giám sát an toàn thông tin mạng quốc gia do VNCERT quản lý, tăng cường hệ thống giám sát trực tiếp và hệ thống giám sát gián tiếp nhằm mở rộng phạm vi giám sát, nâng cao năng lực phát hiện, cảnh báo, hỗ trợ xử lý các vụ tấn công, sự cố, mã độc, điểm yếu, lỗ hổng, rủi ro an toàn thông tin mạng cho hệ thống thông tin phục vụ Chính phủ điện tử. Triển khai giám sát gián tiếp cho các hệ thống, dịch vụ công nghệ thông tin phục vụ Chính phủ điện tử tại các bộ, ngành, địa phương. Khảo sát, lựa chọn một số hệ thống thông tin phục vụ Chính phủ điện tử quan trọng từ cấp độ 3 trở lên và hệ thống thông tin quan trọng quốc gia có điều kiện phù hợp để triển khai giám sát trực tiếp, tiến tới mở rộng phạm vi giám sát trên toàn quốc.

b) Phối hợp, hỗ trợ thiết lập một số thiết bị quan trắc, giám sát cơ sở tại các bộ, ngành, địa phương và các nhà mạng ISP để kết nối, chia sẻ thông tin, nhật ký, dữ liệu về Trung tâm giám sát an toàn thông tin mạng quốc gia phục vụ giám sát an toàn thông tin mạng cho hệ thống thông tin phục vụ Chính phủ điện tử; tổ chức thu thập, phân tích các thông tin, dữ liệu từ nhà mạng ISP phục vụ công tác phát hiện, cảnh báo sớm nguy cơ, sự cố an toàn thông tin mạng. Đầu tư, thiết lập hệ thống thiết bị và triển khai kiểm tra, đánh giá, giám sát mức độ an toàn thông tin cho hệ thống thông tin phục vụ chính phủ điện tử để kịp thời cảnh báo các nguy cơ, lỗ hổng, điểm yếu của hệ thống.

c) Đầu tư, nâng cấp, bổ sung trang thiết bị phần cứng, phần mềm và duy trì, vận hành, bảo dưỡng định kỳ cho các hệ thống của Trung tâm giám sát an toàn thông tin mạng quốc gia. Thuê và duy trì kênh kết nối Internet và truyền dữ liệu đủ lớn đảm bảo kết nối thông suốt từ Trung tâm giám sát an toàn mạng quốc gia tới các bộ, ngành, địa phương và các nhà mạng ISP. Cập nhật, mua bổ sung các mẫu mã độc, thông tin về sự cố, lỗ hổng, kỹ thuật tấn công, các công nghệ liên quan lĩnh vực an toàn thông tin mạng từ các nhà cung cấp nhằm nâng cao năng lực phát hiện sự cố, tấn công mạng cho Trung tâm giám sát an toàn thông tin mạng quốc gia.

d) Tổ chức thu thập, lưu trữ, phân tích, xây dựng cơ sở dữ liệu và hệ thống chia sẻ các báo cáo, cảnh báo nguy cơ, sự cố, tình hình an toàn thông tin mạng của Chính phủ điện tử; xây dựng cơ sở dữ liệu thông tin, dữ liệu giám sát và báo cáo phân tích sự cố phục vụ hoạt động nghiên cứu, phân tích và xử lý các tình huống mất an toàn thông tin có thể xảy ra. Tổ chức tuyên truyền, phổ biến để hướng dẫn và thu hút các tổ chức, doanh nghiệp, người dân tham gia đóng góp cho hoạt động giám sát an toàn thông tin mạng.

đ) Tăng cường nhân sự và thuê bổ sung chuyên gia an toàn thông tin để đảm bảo tính liên tục của hoạt động giám sát an toàn mạng 24giờ/7ngày; theo dõi, phân tích, điều tra, xác minh và kịp thời cảnh báo dấu hiệu tấn công, sự cố an toàn thông tin mạng liên quan đến các hệ thống thông tin phục vụ Chính phủ điện tử.

3. Thiết lập và nâng cao hiệu quả hoạt động các hệ thống quan trắc cơ sở và giám sát an toàn mạng cơ sở của các bộ, ngành, địa phương

a) Các bộ, ngành, địa phương đầu tư xây dựng hoặc thuê dịch vụ thiết lập và duy trì hệ thống quan trắc, giám sát cơ sở phục vụ giám sát an toàn thông tin mạng cho hệ thống thông tin phục vụ Chính phủ điện tử thuộc quyền quản lý; các tổ chức được giao quản lý, vận hành hệ thống thông tin quan trọng quốc gia, các tập đoàn, tổng công ty lớn của Nhà nước chủ động xây dựng hoặc thuê dịch vụ thiết lập hệ thống quan trắc, giám sát hệ thống thông tin thuộc quyền quản lý; các cơ quan, đơn vị theo nhu cầu thực tế đầu tư mua mới các thiết bị phần cứng, phần mềm, phù hợp với mục tiêu giám sát; kết nối hệ thống thiết bị quan trắc, giám sát cơ sở của đơn vị với hệ thống giám sát an toàn thông tin mạng quốc gia theo hướng dẫn của Bộ Thông tin và Truyền thông và Cơ quan điều phối quốc gia VNCERT.

b) Phối hợp, lấy ý kiến hướng dẫn của Bộ Thông tin và Truyền thông và Cơ quan điều phối quốc gia khi đầu tư xây dựng mới hoặc thuê, mua, triển khai hệ thống quan trắc, giám sát cơ sở; áp dụng các quy trình kỹ thuật, kết nối, đồng bộ theo quy định của Bộ Thông tin và Truyền thông phục vụ giám sát an toàn thông tin mạng cho hệ thống thông tin phục vụ Chính phủ điện tử.

c) Đảm bảo các điều kiện kỹ thuật theo yêu cầu của Bộ Thông tin và Truyền thông và Cơ quan điều phối quốc gia VNCERT để Trung tâm giám sát an toàn thông tin mạng quốc gia triển khai giám sát trực tiếp hoặc gián tiếp cho các hệ thống thông tin phục vụ Chính phủ điện tử từ cấp độ 3 trở lên và các hệ thống thông tin quan trọng quốc gia thuộc quyền quản lý. Chủ quản hệ thống thông tin, đơn vị quản lý, vận hành hệ thống thông tin, nhà mạng ISP, các tổ chức, doanh nghiệp quản lý các hệ thống thông tin quan trọng quốc gia phải cung cấp các thông tin kỹ thuật về hạ tầng, hệ thống thông tin, ứng dụng, dịch vụ, địa chỉ IP Internet, bố trí địa điểm, cổng kết nối, các điều kiện kỹ thuật, thiết lập, cấu hình, lắp đặt các thiết bị cần thiết theo yêu cầu của Cơ quan điều phối quốc gia VNCERT để Trung tâm giám sát an toàn thông tin mạng quốc gia triển khai các hệ thống quan trắc và thực hiện giám sát trực tiếp hoặc gián tiếp cho các hệ thống thông tin phục vụ Chính phủ điện tử và hệ thống thông tin quan trọng khác do mình quản lý. Cung cấp các thông tin, nhật ký, dữ liệu giám sát và phối hợp chặt chẽ, thực hiện các yêu cầu của Cơ quan điều phối quốc gia trong công tác giám sát, ứng cứu xử lý sự cố, bảo đảm an toàn thông tin mạng cho hệ thống thông tin phục vụ Chính phủ điện tử và hệ thống thông tin quan trọng quốc gia.

d) Tổ chức đào tạo, huấn luyện nâng cao trình độ, kỹ năng cho đội ngũ nhân lực giám sát an toàn thông tin mạng và nâng cao nhận thức, kiến thức an toàn thông tin cho người dùng và cán bộ liên quan đến hệ thống thông tin phục vụ Chính phủ điện tử. Các bộ, ngành, địa phương tăng cường thuê dịch vụ kỹ thuật và nhân sự trong triển khai giám sát, bảo đảm an toàn thông tin mạng cho hệ thống thông tin phục vụ Chính phủ điện tử.

đ) Đầu tư, thiết lập hệ thống thiết bị và thường xuyên triển khai kiểm tra, đánh giá, giám sát mức độ an toàn thông tin cho hệ thống thông tin phục vụ chính phủ điện tử thuộc quyền quản lý. Định kỳ 6 tháng và hàng năm tổ chức kiểm tra, đánh giá hoạt động của hệ thống quan trắc, giám sát an toàn thông tin mạng cơ sở và việc kết nối, phối hợp, trao đổi thông tin, dữ liệu giám sát, cảnh báo sự cố an toàn thông tin mạng với Trung tâm giám sát an toàn thông tin mạng quốc gia, gửi Bộ Thông tin và Truyền thông (Trung tâm VNCERT) tổng hợp, báo cáo Thủ tướng Chính phủ.

4. Đẩy mạnh hoạt động giám sát an toàn thông tin mạng của các nhà mạng ISP và doanh nghiệp cung cấp hệ thống, dịch vụ phục vụ Chính phủ điện tử

a) Các nhà mạng ISP và doanh nghiệp cung cấp dịch vụ hạ tầng, trung tâm dữ liệu, công nghệ thông tin có liên quan đến hệ thống thông tin phục vụ Chính phủ điện tử phải thiết lập và tăng cường hệ thống quan trắc, giám sát an toàn thông tin mạng đối với hệ thống mạng, trung tâm dữ liệu, hệ thống công nghệ thông tin do mình quản lý. Các doanh nghiệp và nhà mạng ISP thực hiện giám sát an toàn thông tin mạng đối với các kênh truyền, dịch vụ Internet, dịch vụ trung tâm dữ liệu, hệ thống và dịch vụ công nghệ thông tin của mình phục vụ Chính phủ điện tử của các bộ, ngành, địa phương và kết nối, đồng bộ với Trung tâm giám sát an toàn thông tin mạng quốc gia theo hướng dẫn của Cơ quan điều phối quốc gia VNCERT. Định kỳ hàng quý và đột xuất khi có yêu cầu của Cơ quan điều phối quốc gia, các doanh nghiệp, nhà mạng ISP báo cáo kết quả thực hiện giám sát và thông tin sự cố an toàn thông tin mạng có liên quan. Kết nối, cung cấp, chia sẻ các thông tin, dữ liệu, nhật ký liên quan về Trung tâm giám sát an toàn thông tin mạng quốc gia theo yêu cầu của Cơ quan điều phối quốc gia VNCERT nhằm phục vụ phân tích, giám sát an toàn thông tin.

b) Cung cấp các thông tin kỹ thuật về hệ thống mạng, bố trí địa điểm, cổng kết nối, các điều kiện kỹ thuật, thiết lập, cấu hình đường truyền, thiết bị theo yêu cầu của Cơ quan điều phối quốc gia VNCERT để Trung tâm giám sát an toàn thông tin mạng quốc gia thiết lập hệ thống quan trắc cơ sở và thu thập các thông tin, dữ liệu từ hệ thống mạng Internet và Trung tâm dữ liệu, hệ thống do doanh nghiệp, nhà mạng ISP quản lý phục vụ giám sát, phân tích an toàn thông tin mạng. Hỗ trợ, phối hợp chặt chẽ và thực hiện các yêu cầu của Cơ quan điều phối quốc gia trong công tác giám sát, ứng cứu xử lý sự cố, bảo đảm an toàn thông tin mạng cho hệ thống thông tin phục vụ Chính phủ điện tử.

c) Hỗ trợ, phối hợp triển khai hoạt động Giám sát an toàn thông tin mạng trên mạng Internet của nhà mạng ISP; chia sẻ thông tin, nhật ký, dữ liệu giám sát về tình hình an toàn thông tin mạng giữa nhà mạng ISP và doanh nghiệp với Cơ quan điều phối quốc gia VNCERT; phối hợp chặt chẽ với Cơ quan điều phối quốc gia, chủ quản hệ thống Chính phủ điện tử trong công tác giám sát an toàn thông tin mạng và điều phối ứng cứu sự cố có liên quan tới dịch vụ mạng Internet, hệ thống, dịch vụ công nghệ thông tin phục vụ Chính phủ điện tử do mình cung cấp.

5. Xây dựng, phát triển nguồn nhân lực giám sát, bảo đảm an toàn thông tin mạng quốc gia

a) Cơ quan điều phối quốc gia VNCERT xây dựng, trình Bộ Thông tin và Truyền thông ban hành tiêu chuẩn chức danh, vị trí việc làm, chứng chỉ kỹ năng, kỹ thuật an toàn thông tin, giám sát, ứng cứu sự cố và quy định về đào tạo, sát hạch, cấp chứng chỉ cho đội ngũ nhân lực kỹ thuật, cán bộ, chuyên gia an toàn thông tin, giám sát, phân tích, ứng cứu, bảo đảm an toàn thông tin mạng.

b) Xây dựng và triển khai các chương trình, dự án đào tạo, phát triển nguồn nhân lực giám sát, ứng cứu sự cố, bảo đảm an toàn thông tin mạng; tổ chức các khóa đào tạo, bồi dưỡng, sát hạch, cấp chứng chỉ và các chương trình huấn luyện, diễn tập nâng cao kỹ năng, kỹ thuật và nghiệp vụ cho đội ngũ nhân lực, chuyên gia trong các cơ quan nhà nước và các thành viên mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia.

c) Đẩy mạnh nghiên cứu, đón đầu các thành tựu khoa học công nghệ, phát triển các giải pháp công nghệ trong nước; hỗ trợ các doanh nghiệp phát triển các sản phẩm nội địa; tổ chức kiểm thử, đánh giá, thẩm định các sản phẩm an toàn thông tin nội địa và chứng nhận, khuyến nghị để các cơ quan, tổ chức, doanh nghiệp nhà nước ưu tiên lựa chọn các sản phẩm nội địa đã qua thẩm định vào sử dụng trong các gói thầu, dự án mua sắm, đầu tư an toàn thông tin, công nghệ thông tin phục vụ Chính phủ điện tử nói riêng và của cơ quan nhà nước nói chung.

d) Đầu tư xây dựng, phát triển nguồn nhân lực chất lượng cao, kết hợp thuê đội ngũ chuyên gia phục vụ giám sát, phân tích, cảnh báo nguy cơ mất an toàn thông tin mạng và hỗ trợ ứng cứu, xử lý sự cố cho hệ thống thông tin phục vụ Chính phủ điện tử; xây dựng, phát triển đội ngũ chuyên gia trình độ cao trong các tổ chức, doanh nghiệp để nghiên cứu và phát triển các công nghệ, giải pháp an toàn thông tin phục vụ giám sát, bảo đảm an toàn thông tin mạng cho hệ thống thông tin phục vụ Chính phủ điện tử.

đ) Khuyến khích các cơ quan nhà nước thuê dịch vụ kỹ thuật và nhân sự trong triển khai giám sát an toàn thông tin mạng cho hệ thống thông tin phục vụ Chính phủ điện tử.

III. KINH PHÍ THỰC HIỆN

1. Nguồn vốn

Kinh phí thực hiện Đề án được bố trí từ các nguồn sau:

- Nguồn ngân sách nhà nước (ngân sách trung ương, ngân sách địa phương) theo phân cấp quản lý ngân sách hiện hành được bố trí trong dự toán hàng năm cho các bộ, cơ quan trung ương và địa phương theo quy định pháp luật ngân sách nhà nước. Ưu tiên bố trí lồng ghép vào các chương trình quốc gia phát triển công nghệ cao, chương trình phát triển sản phẩm quốc gia.

- Quỹ Dịch vụ viễn thông công ích Việt Nam theo quy định của pháp luật.

- Nguồn thu của cơ quan, đơn vị được phép để lại theo quy định.

- Nguồn vốn hợp pháp khác: Nguồn viện trợ không hoàn lại, nguồn tài trợ, hỗ trợ của tổ chức, cá nhân và các nguồn vốn xã hội khác.

2. Nguyên tắc phân bổ vốn

a) Nguồn vốn từ ngân sách trung ương và nguồn vốn khác do cơ quan trung ương quản lý được phân bổ để thực hiện các nhiệm vụ, dự án thuộc Quyết định này do các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Cơ quan trung ương chủ trì và một số nhiệm vụ khác như quy định trong Phụ lục kèm theo. Các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Cơ quan trung ương căn cứ các nội dung, nhiệm vụ được giao, tổ chức xây dựng kế hoạch, dự án, dự toán kinh phí, và làm thủ tục phê duyệt, phân bổ kinh phí từ ngân sách trung ương và nguồn vốn khác do trung ương quản lý để thực hiện theo quy định hiện hành.

b) Ngân sách địa phương và nguồn vốn khác do địa phương quản lý bảo đảm kinh phí đối với các dự án, nhiệm vụ thuộc Quyết định này do các cơ quan thuộc địa phương thực hiện. Ủy ban nhân dân các tỉnh, thành phố trực thuộc trung ương căn cứ các nội dung, nhiệm vụ được giao, tổ chức xây dựng kế hoạch, dự án, dự toán kinh phí, phê duyệt theo thẩm quyền hoặc trình hội đồng nhân dân phê duyệt, phân bổ kinh phí từ ngân sách địa phương và nguồn vốn khác do địa phương quản lý để thực hiện theo quy định hiện hành.

c) Ưu tiên nguồn vốn viện trợ không hoàn lại, nguồn vốn khoa học và công nghệ, nguồn vốn từ các chương trình quốc gia phát triển công nghệ cao, chương trình phát triển sản phẩm quốc gia để phát triển sản phẩm, dịch vụ, giải pháp an toàn thông tin trong nước và các nhiệm vụ, dự án khác thuộc Quyết định này.

d) Đối với các nội dung, nhiệm vụ sử dụng ngân sách nhà nước, các cơ quan, tổ chức căn cứ các nội dung, nhiệm vụ tại Quyết định này, hàng năm lập dự toán ngân sách, tổng hợp chung trong kế hoạch ngân sách của cơ quan, tổ chức mình, gửi cơ quan tài chính cùng cấp để tổng hợp, trình phê duyệt phân bổ kinh phí theo quy định của pháp luật về ngân sách nhà nước để thực hiện.

3. Đưa các nhiệm vụ, dự án ưu tiên sử dụng nguồn vốn từ Quỹ Dịch vụ viễn thông công ích Việt Nam quy định tại Quyết định này, đặc biệt là các nhiệm vụ, dự án tại Phụ lục II vào chương trình cung cấp dịch vụ viễn thông công ích để triển khai thực hiện. Bộ Thông tin và Truyền thông căn cứ các nội dung, nhiệm vụ được giao, tổ chức xây dựng kế hoạch, dự án cụ thể, dự toán kinh phí và làm thủ tục phê duyệt, triển khai theo quy định.

Với những dự án, nhiệm vụ không bố trí được kinh phí từ Quỹ Dịch vụ viễn thông công ích Việt Nam thì được xem xét, phân bổ từ nguồn ngân sách trung ương để triển khai thực hiện. Bộ Kế hoạch và đầu tư, Bộ Tài chính phối hợp với Bộ Thông tin và Truyền thông rà soát những nhiệm vụ, dự án tại Phụ lục I, Phụ lục II kèm theo Quyết định này để bổ sung, đưa vào kế hoạch ngân sách, kế hoạch đầu tư công đến năm 2020 và giai đoạn 2021 - 2025 để bố trí, phân bổ, bổ sung kinh phí thực hiện.

IV. TỔ CHỨC THỰC HIỆN

1. Các bộ, ngành, địa phương và các cơ quan, tổ chức, doanh nghiệp khác

a) Căn cứ nội dung Quyết định này, văn bản hướng dẫn về giám sát an toàn thông tin mạng của Bộ Thông tin và Truyền thông, Khung Kiến trúc Chính phủ điện tử Việt Nam, Kiến trúc Chính phủ điện tử cấp bộ, Kiến trúc Chính quyền điện tử cấp tỉnh để xây dựng và tổ chức triển khai hoạt động giám sát an toàn mạng tại các khoản 1, 3, 4, 5 Phần II, và các nội dung khác có liên quan thuộc Quyết định này.

b) Tổ chức kiểm tra, đánh giá, thực hiện báo cáo 6 tháng, hàng năm và đột xuất về tình hình thực hiện Quyết định này theo hướng dẫn và yêu cầu của Bộ Thông tin và Truyền thông để tổng hợp, báo cáo Thủ tướng Chính phủ.

c) Bảo đảm kinh phí (chi đầu tư phát triển, chi thường xuyên) để thực hiện các nhiệm vụ, dự án thuộc Quyết định này; tăng cường thuê dịch vụ để triển khai hoạt động Giám sát an toàn thông tin mạng trong phạm vi ngành, lĩnh vực, địa phương mình.

d) Các cơ quan, tổ chức quản lý, vận hành các cơ sở dữ liệu quốc gia, các hệ thống thông tin quan trọng quốc gia, các tổ chức, tập đoàn, tổng công ty lớn của nhà nước có quản lý các hệ thống thông tin quan trọng thuộc các lĩnh vực quan trọng ưu tiên bảo đảm an toàn thông tin mạng xây dựng và tổ chức triển khai hoạt động giám sát an toàn mạng đối với hệ thống của mình theo quy định tại các khoản 3, 4, 5 Phần II và các nội dung khác có liên quan thuộc Quyết định này.

đ) Các cơ quan, tổ chức, doanh nghiệp cung cấp dịch vụ mạng, cho thuê chỗ (hosting), trung tâm dữ liệu, dịch vụ cho thuê phần mềm, hệ thống, thiết bị, dịch vụ công nghệ thông tin, an toàn thông tin, thanh toán điện tử, dịch vụ công trực tuyến phục vụ chính phủ điện tử phải triển khai giám sát an toàn thông tin mạng cho phần dịch vụ liên quan theo các quy định và văn bản hướng dẫn của Bộ Thông tin và Truyền thông.

2. Bộ Thông tin và Truyền thông

a) Chủ trì, phối hợp với các bộ, ngành, địa phương, các cơ quan, tổ chức, doanh nghiệp liên quan triển khai, đôn đốc thực hiện, kiểm tra và định kỳ tổng hợp, đánh giá kết quả thực hiện Quyết định này; báo cáo Thủ tướng Chính phủ kết quả thực hiện và đề xuất điều chỉnh, bổ sung nội dung của Quyết định này trong trường hợp cần thiết.

b) Thành lập Ban điều hành để điều phối, đôn đốc, kiểm tra, hướng dẫn việc triển khai Quyết định này và điều hành việc phối hợp, chia sẻ trong công tác giám sát an toàn thông tin mạng do đại diện lãnh đạo Bộ Thông tin và Truyền thông làm Trưởng ban và bộ phận thường trực Ban điều hành là Cơ quan điều phối quốc gia VNCERT thuộc Bộ Thông tin và Truyền thông. Chủ trì tổ chức triển khai các nội dung, nhiệm vụ thuộc Quyết định này ở cấp quốc gia.

c) Chủ trì, phối hợp cùng các cơ quan, tổ chức liên quan triển khai các khoản 1, 2, 5 Phần II và các nội dung khác có liên quan tại Quyết định này.

d) Hướng dẫn, phối hợp với các bộ, ngành, địa phương và các cơ quan, doanh nghiệp liên quan trong triển khai thực hiện các khoản 3, 4 Phần II và các nội dung khác thuộc Quyết định này.

đ) Chỉ đạo VNCERT thực hiện chức năng điều phối quốc gia về giám sát an toàn thông tin cho hệ thống thông tin phục vụ chính phủ điện tử; tăng cường, đẩy mạnh hoạt động của Trung tâm giám sát an toàn thông tin mạng quốc gia; xây dựng chương trình, triển khai các khóa đào tạo, huấn luyện, diễn tập về giám sát, cảnh báo, ứng cứu, phòng chống tấn công trên không gian mạng phù hợp thực tế; triển khai thực hiện các nhiệm vụ khác tại Quyết định này.

3. Văn phòng Chính phủ

a) Chủ trì, phối hợp với Bộ Thông tin và Truyền thông đầu tư, nâng cấp hệ thống thiết bị quan trắc, giám sát cơ sở phục vụ giám sát hệ thống thông tin phục vụ Chính phủ điện tử tại Văn phòng chính phủ.

b) Phối hợp với Bộ Thông tin và truyền thông thực hiện các nhiệm vụ được giao tại khoản 3 Phần II và các nhiệm vụ khác có liên quan thuộc Quyết định này.

4. Bộ Tài chính

a) Cân đối, bố trí ngân sách Nhà nước nguồn chi thường xuyên theo quy định để thực hiện các nhiệm vụ, dự án thuộc Quyết định này.

b) Chủ trì, phối hợp với Bộ Thông tin và Truyền thông hướng dẫn việc lập, dự toán, quản lý, sử dụng ngân sách nhà nước để triển khai các nhiệm vụ, dự án thuộc Quyết định này. Phối hợp với Bộ Thông tin và Truyền thông triển khai nhiệm vụ tại điểm đ khoản 1 Phần II Quyết định này.

5. Bộ Kế hoạch và Đầu tư

a) Bố trí kinh phí từ nguồn ngân sách nhà nước chi đầu tư phát triển theo quy định để thực hiện các nhiệm vụ, dự án thuộc Quyết định này.

b) Chủ trì, phối hợp với Bộ Thông tin và Truyền thông xem xét bổ sung các dự án, nhiệm vụ thuộc Quyết định này vào các chương trình, kế hoạch đầu tư công, chương trình mục tiêu về công nghệ thông tin và các chương trình, kế hoạch liên quan và cân đối, bố trí các nguồn vốn để đẩy nhanh tiến độ thực hiện.

6. Bộ Khoa học và Công nghệ

a) Chủ trì, phối hợp với Bộ thông tin và Truyền thông và các bộ, ngành, địa phương có liên quan tổ chức nghiên cứu tiêu chuẩn, công nghệ, giải pháp, sản phẩm phục vụ giám sát an toàn thông tin mạng cho hệ thống thông tin phục vụ Chính phủ điện tử.

b) Chủ trì, phối hợp với các cơ quan chức năng liên quan xem xét, bố trí nguồn vốn khoa học và công nghệ, nguồn vốn từ các chương trình quốc gia phát triển công nghệ cao, chương trình phát triển sản phẩm quốc gia để triển khai các nhiệm vụ, dự án thuộc Quyết định này. Đẩy mạnh nghiên cứu, đón đầu các thành tựu khoa học công nghệ, phát triển và hỗ trợ áp dụng các giải pháp, sản phẩm, dịch vụ an toàn thông tin trong nước.

7. Các nhà mạng ISP và doanh nghiệp cung cấp dịch vụ hạ tầng, công nghệ thông tin

a) Chủ động phối hợp với VNCERT và các cơ quan, đơn vị chức năng tại các bộ, ngành, địa phương xây dựng, tổ chức đầu tư, triển khai hoạt động giám sát an toàn thông tin mạng quy định tại khoản 4 Phần II và các nội dung liên quan tại Quyết định này.

b) Tổ chức đào tạo, huấn luyện, diễn tập, rèn luyện, nâng cao kỹ năng cho đội ngũ cán bộ thực hiện nhiệm vụ giám sát, bảo đảm an toàn thông tin mạng thuộc đơn vị mình theo các chương trình đào tạo và tiêu chuẩn, chứng chỉ theo hướng dẫn của Bộ Thông tin và Truyền thông.

c) Định kỳ hàng quý, hàng năm hoặc đột xuất theo yêu cầu của cơ quan chức năng, tổ chức kiểm tra, đánh giá, báo cáo kết quả thực hiện giám sát an toàn thông tin mạng trên hệ thống do mình quản lý và tình hình thực hiện các nhiệm vụ được giao tại Quyết định này gửi Trung tâm VNCERT, Bộ Thông tin và Truyền thông để tổng hợp, báo cáo Thủ tướng Chính phủ.

d) Bảo đảm kinh phí để thực hiện các nhiệm vụ được giao tại Quyết định này.

Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày ký ban hành.

Điều 3. Bộ trưởng, Thủ trưởng các cơ quan ngang bộ, Thủ trưởng cơ quan thuộc Chính phủ, Chủ tịch Ủy ban nhân dân các tỉnh, thành phố trực thuộc trung ương, Thủ trưởng các nhà mạng ISP và các tổ chức, doanh nghiệp liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Ban Bí thư Trung ương Đảng;
- Thủ tướng, các Phó Thủ tướng Chính phủ;
- Các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ;
- UBND các tỉnh, thành phố trực thuộc trung ương;
- Văn phòng Trung ương Đảng;
- Văn phòng Tổng Bí thư;
- Văn phòng Chủ tịch nước;
- Văn phòng Quốc hội;
- Tòa án nhân dân tối cao;
- Viện kiểm sát nhân dân tối cao;
- Kiểm toán nhà nước;
- Ủy ban trung ương Mặt trận Tổ quốc Việt Nam;
- Cơ quan trung ương của các đoàn thể;
- Các tập đoàn kinh tế và tổng công ty nhà nước;
- Hiệp hội An toàn thông tin VN, Hiệp hội Internet VN, Hiệp hội phần mềm và dịch vụ CNTT VN, Hiệp hội Thương mại điện tử VN;
- VPCP: BTCN, các PCN, Trợ lý TTg, TGĐ Cổng TTĐT, các Vụ, đơn vị: TH, KTTH, QHĐP, CN, KGVX, TTTH;
- Lưu: VT, KSTT (2).XH 243

KT. THỦ TƯỚNG
PHÓ THỦ TƯỚNG

Vũ Đức Đam

Phụ lục I

DANH MỤC MỘT SỐ DỰ ÁN, NHIỆM VỤ SỬ DỤNG NGUỒN VỐN TỪ NGÂN SÁCH TRUNG ƯƠNG

(Kèm theo Quyết định số 1017/QĐ-TTg ngày 14 tháng 8 năm 2018 của Thủ tướng Chính phủ)

TT	Tên dự án/Nhiệm vụ	Đơn vị chủ trì	Đơn vị phối hợp	Thời gian
I	**Các dự án, nhiệm vụ sử dụng nguồn vốn đầu tư phát triển từ ngân sách trung ương**			
1	Đầu tư tăng cường năng lực Trung tâm giám sát an toàn thông tin mạng quốc gia tại VNCERT.	Bộ Thông tin và Truyền thông	Các bộ, cơ quan trung ương, các tỉnh, thành phố trực thuộc trung ương, các doanh nghiệp, nhà mạng ISP	2018 - 2021
2	Đầu tư trang thiết bị và thuê dịch vụ kỹ thuật xây dựng hệ thống giám sát cơ sở, phòng chống tấn công mạng cho Văn phòng Chính phủ.	Văn phòng Chính phủ	Bộ Thông tin và Truyền thông	2018 - 2021
3	Đầu tư trang thiết bị và thuê dịch vụ kỹ thuật xây dựng hệ thống quan trắc, giám sát cơ sở tại các bộ, cơ quan trung ương.	Các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, cơ quan trung ương	Bộ Thông tin và Truyền thông	2018 - 2025
4	Đầu tư mua sắm và thuê dịch vụ kỹ thuật xây dựng, vận hành Hệ thống giám sát trực tiếp, Hệ thống giám sát gián tiếp, Hệ thống, theo dõi, phân tích thường xuyên nguy cơ, lỗ hổng, điểm yếu đối với hệ thống, dịch vụ phục vụ Chính phủ điện tử.	Bộ Thông tin và Truyền thông	Các bộ, cơ quan trung ương, các tỉnh, thành phố trực thuộc trung ương, các doanh nghiệp, nhà mạng ISP	2018 - 2025

5	Đầu tư trang thiết bị và thuê dịch vụ kỹ thuật xây dựng hệ thống quan trắc, giám sát cho hệ thống thông tin phục vụ Chính phủ điện tử để hỗ trợ một số tỉnh, thành phố khó khăn về nguồn vốn, chưa đủ nguồn lực để thực hiện.	Bộ Thông tin và Truyền thông	Các tỉnh, thành phố trực thuộc trung ương, các doanh nghiệp, nhà mạng ISP	2018 - 2025
II	**Các dự án, nhiệm vụ sử dụng nguồn vốn sự nghiệp từ ngân sách trung ương**			
1	Triển khai nhiệm vụ giám sát, cảnh báo cho các hệ thống thông tin phục vụ Chính phủ điện tử thuộc trách nhiệm của Bộ Thông tin và Truyền thông.	Bộ Thông tin và Truyền thông	Các bộ, cơ quan trung ương, các tỉnh, thành phố trực thuộc trung ương, các doanh nghiệp, nhà mạng ISP	Hàng năm
2	Triển khai, thực hiện thu thập, điều tra, phân tích, phát hiện và cảnh báo các sự cố, mã độc, tấn công vào các hệ thống mạng, trung tâm dữ liệu phục vụ Chính phủ điện tử và hạ tầng thông tin quan trọng của quốc gia.	Bộ Thông tin và Truyền thông	Các doanh nghiệp Viễn thông, Internet	Hàng năm
3	Nghiên cứu xây dựng các tiêu chuẩn, quy chuẩn kỹ thuật, các quy trình, tài liệu hướng dẫn và nghiên cứu chuyên môn phục vụ giám sát, bảo đảm an toàn thông tin mạng cho Chính phủ điện tử.	Bộ Thông tin và Truyền thông	Các bộ, cơ quan trung ương, các tỉnh, thành phố trực thuộc trung ương, các doanh nghiệp, nhà mạng ISP	Hàng năm
4	Thực hiện kiểm tra, đánh giá an toàn thông tin cho các hệ thống thông tin, hạ tầng mạng, phần mềm, thiết bị, dịch vụ công nghệ thông tin phục vụ Chính phủ điện tử (cả trước khi đưa vào sử dụng và trong quá trình vận hành, khai thác).	Bộ Thông tin và Truyền thông	Các bộ, cơ quan trung ương, các tỉnh, thành phố trực thuộc trung ương, các doanh nghiệp, nhà mạng ISP	Hàng năm

5	Tổ chức các hội thảo, hội nghị, khóa đào tạo, bồi dưỡng, sát hạch, cấp chứng chỉ và các chương trình huấn luyện, diễn tập nâng cao kỹ năng, kỹ thuật và nghiệp vụ giám sát cho đội ngũ nhân lực, chuyên gia trong các cơ quan nhà nước và các thành viên mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia; tổ chức nghiên cứu khoa học, xây dựng tiêu chuẩn, quy trình, sản phẩm, giải pháp về giám sát, cảnh báo an toàn thông tin mạng.	Bộ Thông tin và Truyền thông	Các bộ, cơ quan trung ương, các tỉnh, thành phố trực thuộc trung ương, các doanh nghiệp, nhà mạng ISP	Hàng năm

Phụ lục II

DANH MỤC MỘT SỐ DỰ ÁN, NHIỆM VỤ ƯU TIÊN SỬ DỤNG NGUỒN VỐN QUỸ DỊCH VỤ VIỄN THÔNG CÔNG ÍCH VIỆT NAM

(Kèm theo Quyết định số 1017/QĐ-TTg ngày 14 tháng 8 năm 2018 của Thủ tướng Chính phủ)

TT	Tên dự án/Nhiệm vụ	Đơn vị chủ trì	Đơn vị phối hợp	Thời gian
1	Đầu tư xây dựng và thuê dịch vụ kỹ thuật triển khai, vận hành Hệ thống hỗ trợ giám sát an toàn thông tin mạng trên các kênh Internet phục vụ việc đảm bảo an toàn thông tin cho Chính phủ điện tử.	Bộ Thông tin và Truyền thông	Các doanh nghiệp Viễn thông, Internet	2018 - 2025
2	Đầu tư xây dựng và thuê dịch vụ kỹ thuật triển khai, vận hành Hệ thống hỗ trợ giám sát an toàn thông tin mạng cho các trung tâm dữ liệu, hệ thống thông tin của các doanh nghiệp cung cấp dịch vụ phục vụ Chính phủ điện tử.	Bộ Thông tin và Truyền thông	Các doanh nghiệp Viễn thông, Internet, doanh nghiệp cung cấp hệ thống, dịch vụ phục vụ chính phủ điện tử và các bộ, ngành, địa phương	2018 - 2025
3	Đầu tư xây dựng và thuê dịch vụ kỹ thuật triển khai, vận hành Hệ thống giám sát trực tiếp, Hệ thống giám sát gián tiếp, Hệ thống chống mã độc, tấn công APT vào các hệ thống, dịch vụ phục vụ Chính phủ điện tử.	Bộ Thông tin và Truyền thông	Các bộ, cơ quan trung ương, các tỉnh, thành phố trực thuộc trung ương, các doanh nghiệp, nhà mạng ISP	2018 - 2025
4	Thuê mua, nâng cấp phần mềm, thiết bị, đường truyền, hạ tầng và dịch vụ nhân sự kỹ thuật phục vụ hoạt động của Trung tâm giám sát an toàn thông tin mạng quốc gia do VNCERT quản lý.	Bộ Thông tin và Truyền thông	Các doanh nghiệp an toàn thông tin, doanh nghiệp Internet, Viễn thông	2018 - 2025

5	Hỗ trợ xây dựng và áp dụng chuẩn quốc tế về an toàn thông tin (như ISO 27xxx) và chuẩn hóa quy trình, nghiệp vụ cho các hệ thống giám sát an toàn thông tin Trung tâm giám sát an toàn thông tin mạng quốc gia, các hệ thống quan trắc, giám sát cơ sở của các bộ, ngành, địa phương và các nhà mạng ISP.	Bộ Thông tin và Truyền thông	Các bộ, cơ quan trung ương, các tỉnh, thành phố trực thuộc trung ương, các doanh nghiệp viễn thông, nhà mạng ISP	2018 - 2025
6	Đầu tư xây dựng, vận hành Hệ thống kiểm tra, phát hiện, cảnh báo các điểm yếu, nguy cơ sự cố an toàn thông tin mạng và thực hiện kiểm tra, đánh giá thường xuyên cho các hệ thống thông tin phục vụ Chính phủ điện tử.	Bộ Thông tin và Truyền thông	Các bộ, cơ quan trung ương, các tỉnh, thành phố trực thuộc trung ương, các doanh nghiệp viễn thông, nhà mạng ISP	2018 - 2025
7	Đầu tư xây dựng cơ sở dữ liệu nguy cơ, sự cố an toàn thông tin trên không gian mạng và thuê dịch vụ kỹ thuật để triển khai, vận hành hệ thống giám sát, phân tích, phát hiện, cảnh báo, chia sẻ nguy cơ, sự cố an toàn thông tin mạng cho hệ thống thông tin phục vụ Chính phủ điện tử.	Bộ Thông tin và Truyền thông	Các bộ, cơ quan trung ương, các tỉnh, thành phố trực thuộc trung ương, các doanh nghiệp viễn thông, nhà mạng ISP	2018 - 2025
		Văn phòng Chính phủ	Bộ Thông tin và Truyền thông	2018 - 2025
8	Xây dựng và tổ chức thực hiện các đợt tập huấn, sự kiện, chương trình, sản phẩm truyền thông nhằm phổ biến kiến thức và nâng cao nhận thức về giám sát, ứng cứu sự cố, bảo đảm an toàn thông tin mạng cho cơ quan, tổ chức, doanh nghiệp, người dân và truyền thông ra quốc tế.	Bộ Thông tin và Truyền thông	Các bộ, cơ quan trung ương, các tỉnh, thành phố trực thuộc trung ương, các doanh nghiệp viễn thông, nhà mạng ISP	Hàng năm

Ghi chú: Các dự án, nhiệm vụ nêu trên nhằm hỗ trợ triển khai các giải pháp tăng cường bảo đảm liên lạc an toàn, tin cậy trong việc thiết lập mạng và cung cấp dịch vụ viễn thông cho công cộng và cho chỉ đạo điều hành của chính quyền các cấp (theo nhiệm vụ 5 thuộc điểm b khoản 1 Mục IV Điều 1 Quyết định số 1168/QĐ-TTg ngày 24 tháng 7 năm 2015 của Thủ tướng Chính phủ phê duyệt Chương trình cung cấp dịch vụ viễn thông công ích đến năm 2020).