DỰ THẢO NGHỊ ĐỊNH QUY ĐỊNH
CHI TIẾT MỘT SỐ ĐIỀU CỦA LUẬT AN NINH MẠNG

CHÍNH PHỦ	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: /2018/NĐ-CP	*Hà Nội, ngày tháng năm 2018*

Dự thảo 2 ngày 31.10.2018

NGHỊ ĐỊNH
Quy định chi tiết một số điều của Luật An ninh mạng

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

Căn cứ Luật An ninh quốc gia ngày 03 tháng 12 năm 2014;

Căn cứ Luật An ninh mạng ngày 12 tháng 6 năm 2018;

Theo đề nghị của Bộ trưởng Bộ Công an,

Chính phủ ban hành Nghị định quy định chi tiết một số điều của Luật An ninh mạng,

Chương I
NHỮNG QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Nghị định này quy định chi tiết Khoản 4 Điều 10, Khoản 5 Điều 12, Điểm d Khoản 1 Điều 23, Khoản 7 Điều 24, Điểm b Khoản 2 và Khoản 4 Điều 26, Khoản 5 Điều 36 Luật An ninh mạng.

Điều 2. Giải thích từ ngữ

Trong Nghị định này, các từ ngữ dưới đây được hiểu như sau:

1. *Doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng tại Việt Nam* là doanh nghiệp trong nước hoặc ngoài nước, hoạt động theo quy định của pháp luật Việt Nam hoặc pháp luật quốc tế, cung cấp các dịch vụ quy định tại Điều 24 Nghị định này.

2. *Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia* là cơ quan, tổ chức, cá nhân có thẩm quyền quản lý trực tiếp đối với hệ thống thông tin quan trọng về an ninh quốc gia.

Chương II
XÁC LẬP DANH MỤC, CƠ CHẾ PHỐI HỢP, ĐIỀU KIỆN BẢO VỆ HỆ THỐNG THÔNG TIN QUAN TRỌNG VỀ AN NINH QUỐC GIA

MỤC 1

XÁC LẬP DANH MỤC
HỆ THỐNG THÔNG TIN QUAN TRỌNG VỀ AN NINH QUỐC GIA

Điều 3. Căn cứ xác lập hệ thống thông tin quan trọng về an ninh quốc gia

Hệ thống thông tin quan trọng về an ninh quốc gia thuộc các lĩnh vực được quy định tại khoản 2 Điều 10 của Luật An ninh mạng và khi bị sự cố, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt, tấn công hoặc phá hoại sẽ gây ra một trong các hậu quả sau đây:

1. Trực tiếp tác động đến sự tồn tại của chế độ và Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam.

2. Gây tổn hại nghiêm trọng đến quốc phòng, an ninh quốc gia; làm suy yếu khả năng phòng thủ bảo vệ Tổ quốc.

3. Trở thành phương tiện thông tin, tuyên truyền chống lại chính quyền nhà nước, lật đổ chế độ.

4. Gây hậu quả đặc biệt nghiêm trọng đến nền kinh tế quốc dân.

5. Gây thảm họa đối với đời sống con người, môi trường sinh thái.

6. Ảnh hưởng nghiêm trọng đến cơ sở hạ tầng không gian mạng quốc gia.

7. Ảnh hưởng nghiêm trọng đến hoạt động của công trình xây dựng cấp I và cấp đặc biệt theo phân cấp của pháp luật về xây dựng.

8. Ảnh hưởng nghiêm trọng đến hoạt động nghiên cứu, hoạch định chủ trương, chính sách thuộc phạm vi bí mật nhà nước.

9. Ảnh hưởng nghiêm trọng đến sự chỉ đạo điều hành trực tiếp của các cơ quan Đảng, Nhà nước ở Trung ương.

Điều 4. Lập hồ sơ đề nghị đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia

1. Căn cứ vào quy định tại Điều 3 của Nghị định này, Bộ trưởng, Thủ trưởng cơ quan ngang Bộ, cơ quan thuộc Chính phủ, Chủ tịch Ủy ban nhân dân tỉnh, thành phố trực thuộc Trung ương, các tổ chức chính trị ở Trung ương có trách nhiệm rà soát, đối chiếu với căn cứ xác lập hệ thống thông tin quan trọng về an ninh quốc gia, lập hồ sơ và đề nghị đưa hệ thống thông tin thuộc thẩm quyền quản lý của mình vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

Trường hợp cần thiết, lực lượng chuyên trách bảo vệ an ninh mạng rà soát các hệ thống thông tin có căn cứ xác lập phù hợp với quy định tại Điều 3 Nghị định này và yêu cầu chủ quản hệ thống thông tin quan trọng về an ninh quốc gia

lập hồ sơ đề nghị đưa hệ thống thông tin thuộc thẩm quyền quản lý của mình vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

2. Hồ sơ đề nghị đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia:

a) Công văn đề nghị đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia, gồm: sự cần thiết phải đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia, mục tiêu, yêu cầu bảo vệ; sự phù hợp với căn cứ xác lập;

b) Văn bản, tài liệu chứng minh sự phù hợp với căn cứ xác lập hệ thống thông tin quan trọng về an ninh quốc gia.

Điều 5. Thẩm định hồ sơ đề nghị đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia

1. Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an rà soát, hướng dẫn lập hồ sơ, tiếp nhận và thẩm định hồ sơ đề nghị đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia, trừ quy định tại Khoản 2 Điều này.

2. Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng hướng dẫn lập hồ sơ, tiếp nhận và thẩm định hồ sơ đề nghị đưa hệ thống thông tin quân sự vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

3. Trong trường hợp cần thiết, Bộ trưởng Bộ Công an, Bộ trưởng Bộ Quốc phòng quyết định thành lập Hội đồng để thẩm định hồ sơ đề nghị đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

4. Trong thời hạn 60 ngày, kể từ ngày nhận đủ hồ sơ hợp lệ đề nghị đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia, lực lượng chuyên trách bảo vệ an ninh mạng đề xuất Bộ trưởng Bộ Công an, Bộ Quốc phòng trình Thủ tướng Chính phủ quyết định. Trường hợp cần gia hạn thời gian do Bộ trưởng Bộ Công an, Bộ Quốc phòng quyết định.

Trường hợp cần thiết, lực lượng chuyên trách bảo vệ an ninh mạng tổ chức khảo sát thực tế để thẩm định đề nghị đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

5. Cơ quan đề nghị đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia có trách nhiệm phối hợp, tạo điều kiện cho việc thẩm định của lực lượng chuyên trách bảo vệ an ninh mạng.

6. Bộ trưởng Bộ Công an, Bộ trưởng Bộ Quốc phòng trình Thủ tướng Chính phủ ban hành và sửa đổi, bổ sung Danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

Điều 6. Đưa hệ thống thông tin ra khỏi danh mục hệ thống thông tin quan trọng về an ninh quốc gia

1. Hằng năm, Bộ trưởng, Thủ trưởng cơ quan ngang Bộ, cơ quan thuộc Chính phủ, Chủ tịch Ủy ban nhân dân tỉnh, thành phố trực thuộc Trung ương, tổ chức chính trị thuộc Trung ương chịu trách nhiệm xem xét, xác định hệ thống thông tin không còn đáp ứng căn cứ quy định tại Điều 3 Nghị định này và lập hồ sơ đề nghị đưa ra khỏi Danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

2. Hồ sơ đề nghị đưa hệ thống thông tin ra khỏi Danh mục hệ thống thông tin quan trọng về an ninh quốc gia, bao gồm:

a) Công văn đề nghị đưa hệ thống thông tin ra khỏi Danh mục hệ thống thông tin quan trọng về an ninh quốc gia, gồm các nội dung cơ bản: lý do và sự cần thiết đưa hệ thống thông tin ra khỏi Danh mục hệ thống thông tin quan trọng về an ninh quốc gia;

b) Văn bản, tài liệu khác có liên quan đến việc đề nghị đưa hệ thống thông tin ra khỏi Danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

3. Trình tự, thủ tục, thẩm quyền xem xét, quyết định đưa hệ thống thông tin ra khỏi Danh mục hệ thống thông tin quan trọng về an ninh quốc gia được áp dụng theo quy định về trình tự, thủ tục, thẩm quyền xem xét, quyết định đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

MỤC 2

PHỐI HỢP THẨM ĐỊNH, KIỂM TRA, GIÁM SÁT ĐỐI VỚI HỆ THỐNG THÔNG TIN ĐỒNG THỜI THUỘC DANH MỤC HỆ THỐNG THÔNG TIN QUAN TRỌNG VỀ AN NINH QUỐC GIA VÀ DANH MỤC HỆ THỐNG THÔNG TIN QUAN TRỌNG QUỐC GIA

Điều 7. Nguyên tắc phối hợp

1. Tuân thủ quy định của Luật An ninh mạng và pháp luật có liên quan.

2. Bảo đảm thực hiện đúng chức năng, nhiệm vụ, quyền hạn của từng cơ quan.

3. Chủ động, thường xuyên, chặt chẽ, kịp thời.

4. Bảo đảm sự hoạt động bình thường của hệ thống thông tin quan trọng về an ninh quốc gia.

5. Việc phối hợp thẩm định, kiểm tra, giám sát được áp dụng đối với hệ thống thông tin đồng thời thuộc Danh mục hệ thống thông tin quan trọng quốc gia và Danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

Các hệ thống thông tin quan trọng về an ninh quốc gia khác không thuộc Danh mục hệ thống thông tin quan trọng quốc gia thì áp dụng theo quy định của pháp luật về bảo vệ an ninh mạng.

Điều 8. Phương thức phối hợp

1. Trao đổi trực tiếp, gửi công văn, thông báo bằng văn bản.

2. Tổ chức họp liên ngành.

3. Thành lập các đoàn công tác liên ngành.

4. Các hình thức khác.

Điều 9. Phối hợp kiểm tra đối với hệ thống thông tin đồng thời thuộc Danh mục hệ thống thông tin quan trọng quốc gia và Danh mục hệ thống thông tin quan trọng về an ninh quốc gia

1. Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an chủ trì, phối hợp với cơ quan quản lý nhà nước về an toàn thông tin của Bộ Thông tin và Truyền thông và các cơ quan, tổ chức có liên quan kiểm tra an ninh mạng, an toàn thông tin mạng đối với hệ thống thông tin đồng thời thuộc Danh mục hệ thống thông tin quan trọng quốc gia và Danh mục hệ thống thông tin quan trọng về an ninh quốc gia, trừ quy định tại khoản 2 Điều này.

2. Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng chủ trì, phối hợp kiểm tra an ninh mạng, an toàn thông tin mạng đối với hệ thống thông tin quân sự thuộc Danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

3. Kết quả kiểm tra được sử dụng phục vụ công tác bảo vệ an ninh mạng, an toàn thông tin mạng.

Điều 10. Phối hợp giám sát đối với hệ thống thông tin đồng thời thuộc Danh mục hệ thống thông tin quan trọng quốc gia và Danh mục hệ thống thông tin quan trọng về an ninh quốc gia

1. Lực lượng chuyên trách bảo vệ an ninh mạng thực hiện giám sát và có trách nhiệm chia sẻ dữ liệu từ thiết bị quan trắc cơ sở để các cơ quan có thẩm quyền dùng chung phục vụ công tác bảo vệ an ninh mạng, an toàn thông tin mạng.

2. Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia bố trí mặt bằng, điều kiện kỹ thuật, thiết lập, kết nối hệ thống, thiết bị giám sát của lực lượng chuyên trách bảo vệ an ninh mạng vào hệ thống thông tin do mình quản lý nhằm phát hiện, cảnh báo cáo sớm nguy cơ mất an ninh mạng.

3. Trường hợp đã có cơ quan có thẩm quyền thực hiện giám sát, dữ liệu từ thiết bị quan trắc cơ sở sẽ được chia sẻ cho lực lượng chuyên trách bảo vệ an ninh mạng để dùng chung phục vụ công tác bảo vệ an ninh mạng, an toàn thông tin mạng.

Điều 11. Phối hợp thẩm định đối với hệ thống thông tin đồng thời thuộc Danh mục hệ thống thông tin quan trọng quốc gia và Danh mục hệ thống thông tin quan trọng về an ninh quốc gia

1. Khi thiết lập, mở rộng hoặc nâng cấp hệ thống thông tin, chủ quản hệ thống thông tin gửi hồ sơ đề nghị thẩm định phương án bảo đảm an toàn thông tin mạng đồng thời cho lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an và cơ quan quản lý nhà nước về an toàn thông tin của Bộ Thông tin và Truyền thông.

2. Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an chủ trì, phối hợp với cơ quan quản lý nhà nước về an toàn thông tin của Bộ Thông tin và Truyền thông và các cơ quan, tổ chức có liên quan thẩm định an ninh mạng; thẩm định phương án bảo đảm an toàn thông tin mạng khi thiết lập, mở rộng hoặc nâng cấp hệ thống thông tin đối với hệ thống thông tin đồng thời thuộc Danh mục hệ thống thông tin quan trọng quốc gia và Danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

MỤC 3
ĐIỀU KIỆN AN NINH MẠNG ĐỐI VỚI HỆ THỐNG THÔNG TIN QUAN TRỌNG VỀ AN NINH QUỐC GIA

Điều 12. Điều kiện về quy định, quy trình, phương án bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia

1. Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia xây dựng các quy định, quy trình, phương án bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia do mình quản lý, căn cứ vào các quy định bảo vệ an ninh mạng, bảo vệ bí mật nhà nước, tiêu chuẩn, quy chuẩn kỹ thuật an toàn thông tin mạng và các tiêu chuẩn kỹ thuật chuyên ngành khác có liên quan.

2. Nội dung các quy định, quy trình, phương án về bảo vệ an ninh mạng phải quy định rõ hệ thống thông tin và thông tin quan trọng cần ưu tiên bảo vệ; quy trình quản lý, kỹ thuật, nghiệp vụ trong sử dụng, bảo vệ an ninh mạng đối với dữ liệu, hạ tầng kỹ thuật; điều kiện về nhân sự, nhất là nhân sự làm công tác quản trị mạng, vận hành hệ thống, bảo đảm an ninh, an toàn thông tin mạng và hoạt động soạn thảo, lưu trữ, truyền đưa bí mật nhà nước qua hệ thống thông tin; trách nhiệm của từng bộ phận, cá nhân trong quản lý, vận hành, sử dụng và có chế tài xử lý nghiêm những hành vi vi phạm.

Điều 13. Điều kiện về nhân sự vận hành, quản trị hệ thống, bảo vệ an ninh mạng

1. Có bộ phận phụ trách về vận hành, quản trị hệ thống và bảo vệ an ninh mạng.

2. Nhân sự phụ trách về vận hành, quản trị hệ thống và bảo vệ an ninh mạng phải được đánh giá về phẩm chất đạo đức thông qua lý lịch, lý lịch tư pháp; có trình độ chuyên môn về an ninh mạng, an toàn thông tin mạng, công nghệ thông tin phù hợp với vị trí công tác; được huấn luyện, đào tạo, phổ biến các quy định về an ninh mạng; có cam kết bảo mật thông tin liên quan đến hệ thống thông tin quan trọng về an ninh quốc gia trong quá trình làm việc và sau khi nghỉ việc.

3. Thiết lập cơ chế hoạt động độc lập của bộ phận nhân sự thực hiện nhiệm vụ quản trị với vận hành hệ thống thông tin; kiểm tra an ninh mạng với phát triển, quản trị, vận hành hệ thống thông tin.

Điều 14. Điều kiện bảo đảm an ninh mạng đối với trang thiết bị, phần cứng, phần mềm là thành phần hệ thống

1. Được kiểm tra an ninh mạng để phát hiện điểm yếu, lỗ hổng bảo mật, mã độc, bảo đảm sự tương thích với các thành phần khác trong hệ thống thông tin quan trọng về an ninh quốc gia.

2. Không sử dụng sản phẩm hoặc phải có biện pháp xử lý, khắc phục điểm yếu, lỗ hổng bảo mật, mã độc trước khi đưa vào sử dụng đã được lực lượng chuyên trách bảo vệ an ninh mạng cảnh báo nguy cơ gây mất an ninh mạng.

3. Dữ liệu, thông tin ở dạng số được xử lý, lưu trữ thông qua hệ thống thông tin thuộc bí mật nhà nước phải được mã hóa hoặc có biện pháp bảo vệ theo quy định của pháp luật trong quá trình tạo lập, trao đổi, lưu trữ.

4. Thiết bị công nghệ thông tin, phương tiện truyền thông, vật mang tin và các thiết bị phục vụ cho hoạt động của hệ thống thông tin phải được quản lý chặt chẽ theo quy định của chủ quản hệ thống thông tin.

5. Phần mềm hệ thống, phần mềm tiện ích, phần mềm lớp giữa, cơ sở dữ liệu, chương trình ứng dụng, mã nguồn và công cụ phát triển định kỳ được rà soát và cập nhật các bản vá lỗi.

6. Thiết bị di động khi kết nối vào hệ thống mạng nội bộ của hệ thống thông tin quan trọng về an ninh quốc gia phải được kiểm tra, kiểm soát bảo đảm an toàn và chỉ được phép sử dụng tại hệ thống thông tin quan trọng về an ninh quốc gia.

7. Thiết bị, phương tiện lưu trữ thông tin phải được:

a) Kiểm tra bảo mật trước khi kết nối thiết bị, phương tiện lưu trữ thông tin với hệ thống thông tin quan trọng về an ninh quốc gia.

b) Kiểm soát việc đấu nối, gỡ bỏ thiết bị, phương tiện lưu trữ thông tin với thiết bị thuộc hệ thống thông tin quan trọng về an ninh quốc gia.

c) Triển khai các biện pháp bảo đảm an toàn thiết bị, phương tiện lưu trữ thông tin khi vận chuyển, lưu trữ.

d) Thực hiện biện pháp bảo vệ đối với thông tin bí mật được lưu trữ trong thiết bị, phương tiện lưu trữ thông tin.

Điều 15. Điều kiện về biện pháp kỹ thuật để giám sát, bảo vệ an ninh mạng

1. Môi trường vận hành của hệ thống thông tin quan trọng về an ninh quốc gia phải đáp ứng yêu cầu:

a) Tách biệt với các môi trường phát triển, kiểm tra và thử nghiệm;

b) Áp dụng các giải pháp bảo đảm an toàn thông tin.

c) Không cài đặt các công cụ, phương tiện phát triển ứng dụng.

d) Loại bỏ hoặc tắt các tính năng, phần mềm tiện ích không sử dụng trên hệ thống thông tin.

2. Dữ liệu của hệ thống thông tin quan trọng về an ninh quốc gia phải có phương án tự động sao lưu dự phòng phù hợp, ra phương tiện lưu trữ ngoài với tần suất thay đổi của dữ liệu và bảo đảm nguyên tắc dữ liệu phát sinh phải được sao lưu trong vòng 24 giờ. Dữ liệu sao lưu dự phòng phải được kiểm tra, bảo đảm khả năng khôi phục định kỳ 6 tháng một lần.

3. Hệ thống mạng phải đáp ứng yêu cầu sau:

a) Chia tách thành các vùng mạng khác nhau theo đối tượng sử dụng, mục đích sử dụng, tối thiểu: có phân vùng mạng riêng cho máy chủ của hệ thống thông tin; có phân vùng mạng trung gian (DMZ) để cung cấp dịch vụ trên mạng Internet; có phân vùng mạng riêng để cung cấp dịch vụ mạng không dây;

b) Có thiết bị, phầm mềm thực hiện chức năng kiểm soát các kết nối, truy cập vào ra các vùng mạng quan trọng;

c) Có thiết bị, phần mềm thực hiện chức năng kết nối, phát hiện, phòng chống xâm nhập từ mạng không tin cậy vào hệ thống thông tin quan trọng về an ninh quốc gia;

d) Có giải pháp kiểm soát, phát hiện và ngăn chặn kịp thời các kết nối, truy cập trái phép vào hệ thống thông tin quan trọng về an ninh quốc gia;

đ) Có phương án cân bằng tải và phương án ứng phó tấn công từ chối dịch vụ và các hình thức tấn công khác phù hợp với quy mô, tính chất của hệ thống thông tin quan trọng về an ninh quốc gia.

4. Có biện pháp, giải pháp để dò tìm và phát hiện kịp thời các điểm yếu, lỗ hổng về mặt kỹ thuật của hệ thống mạng và những kết nối, trang thiết bị, phần mềm cài đặt bất hợp pháp vào mạng.

5. Ghi và lưu trữ nhật ký về hoạt động của hệ thống thông tin và người sử dụng, các lỗi phát sinh, các sự cố an toàn thông tin tối thiểu 3 tháng theo hình thức tập trung và sao lưu tối thiểu một năm một lần.

6. Kiểm soát truy cập đối với người sử dụng, nhóm người sử dụng thiết bị công cụ sử dụng:

a) Đăng ký, cấp phát, gia hạn và thu hồi quyền truy cập của thiết bị, người sử dụng;

b) Mỗi tài khoản truy cập hệ thống phải được gán cho một người sử dụng duy nhất; trường hợp chia sẻ tài khoản dùng chung để truy cập hệ thống thông tin quan trọng về an ninh quốc gia thì phải được phê duyệt bởi cấp có thẩm quyền và xác định được trách nhiệm cá nhân tại mỗi thời điểm sử dụng;

c) Giới hạn và kiểm soát các truy cập sử dụng tài khoản có quyền quản trị: (i) Thiết lập cơ chế kiểm soát việc tạo tài khoản có quyền quản trị để bảo đảm không một tài khoản nào sử dụng được khi chưa được cấp có thẩm quyền phê duyệt; (ii) Phải có biện pháp giám sát việc sử dụng tài khoản có quyền quản trị; (iii) Việc sử dụng tài khoản có quyền quản trị phải được giới hạn đảm bảo chỉ có 1 truy cập quyền quản trị duy nhất, tự động thoát khỏi phiên đăng nhập khi không có hoạt động trong khoảng thời gian nhất định;

d) Quản lý, cấp phát mã khóa bí mật truy cập hệ thống thông tin;

đ) Rà soát, kiểm tra, xét duyệt lại quyền truy cập của người sử dụng;

e) Yêu cầu, điều kiện an toàn thông tin đối với các thiết bị, công cụ sử dụng để truy cập.

Điều 16. Điều kiện về an ninh vật lý

1. Được bố trí, lắp đặt tại các địa điểm an toàn và được bảo vệ để giảm thiểu những rủi ro do các đe dọa, hiểm họa từ môi trường và các xâm nhập trái phép.

2. Được bảo đảm về nguồn điện và các hệ thống hỗ trợ khi nguồn điện chính bị gián đoạn; có biện pháp chống quá tải hay sụt giảm điện áp, chống sét lan

truyền; có hệ thống tiếp địa; có hệ thống máy phát điện dự phòng và hệ thống lưu điện bảo đảm thiết bị hoạt động liên tục.

3. Có phương án, biện pháp bảo vệ, chống sự xâm nhập thu thập thông tin của các thiết bị bay không người lái - UAV.

4. Trung tâm dữ liệu phải có người kiểm soát và bảo vệ 24/7.

Chương III

TRÌNH TỰ, THỦ TỤC THẨM ĐỊNH, ĐÁNH GIÁ, KIỂM TRA, ỨNG PHÓ, KHẮC PHỤC SỰ CỐ AN NINH MẠNG

Điều 17. Thẩm định an ninh mạng

1. Trình tự thực hiện thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia.

a) Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia nộp hồ sơ đề nghị thẩm định an ninh mạng cho lực lượng chuyên trách bảo vệ an ninh mạng có thẩm quyền;

b) Lực lượng chuyên trách bảo vệ an ninh mạng tiếp nhận, kiểm tra, hướng dẫn hoàn thiện hồ sơ đề nghị thẩm định an ninh mạng;

c) Lực lượng chuyên trách bảo vệ an ninh mạng tiến hành thẩm định an ninh mạng theo nội dung quy định tại Khoản 3 Điều 11 Luật An ninh mạng và thông báo kết quả trong thời hạn 60 ngày làm việc, kể từ ngày cấp giấy tiếp nhận hồ sơ của chủ quản hệ thống thông tin quan trọng về an ninh quốc gia.

2. Hồ sơ đề nghị thẩm định đối với hệ thống thông tin quan trọng về an ninh quốc gia, bao gồm:

a) Văn bản đề nghị thẩm định an ninh mạng;

b) Báo cáo nghiên cứu tiền khả thi, hồ sơ thiết kế thi công dự án đầu tư xây dựng hệ thống thông tin trước khi phê duyệt;

c) Đề án nâng cấp hệ thống thông tin trước khi phê duyệt trong trường hợp nâng cấp hệ thống thông tin quan trọng về an ninh quốc gia.

3. Trường hợp cần thiết, lực lượng chuyên trách bảo vệ an ninh mạng tiến hành khảo sát, đánh giá hiện trạng thực tế của hệ thống thông tin quan trọng về an ninh quốc gia để đối chiếu với hồ sơ đề nghị thẩm định. Việc khảo sát, đánh giá thực tế bảo đảm không gây ảnh hưởng tới hoạt động bình thường của chủ quản cũng như hệ thống thông tin quan trọng về an ninh quốc gia.

4. Đối với hệ thống thông tin không thuộc Danh mục hệ thống thông tin quan trọng về an ninh quốc gia, việc thẩm định an ninh mạng do chủ quản hệ thống thông tin quyết định.

Điều 18. Đánh giá điều kiện an ninh mạng

1. Chủ quản hệ thống thông tin quyết định đánh giá điều kiện an ninh mạng đối với hệ thống thông tin do mình quản lý theo quy định tại Mục 3 Chương II Nghị định này, trừ hệ thống thông tin quan trọng về an ninh quốc gia.

2. Trình tự đánh giá điều kiện an ninh mạng đối với thống thông tin quan trọng về an ninh quốc gia

a) Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia nộp hồ sơ đề nghị đánh giá điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia cho lực lượng chuyên trách bảo vệ an ninh mạng có thẩm quyền đánh giá điều kiện an ninh mạng theo quy định tại Khoản 3 Điều 12 Luật An ninh mạng;

b) Lực lượng chuyên trách bảo vệ an ninh mạng đánh giá điều kiện an ninh mạng tiếp nhận, kiểm tra, hướng dẫn hoàn thiện hồ sơ đề nghị đánh giá điều kiện an ninh mạng;

c) Sau khi tiếp nhận đủ hồ sơ hợp lệ, lực lượng chuyên trách bảo vệ an ninh mạng tiến hành đánh giá điều kiện an ninh mạng và thông báo kết quả trong thời hạn 15 ngày làm việc, kể từ ngày cấp giấy tiếp nhận đủ hồ sơ hợp lệ của chủ quản hệ thống thông tin quan trọng về an ninh quốc gia;

d) Trường hợp đủ điều kiện an ninh mạng, Thủ trưởng cơ quan đánh giá điều kiện an ninh mạng cấp Giấy chứng nhận đủ điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia trong vòng 03 ngày làm việc kể từ khi kết thúc đánh giá điều kiện an ninh mạng.

3. Hồ sơ đề nghị chứng nhận đủ điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia bao gồm:

a) Văn bản đề nghị chứng nhận điều kiện an ninh mạng;

b) Hồ sơ thiết kế và hồ sơ giải pháp bảo đảm an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia.

4. Trường hợp không bảo đảm điều kiện an ninh mạng, lực lượng chuyên trách bảo vệ an ninh mạng đánh giá điều kiện an ninh mạng yêu cầu chủ quản hệ thống thông tin quan trọng về an ninh quốc gia bổ sung, nâng cấp hệ thống thông tin quan trọng về an ninh quốc gia để bảo đảm đủ điều kiện.

Điều 19. Kiểm tra an ninh mạng

1. Chủ quản hệ thống thông tin quyết định kiểm tra an ninh mạng đối với hệ thống thông tin do mình quản lý, trừ hệ thống thông tin quan trọng về an ninh quốc gia.

a) Trường hợp, đối tượng kiểm tra an ninh mạng được quy định tại khoản 1, 2, 3 Điều 13, khoản 1 Điều 24 Luật An ninh mạng;

b) Nội dung kiểm tra an ninh mạng, bao gồm: kiểm tra việc tuân thủ các quy định của pháp luật về bảo đảm an ninh mạng, bảo vệ bí mật nhà nước trên không gian mạng; kiểm tra, đánh giá hiệu quả các phương án, biện pháp bảo đảm an ninh mạng, phương án, kế hoạch ứng phó, khắc phục sự cố an ninh mạng; kiểm tra, đánh giá phát hiện lỗ hổng, điểm yếu bảo mật, mã độc và tấn công thử nghiệm xâm nhập hệ thống; kiểm tra, đánh giá khác do chủ quản hệ thống thông tin quy định.

2. Trình tự, thủ tục kiểm tra an ninh mạng đột xuất của lực lượng chuyên trách bảo vệ an ninh mạng:

a) Thông báo về kế hoạch kiểm tra an ninh mạng;

b) Thành lập Đoàn kiểm tra theo chức năng, nhiệm vụ được giao;

c) Tiến hành kiểm tra an ninh mạng, phối hợp chặt chẽ với chủ quản hệ thống thông tin trong quá trình kiểm tra;

d) Lập biên bản về quá trình, kết quả kiểm tra an ninh mạng và bảo quản theo quy định của pháp luật;

đ) Thông báo kết quả kiểm tra an ninh mạng trong 07 ngày làm việc kể từ ngày hoàn thành kiểm tra.

3. Trường hợp cần giữ nguyên hiện trạng hệ thống thông tin, phục vụ điều tra, xử lý hành vi vi phạm pháp luật, lực lượng chuyên trách bảo vệ an ninh mạng gửi văn bản đề nghị chủ quản hệ thống thông tin tạm ngừng tiến hành kiểm tra an ninh mạng. Nội dung văn bản phải ghi rõ lý do, mục đích, thời gian tạm ngừng hoạt động kiểm tra an ninh mạng.

Điều 20. Ứng phó, khắc phục sự cố an ninh mạng

1. Chủ quản hệ thống thông tin quyết định việc thực hiện ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin do mình quản lý, trừ hệ thống thông tin quan trọng về an ninh quốc gia.

2. Khi phát hiện sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia:

a) Lực lượng chuyên trách bảo vệ an ninh mạng thông báo bằng văn bản tới chủ quản hệ thống thông tin quan trọng về an ninh quốc gia.

Trường hợp khẩn cấp, thông báo bằng điện thoại hoặc các hình thức khác trước khi thông báo bằng văn bản.

b) Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia có trách nhiệm khắc phục sự cố an ninh mạng ngay sau khi nhận được thông báo, trừ quy định tại điểm c khoản này.

Trường hợp vượt quá khả năng xử lý, kịp thời thông báo cho lực lượng chuyên trách bảo vệ an ninh mạng để điều phối, ứng phó khắc phục sự cố an ninh mạng;

c) Trường hợp cần thiết, lực lượng chuyên trách bảo vệ an ninh mạng quyết định trực tiếp điều phối, ứng phó khắc phục sự cố an ninh mạng.

3. Điều phối, ứng phó khắc phục sự cố an ninh mạng của lực lượng chuyên trách bảo vệ an ninh mạng:

a) Đánh giá, quyết định phương án ứng phó, khắc phục sự cố an ninh mạng;

b) Điều hành công tác ứng phó, khắc phục sự cố an ninh mạng;

c) Chủ trì tiếp nhận, thu thập, xử lý, trao đổi thông tin về ứng phó, khắc phục sự cố an ninh mạng;

d) Huy động các tổ chức, cá nhân có liên quan tham gia ứng phó, khắc phục sự cố an ninh mạng trong trường hợp cần thiết;

đ) Chỉ định đơn vị đầu mối phối hợp với các đơn vị chức năng của các quốc gia khác hoặc các tổ chức quốc tế trong hoạt động ứng phó, xử lý các sự cố liên quốc gia;

e) Kiểm tra, giám sát, đôn đốc việc thực hiện của các đơn vị liên quan ứng phó, khắc phục sự cố an ninh mạng.

4. Tổ chức, cá nhân tham gia ứng phó, khắc phục sự cố an ninh mạng có trách nhiệm thực hiện các biện pháp, hoạt động ứng phó, khắc phục sự cố theo sự điều phối của lực lượng chuyên trách bảo vệ an ninh mạng.

5. Doanh nghiệp viễn thông, doanh nghiệp cung cấp dịch vụ Internet bố trí mặt bằng, cổng kết nối và các biện pháp kỹ thuật cần thiết để lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an thực hiện nhiệm vụ bảo đảm an ninh mạng.

Chương IV

TRIỂN KHAI HOẠT ĐỘNG BẢO VỆ AN NINH MẠNG TRONG CƠ QUAN NHÀ NƯỚC, TỔ CHỨC CHÍNH TRỊ Ở TRUNG ƯƠNG VÀ ĐỊA PHƯƠNG

Điều 21. Xây dựng, hoàn thiện quy định, quy chế sử dụng mạng máy tính của cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương

1. Chủ quản hệ thống thông tin của cơ quan nhà nước, tổ chức chính trị ở Trung ương và địa phương phải xây dựng quy định, quy chế sử dụng, quản lý và bảo đảm an ninh mạng máy tính nội bộ, mạng máy tính có kết nối mạng Internet do cơ quan, tổ chức mình quản lý. Nội dung các quy định, quy chế về bảo đảm an ninh mạng căn cứ vào những quy định về bảo vệ an ninh mạng, bảo vệ bí mật nhà nước, tiêu chuẩn, quy chuẩn kỹ thuật an toàn thông tin mạng và các tiêu chuẩn kỹ thuật chuyên ngành khác có liên quan.

2. Quy định, quy chế sử dụng, bảo đảm an ninh mạng máy tính của cơ quan nhà nước, tổ chức chính trị ở Trung ương và địa phương phải bao gồm các nội dung cơ bản sau:

a) Xác định rõ hệ thống mạng thông tin và thông tin quan trọng cần ưu tiên bảo đảm an ninh mạng;

b) Quy định rõ các điều cấm và các nguyên tắc quản lý, sử dụng và bảo đảm an ninh mạng, trong đó mạng máy tính nội bộ có lưu trữ, truyền đưa bí mật nhà nước phải được tách biệt vật lý hoàn toàn với mạng máy tính, các thiết bị, phương tiện điện tử có kết nối mạng Internet;

c) Quy trình quản lý, nghiệp vụ, kỹ thuật trong vận hành, sử dụng và bảo đảm an ninh mạng đối với dữ liệu, hạ tầng kỹ thuật, trong đó phải đáp ứng các yêu cầu cơ bản bảo đảm an toàn hệ thống thông tin;

d) Điều kiện về nhân sự, nhất là nhân sự làm công tác quản trị mạng, vận hành hệ thống, bảo đảm an ninh mạng, an toàn thông tin và liên quan đến hoạt động soạn thảo, lưu trữ, truyền đưa bí mật nhà nước qua hệ thống mạng máy tính;

đ) Quy định rõ trách nhiệm của từng bộ phận, cán bộ, nhân viên trong quản lý, sử dụng, bảo đảm an ninh mạng, an toàn thông tin;

e) Chế tài xử lý những vi phạm quy định về đảm bảo an ninh mạng.

Điều 22. Xây dựng, hoàn thiện phương án bảo đảm an ninh mạng đối với hệ thống thông tin của cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương

1. Người đứng đầu cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương có trách nhiệm ban hành phương án bảo đảm an ninh mạng đối với hệ thống thông tin do mình quản lý, bảo đảm đồng bộ, thống nhất, tập trung, có sự dùng chung, chia sẻ tài nguyên để tối ưu hiệu năng, tránh đầu tư trùng lặp.

2. Căn cứ tính chất quan trọng của hệ thống thông tin, thông tin lưu trữ, truyền đưa trên hệ thống thông tin, phương án bảo đảm an ninh mạng đối với hệ thống thông tin có thể bao gồm những nội dung sau:

a) Quy định bảo đảm an ninh mạng trong thiết kế, xây dựng hệ thống thông tin, đáp ứng yêu cầu cơ bản như yêu cầu quản lý, kỹ thuật, nghiệp vụ;

b) Thẩm định an ninh mạng;

c) Kiểm tra, đánh giá an ninh mạng;

d) Giám sát an ninh mạng;

e) Dự phòng, ứng phó, khắc phục sự cố, tình huống nguy hiểm về an ninh mạng;

g) Quản lý rủi ro;

h) Kết thúc vận hành, khai thác, sửa chữa, thanh lý, hủy bỏ.

Điều 23. Phương án ứng phó, khắc phục sự cố an ninh mạng của cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương

1. Căn cứ tính chất quan trọng của hệ thống thông tin, thông tin lưu trữ, truyền đưa trên hệ thống thông tin, phương án ứng phó, khắc phục sự cố an ninh mạng có thể bao gồm:

a) Phương án phòng ngừa, xử lý thông tin có nội dung tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng; làm nhục, vu khống; xâm phạm trật tự quản lý kinh tế bị đăng tải trên hệ thống thông tin;

b) Phương án phòng, chống gián điệp mạng; bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên hệ thống thông tin;

c) Phương án phòng, chống hành vi sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về an ninh quốc gia, trật tự, an toàn xã hội;

d) Phương án phòng, chống tấn công mạng;

đ) Phương án phòng, chống khủng bố mạng;

e) Phương án phòng ngừa, xử lý tình huống nguy hiểm về an ninh mạng.

2. Nội dung phương án ứng phó, khắc phục sự cố an ninh mạng

a) Các quy định chung;

b) Đánh giá các nguy cơ, sự cố an ninh mạng;

c) Phương án ứng phó, khắc phục đối với một số tình huống cụ thể;

d) Nhiệm vụ, trách nhiệm của các cơ quan trong tổ chức, điều phối, xử lý, ứng phó, khắc phục sự cố;

đ) Huấn luyện, diễn tập, phòng ngừa sự cố, giám sát phát hiện, bảo đảm các điều kiện sẵn sàng đối phó, khắc phục sự cố;

e) Các giải pháp đảm bảo, tổ chức triển khai phương án, kế hoạch và kinh phí thực hiện.

3. Hoạt động ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin của của cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương thực hiện theo nội dung quy định tại Khoản 1 Điều 15 Luật An nin mạng.

Chương V

LƯU TRỮ DỮ LIỆU VÀ ĐẶT CHI NHÁNH HOẶC VĂN PHÒNG ĐẠI DIỆN TẠI VIỆT NAM

Điều 24. Dữ liệu phải lưu trữ tại Việt Nam

1. Dữ liệu về thông tin cá nhân của người sử dụng dịch vụ tại Việt Nam, gồm: họ tên, ngày tháng năm sinh, nơi sinh, quốc tịch, nghề nghiệp, chức danh, nơi cư trú, địa chỉ liên hệ, địa chỉ thư điện tử, số điện thoại, số chứng minh nhân dân, mã số định danh cá nhân, số căn cước công dân, số hộ chiếu, số thẻ bảo hiểm xã hội, số thẻ tín dụng, tình trạng sức khỏe, hồ sơ y tế, sinh trắc học.

2. Dữ liệu do người sử dụng dịch vụ tại Việt Nam tạo ra, gồm: thông tin chọn tải lên, đồng bộ hoặc nhập từ thiết bị.

3. Dữ liệu về mối quan hệ của người sử dụng dịch vụ tại Việt Nam, gồm: bạn bè, nhóm mà người sử dụng kết nối hoặc tương tác.

Điều 25. Doanh nghiệp phải lưu trữ dữ liệu, đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam

1. Doanh nghiệp trong và ngoài nước có đầy đủ các điều kiện sau đây phải lưu trữ dữ liệu và đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam:

a) Là doanh nghiệp cung cấp một trong các dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng có hoạt động kinh doanh tại Việt Nam sau đây: Dịch vụ viễn thông; Dịch vụ lưu trữ, chia sẻ dữ liệu trên không gian mạng; Cung cấp tên miền quốc gia hoặc quốc tế cho người sử dụng dịch vụ tại Việt Nam; Thương mại điện tử; Thanh toán trực tuyến; Trung gian thanh toán; Dịch vụ kết nối vận chuyển qua không gian mạng; Mạng xã hội và truyền thông xã hội; Trò chơi điện tử trên mạng; Thư điện tử;

b) Có hoạt động thu thập, khai thác, phân tích, xử lý các loại dữ liệu quy định tại Điều 24 Nghị định này;

c) Để cho người sử dụng dịch vụ thực hiện hành vi được quy định tại Khoản 1, 2 Điều 8 Luật An ninh mạng;

d) Vi phạm quy định tại Khoản 4 Điều 8, điểm a hoặc điểm b khoản 2 Điều 26 Luật An ninh mạng.

2. Bộ trưởng Bộ Công an yêu cầu doanh nghiệp đủ điều kiện quy định tại Khoản 1 Điều này lưu trữ dữ liệu quy định tại Điều 24 Nghị định này và đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam.

3. Các doanh nghiệp không chấp hành quy định tại Khoản 2 Điều này thì tùy theo tính chất, mức độ vi phạm mà bị xử lý theo quy định của pháp luật.

Điều 26. Thời gian lưu trữ dữ liệu

1. Nhật ký hệ thống theo quy định tại điểm b khoản 2 Điều 26 của Luật An ninh mạng phải lưu trữ trong thời hạn tối thiểu 12 tháng.

2. Thời gian lưu trữ dữ liệu được quy định tại Khoản 1 Điều 24 Nghị định này được lưu trữ theo thời gian hoạt động của doanh nghiệp hoặc đến khi không còn cung cấp dịch vụ.

3. Thời gian lưu trữ dữ liệu được quy định tại Khoản 2, 3 Điều 24 Nghị định này tối thiểu là 36 tháng.

Chương VI
ĐIỀU KHOẢN THI HÀNH

Điều 27. Kinh phí bảo đảm

1. Kinh phí thực hiện bảo đảm an ninh mạng trong hoạt động của cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương do ngân sách nhà nước bảo đảm.

2. Kinh phí đầu tư cho an ninh mạng sử dụng vốn đầu tư công thực hiện theo quy định của Luật Đầu tư công. Đối với dự án đầu tư công để xây dựng mới hoặc mở rộng, nâng cấp hệ thống thông tin, kinh phí đầu tư được bố trí trong vốn đầu tư của dự án tương ứng.

3. Kinh phí thực hiện thẩm định, giám sát, kiểm tra, đánh giá điều kiện an ninh mạng; thực hiện các phương án bảo đảm an ninh mạng của cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương được cân đối, bố trí trong dự toán ngân sách hàng năm của cơ quan, tổ chức đó theo phân cấp của Luật Ngân sách nhà nước.

4. Bộ Tài chính hướng dẫn mục chi cho công tác bảo vệ an ninh mạng trong dự toán ngân sách, hướng dẫn quản lý và sử dụng kinh phí sự nghiệp cho công tác bảo đảm an ninh mạng của cơ quan, tổ chức nhà nước.

5. Căn cứ nhiệm vụ được giao, cơ quan, tổ chức nhà nước thực hiện lập dự toán, quản lý, sử dụng và quyết toán kinh phí thực hiện nhiệm vụ bảo đảm an ninh mạng theo quy định của Luật Ngân sách nhà nước.

Điều 28. Hiệu lực thi hành

Nghị định này có hiệu lực thi hành từ ngày 01 tháng 01 năm 2019.

Điều 29. Điều khoản chuyển tiếp

Trong thời hạn 12 tháng kể từ ngày Bộ trưởng Bộ Công an yêu cầu, các doanh nghiệp quy định tại Điều 25 Nghị định này phải lưu trữ dữ liệu, đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam.

Điều 30. Trách nhiệm thi hành

1. Bộ trưởng Bộ Công an đôn đốc, kiểm tra, hướng dẫn việc thực hiện Nghị định này.

2. Bộ trưởng, Thủ trưởng 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 chịu trách nhiệm thi hành Nghị 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;
- HĐND, UBND các tỉnh, thành phố trực thuộc trung ương;
- Văn phòng Trung ương và các Ban của Đảng;
- Văn phòng Tổng Bí thư;
- Văn phòng Chủ tịch nước;
- Hội đồng dân tộc và các Ủy ban của Quốc hội;
- Văn phòng Quốc hội;
- Tòa án nhân dân tối cao;
- Viện kiểm sát nhân dân tối cao;
- Kiểm toán nhà nước;
- Ủy ban Giám sát tài chính Quốc gia;
- Ủy ban trung ương Mặt trận Tổ quốc Việt Nam;
- Cơ quan Trung ương của các đoàn thể;
- VPCP: BTCN, các PCN, Trợ lý TTG, các Vụ, Cục;
- Lưu: VT, NC (3b).

TM. CHÍNH PHỦ
THỦ TƯỚNG

Nguyễn Xuân Phúc