THỦ TƯỚNG CHÍNH PHỦ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
	Độc lập - Tự do - Hạnh phúc
Số: 63/QĐ-TTg	*Hà Nội, ngày 13 tháng 01 năm 2010*

CỔNG THÔNG TIN ĐIỆN TỬ CHÍNH PHỦ
CÔNG VĂN ĐẾN
Số: 406
Ngày 14 tháng 1 năm 2010
Kính chuyển:

QUYẾT ĐỊNH

Phê duyệt Quy hoạch phát triển an toàn thông tin số quốc gia đến năm 2020

THỦ TƯỚNG CHÍNH PHỦ

Căn cứ Luật Tổ chức Chính phủ ngày 25 tháng 12 năm 2001;

Căn cứ Pháp lệnh Bưu chính, Viễn thông ngày 25 tháng 5 năm 2002;

Căn cứ Luật Giao dịch điện tử ngày 29 tháng 11 năm 2005;

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

Căn cứ Nghị định số 160/2004/NĐ-CP ngày 03 tháng 9 năm 2004 của Chính phủ quy định chi tiết thi hành một số điều của Pháp lệnh Bưu chính, Viễn thông về viễn thông;

Căn cứ Nghị định số 26/2007/NĐ-CP ngày 15 tháng 2 năm 2007 của Chính phủ Quy định chi tiết thi hành Luật Giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số;

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính phủ quy định về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước;

Căn cứ Nghị định số 97/2008/NĐ-CP ngày 28 tháng 8 năm 2008 của Chính phủ quy định về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin điện tử trên Internet;

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

QUYẾT ĐỊNH:

Điều 1. Phê duyệt Quy hoạch phát triển an toàn thông tin số quốc gia đến năm 2020 với các nội dung chủ yếu sau:

I. QUAN ĐIỂM QUY HOẠCH

1. Khái niệm an toàn thông tin số:

"An toàn thông tin số" là thuật ngữ dùng để chỉ việc bảo vệ thông tin số và các hệ thống thông tin chống lại các nguy cơ tự nhiên, các hành động truy cập, sử dụng, phát tán, phá hoại, sửa đổi và phá hủy bất hợp pháp nhằm bảo đảm cho các hệ thống thông tin thực hiện đúng chức năng, phục vụ đúng đối tượng một cách sẵn sàng, chính xác và tin cậy (sau đây gọi chung là an toàn thông tin).

Nội dung của an toàn thông tin bao gồm bảo vệ an toàn mạng và hạ tầng thông tin, an toàn máy tính, dữ liệu và ứng dụng công nghệ thông tin.

2. Việc đảm bảo an toàn thông tin cần được xem xét một cách toàn diện dưới các góc độ sau đây:

a) Đảm bảo quy hoạch phù hợp với các quy định pháp lý về công nghệ thông tin nói chung và an toàn thông tin nói riêng.

b) Đảm bảo các hệ thống thông tin từ khi lập kế hoạch, thiết kế, xây dựng, vận hành đến lúc thanh lý được quản lý theo các qui trình, tiêu chuẩn, quy chuẩn kỹ thuật.

c) Các đối tượng có quyền truy cập hợp pháp vào các hệ thống thông tin đều cần được bảo vệ và có trách nhiệm đảm bảo an toàn thông tin cho hệ thống.

3. Chính phủ khuyến khích các tổ chức, cá nhân bảo vệ và phát triển an toàn thông tin dưới các hình thức khác nhau trong khuôn khổ cho phép của pháp luật để góp phần thúc đẩy các hoạt động ứng dụng và phát triển công nghệ thông tin.

4. Chính phủ khuyến khích các tổ chức, cá nhân trong nước nghiên cứu, phát triển các sản phẩm và giải pháp trong lĩnh vực an toàn thông tin bổ sung cho sản phẩm nhập khẩu, tiến tới làm chủ hoàn toàn về công nghệ để đảm bảo an toàn thông tin cho hệ thống thông tin trọng yếu quốc gia ở mức độ ngày càng cao.

II. MỤC TIÊU TỔNG QUÁT ĐẾN NĂM 2020

1. Đảm bảo an toàn mạng và hạ tầng thông tin

a) Hệ thống thông tin trọng yếu quốc gia được đảm bảo an toàn thông tin bởi các hệ thống bảo mật chuyên dùng có độ tin cậy cao;

b) Hoạt động của các hệ thống xác thực chữ ký điện tử và hạ tầng mã khóa công khai được kiểm soát và tuân thủ các tiêu chuẩn kỹ thuật cần thiết;

c) Hình thành mạng lưới điều phối ứng cứu sự cố về an toàn mạng và hạ tầng thông tin quốc gia với sự tham gia của các thành phần kinh tế;

d) Đến năm 2020, an toàn mạng và hạ tầng thông tin được bảo đảm ở mức độ đáp ứng được nhu cầu phát triển của ngành công nghệ thông tin.

2. Đảm bảo an toàn cho dữ liệu và ứng dụng công nghệ thông tin

a) Các ứng dụng về chính phủ điện tử và thương mại điện tử đều được đảm bảo an toàn thông tin ở mức cao nhất trong quá trình cung cấp các dịch vụ trực tuyến cho người dân;

b) Hệ thống thông tin trọng yếu quốc gia đạt được mức độ an toàn thông tin theo các tiêu chuẩn quốc tế;

c) Hầu hết các ứng dụng công nghệ thông tin và trao đổi dữ liệu đều tương thích về chuẩn an toàn thông tin.

3. Phát triển nguồn nhân lực và nâng cao nhận thức về an toàn thông tin

a) Nhân lực công nghệ thông tin của Việt Nam được đào tạo về an toàn thông tin với trình độ tương đương với các nước dẫn đầu trong khu vực ASEAN;

b) Nhận thức xã hội về an toàn thông tin được phổ cập và ngày một nâng cao. Người sử dụng đều được trang bị hiểu biết cần thiết về cách khai thác các chức năng an toàn thông tin có sẵn trong hệ thống;

c) 100% cán bộ quản trị hệ thống trong hệ thống thông tin trọng yếu quốc gia được đào tạo và cấp chứng chỉ quốc gia về an toàn thông tin.

4. Môi trường pháp lý về an toàn thông tin

a) Môi trường pháp lý về an toàn thông tin được hoàn thiện và trở thành công cụ hữu hiệu để:

- Bắt buộc việc thực hiện các quy định về an toàn thông tin.

- Quy định trách nhiệm của cá nhân, tổ chức trong việc thực hiện nhiệm vụ đảm bảo an toàn thông tin.

- Xử lý vi phạm các quy định về an toàn thông tin.

- Trấn áp tội phạm xâm phạm an toàn thông tin;

b) Hệ thống chính sách về an toàn thông tin được triển khai có hiệu lực dựa trên một hệ thống tiêu chí đánh giá mức độ đảm bảo an toàn thông tin và mức độ tội phạm về an toàn thông tin;

c) Hoàn thiện các quy định pháp luật về tội phạm trên mạng máy tính.

III. CÁC MỤC TIÊU PHÁT TRIỂN ĐẾN NĂM 2015

1. Đảm bảo an toàn thông tin cho cơ sở hạ tầng thông tin quốc gia đạt trình độ quốc tế

a) Các mạng nội bộ và thiết bị đầu cuối trong cơ quan nhà nước đều được trang bị các giải pháp kỹ thuật cần thiết và vận hành theo các quy chế, qui trình tiêu chuẩn hóa để đảm bảo an toàn thông tin;

b) Các cơ sở dữ liệu quốc gia đều được trang bị các giải pháp kỹ thuật cần thiết và có các quy chế, quy trình đảm bảo an toàn thông tin theo tiêu chuẩn quốc tế;

c) Xây dựng và đưa vào hoạt động các hệ thống theo dõi, giám sát, cảnh báo những rủi ro về an toàn thông tin trong toàn quốc;

d) Hệ thống thông tin trọng yếu quốc gia bắt buộc phải tuân thủ các qui định chung về đảm bảo an toàn thông tin do Chính phủ ban hành. Chính phủ có cơ chế giám sát và đưa ra đánh giá thường niên về mức độ đảm bảo an toàn thông tin của hệ thống này;

đ) Các mạng nội bộ của doanh nghiệp và tổ chức đều được thiết kế giải pháp đồng bộ, thích hợp đảm bảo an toàn thông tin cho hệ thống của mình.

2. Đảm bảo an toàn dữ liệu và ứng dụng công nghệ thông tin cho các cơ quan nhà nước ở trung ương, địa phương và toàn xã hội

a) Các hệ thống thông tin điện tử của các cơ quan nhà nước được kiểm tra định kỳ, đánh giá, kiểm định hàng năm về mức độ đảm bảo an toàn thông tin theo các tiêu chuẩn do nhà nước quy định;

b) 100% trang thông tin điện tử của Chính phủ, các Bộ, ngành và các tỉnh, thành phố trực thuộc Trung ương có giải pháp hiệu quả chống lại các tấn công gây mất an toàn thông tin và có phương án dự phòng khắc phục sự cố đảm bảo hoạt động liên tục ở mức tối đa;

c) Các dự án ứng dụng công nghệ thông tin sử dụng ngân sách phải lập luận chứng về an toàn và bảo mật thông tin ngay từ khi lập kế hoạch, thiết kế hệ thống thông tin. Các hệ thống thông tin của các cơ quan nhà nước phải trang bị các giải pháp kỹ thuật an toàn và bảo mật thông tin cùng với quy chế quản lý kèm theo đối với các cơ quan và người sử dụng;

d) Các nhà cung cấp dịch vụ truyền số liệu và viễn thông có cam kết đảm bảo an toàn dữ liệu trên đường truyền với chuẩn chất lượng công bố công khai cho các đối tượng sử dụng dịch vụ của mình;

đ) Các nhà cung cấp dịch vụ truy cập Internet và các đại lý phải quản lý được việc truy cập sử dụng Internet theo quy định của pháp luật;

e) 100% các giao dịch điện tử có biện pháp bảo đảm an toàn thông tin. Các dịch vụ thương mại điện tử mới phải công bố công khai và cam kết tuân thủ các tiêu chuẩn chất lượng về an toàn thông tin trước khi vận hành chính thức.

3. Phát triển nhân lực và nâng cao nhận thức xã hội về an toàn thông tin

a) Xây dựng tiêu chuẩn, kỹ năng cần thiết cho các chuyên gia trong lĩnh vực đảm bảo an toàn thông tin. Tổ chức đào tạo và cấp chứng chỉ cấp quốc gia cho trên 80% cán bộ quản trị hệ thống của các hệ thống thông tin trọng yếu quốc gia;

b) Đào tạo 1000 chuyên gia an toàn thông tin theo tiêu chuẩn quốc tế để đảm bảo an ninh thông tin cho hệ thống thông tin trọng yếu quốc gia và toàn xã hội;

c) Người sử dụng các phương tiện và dịch vụ thông tin thường xuyên được thông báo, cập nhật về những rủi ro mất an toàn thông tin mới phát sinh và có thể báo cáo các rủi ro này cho các cơ quan có trách nhiệm.

4. Môi trường pháp lý về an toàn thông tin

a) Hoàn thiện môi trường pháp lý về tội phạm trên mạng máy tính, các quy định về điều tra, đấu tranh phòng, chống tội phạm trong môi trường mạng máy tính;

b) Xây dựng và hoàn thiện hệ thống môi trường pháp lý trong hoạt động cơ yếu, tạo điều kiện cho việc phát triển hạ tầng mã khóa công khai và sử dụng mã hóa trong các hoạt động kinh tế - xã hội;

c) Năm 2010, ban hành:

- Các tiêu chuẩn về hệ thống mã hóa quốc gia cho phép quản lý các hệ thống hạ tầng mã khóa công khai tại Việt Nam;

- Hệ thống các tiêu chuẩn và tiêu chí đánh giá an toàn thông tin cho các hệ thống thông tin; từ năm 2015, các tiêu chuẩn này được áp dụng rộng rãi trong toàn bộ các hệ thống thông tin trọng yếu của quốc gia.

5. Khuyến khích và hỗ trợ việc xây dựng các sản phẩm nội địa về an toàn thông tin

a) Chú trọng đầu tư và hỗ trợ cho việc nghiên cứu phát triển các sản phẩm, giải pháp và mô hình dịch vụ nội địa về an toàn thông tin trong Chương trình Kỹ thuật - Kinh tế về Công nghệ thông tin để bổ sung cho các sản phẩm nhập khẩu;

b) Khuyến khích và hỗ trợ để các doanh nghiệp nội địa sớm có các sản phẩm chống vi rút, ngăn chặn thư rác và các cuộc tấn công trên mạng, phát hiện các hiểm họa tấn công và có chất lượng ngày càng cao đáp ứng được nhu cầu thực tế;

c) Khuyến khích nghiên cứu phát triển, khai thác mã nguồn mở để tiến tới làm chủ công nghệ đồng thời có những phòng thí nghiệm đánh giá kiểm định chất lượng sản phẩm và giải pháp an toàn thông tin để bảo vệ quyền lợi cho người sử dụng.

IV. CÁC GIẢI PHÁP

1. Nâng cao nhận thức và đẩy mạnh việc thông tin, tuyên truyền về an toàn thông tin

Nâng cao nhận thức và đẩy mạnh việc thông tin, tuyên truyền về nội dung của Quy hoạch này thông qua các phương tiện thông tin đại chúng. Tổ chức các hội nghị, hội thảo về an toàn thông tin cho các cơ quan nhà nước, doanh nghiệp và người dân.

2. Hoàn thiện các cơ chế và chính sách nhà nước về an toàn thông tin

Rà soát và hoàn thiện các văn bản quy phạm pháp luật, cơ chế và chính sách của Nhà nước, tạo môi trường thuận lợi để đảm bảo an toàn thông tin, đáp ứng các yêu cầu về hội nhập toàn diện kinh tế quốc tế, thúc đẩy hợp tác và cạnh tranh lành mạnh giữa các doanh nghiệp. Tổ chức nghiên cứu, xây dựng Luật tội phạm trên mạng máy tính. Tăng cường các khung hình phạt xử lý mạnh và kiên quyết khi có vi phạm về an toàn thông tin.

3. Xây dựng các thiết chế và tăng cường các hoạt động đảm bảo an toàn thông tin

Tiếp tục hoàn thiện bộ máy quản lý nhà nước về an toàn thông tin từ Trung ương đến địa phương trong đó chú trọng nâng cao năng lực các cơ quan quản lý chuyên trách về an toàn thông tin. Tăng cường các hoạt động dự báo, kiểm soát, phát hiện tấn công, cảnh báo sớm, ngăn chặn kịp thời và khắc phục sự cố khi có các cuộc tấn công. Tổ chức đánh giá định kỳ và công bố các báo cáo hàng năm về năng lực đảm bảo an toàn thông tin đối với các hệ thống thông tin của Chính phủ, hệ thống thông tin trọng yếu quốc gia.

4. Phát triển nguồn lực về an toàn thông tin

a) Huy động vốn đầu tư

Việc huy động vốn đầu tư cho bảo đảm an toàn thông tin được triển khai theo hướng: Bố trí kinh phí ngân sách đảm bảo an toàn thông tin từ cấp trung ương đến cấp địa phương trong khu vực nhà nước (ngân sách Trung ương bảo đảm an ninh cho hệ thống thông tin quốc gia, ngân sách địa phương đảm bảo an toàn thông tin cho các cơ quan địa phương).

Đối với việc bảo đảm an ninh thông cho các doanh nghiệp, các tổ chức khác, sử dụng nguồn vốn tự có từ các doanh nghiệp và huy động từ xã hội.

b) Đào tạo, bồi dưỡng nhân lực

Xây dựng hệ thống tiêu chí kỹ năng cần thiết đối với các chuyên gia an toàn thông tin;

Xây dựng chương trình và tổ chức đào tạo đội ngũ chuyên gia trong lĩnh vực đảm bảo an toàn thông tin phù hợp với yêu cầu của giai đoạn cạnh tranh và hội nhập;

Xây dựng và duy trì cơ chế thông báo tới người sử dụng về các nguy cơ gây mất an toàn thông tin mới phát sinh;

Phát triển nguồn nhân lực đón đầu các thành tựu khoa học công nghệ, có khả năng phát triển các giải pháp công nghệ tránh bị lệ thuộc vào nước ngoài.

5. Đẩy mạnh hợp tác trong và ngoài nước

Tăng cường hợp tác phòng chống tấn công mạng thông qua việc chia sẻ, trao đổi thông tin giữa các quốc gia trong khu vực và trên thế giới. Đẩy mạnh hợp tác với các tổ chức quốc tế trong lĩnh vực an toàn thông tin, phối hợp trao đổi, đào tạo chuyên gia trong lĩnh vực kỹ thuật và quản lý an toàn thông tin;

Tăng cường hợp tác giữa các tổ chức trong nước trong việc bảo vệ cơ sở hạ tầng thông tin quốc gia, thiết lập mạng lưới theo dõi và cảnh báo sớm, điều phối ngăn chặn các tấn công;

Phối hợp giữa các đơn vị tư vấn, chuyên gia an toàn thông tin sẵn sàng ứng phó với những sự cố liên quan tới mất an toàn thông tin.

V. CÁC NHIỆM VỤ

1. Xây dựng các thiết chế và hạ tầng kỹ thuật đảm bảo an toàn thông tin

a) Năm 2010 xây dựng và ban hành chính sách và hệ thống tiêu chuẩn, quy trình an toàn thông tin làm căn cứ cho các cơ quan nhà nước và các doanh nghiệp có mạng nội bộ xây dựng quy chế an toàn thông tin của mình trong giai đoạn 2011 - 2015. Khuyến khích mọi thành phần kinh tế xã hội xây dựng và ban hành quy chế đảm bảo an toàn thông tin tại đơn vị mình;

b) Thành lập Cục An toàn thông tin quốc gia có trách nhiệm quản lý, điều phối và hướng dẫn cho các hoạt động đảm bảo an toàn thông tin trên phạm vi cả nước. Thành lập các Nhóm ứng cứu sự cố máy tính (CSIRT) tại các cơ quan đơn vị và liên kết các CSIRT thành một mạng lưới trên toàn quốc nhằm ứng phó kịp thời khi xảy ra các sự cố mất an toàn thông tin;

c) Xây dựng hạ tầng kỹ thuật bao gồm các hệ thống kiểm soát an toàn thông tin mạng, chống gửi và phát tán vi rút, thư rác và các phần mềm tạo lỗ hổng và gây hiểm họa an ninh máy tính, rà soát và khắc phục điểm yếu, phát hiện tấn công và cảnh báo sớm và các phương án phản ứng ngăn chặn kịp thời khi có các hiểm họa gây mất an toàn thông tin;

d) Triển khai các hệ thống bảo vệ mạng Internet nhằm đảm bảo phục vụ nhu cầu học tập, cung cấp thông tin lành mạnh cho người dân, ngăn chặn các thông tin độc hại;

đ) Khảo sát về hạ tầng thông tin trọng yếu quốc gia ở tất cả các tỉnh/ thành phố trong khuôn khổ các dự án ứng dụng công nghệ thông tin đang được triển khai trong năm 2010. Lập kế hoạch và lộ trình triển khai áp dụng các quy chế và quy trình đảm bảo an toàn thông tin cho các hệ thống này.

2. Tuyên truyền nâng cao nhận thức và phát triển năng lực công nghệ về an toàn thông tin

a) Tổ chức các chương trình đào tạo phổ cập kiến thức và kỹ năng đảm bảo an toàn thông tin cho toàn xã hội. Sử dụng các phương tiện thông tin đại chúng, tổ chức các sự kiện, hội nghị, hội thảo để tuyên truyền nâng cao nhận thức của người dân về an toàn thông tin;

b) Xây dựng và ban hành tiêu chuẩn kỹ năng và chương trình đào tạo cần thiết đối với các chuyên gia an toàn thông tin, có khả năng theo dõi, giám sát, phát hiện, cảnh báo sớm và phản ứng kịp thời với những hiểm họa đồng thời có các kỹ năng cần thiết để đánh giá và kiểm định chất lượng an toàn thông tin. Tổ chức đào tạo, cấp chứng chỉ và phát triển đội ngũ các chuyên gia an toàn thông tin trong các cơ quan nhà nước, doanh nghiệp và đội ngũ kiểm định viên;

c) Điều tra và bổ sung các dữ liệu về nhân lực chuyên sâu trong lĩnh vực an toàn thông tin và tổ chức dự báo về thị trường lao động về an toàn thông tin;

d) Xây dựng đội ngũ nghiên cứu và phát triển các công nghệ và các giải pháp đảm bảo an toàn thông tin và có chính sách nâng cao đội ngũ này cả về chất lượng và số lượng;

đ) Hàng năm tổ chức đánh giá mức độ an toàn của các sản phẩm an toàn thông tin sử dụng; mức độ sẵn sàng của các hệ thống đảm bảo an toàn thông tin trong các tổ chức công và doanh nghiệp;

e) Đẩy mạnh hợp tác quốc tế và thu hút các dự án đầu tư nước ngoài trên cơ sở chuyển giao công nghệ, từng bước thử nghiệm, nghiên cứu và triển khai, tiến tới làm chủ công nghệ và phát triển các sản phẩm an toàn thông tin đặc thù của Việt Nam.

3. Triển khai các dự án và chương trình về an toàn thông tin

a) Nhanh chóng xây dựng và triển khai các dự án ưu tiên sử dụng nguồn ngân sách đầu tư của nhà nước nhằm xây dựng các thiết chế và cơ sở hạ tầng kỹ thuật đảm bảo an toàn thông tin quốc gia;

b) Các cơ quan nhà nước xây dựng các dự án đầu tư về hạ tầng kỹ thuật đảm bảo an toàn thông tin theo yêu cầu thực tế và dành một phần kinh phí đầu tư trong các dự án ứng dụng công nghệ thông tin để trang bị các giải pháp bảo đảm an toàn thông tin;

c) Xây dựng chương trình tuyên truyền nâng cao nhận thức về an toàn thông tin và bố trí kinh phí hàng năm cho chương trình này;

d) Chú trọng đến các đề án nghiên cứu phát triển sản phẩm, công nghệ, giải pháp kỹ thuật và mô hình cung cấp dịch vụ trong Chương trình Kỹ thuật - Kinh tế về Công nghệ thông tin.

Điều 2. Tổ chức thực hiện:

1. Bộ Thông tin và Truyền thông

a) Chủ trì, phối hợp với các Bộ, ngành liên quan, Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương và Hiệp hội An toàn thông tin Việt Nam tổ chức triển khai Quy hoạch;

b) Kiểm tra thường xuyên việc thực hiện Quy hoạch và định kỳ tổng hợp kết quả, báo cáo Thủ tướng Chính phủ;

c) Căn cứ vào tình hình phát triển kinh tế của đất nước, trình Thủ tướng Chính phủ những nội dung cần cập nhật, điều chỉnh quy hoạch cho phù hợp;

d) Xây dựng và ban hành chính sách và quy chuẩn kỹ thuật quốc gia về an toàn thông tin; xây dựng và trình cơ quan có thẩm quyền công bố tiêu chuẩn kỹ thuật quốc gia về an toàn thông tin theo quy định của pháp luật;

đ) Chủ trì, phối hợp với Bộ Công an thanh tra, kiểm tra và xử lý vi phạm đối với các tổ chức, cá nhân vi phạm quy định về đảm bảo an toàn thông tin.

2. Bộ Kế hoạch và Đầu tư

a) Chủ trì, phối hợp với Bộ Thông tin và Truyền thông, Bộ Tài chính cân đối tổng hợp các nguồn lực trong kế hoạch Nhà nước 5 năm và hàng năm cho các dự án, chương trình và nhiệm vụ trong Quy hoạch;

b) Chủ trì, phối hợp với Bộ Tài chính bố trí dự toán chi đầu tư phát triển hàng năm để thực hiện các dự án an toàn thông tin quốc gia.

3. Bộ Tài chính

a) Chủ trì, phối hợp với Bộ Kế hoạch và Đầu tư bố trí kinh phí thường xuyên hàng năm để thực hiện Quy hoạch trong dự toán ngân sách các Bộ, cơ quan Trung ương;

b) Phối hợp với Bộ Thông tin và Truyền thông trình cấp có thẩm quyền xem xét, ban hành cơ chế, chính sách về tài chính cho việc thực hiện Quy hoạch.

4. Bộ Công an

a) Chủ trì việc nghiên cứu bổ sung các điều luật về tội phạm trên mạng máy tính vào Bộ luật Hình sự và bổ sung nội dung Bộ luật Tố tụng hình sự phù hợp với đặc thù của công tác điều tra tội phạm trong môi trường mạng máy tính để trình Quốc hội;

b) Chịu trách nhiệm quản lý, kiểm soát, phòng ngừa, phát hiện, ngăn chặn, đấu tranh chống âm mưu, hoạt động lợi dụng hệ thống thông tin gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội và lợi ích của công dân;

c) Thực hiện nhiệm vụ bảo vệ an toàn các công trình quan trọng về an ninh quốc gia trên lĩnh vực thông tin.

5. Bộ Quốc phòng

a) Thực hiện quản lý nhà nước về an toàn thông tin trong lĩnh vực quốc phòng;

b) Xây dựng, khai thác hiệu quả phòng thí nghiệm trọng điểm an toàn thông tin tại Bộ Quốc phòng

6. Các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương

a) Căn cứ vào Quy hoạch này, bổ sung các nội dung về an toàn thông tin trong kế hoạch giai đoạn 2011 - 2015 và kế hoạch hàng năm về ứng dụng công nghệ thông tin;

b) Xây dựng và ban hành quy chế đảm bảo an toàn cho các hệ thống thông tin của đơn vị mình quản lý;

c) Có luận chứng về an toàn thông tin và dự toán một phần kinh phí thích đáng để trang bị các giải pháp kỹ thuật đảm bảo an toàn thông tin trong các dự án ứng dụng công nghệ thông tin của đơn vị.

Điều 3. Quyết định này có hiệu lực thi hành kể từ ngày ký ban hành.

Các Bộ trưởng, Thủ trưởng cơ quan ngang Bộ, Thủ trưởng cơ quan thuộc Chính phủ, Chủ tịch Ủy ban nhân dân tỉnh, thành phố trực thuộc Trung ương và Tổng giám đốc các doanh nghiệp nhà nước 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 CP;
- VP BCĐ TW về phòng, chống tham nhũng;
- HĐND, UBND các tỉnh, thành phố trực thuộc TW;
- Văn phòng TW và các Ban của Đảng;
- Văn phòng Chủ tịch nước;
- Hội đồng Dân tộc và các UB của Quốc hội;
- Văn phòng Quốc hội;
- Tòa án nhân dân tối cao;
- Viện Kiểm sát nhân dân tối cao;
- UB Giám sát tài chính QG;
- Kiểm toán Nhà nước;
- Ngân hàng Chính sách Xã hội;
- Ngân hàng Phát triển Việt Nam;
- Ủy ban TW Mặt trận Tổ quốc Việt Nam;
- Cơ quan Trung ương của các đoàn thể;
- VPCP: BTCN, các PCN, Cổng TTĐT, các Vụ, Cục, đơn vị trực thuộc, Công báo;
- Lưu: Văn thư, KTN (5b).M 240

THỦ TƯỚNG

Nguyễn Tấn Dũng

Phụ lục

DANH MỤC CÁC DỰ ÁN ƯU TIÊN SỬ DỤNG NGÂN SÁCH NHÀ NƯỚC

(Ban hành kèm theo Quyết định số 63/QĐ-TTg ngày 13 tháng 01 năm 2010 của Thủ tướng Chính phủ)

STT	Tên dự án	Đơn vị chủ trì	Dự kiến kinh phí (tỷ đồng)	Thời gian thực hiện
1	Xây dựng Trung tâm hệ thống kỹ thuật an toàn mạng quốc gia	Bộ Thông tin và Truyền thông	300	2010 - 2015
2	Xây dựng Hệ thống đánh giá, kiểm định an toàn thông tin quốc gia	Bộ Thông tin và Truyền thông	150	2010 - 2015
3	Xây dựng Hệ thống cảnh báo, phát hiện và phòng chống tội phạm trên mạng	Bộ Công an	100	2011 - 2015
4	Xây dựng Hệ thống xác thực, bảo mật cho các hệ thống thông tin chính phủ	Ban Cơ yếu Chính phủ	100	2011 - 2015
5	Đào tạo chuyên gia an toàn thông tin cho cơ quan chính phủ và hệ thống thống tin trọng yếu quốc gia	Bộ Thông tin và Truyền thông	50	2010 - 2020
6	Xây dựng hệ thống đảm bảo an toàn thông tin số trong các hoạt động giao dịch thương mại điện tử phục vụ ngành Công thương.	Bộ Công thương	65	2010 - 2015
	Tổng cộng		**765**	