THỦ TƯỚNG CHÍNH PHỦ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
	Độc lập - Tự do - Hạnh phúc
Số: 515/QĐ-TTg	*Hà Nội, ngày 30 tháng 3 năm 2026*

QUYẾT ĐỊNH
Phê duyệt Đề án "Nâng cao năng lực hoạt động của lực lượng bảo vệ an ninh mạng quốc gia"

THỦ TƯỚNG CHÍNH PHỦ

Căn cứ Luật Tổ chức Chính phủ ngày 18 tháng 02 năm 2025;

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

Nghị quyết số 71/NQ-CP ngày 01 tháng 04 năm 2025 của Chính phủ sửa đổi, bổ sung cập nhật chương trình hành động của Chính phủ thực hiện Nghị quyết số 57-NQ/TW ngày 22 tháng 12 năm 2024 của Bộ Chính trị về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia;

Theo đề nghị của Bộ trưởng Bộ Công an.

QUYẾT ĐỊNH:

Điều 1. Phê duyệt Đề án "Nâng cao năng lực hoạt động của lực lượng bảo vệ an ninh mạng quốc gia" kèm theo Quyết định này.

Điều 2. Hiệu lực thi hành

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

2. Kể từ ngày Quyết định này có hiệu lực thi hành, các Quyết định sau đây hết hiệu lực thi hành:

a) Quyết định số 21/QĐ-TTg, ngày 06 tháng 01 năm 2021, phê duyệt đề án "Đào tạo và phát triển nguồn nhân lực an toàn thông tin giai đoạn 2021 - 2025";

b) Quyết định số 49/QĐ-TTg, ngày 15 tháng 7 năm 2022, phê duyệt Đề án "Đào tạo nguồn nhân lực an ninh mạng đến năm 2025, tầm nhìn đến năm 2030".

Điều 3. Các 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 và Thủ trưởng các cơ quan, tổ chức liên quan chịu trách nhiệm thi hành Quyết định này.

Nơi nhận:
- Ban Bí thư Trung ương Đảng;
- Ủy ban Thường vụ Quốc hội;
- 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;
- Văn phòng Quốc hội;
- Hội đồng Dân tộc và các Ủy ban của Quốc hội;
- Ủy ban Trung ương Mặt trận Tổ quốc Việt Nam;
- Hiệp hội An ninh mạng quốc gia;
- VPCP: BTCN, các PCN, Trợ lý TTg và các PTTg, TGĐ Cổng TTĐT, các Vụ: TH, PL, KGVX;
- Lưu: VT, CĐS (2). 60

THỦ TƯỚNG

THỦ TƯỚNG CHÍNH PHỦ

Phạm Minh Chính

THƯ VIỆN PHÁP LUẬT • Tel: +84-28-3930 3279 • www.ThuVienPhapLuat.vn

THỦ TƯỚNG CHÍNH PHỦ

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

ĐỀ ÁN
Nâng cao năng lực hoạt động của lực lượng bảo vệ an ninh mạng quốc gia

(Kèm theo Quyết định số 515/QĐ-TTg ngày 30 tháng 3 năm 2026 của Thủ tướng Chính phủ)

Chính phủ ban hành Đề án "Nâng cao năng lực hoạt động của lực lượng bảo vệ an ninh mạng quốc gia", với những nội dung sau:

I. QUAN ĐIỂM

1. An ninh mạng là trọng tâm của quá trình chuyển đổi số, là trụ cột quan trọng tạo lập, củng cố niềm tin và kiến tạo cho sự phát triển thịnh vượng trong kỷ nguyên số. An ninh mạng là nhiệm vụ trọng yếu, thường xuyên, lâu dài, gắn liền với phát triển kinh tế - xã hội bền vững nhằm duy trì môi trường mạng lành mạnh, tin cậy cho các cơ quan, tổ chức, doanh nghiệp và mỗi người dân.

2. Tăng cường năng lực hoạt động của lực lượng bảo vệ an ninh mạng trên toàn quốc theo hướng cách mạng, chính quy, tinh nhuệ, hiện đại; trong đó, lực lượng chuyên trách bảo vệ an ninh mạng được bố trí tại Bộ Công an, Bộ Quốc phòng là lực lượng nòng cốt, chủ lực ở phạm vi quốc gia; lực lượng bảo vệ an ninh mạng được bố trí tại các bộ, ngành, ủy ban nhân dân cấp tỉnh, cơ quan, tổ chức quản lý trực tiếp hệ thống thông tin quan trọng quốc gia và các tổ chức, doanh nghiệp, cá nhân là lực lượng quan trọng ở phạm vi ngành, địa phương và cơ sở, tạo nền tảng sức mạnh tổng thể cho công tác bảo vệ an ninh mạng. Phối hợp đồng bộ, thống nhất, hiệu quả giữa các lực lượng, xây dựng thế trận an ninh nhân dân trên không gian mạng, huy động sức mạnh tổng hợp của cả hệ thống chính trị và toàn dân trong bảo vệ chủ quyền quốc gia trên không gian mạng.

3. Nâng cao năng lực của lực lượng bảo vệ an ninh mạng theo hướng toàn diện, tự chủ, tự lực, tự cường bao gồm: phát triển nguồn nhân lực chất lượng cao, xây dựng và nâng cấp cơ sở vật chất, hạ tầng kỹ thuật hiện đại, nghiên cứu ứng dụng và làm chủ các giải pháp, công nghệ tiên tiến, hoàn thiện cơ chế, chính sách bảo đảm các lực lượng được trang bị đầy đủ nguồn lực, sẵn sàng, chủ động ứng phó từ sớm, từ xa với các nguy cơ, thách thức từ không gian mạng.

4. Chủ động, tích cực hội nhập quốc tế sâu rộng trong lĩnh vực an ninh mạng trên cơ sở giữ vững độc lập, tự chủ, bảo đảm cao nhất chủ quyền, lợi ích và an ninh quốc gia.

II. MỤC TIÊU

1. Mục tiêu tổng quát

Nâng cao năng lực tổng thể, xây dựng lực lượng bảo vệ an ninh mạng tinh nhuệ, hiện đại, nhằm chủ động phòng ngừa, sẵn sàng ứng phó hiệu quả với mọi nguy cơ, thách thức trên không gian mạng, bảo vệ vững chắc an ninh quốc gia, trật tự an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân trên không gian mạng.

2. Mục tiêu đến năm 2030

a) Việt Nam nằm trong nhóm 15 quốc gia dẫn đầu thế giới theo Chỉ số an ninh mạng toàn cầu (ITU-GCI).

b) Hình thành và phát triển Trung tâm Đào tạo khu vực về phòng, chống tội phạm mạng và an ninh mạng tại Việt Nam để nâng cao vị thế và năng lực dẫn dắt trong khu vực.

c) Phấn đấu đến năm 2030, Việt Nam có ít nhất 10.000 chuyên gia an ninh mạng chuyên sâu, trong đó 20% đạt trình độ quốc tế.

d) Ban hành chuẩn kiến thức, kỹ năng chuyên sâu, chương trình, nội dung tập huấn kiến thức, kỹ năng chuyên sâu về an ninh mạng; quản lý, hướng dẫn và tổ chức triển khai hoạt động chứng nhận tập huấn kiến thức, kỹ năng chuyên sâu về an ninh mạng.

đ) 100% lực lượng chuyên trách bảo vệ an ninh mạng được bố trí tại Bộ Công an, Bộ Quốc phòng, lực lượng bảo vệ an ninh mạng được bố trí tại Bộ, ngành, Ủy ban nhân dân cấp tỉnh, cơ quan, tổ chức quản lý trực tiếp hệ thống thông tin quan trọng về an ninh quốc gia, cán bộ trực tiếp quản trị vận hành hệ thống thông tin cấp độ 3, cấp độ 4, cấp độ 5, trong cơ quan, tổ chức, doanh nghiệp Nhà nước có chứng nhận đáp ứng yêu cầu kiến thức, kỹ năng chuyên sâu về an ninh mạng do cơ quan có thẩm quyền cấp; được cập nhật kiến thức an ninh mạng ít nhất 01 lần/năm.

e) 90% người sử dụng Internet có cơ hội tiếp cận hoạt động nâng cao nhận thức, kỹ năng và công cụ bảo đảm an ninh mạng.

g) Nghiên cứu, phát triển, từng bước làm chủ công nghệ chiến lược về an ninh mạng. Phát triển hệ sinh thái sản phẩm, dịch vụ an ninh mạng do Việt Nam làm chủ công nghệ. Nhà nước lựa chọn tối thiểu 02 tổ chức, doanh nghiệp làm chủ công nghệ cho mỗi loại sản phẩm, dịch vụ an ninh mạng trọng điểm, nền tảng để tập trung nguồn lực thúc đẩy.

h) Thiết lập cơ chế chia sẻ thông tin, cảnh báo, điều phối ứng phó sự cố giữa các lực lượng bảo vệ an ninh mạng và các doanh nghiệp an ninh mạng để nâng cao năng lực phòng thủ quốc gia.

i) 70% các ban, bộ, ngành, địa phương và các hệ thống thông tin quan trọng quốc gia sử dụng sản phẩm công nghệ chiến lược "Make in Vietnam"; 100% các sản phẩm, dịch vụ an ninh mạng phải được kiểm định, đánh giá trước khi đưa vào sử dụng, áp dụng trước hết đối với hạ tầng thông tin quan trọng quốc gia, hệ thống thông tin của các cơ quan trong hệ thống chính trị có ảnh hưởng trực tiếp đến an ninh quốc gia, trật tự xã hội và đời sống nhân dân.

k) 100% các hệ thống thông tin sử dụng vốn ngân sách nhà nước được triển khai đầy đủ các phương án bảo đảm an ninh mạng theo cấp độ;

l) Tham gia tích cực và từng bước đóng vai trò dẫn dắt hoạt động của các tổ chức đa phương uy tín về an ninh mạng, thiết lập và mở rộng mạng lưới đối tác chiến lược về an ninh mạng với tối thiểu 20 quốc gia hàng đầu về an ninh mạng. Thiết lập đường dây nóng 24/7 tham gia mạng lưới ứng cứu xử lý sự cố với các quốc gia trên thế giới.

m) Thu hút ít nhất 01 tập đoàn công nghệ về an ninh mạng có quy mô toàn cầu đặt trung tâm nghiên cứu và phát triển tại Việt Nam.

n) Mỗi năm cử ít nhất 50 cán bộ lực lượng bảo vệ an ninh mạng quốc gia tham gia huấn luyện tại các cơ sở đào tạo/huấn luyện an ninh mạng hàng đầu thế giới. Hình thành và phát triển đội ngũ cán bộ chuyên trách về ngoại giao an ninh mạng.

3. Tầm nhìn đến 2045

Việt Nam thuộc nhóm quốc gia dẫn đầu khu vực châu Á - Thái Bình Dương về an ninh mạng, có năng lực mạnh trong phòng thủ, tấn công trấn áp tội phạm mạng và các thế lực thù địch, bảo vệ vững chắc chủ quyền số, bảo vệ cho mọi hoạt động của Nhà nước, doanh nghiệp và người dân trên không gian mạng. Công nghiệp an ninh mạng trở thành ngành kinh tế - kỹ thuật mũi nhọn, có 03 doanh nghiệp an ninh mạng Việt Nam nằm trong nhóm 50 doanh nghiệp dẫn đầu toàn cầu về cung cấp giải pháp an ninh mạng, xuất khẩu sản phẩm, dịch vụ, công nghệ ra thị trường thế giới.

III. NHIỆM VỤ, GIẢI PHÁP

1. Hoàn thiện thể chế, xây dựng và triển khai các cơ chế, chính sách đặc thù

a) Rà soát, cập nhật, hoàn thiện các văn bản quy phạm pháp luật, văn bản hướng dẫn công tác bảo đảm an ninh mạng bảo đảm đồng bộ, thống nhất, hiệu quả giữa các lực lượng, đáp ứng yêu cầu quản lý, bảo vệ không gian mạng trong bối cảnh phát triển nhanh chóng của các công nghệ mới, trong đó tập trung xây dựng và hoàn thiện Luật An ninh dữ liệu, hướng dẫn thi hành Luật An ninh mạng.

b) Triển khai công tác phê chuẩn Công ước Liên Hợp quốc về chống tội phạm mạng, nghiên cứu hoàn chỉnh hành lang pháp lý về công tác phòng chống tội phạm mạng theo khuyến nghị của Công ước; điều chỉnh, bổ sung xây dựng các quy định thống nhất nhằm thực hiện các thủ tục và thực thi pháp luật phù hợp với quy định của Công ước; sẵn sàng các điều kiện cho việc thiết lập đường dây nóng 24/7 tham gia mạng lưới ứng cứu xử lý sự cố theo quy định của Công ước.

c) Xây dựng, ban hành các tiêu chuẩn quốc gia, quy chuẩn kỹ thuật đối với các sản phẩm, dịch vụ an ninh mạng, bảo mật thông tin, thiết lập cơ chế hợp chuẩn, hợp quy, đánh giá sự phù hợp, tổ chức đánh giá, công bố sản phẩm đáp ứng các tiêu chuẩn, quy chuẩn đã ban hành, áp dụng trước hết đối với hạ tầng thông tin quan trọng quốc gia, hệ thống thông tin của các cơ quan trong hệ thống chính trị có ảnh hưởng trực tiếp đến an ninh quốc gia, trật tự xã hội và đời sống nhân dân;

d) Xây dựng khung quản lý rủi ro an ninh mạng quốc gia, chuyển đổi từ quản lý kỹ thuật thuần túy sang quản trị rủi ro toàn diện, dựa trên các tiêu chuẩn quốc tế nhằm tăng tính chủ động của các cơ quan, tổ chức trong việc phân bổ nguồn lực, giảm thiểu tổn thất từ các cuộc tấn công.

đ) Tiếp tục nghiên cứu, hoàn thiện, tổ chức triển khai có hiệu quả các cơ chế và chính sách ưu đãi nhằm thu hút, trọng dụng, bồi dưỡng, nâng cao chất lượng nguồn nhân lực cho lực lượng bảo vệ an ninh mạng trên phạm vi toàn quốc.

2. Tổ chức lực lượng an ninh mạng

a) Củng cố, kiện toàn Ban Chỉ đạo An ninh mạng Quốc gia và các tiểu ban tại các bộ, ngành, địa phương;

b) Củng cố, kiện toàn cơ quan chuyên trách về an ninh mạng tại Bộ Công an, Bộ Quốc phòng, hướng dẫn các bộ, ngành, Ủy ban nhân dân cấp tỉnh, cơ quan, tổ chức quản lý trực tiếp hệ thống thông tin quan trọng về an ninh quốc gia tổ chức lực lượng bảo vệ an ninh mạng.

c) Xây dựng mạng lưới liên kết các chuyên gia an ninh mạng trong nước và nước ngoài tham gia hỗ trợ công tác bảo đảm an ninh mạng. Mở rộng Liên minh ứng phó, khắc phục sự cố an ninh mạng quốc gia.

Hoàn thiện các cơ chế trao đổi, chia sẻ thông tin và quy trình phối hợp xử lý giữa các ban, bộ, ngành, địa phương; giữa các cơ quan, tổ chức và người dân; giữa Việt Nam và các nước trong khu vực và trên thế giới trong công tác bảo vệ an ninh mạng và ứng cứu sự cố an ninh mạng.

d) Hình thành đội ngũ chuyên gia an ninh mạng có năng lực chuyên sâu về các công nghệ trọng yếu (AI, mật mã kháng lượng tử, blockchain, ...) đạt đẳng cấp thế giới.

3. Đào tạo, phát triển nguồn nhân lực an ninh mạng chất lượng cao

a) Xây dựng, ban hành tiêu chuẩn chức danh, vị trí việc làm, khung kiến thức, kỹ năng chuyên sâu về an ninh mạng; quy định về đào tạo, sát hạch, cấp chứng nhận đáp ứng yêu cầu kiến thức, kỹ năng chuyên sâu về an ninh mạng cho lực lượng bảo vệ an ninh mạng, cán bộ trực tiếp quản trị vận hành hệ thống thông tin cấp độ 3, cấp độ 4, cấp độ 5, trong cơ quan, tổ chức, doanh nghiệp Nhà nước.

b) Xây dựng, ban hành và định kỳ cập nhật các chương trình khung, tài liệu, giáo trình đào tạo tập huấn về bảo vệ an ninh mạng; chuẩn hóa hoạt động đào tạo, tập huấn đáp ứng yêu cầu về chuẩn kỹ năng và kiến thức về an ninh mạng tương ứng với từng cấp độ năng lực.

c) Hàng năm, trên cơ sở khảo sát nhu cầu thực tiễn, tổ chức các khóa đào tạo, tập huấn ngắn hạn theo hình thức tập trung, trực tuyến hoặc kết hợp cho các cơ quan của Đảng, Nhà nước, Mặt trận Tổ quốc Việt Nam (gồm các tổ chức chính trị - xã hội) từ Trung ương đến cấp xã và lực lượng vũ trang để cập nhật kiến thức, huấn luyện chuyên sâu kiến thức, kỹ năng an ninh mạng. Nội dung đào tạo bao gồm:

- Đào tạo nghiệp vụ quản lý và kỹ năng bảo đảm an ninh mạng cho đội ngũ lãnh đạo, quản lý;

- Đào tạo kiến thức, kỹ năng bảo đảm an ninh mạng của người dùng cho các cán bộ công chức, viên chức và người lao động;

- Huấn luyện, đào tạo kỹ năng chuyên sâu cho lực lượng chuyên trách bảo vệ an ninh mạng được bố trí tại Bộ Công an, Bộ Quốc phòng, lực lượng bảo vệ an ninh mạng được bố trí tại Bộ, ngành, Ủy ban nhân dân cấp tỉnh, cơ quan, tổ chức quản lý trực tiếp hệ thống thông tin quan trọng về an ninh quốc gia, cán bộ trực tiếp quản trị vận hành hệ thống thông tin cấp độ 3, cấp độ 4, cấp độ 5, trong cơ quan, tổ chức, doanh nghiệp Nhà nước theo khung chương trình, yêu cầu kỹ năng do Bộ Công an ban hành, các chương trình đào tạo theo chứng chỉ quốc tế, lựa chọn nhân sự xuất sắc tham gia thi chứng chỉ quốc tế. Định kỳ tổ chức bồi dưỡng, cập nhật bổ sung các kiến thức, kỹ năng theo các chuyên đề chuyên sâu về công nghệ mới.

d) Hàng năm tổ chức ít nhất 01 chương trình diễn tập cấp quốc gia, 03 chương trình diễn tập theo vùng, miền hoặc theo ngành, lĩnh vực; 03 đến 05 cuộc diễn tập quốc tế (Diễn tập với các Cơ quan, tổ chức ứng cứu sự cố mạng khu vực Châu Á - Thái Bình Dương (APCERT), diễn tập với Nhật Bản và các nước Đông Nam Á (ASEAN - JAPAN), diễn tập khu vực Đông Nam Á (ACID), ...) nhằm nâng cao năng lực ứng phó và phối hợp tác chiến mạng.

đ) Đưa kiến thức an ninh mạng vào chương trình giáo dục phổ thông (từ trung học cơ sở đến trung học phổ thông), giáo dục nghề nghiệp và đại học; tổ chức cuộc thi, diễn đàn, câu lạc bộ an ninh mạng học đường và duy trì hoạt động hằng năm.

e) Phổ biến, nâng cao kiến thức an ninh mạng cho người dân qua các nền tảng học tập số, "Bình dân học vụ số", các khóa học trực tuyến đại chúng mở (MOOC) và các chiến dịch truyền thông đại chúng.

g) Xây dựng nền tảng quản lý hoạt động tập huấn, đánh giá và chứng nhận kiến thức, kỹ năng chuyên sâu về an ninh mạng; quản lý, xác thực dữ liệu các chứng chỉ an ninh mạng trong nước và quốc tế uy tín, quản lý các tổ chức đủ điều kiện thi, cấp, gia hạn, thu hồi chứng chỉ an ninh mạng phục vụ công nhận tương đương, hình thành và phát triển bản đồ chuyên gia an ninh mạng.

h) Phát triển nhân lực an ninh mạng quốc gia, kết nối nhà trường/viện nghiên cứu (sinh viên, giảng viên, nghiên cứu viên), doanh nghiệp và cơ quan nhà nước trong lĩnh vực an ninh mạng, thúc đẩy liên kết công - tư và bồi dưỡng thế hệ chuyên gia an ninh mạng mới.

4. Giám sát, chia sẻ thông tin và đánh giá năng lực an ninh mạng quốc gia.

a) Xây dựng bộ chỉ số đánh giá năng lực bảo đảm an ninh mạng đối với cơ quan tổ chức, doanh nghiệp.

b) Xây dựng hệ thống chia sẻ thông tin tình báo an ninh mạng (Threat Intelligence), hướng tới hình thành các trung tâm phân tích và chia sẻ thông tin an ninh mạng (ISAC - Information Sharing Analysis Center) cho từng ngành, lĩnh vực trọng yếu (tài chính, ngân hàng, giao thông, năng lượng,...)., thúc đẩy cơ chế chia sẻ thông tin tình báo về các mối đe dọa, lỗ hổng bảo mật và các cuộc tấn công an ninh mạng giữa khu vực công và tư nhân, đảm bảo tính đồng bộ, hiệu quả và bảo mật.

c) Xây dựng nền tảng giám sát, điều hành an ninh mạng quốc gia cho phép báo cáo, thống kê, cập nhật dữ liệu an ninh mạng trên toàn quốc, đảm bảo dữ liệu "đúng, đủ, sạch, sống, dùng chung, thống nhất".

5. Nghiên cứu phát triển, nâng cao năng lực tự chủ công nghệ, làm chủ công nghệ lõi trong lĩnh vực an ninh mạng

a) Rà soát, xây dựng, công bố danh mục công nghệ, danh mục sản phẩm, dịch vụ an ninh mạng cốt lõi quốc gia ưu tiên làm chủ, tự chủ.

b) Thúc đẩy cơ chế để cơ quan nhà nước đặt hàng doanh nghiệp phát triển các sản phẩm về an ninh mạng; ưu tiên thí điểm, thử nghiệm các sản phẩm do Việt Nam làm chủ công nghệ:

- Xây dựng và triển khai chương trình quốc gia về thúc đẩy phát triển sản phẩm, dịch vụ an ninh mạng nội địa theo hướng hỗ trợ đầu ra, tạo thị trường cho doanh nghiệp. Tổ chức các cuộc thi, giải thưởng quốc gia nhằm tìm kiếm, đánh giá và công nhận các sản phẩm, dịch vụ an ninh mạng xuất sắc, chất lượng cao của các doanh nghiệp Việt Nam;

- Triển khai các giải pháp hỗ trợ các doanh nghiệp khởi nghiệp sáng tạo về an ninh mạng thông qua việc cung cấp các ưu đãi, hỗ trợ các doanh nghiệp trong nước chuyên về nghiên cứu và phát triển sản phẩm, dịch vụ an ninh mạng.

- Triển khai các giải pháp hỗ trợ các doanh nghiệp vừa và nhỏ bảo đảm an ninh mạng thông qua các gói hỗ trợ đào tạo, tư vấn, cung cấp giải pháp an ninh mạng nội địa.

c) Nghiên cứu, kiện toàn và phát triển đơn vị nòng cốt trong lĩnh vực đổi mới sáng tạo và huấn luyện an ninh mạng thuộc Bộ Công an, làm trung tâm kết nối và phát triển hệ sinh thái an ninh mạng Việt Nam; thực hiện chức năng định hướng chiến lược, xác định ưu tiên phát triển, kết nối và điều phối các nguồn lực, hỗ trợ nghiên cứu, đề xuất hoàn thiện chính sách và pháp luật thúc đẩy phát triển ngành công nghiệp an ninh mạng, đồng thời tổ chức đào tạo, huấn luyện bồi dưỡng chuyên sâu về an ninh mạng.

d) Thúc đẩy phát triển các trung tâm đo kiểm an ninh mạng đủ năng lực thực hiện thử nghiệm, đánh giá sự phù hợp tiêu chuẩn, quy chuẩn đối với sản phẩm, dịch vụ an ninh mạng trong nước và quốc tế.

đ) Tham gia các cơ chế hợp tác song phương, đa phương nhằm mục tiêu thừa nhận lẫn nhau kết quả đánh giá sự phù hợp tiêu chuẩn, quy chuẩn kỹ thuật với các tổ chức nước ngoài, quốc tế đối với sản phẩm, dịch vụ an ninh mạng.

e) Tăng cường phối hợp công tư, xây dựng và vận hành có hiệu quả tam giác chiến lược Nhà nước - Nhà trường (Viện nghiên cứu) - Doanh nghiệp trong việc định hướng, nghiên cứu, nắm bắt các công nghệ lõi, công nghệ chiến lược, phát triển, triển khai các công nghệ, sản phẩm, dịch vụ an ninh mạng.

6. Nâng cao uy tín quốc gia và tăng cường hợp tác quốc tế

a) Tăng cường hợp tác song phương với các quốc gia tiên tiến về an ninh mạng, các tổ chức lớn thông qua các hoạt động chia sẻ thông tin, hỗ trợ kỹ thuật, và đào tạo nhân lực, ưu tiên mở rộng hợp tác với các đối tác như Hoa Kỳ, Liên minh Châu Âu, Nhật Bản, Hàn Quốc, Ấn Độ, Israel, Trung Quốc, Anh, Pháp, Đức, ...

b) Chủ động tham gia các tổ chức như: ITU, FIRST, APCERT, GFCE, ISO, IEC[1], ... đề xuất sáng kiến, chia sẻ thông tin, tài liệu, phối hợp tổ chức các hoạt động, sự kiện quốc tế để nâng cao hình ảnh, vị thế quốc gia, tranh cử các vị trí lãnh đạo hoặc điều phối trong các nhóm công tác chuyên môn. Thiết lập các tổ chức, diễn đàn quốc tế do Việt Nam dẫn dắt về an ninh mạng.

c) Tham gia hoạt động của Liên Hợp quốc, ASEAN, APEC[2],... để xây dựng và thúc đẩy các chuẩn mực, quy tắc ứng xử toàn cầu về an ninh mạng. Tích cực thúc đẩy các nước ký và phê chuẩn Công ước Liên Hợp quốc về chống tội phạm mạng sớm đưa Công ước có hiệu lực thực thi.

d) Thu hút nguồn lực từ nước ngoài và các đối tác quốc tế cho hoạt động nghiên cứu, ứng dụng, đổi mới sáng tạo, khởi nghiệp, chuyển giao công nghệ về bảo đảm an ninh mạng.

đ) Đưa chuyên gia, tổ chức trong nước tham gia các hoạt động toàn cầu, các hội nghị như: RSAC Conference, Black Hat, DEFCON, CyberTech, Hack in the Box...; khuyến khích doanh nghiệp, viện nghiên cứu đạt các chứng nhận, giải thưởng quốc tế về an ninh mạng.

e) Tổ chức hội nghị, hội thảo, triển lãm và các cuộc thi quốc tế tại Việt Nam về bảo đảm an ninh mạng nhằm nâng cao hình ảnh quốc gia, chia sẻ thông tin, kinh nghiệm, thúc đẩy, tìm kiếm cơ hội hợp tác với các tổ chức/doanh nghiệp phát triển các sản phẩm, dịch vụ công nghệ chiến lược về an ninh mạng.

g) Thúc đẩy ngoại giao an ninh mạng: Bố trí nguồn nhân lực có năng lực triển khai hợp tác về an ninh mạng cho cơ quan đại diện Việt Nam tại các địa bàn có thế mạnh về an ninh mạng. Tổ chức đối thoại an ninh mạng thường niên giữa Việt Nam và các quốc gia đối tác.

7. Bảo đảm nguồn lực triển khai Đề án

Nguồn ngân sách nhà nước; nguồn của các doanh nghiệp, tổ chức để triển khai các hoạt động nâng cao năng lực tại đơn vị; các nguồn hợp pháp khác theo quy định.

IV. TỔ CHỨC THỰC HIỆN

1. Bộ Công an

a) Giúp Chính phủ thống nhất triển khai các hoạt động nâng cao năng lực các lực lượng bảo vệ an ninh mạng.

---

[1] ITU (International Telecomunication Union): Liên minh Viễn thông Quốc tế; FIRST (Forum of Incident Response and Security Teams) - Diễn đàn toàn cầu của các nhóm ứng phó sự cố và an ninh; APCERT (Asia Pacific Computer Emergency Response Team) - Hiệp hội các tổ chức ứng cứu sự cố máy tính quốc gia khu vực Châu Á - Thái Bình Dương; GFCE (Global Forum on Cyber Expertise) - Diễn đàn toàn cầu về chuyên môn an ninh mạng; ISO (International Organization for Standardization) - Tổ chức Tiêu chuẩn hóa Quốc tế; IEC (International Electrotechnical Commission) - Ủy ban Kỹ thuật Điện Quốc tế.

[2] ASEAN (Association of Southeast Asian Nations), APEC (Asia-Pacific Economic Cooperation).

b) Rà soát, sửa đổi, bổ sung theo thẩm quyền hoặc kiến nghị cơ quan có thẩm quyền sửa đổi, bổ sung, hoàn thiện, chính sách pháp luật về an ninh mạng, tổ chức lực lượng an ninh mạng tại khoản 1, khoản 2 mục III và Phụ lục kèm theo.

c) Chủ trì, phối hợp với Bộ Giáo dục và Đào tạo, Bộ Nội vụ và các bộ, ngành có liên quan triển khai các nhiệm vụ phát triển nguồn nhân lực an ninh mạng quốc gia tại khoản 3, mục III và Phụ lục kèm theo.

d) Chủ trì xây dựng triển khai các giải pháp giám sát, chia sẻ thông tin và đánh giá năng lực an ninh mạng quốc gia, triển khai các chương trình, thúc đẩy hoạt động nghiên cứu phát triển, nâng cao năng lực tự chủ công nghệ, đặc biệt chú trọng làm chủ các công nghệ lõi trong lĩnh vực an ninh mạng tại khoản 4, khoản 5, mục III và Phụ lục kèm theo.

đ) Chủ trì, phối hợp với Bộ Ngoại giao tham gia theo thẩm quyền hoặc đề xuất Việt Nam tham gia các cơ chế, cam kết quốc tế về an ninh mạng; chủ trì cung cấp nội dung về an ninh mạng trong các xếp hạng, đánh giá của quốc tế.

e) Chủ trì, phối hợp với Bộ Tài chính và các cơ quan, tổ chức liên quan đề xuất các dự án từ nguồn hỗ trợ phát triển chính thức (ODA) để triển khai các nhiệm vụ, giải pháp vì mục đích bảo đảm an ninh mạng.

g) Định kỳ sơ kết, tổng kết, đánh giá tình hình thực hiện Đề án; trường hợp cần thiết, báo cáo Thủ tướng Chính phủ quyết định chỉnh sửa, bổ sung các nội dung liên quan thuộc Đề án nhằm phù hợp với tình hình thực tiễn.

2. Bộ Khoa học và Công nghệ

a) Chủ trì, phối hợp với Bộ Công an và các cơ quan, tổ chức, doanh nghiệp liên quan nghiên cứu, thực hiện chuyển giao công nghệ; thẩm định và công bố các tiêu chuẩn quốc gia về an ninh mạng; đề xuất các hoạt động thúc đẩy hợp tác đa phương về an ninh mạng nhằm mục tiêu tăng cường thừa nhận lẫn nhau đối với kết quả đánh giá sự phù hợp về tuân thủ tiêu chuẩn quốc tế đối với sản phẩm, dịch vụ an ninh mạng.

b) Chủ trì, phối hợp với Bộ Công an trong tổ chức đánh giá, công nhận năng lực phòng thử nghiệm, tổ chức giám định, chứng nhận hợp chuẩn, hợp quy đối với sản phẩm, dịch vụ an ninh mạng; xây dựng năng lực kỹ thuật của các tổ chức đánh giá sự phù hợp trong nước, hướng đến mục tiêu được thừa nhận quốc tế, khu vực, nước ngoài.

c) Chủ trì triển khai nội dung điểm b, d, đ khoản 5, mục III và Phụ lục kèm theo.

d) Chủ trì, đề xuất phương án dự toán chi ngân sách nhà nước cho các nhiệm vụ, dự án phù hợp với ngành, lĩnh vực khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số của các Bộ, cơ quan trung ương và địa phương để triển khai Đề án Nâng cao năng lực hoạt động của lực lượng bảo vệ an ninh

mạng quốc gia theo pháp luật về ngân sách nhà nước, đầu tư công, khoa học, công nghệ, đổi mới sáng tạo, chuyển đổi số và pháp luật liên quan, gửi Bộ Tài chính tổng hợp, trình cấp có thẩm quyền quyết định.

3. Bộ Giáo dục và Đào tạo

a) Chủ trì, phối hợp với Bộ Công an triển khai xây dựng chương trình khung, biên soạn, phát hành các bộ tài liệu, giáo trình; chuẩn hóa hoạt động đào tạo đáp ứng yêu cầu về khung chuẩn kỹ năng và kiến thức về an ninh mạng.

b) Nghiên cứu, tổng hợp đề xuất của các bộ, cơ quan liên quan, báo cáo cấp có thẩm quyền xem xét sửa đổi, bổ sung các chính sách ưu đãi, miễn giảm học phí, học bổng cho học sinh, sinh viên, thạc sỹ, tiến sỹ nhằm thu hút nguồn nhân lực và đào tạo nguồn nhân lực ngành an ninh mạng.

c) Chỉ đạo các cơ sở giáo dục đại học triển khai các chương trình đào tạo kỹ sư, thạc sĩ, tiến sĩ tài năng về an ninh mạng.

d) Chủ trì, phối hợp với Bộ Công an, Bộ Tài chính nghiên cứu, đề xuất và tổ chức triển khai mô hình liên kết giữa nhà nước, nhà trường, doanh nghiệp trong đào tạo nguồn nhân lực ngành an ninh mạng.

4. Bộ Nội vụ

Phối hợp với Bộ Công an trong xây dựng tiêu chuẩn chuyên môn, nghiệp vụ cho lực lượng bảo vệ an ninh mạng, đề xuất cơ chế thu hút nhân lực chất lượng cao làm việc trong lĩnh vực an ninh mạng, cơ chế giữ chân nhân lực an ninh mạng làm việc tại cơ quan nhà nước.

5. Bộ Tài chính

a) Cân đối nguồn ngân sách nhà nước hằng năm cho lĩnh vực khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số theo quy định của pháp luật về ngân sách, về đầu tư công và pháp luật quản lý ngành, lĩnh vực. Tổng hợp, trình cấp có thẩm quyền xem xét, quyết định trên cơ sở đề xuất của Bộ Khoa học và Công nghệ về dự toán chi ngân sách nhà nước cho lĩnh vực khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số.

b) Phối hợp với Bộ Công an vận động các nguồn hỗ trợ không hoàn lại của nước ngoài cho các hoạt động nghiên cứu, ứng dụng, đổi mới sáng tạo, khởi nghiệp, chuyển giao công nghệ về bảo đảm an ninh mạng theo quy định của pháp luật về thu hút, tiếp nhận, quản lý, sử dụng vốn viện trợ không hoàn lại của nước ngoài cho Việt Nam.

c) Tiếp tục chỉ đạo Trung tâm Đổi mới sáng tạo Quốc gia và Mạng lưới Đổi mới sáng tạo và chuyên gia An ninh mạng Việt Nam (ViSecurity) phối hợp với Bộ Công an (Cục An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao) phát triển hệ sinh thái đổi mới sáng tạo, nghiên cứu phát triển và ứng dụng trong lĩnh vực an ninh mạng.

6. Bộ Quốc phòng

a) Triển khai đồng bộ, hiệu quả các giải pháp bảo đảm an ninh mạng đối với các hệ thống thông tin thuộc phạm vi quản lý.

b) Chỉ đạo các cơ quan, tổ chức, doanh nghiệp nghiên cứu, phát triển các sản phẩm an ninh mạng theo hướng lưỡng dụng, tập trung vào các sản phẩm công nghệ chiến lược "Make in Vietnam" trong phạm vi quản lý.

c) Thúc đẩy hợp tác quốc tế trong lĩnh vực an ninh mạng thuộc phạm vi quản lý;

d) Tăng cường triển khai các giải pháp giám sát, bảo đảm an ninh mạng đối với các hệ thống thông tin quan trọng quốc gia theo chức trách, nhiệm vụ được giao.

đ) Rà soát, hoàn thiện mô hình tổ chức lực lượng chuyên trách bảo vệ an ninh mạng thuộc phạm vi quản lý.

e) Tổ chức tập huấn và chứng nhận kiến thức, kỹ năng chuyên sâu về an ninh mạng cho các đối tượng thuộc phạm vi quản lý.

g) Nghiên cứu hướng dẫn hoạt động đăng ký, chỉ định và quản lý hoạt động của tổ chức chứng nhận sự phù hợp về an ninh mạng trong phạm vi quản lý.

h) Phối hợp chặt chẽ với Bộ Công an trong triển khai các nhiệm vụ, giải pháp, đặc biệt là phát triển nguồn nhân lực, tổ chức diễn tập cấp quốc gia; giám sát, chia sẻ thông tin và đánh giá năng lực an ninh mạng quốc gia.

7. Bộ Ngoại giao

a) Phối hợp với Bộ Công an trong tăng cường hợp tác song phương, đa phương về an ninh mạng; huy động nguồn lực quốc tế để hỗ trợ phát triển và đào tạo nguồn nhân lực cho ngành an ninh mạng.

b) Tích cực truyền thông, lan tỏa hình ảnh Việt Nam là điểm đến của ngành công nghiệp an ninh mạng.

c) Chỉ đạo các cơ quan đại diện Việt Nam ở nước ngoài thúc đẩy hợp tác quốc tế về an ninh mạng, cập nhật danh sách chuyên gia, nhân tài người Việt Nam ở nước ngoài liên quan đến lĩnh vực an ninh mạng.

d) Bố trí nhân lực chuyên trách hợp tác về an ninh mạng cho đại sứ quán Việt Nam tại các quốc gia mạnh về an ninh mạng.

8. Các bộ, ngành, địa phương

a) Ưu tiên bố trí nguồn lực (nhân lực, kinh phí) và điều kiện để triển khai hoạt động bảo đảm an ninh mạng trong hoạt động nội bộ của cơ quan, tổ chức và lĩnh vực quản lý.

b) Hàng năm tổ chức ít nhất 01 cuộc diễn tập chuyên đề an ninh mạng, ứng cứu sự cố mạng trong phạm vi của bộ, ngành, địa phương mình; phối hợp, tham gia các cuộc diễn tập quốc gia và quốc tế do Bộ Công an tổ tổ chức.

c) Hàng năm tổ chức các khóa đào tạo, tập huấn trực tiếp hoặc trực tuyến nhằm cập nhật, nâng cao năng lực, kiến thức, kỹ năng cho cán bộ các cấp (gồm quản lý, lãnh đạo; người dùng cuối; nhân sự kỹ thuật an ninh mạng) theo hướng dẫn Bộ Công an, khuyến khích thi lấy chứng chỉ quốc tế.

d) Trang bị hệ thống, công cụ chuyên dụng cho lực lượng bảo vệ an ninh mạng, tối thiểu gồm: hệ thống, công cụ rà quét phát hiện lỗ hổng bảo mật; hệ thống, công cụ hỗ trợ điều tra số, ứng cứu, khắc phục sự cố an ninh mạng.

đ) Đẩy mạnh hoạt động bảo đảm an ninh mạng trong phạm vi quản lý; tuân thủ tiêu chuẩn, quy chuẩn kỹ thuật, hướng dẫn nghiệp vụ của Bộ Công an và quy định của pháp luật; ưu tiên sử dụng sản phẩm, giải pháp, dịch vụ an ninh mạng "Make in Vietnam". Gắn kết công tác bảo đảm an ninh mạng với công tác triển khai chuyển đổi số, ứng dụng công nghệ thông tin, phát triển Chính phủ điện tử hướng tới Chính phủ số, phát triển đô thị thông minh, kinh tế số và xã hội số.

9. Hiệp hội An ninh mạng quốc gia

a) Phối hợp chặt chẽ với Bộ Công an trong triển khai thực các nhiệm vụ tại Đề án.

b) Vận động các hội viên, doanh nghiệp tích cực nghiên cứu, phát triển, sản xuất, cung cấp sản phẩm, dịch vụ, giải pháp an ninh mạng chất lượng cao; vận động các cơ quan, tổ chức ưu tiên sử dụng sản phẩm, dịch vụ, giải pháp an ninh mạng Make in Vietnam; thúc đẩy phát triển hệ thống chia sẻ thông tin tình báo an ninh mạng giữa khu vực công và tư; định kỳ tổ chức cuộc thi, giải thưởng quốc gia nhằm tìm kiếm, đánh giá và công nhận các sản phẩm, dịch vụ an ninh mạng xuất sắc, chất lượng cao của các doanh nghiệp Việt Nam.

Phụ lục

DANH MỤC CÁC NHIỆM VỤ, GIẢI PHÁP CHÍNH TRIỂN KHAI ĐỀ ÁN "NÂNG CAO NĂNG LỰC HOẠT ĐỘNG CỦA LỰC LƯỢNG BẢO VỆ AN NINH MẠNG QUỐC GIA"

(Kèm theo Đề án tại Quyết định số 515/QĐ-TTg ngày 30 tháng 3 năm 2026 của Thủ tướng Chính phủ)

STT	Nhiệm vụ, giải pháp	Cơ quan chủ trì	Cơ quan phối hợp	Thời gian triển khai
I. Hoàn thiện hành lang pháp lý, đẩy mạnh triển khai các cơ chế, chính sách				
1.	Rà soát, cập nhật, hoàn thiện hành lang pháp lý, văn bản hướng dẫn công tác bảo đảm an ninh mạng theo thẩm quyền.	Bộ Công an	Bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc trung ương	Thường xuyên
2.	Tham mưu trình các cấp có thẩm quyền ban hành Luật An ninh dữ liệu.	Bộ Công an	Bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc trung ương	Quý IV/2026
3.	Tham mưu xây dựng, trình cấp có thẩm quyền ban hành Nghị định, văn bản hướng dẫn thi hành Luật An ninh mạng gồm: Nghị định quy định chi tiết một số điều Luật An ninh mạng, Nghị định về bảo vệ an ninh hệ thống thông tin theo cấp độ, Nghị định về ngăn chặn xung đột thông tin trên mạng, Nghị định quy định điều kiện kinh doanh sản phẩm, dịch vụ an ninh mạng, Nghị định kinh doanh sản phẩm, dịch vụ mật mã dân sự, xuất khẩu, nhập khẩu sản phẩm mật mã dân sự, Nghị định quy định biện pháp bảo đảm an ninh mạng.	Bộ Công an	Bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc trung ương	Quý II/2026

STT	Nhiệm vụ, giải pháp	Cơ quan chủ trì	Cơ quan phối hợp	Thời gian triển khai
4.	Triển khai công tác phê chuẩn Công ước Liên Hợp quốc về chống tội phạm mạng.	Bộ Ngoại giao	Bộ Công an, Bộ Tư pháp	Quý IV/2026
5.	Nghiên cứu hoàn chỉnh hành lang pháp lý về công tác phòng chống tội phạm mạng theo khuyến nghị của Công ước; điều chỉnh, bổ sung xây dựng các quy định thống nhất nhằm thực hiện các biện pháp thủ tục và thực thi pháp luật phù hợp với quy định của Công ước; sẵn sàng các điều kiện cho việc xây dựng lực lượng tham gia mạng lưới 24/7 theo quy định của Công ước.	Bộ Công an, Bộ Tư pháp	Bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc trung ương	2026 - 2027
6.	Rà soát sửa đổi TCVN 14423:2025 trên cơ sở hợp nhất TCVN 14423:2025 và TCVN 11930:2017 cho phù hợp với các cấp độ hệ thống thông tin theo Luật An ninh mạng 116/2025/QH15.	Bộ Công an	Bộ Khoa học và Công nghệ	Quý II/2026
7.	Ban hành Khung quản lý rủi ro an ninh mạng quốc gia, ban hành hướng dẫn về quản lý rủi ro an ninh mạng để các bộ, ngành, địa phương nghiên cứu, chuẩn bị nguồn lực thực hiện.	Bộ Công an	Bộ Khoa học và Công nghệ, Bộ Quốc phòng	Quý IV/2026
8.	Rà soát, đề xuất chính sách ưu đãi cho doanh nghiệp nghiên cứu phát triển sản phẩm an ninh mạng trong nước.	Bộ Tài chính, Bộ Công an	Bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc trung ương	2026 - 2027
II. Tổ chức lực lượng an ninh mạng				
1.	Kiện toàn Ban Chỉ đạo An ninh mạng Quốc gia và các tiểu ban tại các bộ, ngành, địa phương.	Bộ Công an	Bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh,	Quý I/2026

STT	Nhiệm vụ, giải pháp	Cơ quan chủ trì	Cơ quan phối hợp	Thời gian triển khai
			thành phố trực thuộc trung ương	
2.	Rà soát, hướng dẫn xây dựng mô hình tổ chức lực lượng bảo vệ an ninh mạng tại bộ, ngành, địa phương, cơ quan, tổ chức quản lý trực tiếp hệ thống thông tin quan trọng về an ninh quốc gia.	Bộ Công an	Bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc trung ương	Quý IV/2026
3.	Xây dựng mạng lưới liên kết các chuyên gia an ninh mạng trong nước và nước ngoài tham gia hỗ trợ công tác bảo đảm an ninh mạng. Mở rộng Liên minh ứng phó, khắc phục sự cố an ninh mạng quốc gia.	Hiệp hội An ninh mạng quốc gia	Bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc trung ương, các doanh nghiệp tham gia bảo vệ an ninh mạng	Thường xuyên
III. Phát triển nguồn nhân lực an ninh mạng chất lượng cao				
1.	Xây dựng, khung kiến thức, kỹ năng chuyên sâu về an ninh mạng; quy định về chứng nhận đáp ứng yêu cầu kiến thức, kỹ năng chuyên sâu về an ninh mạng cho lực lượng bảo vệ an ninh mạng, cán bộ trực tiếp quản trị vận hành hệ thống thông tin cấp độ 3, cấp độ 4, cấp độ 5, trong cơ quan, tổ chức, doanh nghiệp Nhà nước.	Bộ Công an	Bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc trung ương, các tổ chức, doanh nghiệp nhà nước	2026 - 2027
2.	Xây dựng, ban hành các chương trình khung, tài liệu, giáo trình đào tạo tập huấn về bảo vệ an ninh mạng; chuẩn hóa hoạt động đào tạo, tập huấn đáp ứng yêu cầu về chuẩn kỹ	Bộ Giáo dục và Đào tạo, Bộ Công an	Bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc	2026 - 2027

STT	Nhiệm vụ, giải pháp	Cơ quan chủ trì	Cơ quan phối hợp	Thời gian triển khai
	năng và kiến thức về an ninh mạng tương ứng với từng cấp độ năng lực.		trung ương, các tổ chức, doanh nghiệp nhà nước	
3.	Tổ chức các chương trình diễn tập quốc gia, quốc tế, tổ chức các chương trình đào tạo, huấn luyện, bồi dưỡng về an ninh mạng nhằm nâng cao năng lực, kiến thức, kỹ năng cho cán bộ các cấp gồm quản lý, lãnh đạo; cán bộ, công chức; nhân sự kỹ thuật an ninh mạng, các chương trình đào tạo, thi lấy chứng chỉ quốc tế.	Bộ Công an	Bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc trung ương, các tổ chức, doanh nghiệp nhà nước	Hằng năm
4.	Tổ chức diễn tập chuyên đề an ninh mạng, ứng cứu sự cố mạng trong phạm vi quản lý, tổ chức các khóa đào tạo, tập huấn trực tiếp hoặc trực tuyến nhằm cập nhật, nâng cao năng lực, kiến thức, kỹ năng cho cán bộ các cấp (gồm quản lý, lãnh đạo; người dùng cuối; nhân sự kỹ thuật an ninh mạng) theo hướng dẫn Bộ Công an, khuyến khích thi lấy chứng chỉ quốc tế.	Bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc trung ương, các tổ chức, doanh nghiệp nhà nước		Hằng năm
5.	Nghiên cứu xây dựng nền tảng quản lý hoạt động tập huấn, đánh giá và chứng nhận kiến thức, kỹ năng an ninh mạng; quản lý, xác thực dữ liệu các chứng chỉ an ninh mạng trong nước và quốc tế uy tín, quản lý các tổ chức đủ điều kiện thi, cấp, gia hạn, thu hồi chứng chỉ an ninh mạng phục vụ công	Bộ Công an	Các ban, bộ, ngành, địa phương, các cơ quan, doanh nghiệp có liên quan	2026 - 2027

STT	Nhiệm vụ, giải pháp	Cơ quan chủ trì	Cơ quan phối hợp	Thời gian triển khai
	nhận tương đương, từng bước phát triển bản đồ chuyên gia an ninh mạng.			
6.	Phổ biến, nâng cao kiến thức an ninh mạng cho người dân qua các nền tảng học tập số, "Bình dân học vụ số", các khóa học tuyến đại chúng mở (MOOC) và các chiến dịch truyền thông đại chúng.	Bộ Công an	Bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc trung ương, các tổ chức, doanh nghiệp nhà nước	Hằng năm
IV. Giải pháp giám sát, chia sẻ thông tin và đánh giá năng lực an ninh mạng quốc gia				
1.	Xây dựng chỉ số đảm bảo an ninh mạng để đánh giá năng lực bảo đảm an ninh mạng của các cơ quan tổ chức, doanh nghiệp.	Bộ Công an	Bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc trung ương	2026 - 2027
2.	Xây dựng hệ thống chia sẻ thông tin tình báo an ninh mạng (Threat Intelligence), hướng tới hình thành các trung tâm phân tích và chia sẻ thông tin an ninh mạng (ISAC - Information Sharing Analysis Center) cho từng ngành, lĩnh vực trọng yếu (tài chính, ngân hàng, giao thông, năng lượng,…)., thúc đẩy cơ chế chia sẻ thông tin tình báo về các mối đe dọa, lỗ hổng bảo mật và các cuộc tấn công an ninh mạng giữa khu vực công và tư nhân, đảm bảo tính đồng bộ, hiệu quả và bảo mật.	Bộ Công an, Hiệp hội an ninh mạng quốc gia	Bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc trung ương, các doanh nghiệp tham gia bảo vệ an ninh mạng	2026 - 2028
3.	Xây dựng nền tảng theo dõi, điều hành an ninh mạng quốc gia cho phép báo cáo, thống kê, cập nhật dữ liệu an ninh	Bộ Công an	Bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh,	2026 - 2027

STT	Nhiệm vụ, giải pháp	Cơ quan chủ trì	Cơ quan phối hợp	Thời gian triển khai
	mạng trên toàn quốc, đảm bảo dữ liệu "đúng, đủ, sạch sống, dùng chung, thống nhất".		thành phố trực thuộc trung ương	
4.	Trang bị hệ thống, công cụ chuyên dụng cho các lực lượng bảo vệ an ninh mạng, tối thiểu gồm hệ thống, công cụ rà quét phát hiện lỗ hổng bảo mật; hệ thống, công cụ hỗ trợ điều tra số, ứng cứu, khắc phục sự cố an ninh mạng.	Bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc trung ương		Thường xuyên
V. Nghiên cứu phát triển, nâng cao năng lực tự chủ công nghệ, đặc biệt chú trọng làm chủ các công nghệ lõi trong lĩnh vực an ninh mạng				
1.	Xây dựng và triển khai các chương trình, thúc đẩy cơ chế để cơ quan nhà nước đặt hàng doanh nghiệp phát triển các sản phẩm về an ninh mạng; ưu tiên thí điểm, thử nghiệm các sản phẩm do Việt Nam làm chủ công nghệ.	Bộ Công an, Bộ Khoa học và Công nghệ	Bộ Tài chính, VCCI, Các cơ quan, doanh nghiệp và hội, hiệp hội trong lĩnh vực an ninh mạng, CNTT-TT.	2026 - 2030
2.	Thúc đẩy phát triển các trung tâm đo kiểm an ninh mạng theo hướng xã hội hóa, đủ năng lực thực hiện thử nghiệm, đánh giá sự phù hợp tiêu chuẩn, quy chuẩn đối với sản phẩm an ninh mạng.	Bộ Khoa học và Công nghệ, Bộ Công an	Các cơ quan, doanh nghiệp và hội, hiệp hội trong lĩnh vực an ninh mạng, CNTT-TT.	2026 - 2027
3.	Tham gia các cơ chế hợp tác song phương, đa phương nhằm mục tiêu thừa nhận lẫn nhau kết quả đánh giá sự phù hợp tiêu chuẩn, quy chuẩn kỹ thuật với các tổ chức nước ngoài, quốc tế đối sản phẩm, dịch vụ an ninh mạng	Bộ Khoa học và Công nghệ, Bộ Ngoại giao	Các Bộ, ban ngành, địa phương có liên quan	2026 - 2030

STT	Nhiệm vụ, giải pháp	Cơ quan chủ trì	Cơ quan phối hợp	Thời gian triển khai
4.	Tăng cường phối hợp công tư, xây dựng và vận hành có hiệu quả tam giác chiến lược Nhà nước - Nhà trường (Viện nghiên cứu) - Doanh nghiệp trong việc định hướng, nghiên cứu, nắm bắt các công nghệ lõi, công nghệ chiến lược, phát triển, triển khai các công nghệ, sản phẩm, dịch vụ an ninh mạng.	Bộ Khoa học và Công nghệ, Bộ Giáo dục và Đào tạo, Bộ Công an	Các cơ quan, doanh nghiệp và hội, hiệp hội trong lĩnh vực an ninh mạng, CNTT-TT.	2026 - 2030
VI. Nâng cao uy tín quốc gia và tăng cường hợp tác quốc tế				
1.	Tham gia theo thẩm quyền hoặc đề xuất Việt Nam tham gia các tổ chức, quốc tế về an ninh mạng, cung cấp nội dung về an ninh mạng trong các xếp hạng, đánh giá của quốc tế; tăng cường kết nối, chuyển giao công nghệ và trao đổi hợp tác quốc tế về an ninh mạng.	Bộ Công an	Bộ Ngoại giao; các tổ chức quốc tế liên quan	Thường xuyên
2.	Vận động các nguồn hỗ trợ phát triển chính thức (ODA), thu hút nguồn lực từ nước ngoài và các đối tác quốc tế cho hoạt động nghiên cứu, ứng dụng, đổi mới sáng tạo, khởi nghiệp, chuyển giao công nghệ về bảo đảm an ninh mạng.	Bộ Công An, Bộ Tài chính	Bộ Ngoại giao; Bộ Khoa học và Công nghệ; các bộ, ngành, địa phương	Thường xuyên