

BAN CHỈ ĐẠO TRUNG ƯƠNG
VỀ PHÁT TRIỂN KHOA HỌC, CÔNG NGHỆ,
ĐỔI MỚI SÁNG TẠO VÀ CHUYỂN ĐỔI SỐ
CƠ QUAN THƯỜNG TRỰC

ĐẢNG CỘNG SẢN VIỆT NAM

Hà Nội, ngày 27 tháng 9 năm 2025

Số 06-TB/CQTTBCĐ

THÔNG BÁO KẾT LUẬN
CỦA ĐỒNG CHÍ TỔNG BÍ THƯ TÔ LÂM,
TRƯỞNG BAN CHỈ ĐẠO TRUNG ƯƠNG VỀ PHÁT TRIỂN KHOA HỌC,
CÔNG NGHỆ, ĐỔI MỚI SÁNG TẠO VÀ CHUYỂN ĐỔI SỐ
**tại Phiên họp Thường trực Ban Chỉ đạo về công tác bảo đảm
an ninh mạng, bảo mật thông tin, an toàn dữ liệu**

Ngày 18/9/2025, Thường trực Ban Chỉ đạo Trung ương về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số (sau đây gọi tắt là Ban Chỉ đạo) đã họp để đánh giá tình hình triển khai thực hiện và các giải pháp bảo đảm an ninh mạng, bảo mật thông tin, an toàn dữ liệu. Phiên họp do đồng chí Tổng Bí thư Tô Lâm, Trưởng Ban Chỉ đạo chủ trì với sự tham gia của các đồng chí Thường trực Ban Chỉ đạo, Thường trực Tổ Giúp việc và đại diện lãnh đạo các bộ, cơ quan liên quan.

Trên cơ sở báo cáo của Bộ Công an, ý kiến phát biểu của các đồng chí tham dự Phiên họp, đồng chí Tổng Bí thư Tô Lâm, Trưởng Ban Chỉ đạo cơ bản thống nhất với báo cáo trung tâm, những đề xuất tại cuộc họp và ý kiến của đồng chí Thủ tướng Chính phủ, Phó Trưởng Ban Chỉ đạo, đồng thời nhấn mạnh một số nội dung kết luận như sau:

I- TÌNH HÌNH TRIỂN KHAI THỰC HIỆN

1. Ghi nhận một số kết quả đã đạt được trong công tác bảo đảm an ninh mạng, bảo mật thông tin, an toàn dữ liệu của các cơ quan Trung ương và địa phương trong thời gian qua: (i) Nhận thức của các cấp, các ngành và người dân về tầm quan trọng của an ninh mạng, bảo mật thông tin, an toàn dữ liệu đã có những chuyển biến tích cực. (ii) Thể chế, chính sách pháp luật về an toàn thông tin, an ninh mạng tiếp tục được hoàn thiện, tạo hành lang pháp lý đồng bộ, làm cơ sở quan trọng cho công tác quản lý, bảo vệ an ninh quốc gia trên không gian mạng và thúc đẩy chuyển đổi số quốc gia. (iii) Năng lực kỹ thuật của một số cơ quan, đơn vị cũng đã được tăng cường, chủ động hơn trong việc phát hiện và ứng phó với các sự cố. (iv) Việt Nam đã vươn lên xếp hạng 17 thế giới về chỉ số an toàn, an ninh mạng toàn cầu (GCI). Ngành công nghiệp an ninh mạng nội địa đã có sự tăng trưởng và các doanh nghiệp trong nước bước đầu đã làm chủ được một số chủng loại sản phẩm thiết yếu...

2. Tuy nhiên, bên cạnh những kết quả tích cực đạt được, vẫn còn nhiều tồn tại, hạn chế như: **(i)** Công tác quản lý nhà nước vẫn theo lối mòn cũ, cách làm còn nhiều bất cập, tổ chức thực hiện còn chông chéo, thiếu sự phối hợp đồng bộ giữa các cơ quan, hoạt động còn trùng lắp nhau. **(ii)** Hệ thống quy định pháp luật và văn bản chỉ đạo chưa được cập nhật kịp thời, còn "*khoảng trống*", "*độ trễ*" so với thực tiễn. **(iii)** Nhận thức của một bộ phận lãnh đạo, cán bộ, đảng viên và Nhân dân về chuyển đổi số còn chưa đầy đủ và sâu sắc; chưa tuân thủ và thực thi đầy đủ các quy định của pháp luật, các quy trình, tiêu chuẩn về công tác bảo đảm an toàn, an ninh mạng và bảo mật thông tin, còn nhiều lỗ hổng bảo mật, tình trạng "*nợ tuân thủ*" các điều kiện về an ninh, an toàn vẫn còn diễn ra. **(iv)** Nguồn nhân lực chất lượng cao còn thiếu; ngân sách dành cho an toàn, bảo mật thông tin còn chưa đáp ứng yêu cầu. **(v)** Hạ tầng số chưa đồng bộ, hầu hết chưa có giải pháp tổng thể; đầu tư manh mún, khó áp dụng đầy đủ các tiêu chuẩn bảo đảm an ninh mạng tối thiểu; đặc biệt, các thiết bị đầu cuối cơ bản vẫn sử dụng hệ điều hành và phần mềm của nước ngoài, tiềm ẩn nguy cơ bị cài cắm mã độc, bị chiếm quyền điều khiển từ xa, hoặc bị đánh cắp dữ liệu một cách tinh vi...

Với những tồn tại, hạn chế nêu trên, chúng ta đang phải đối mặt với 2 thách thức lớn: **(i)** Bản chất của các mối đe dọa hiện nay đã hoàn toàn khác. Các cuộc tấn công mạng không còn là hành vi tự phát, nhỏ lẻ mà đã được "*công nghiệp hoá*", trở thành các chiến dịch được đầu tư bài bản, có sử dụng trí tuệ nhân tạo, được tổ chức bởi các thế lực thù địch và tội phạm chuyên nghiệp, tinh vi tấn công trên quy mô lớn; tấn công vào chuỗi cung ứng cũng ngày càng trở nên phổ biến, nguy hiểm hơn là thông qua việc xâm nhập qua các nhà cung cấp phần mềm, dịch vụ, gây ra thiệt hại lớn về giá trị và quy mô trên diện rộng, đe dọa trực tiếp đến sự ổn định kinh tế vĩ mô và an ninh quốc gia. **(ii)** Hoạt động sử dụng không gian mạng xâm phạm an ninh quốc gia, trật tự xã hội, các loại tội phạm mạng, tội phạm sử dụng công nghệ cao diễn ra rất phức tạp, nhất là tán phát thông tin xấu độc, tuyên truyền phá hoại tư tưởng, xuyên tạc chống Đảng, Nhà nước; tấn công mạng, gián điệp mạng nhằm vào các hệ thống thông tin quan trọng về an ninh quốc gia, hệ thống thông tin trọng yếu của cơ quan Đảng, Nhà nước, ngành kinh tế mũi nhọn... để chiếm đoạt bí mật nhà nước, bí mật kinh tế hoặc thực hiện hành vi phá hoại; các loại tội phạm sử dụng công nghệ cao có nhiều diễn biến nguy hiểm với các thủ đoạn mới, tinh vi, gây thiệt hại lớn về kinh tế, nhức nhối trong dư luận người dân...

II- QUAN ĐIỂM CHỈ ĐẠO VÀ CÔNG TÁC CHỈ ĐẠO, ĐIỀU HÀNH

1. Về quan điểm chỉ đạo

a) Bảo đảm an ninh mạng, bảo mật thông tin, an toàn dữ liệu là nhiệm vụ trọng yếu, thường xuyên, vừa cấp bách trước mắt, vừa chiến lược lâu dài, gắn

liên với sự phát triển kinh tế - xã hội bền vững, bảo vệ vững chắc chủ quyền quốc gia và sự nghiệp bảo vệ Tổ quốc từ sớm, từ xa. Phải xử lý hài hoà mối quan hệ: An ninh để phát triển, phát triển phải đi đôi với an ninh.

b) Lấy phòng ngừa chủ động là chính, đi trước một bước, không để bị động, bất ngờ trong mọi tình huống. Mọi nguy cơ, thách thức về an ninh mạng, bảo mật thông tin, an toàn dữ liệu phải được nhận diện và xử lý từ sớm. Tập trung bảo vệ hệ thống của các cơ quan Trung ương (Đảng, Quốc hội, Chính phủ, Mặt trận Tổ quốc và các tổ chức chính trị - xã hội), quân đội, công an; các trung tâm dữ liệu quốc gia; trung tâm điều hành kinh tế quốc gia quan trọng như ngân hàng, năng lượng, giao thông...

c) Xây dựng và củng cố năng lực tự chủ, tự cường về công nghệ, con người và cơ chế quản trị là nền tảng cốt lõi để bảo vệ an toàn hệ thống thông tin quốc gia. Phải ưu tiên nguồn lực quốc gia để làm chủ các công nghệ lõi, phát triển nền công nghiệp an ninh mạng "Make in Vietnam" bền vững.

d) Phát huy sức mạnh tổng hợp của cả hệ thống chính trị và toàn dân, trong đó Nhà nước giữ vai trò chủ đạo, lực lượng chuyên trách bảo vệ an ninh mạng là nòng cốt, phát động phong trào toàn dân bảo vệ an ninh Tổ quốc trên không gian mạng. Đề cao trách nhiệm của người đứng đầu các cấp, đồng thời huy động sự tham gia tích cực, hiệu quả của cộng đồng doanh nghiệp, các tổ chức xã hội và mọi người dân.

đ) 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 lợi ích quốc gia - dân tộc. Hợp tác để học hỏi, chuyển giao công nghệ, chung tay giải quyết các thách thức an ninh phi truyền thống, nhưng phải luôn nêu cao tinh thần cảnh giác, sẵn sàng ứng phó với mọi tình huống.

2. Công tác chỉ đạo, điều hành

a) Người đứng đầu các cơ quan, tổ chức trong hệ thống chính trị từ Trung ương đến địa phương chịu trách nhiệm lãnh đạo, chỉ đạo, kiểm tra, đôn đốc công tác này. Đưa kết quả đánh giá chỉ số bảo đảm an ninh mạng của các cơ quan, tổ chức vào tiêu chí đánh giá tín nhiệm, năng lực của cán bộ, đặc biệt là người đứng đầu để xếp loại cán bộ hằng năm. Triển khai chương trình đánh giá tín nhiệm mạng đối với các tổ chức, cá nhân có ảnh hưởng trên không gian mạng; củng cố lòng tin số của người dân khi hoạt động, tương tác, làm việc trên không gian mạng.

b) Đối với Ban Chỉ đạo Trung ương, Đảng uỷ Công an Trung ương có trách nhiệm thường trực về vấn đề bảo đảm an ninh mạng, bảo mật thông tin, an toàn dữ liệu; cần quán xuyên suốt vấn đề này trong cả hệ thống chính trị từ Trung ương tới cơ sở. Bộ Công an theo chức năng, nhiệm vụ, nâng cao hiệu

lực, hiệu quả đối với hoạt động cung cấp sản phẩm, dịch vụ an ninh mạng, an toàn dữ liệu cho hệ thống thông tin không thuộc lĩnh vực quân sự, cơ yếu.

c) Các doanh nghiệp cung cấp dịch vụ viễn thông, Internet trong nước phải phát huy vai trò là tuyến đầu phòng thủ và có trách nhiệm tuân thủ quy định trong công tác bảo đảm an ninh mạng, bảo mật thông tin, an toàn dữ liệu.

III- CÁC NHIỆM VỤ TRỌNG TÂM CẦN TẬP TRUNG THỰC HIỆN

Để công tác bảo đảm an ninh mạng, bảo mật thông tin, an toàn dữ liệu trong toàn hệ thống chính trị đáp ứng trong tình hình mới, yêu cầu các cấp uỷ, tổ chức đảng, các cơ quan, bộ, ngành Trung ương và địa phương cần tập trung lãnh đạo, chỉ đạo quyết liệt để khắc phục dứt điểm những tồn tại, hạn chế và triển khai ngay các nội dung sau:

1. Nâng cao nhận thức của cán bộ, đảng viên và Nhân dân về bảo đảm an ninh mạng, bảo mật thông tin, an toàn dữ liệu

Tiếp tục triển khai công tác tuyên truyền, phổ biến giáo dục pháp luật về an toàn thông tin, an ninh mạng đồng bộ, có chiều sâu, đa dạng về nội dung, hình thức. Đưa các nội dung kiến thức, kỹ năng cơ bản về an toàn thông tin, 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 giúp thế hệ trẻ có ý thức từ sớm về việc sử dụng không gian mạng an toàn. Tăng cường tuyên truyền, phổ biến, đào tạo kiến thức an ninh mạng trên nền tảng "Bình dân học vụ số", nhất là các quy định và kỹ năng bảo vệ dữ liệu cá nhân, phòng, chống tội phạm lừa đảo chiếm đoạt tài sản trên không gian mạng...

2. Khẩn trương hoàn thiện thể chế, chính sách pháp luật về an ninh mạng, bảo mật thông tin, an toàn dữ liệu

a) Trong năm 2025 phải tháo gỡ hết những khó khăn, vướng mắc, điểm nghẽn về pháp luật trong lĩnh vực an ninh mạng, bảo mật thông tin, an toàn dữ liệu theo đúng tinh thần Nghị quyết số 66-NQ/TW của Bộ Chính trị. Đảng uỷ Chính phủ, Đảng uỷ Quốc hội chỉ đạo cơ quan chức năng rà soát, hoàn thiện việc sửa đổi, bổ sung các văn bản liên quan để xem xét, thông qua tại Kỳ họp thứ 10, Quốc hội khoá XV, nhất là Luật An ninh mạng (sửa đổi), Luật Bảo vệ bí mật nhà nước (sửa đổi).

b) Các cơ quan theo chức năng, nhiệm vụ được giao khẩn trương: **(i)** Hoàn thiện các tiêu chuẩn quốc gia, quy chuẩn kỹ thuật cho sản phẩm, dịch vụ an ninh mạng thuộc các lĩnh vực then chốt; thiết lập cơ chế kiểm định, chứng nhận bắt buộc cho sản phẩm an ninh mạng. **(ii)** Xây dựng Khung quản lý rủi ro an ninh mạng quốc gia, chuyển đổi tư duy 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. **(iii)** Xây dựng chỉ số bảo đảm an ninh mạng để đánh giá năng lực bảo đảm an ninh mạng của các cơ quan, các bộ, ngành, địa phương, tổ chức, doanh nghiệp. **(iv)** 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 an toàn thông tin, an ninh mạng và ứng cứu sự cố. Thể hiện rõ vai trò chủ trì của Việt Nam trong tổ chức Lễ mở ký Công ước của Liên hợp quốc về chống tội phạm mạng (tổ chức tại Việt Nam).

3. Tập trung phát triển hạ tầng an ninh mạng hiện đại, đồng bộ, đáp ứng yêu cầu bảo vệ chủ quyền quốc gia trên không gian mạng

a) Triển khai kiến trúc bảo vệ an ninh mạng quốc gia hỗ trợ bảo vệ đa lớp cho toàn bộ hạ tầng mạng Internet Việt Nam và các hệ thống thông tin của bộ, ngành, địa phương, tổ chức, doanh nghiệp.

b) Triển khai đồng bộ các nhóm giải pháp: Bảo vệ hạ tầng mạng - bảo vệ thiết bị đầu cuối - bảo vệ ứng dụng, dịch vụ - bảo vệ dữ liệu - bảo vệ người dùng. Phát triển và ứng dụng thuật toán mật mã tiên tiến, *tập trung nguồn lực quốc gia để nghiên cứu, làm chủ các công nghệ lõi chiến lược như công nghệ mật mã, thiết kế và sản xuất chip bảo mật "Make in Vietnam"*. Nghiên cứu, phát triển mã hoá kháng lượng tử để bảo vệ bí mật nhà nước; khuyến khích việc xã hội hoá hoạt động nghiên cứu, phát triển, ứng dụng mật mã dân sự phục vụ bảo mật thông tin, dữ liệu.

c) Rà soát và tăng cường bảo vệ tuyệt đối an toàn các hệ thống thông tin quan trọng, các cơ sở dữ liệu quốc gia về dân cư, đất đai, tài chính, y tế, giáo dục, bảo hiểm, tư pháp... coi đây là tài sản chiến lược, nền tảng quản trị quốc gia hiện đại. Thiết lập cơ chế thống nhất về tiêu chuẩn, quy chuẩn bảo mật; bắt buộc tích hợp yếu tố an toàn thông tin "*ngay từ thiết kế*" đối với các trung tâm dữ liệu quan trọng, các hệ thống số, nền tảng số và ứng dụng mới; khắc phục ngay những lỗ hổng bảo mật trong các hệ thống thông tin, không chấp nhận tình trạng "*nợ tuân thủ*". Xây dựng cơ chế kết nối, chia sẻ dữ liệu liên thông giữa các bộ, ngành, địa phương trên nguyên tắc bảo mật, an toàn, đúng pháp luật, khắc phục tình trạng cát cứ, phân mảnh dữ liệu. Đặc biệt là nâng cao ý thức, trách nhiệm của cán bộ, công chức, viên chức tham gia vào các quy trình công việc liên quan đến các hệ thống thông tin quan trọng này.

4. Tăng cường phát triển công nghiệp an ninh mạng tự chủ và thị trường an ninh mạng cạnh tranh, minh bạch

Nghiên cứu có cơ chế đầu tư cho phát triển hệ sinh thái an toàn thông tin, an ninh mạng, đặc biệt là hệ sinh thái "*Make in Vietnam*"; ưu tiên làm chủ và

sản xuất nội địa các sản phẩm an ninh mạng cốt lõi, nền tảng; xây dựng thị trường cạnh tranh lành mạnh; hỗ trợ doanh nghiệp tư nhân hình thành các trung tâm nghiên cứu, vườn ươm hỗ trợ khởi nghiệp. Ưu tiên sử dụng sản phẩm, giải pháp nội địa trong các dự án, hệ thống trọng yếu, vừa tạo thị trường, vừa thúc đẩy doanh nghiệp Việt phát triển.

5. Bảo đảm nguồn lực tài chính, ngân sách dành cho an ninh mạng, bảo mật thông tin, an toàn dữ liệu

Quy định an ninh mạng, bảo mật thông tin, an toàn dữ liệu là thành phần bắt buộc trong mọi dự án công nghệ thông tin; yêu cầu tỉ lệ kinh phí chi cho các sản phẩm, dịch vụ an ninh mạng, bảo mật thông tin, dữ liệu đạt tối thiểu 15% tổng kinh phí triển khai đề án, dự án công nghệ thông tin, bảo đảm hiệu quả, đúng quy định, tránh lãng phí. Nghiên cứu sửa đổi bổ sung các quy định pháp luật có liên quan để tạo cơ chế thông thoáng trong đầu tư, đấu thầu, triển khai an ninh mạng, bảo mật thông tin, an toàn dữ liệu.

6. Phát triển nguồn nhân lực an ninh mạng, bảo mật thông tin, an toàn dữ liệu đáp ứng yêu cầu trong tình hình mới

Các bộ, ngành, địa phương rà soát đánh giá, xác định nhu cầu nhân lực bảo đảm an ninh mạng, bảo mật thông tin, an toàn dữ liệu và có kế hoạch bổ sung, tăng cường bảo đảm đáp ứng yêu cầu. Bộ Giáo dục và Đào tạo chủ trì xây dựng chương trình đào tạo chuyên sâu về an ninh mạng và công nghệ lõi. Bộ Công an chủ trì, phối hợp các đơn vị có liên quan xây dựng các khoá đào tạo thực tế về công tác bảo đảm an ninh mạng cho cán bộ chuyên trách an ninh mạng của các đơn vị, địa phương. Ban Tổ chức Trung ương, Bộ Nội vụ và Bộ Công an phối hợp nghiên cứu đề xuất và triển khai chính sách đặc thù (lương, phúc lợi) để thu hút và giữ chân chuyên gia an ninh mạng làm việc hoặc cộng tác trong các cơ quan đảng, nhà nước. Hiệp hội An ninh mạng quốc gia 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...

7. Tăng cường hợp tác quốc tế trên lĩnh vực an ninh mạng, bảo mật thông tin, an toàn dữ liệu

Triển khai các hình thức hợp tác song phương, đa phương trên lĩnh vực an ninh mạng, trọng tâm là chia sẻ thông tin tình báo, cảnh báo sớm; phối hợp quốc tế phòng, chống và ứng phó với các cuộc tấn công mạng; điều tra, truy tố tội phạm mạng xuyên quốc gia; xây dựng khung pháp lý và chuẩn mực chung. Tích cực tham gia luyện tập, diễn tập an toàn thông tin, an ninh mạng quốc tế. Chuẩn bị tốt cho việc ký kết và triển khai hiệu quả, thực chất Công ước Hà Nội về chống tội phạm mạng năm 2025...

8. Một số nhiệm vụ, giải pháp cần tập trung hoàn thành ngay trong năm 2025 để bảo đảm an ninh mạng, bảo mật thông tin, an toàn dữ liệu cho toàn hệ thống chính trị đáp ứng yêu cầu chuyển đổi số liên thông, đồng bộ, nhanh, hiệu quả

a) Các cơ quan chủ quản các cơ sở dữ liệu, hệ thống thông tin trong hệ thống chính trị từ Trung ương đến cơ sở chủ trì, phối hợp với Bộ Công an, Ban Cơ yếu Chính phủ tổ chức đánh giá tổng thể về an ninh mạng, bảo mật thông tin, an toàn dữ liệu đối với các cơ sở dữ liệu quốc gia, chuyên ngành, hệ thống thông tin và nguồn nhân lực thuộc phạm vi quản lý; gửi Bộ Công an, Ban Cơ yếu Chính phủ theo chức năng, nhiệm vụ để tổng hợp, đề xuất giải pháp bảo đảm an toàn an ninh mạng, bảo mật thông tin, an toàn dữ liệu cho toàn quốc. **Hoàn thành trong tháng 11/2025.**

b) Bộ Công an trình cấp có thẩm quyền kiện toàn Ban Chỉ đạo An toàn, an ninh mạng Quốc gia và các tiểu ban tại các bộ, ngành, địa phương; giao đồng chí bí thư tỉnh uỷ, thành uỷ, bộ trưởng, thủ trưởng các bộ, cơ quan là trưởng tiểu ban. **Hoàn thành trong tháng 11/2025.**

c) Đảng uỷ Công an Trung ương chủ trì, phối hợp với Văn phòng Trung ương Đảng và các cơ quan liên quan xây dựng, trình Ban Bí thư ban hành Chỉ thị về tăng cường bảo đảm an ninh mạng, bảo mật thông tin, an toàn dữ liệu trong hệ thống chính trị. **Hoàn thành trong tháng 10/2025.**

d) **Bộ Công an:** (i) Tập trung nâng cao năng lực của Trung tâm An ninh mạng quốc gia thuộc Bộ Công an; mở rộng kết nối giám sát an ninh mạng đến toàn bộ cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành, hệ thống thông tin, hệ thống dùng chung của toàn hệ thống chính trị; thiết lập kênh kết nối trao đổi thông tin, dữ liệu phục vụ giám sát, điều phối ứng cứu, khắc phục sự cố an toàn thông tin, an ninh mạng theo hướng dẫn của lực lượng chuyên trách bảo vệ an ninh mạng. **Nhiệm vụ thường xuyên.** (ii) Đẩy nhanh tiến độ xây dựng, vận hành Hệ thống phòng vệ mạng quốc gia trở thành nền tảng dùng chung trong Khung kiến trúc tổng thể quốc gia số nhằm bảo vệ an ninh mạng vòng ngoài cho các hệ thống thông tin, tài nguyên trọng yếu trên Internet của các cơ quan ban, bộ, ngành, địa phương, cơ quan, doanh nghiệp Việt Nam. **Hoàn thành thiết kế kỹ thuật trong tháng 11/2025.** (iii) Chủ trì, phối hợp các bộ, ngành, địa phương ban hành các quy định, tài liệu hướng dẫn về bảo đảm an ninh mạng, an toàn thông tin cho các cơ sở dữ liệu, hệ thống dùng chung trong hệ thống chính trị; tổ chức kiểm tra, đánh giá việc thực hiện các quy định bảo đảm an ninh mạng, an toàn thông tin. **Hoàn thành trong tháng 12/2025.**

đ) **Bộ Khoa học và Công nghệ** chủ trì, phối hợp Bộ Công an và các bộ, ngành, địa phương liên quan rà soát, trình cấp có thẩm quyền xem xét, điều chỉnh hoặc ban hành quy hoạch hạ tầng công nghệ thông tin tổng thể từ Trung

ương đến địa phương theo hướng tập trung các máy chủ về các trung tâm dữ liệu đạt chuẩn, đủ điều kiện để triển khai đầy đủ các biện pháp bảo vệ an ninh mạng theo quy định. **Hoàn thành trong tháng 12/2025.**

e) Văn phòng Trung ương Đảng chủ trì, phối hợp với Đảng uỷ Công an Trung ương và các cơ quan liên quan xây dựng, trình Ban Chỉ đạo ban hành Kế hoạch về bảo đảm an ninh mạng, bảo mật thông tin, an toàn dữ liệu trong hệ thống chính trị. **Hoàn thành trong tháng 9/2025.**

g) Các đồng chí Thường trực Ban Chỉ đạo, các đồng chí thành viên Ban Chỉ đạo Trung ương và các cơ quan liên quan tập trung chỉ đạo, đôn đốc, xử lý những vấn đề còn tồn tại, khó khăn, vướng mắc và triển khai ngay các giải pháp cấp bách và lâu dài để bảo đảm tiến độ và chất lượng. Gắn trách nhiệm cụ thể cho từng cơ quan, tổ chức, nhất là người đứng đầu, xem xét xử lý trách nhiệm khi nhiệm vụ không hoàn thành mà không có lý do chính đáng, đồng thời tăng cường kiểm tra, giám sát việc tổ chức thực hiện.

Văn phòng Trung ương Đảng - Cơ quan Thường trực của Ban Chỉ đạo thông báo để các đồng chí thành viên Ban Chỉ đạo và các cơ quan liên quan biết, thực hiện.

Nơi nhận:

- Bộ Chính trị, Ban Bí thư (để báo cáo),
- Các thành viên Ban Chỉ đạo (để thực hiện),
- Đảng uỷ các cơ quan Đảng Trung ương,
- Đảng uỷ Chính phủ,
- Đảng uỷ Quốc hội,
- Đảng uỷ Mặt trận Tổ quốc, các đoàn thể Trung ương,
- Các ban đảng Trung ương,
- Đảng uỷ các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ,
- Quân uỷ Trung ương,
- Đảng uỷ Công an Trung ương,
- Các tỉnh uỷ, thành uỷ,
- Văn phòng Tổng Bí thư,
- Lãnh đạo Văn phòng Trung ương Đảng,
- Cục Chuyển đổi số - Cơ yếu,
- Lưu Ban Chỉ đạo Trung ương.

CHÁNH VĂN PHÒNG

kiêm

PHÓ TRƯỞNG BAN THƯỜNG TRỰC



Phạm Gia Túc