Ngày 09 tháng 7 năm 2026

GÓP Ý CỦA LIÊN MINH DỮ LIỆU TOÀN CẦU ĐỐI VỚI HỒ SƠ CHÍNH SÁCH CỦA DỰ ÁN LUẬT AN NINH DỮ LIỆU

Liên minh Dữ liệu Toàn cầu (**GDA**)[1] trân trọng cảm ơn Bộ Công an đã tạo cơ hội để chúng tôi đóng góp ý kiến đối với Hồ Sơ Chính Sách của dự án Luật An ninh dữ liệu.

GDA là một liên minh đa ngành gồm các công ty có trụ sở tại nhiều khu vực khác nhau trên thế giới, cam kết tuân thủ các tiêu chuẩn cao về quyền riêng tư và an ninh dữ liệu. GDA ủng hộ các chính sách giúp tăng cường niềm tin vào nền kinh tế số mà không áp đặt các hạn chế không hợp lý đối với hoạt động chuyển dữ liệu xuyên biên giới hoặc yêu cầu địa phương hoá dữ liệu, những yếu tố có thể làm suy yếu an ninh dữ liệu, đổi mới sáng tạo, phát triển kinh tế và thương mại quốc tế. Với trọng tâm hoạt động của GDA là các vấn đề liên quan đến dữ liệu xuyên biên giới, chúng tôi xin tập trung góp ý đối với các nội dung của Hồ Sơ Chính Sách liên quan đến chuyển dữ liệu xuyên biên giới.

Trong những năm vừa qua, GDA đã nhiều lần tham gia đóng góp ý kiến về các đề xuất của Việt Nam liên quan đến yêu cầu địa phương hoá dữ liệu hoặc hạn chế chuyển dữ liệu, bao gồm các ý kiến liên quan đến Luật Dữ liệu, Luật An ninh mạng và Luật Bảo vệ dữ liệu cá nhân. Các ý kiến này có thể được tham khảo tại đây.[2]

Các công ty thành viên GDA là những nhà đầu tư quan trọng tại Việt Nam, đã đầu tư hàng triệu đô la và hỗ trợ hàng nghìn việc làm. Chuyển dữ liệu cho phép cung cấp các công cụ số và thông tin chuyên sâu quan trọng để hỗ trợ các doanh nhân và công ty thuộc mọi quy mô, ở mọi quốc gia, tạo ra các loại việc làm mới, nâng cao hiệu quả, cải thiện chất lượng và gia tăng sản lượng.

Chúng tôi hy vọng các đề xuất này sẽ hỗ trợ Bộ Công an trong quá trình xây dựng Luật An ninh dữ liệu. Chúng tôi cũng mong muốn tiếp tục là nguồn tham khảo hữu ích cho Bộ Công an trong quá trình Việt Nam hoàn thiện khuôn khổ quản trị dữ liệu toàn diện, hiệu quả và có khả năng tương thích với các thông lệ quốc tế tốt nhất — đặc biệt trong lĩnh vực chuyển dữ liệu xuyên biên giới — đồng thời hỗ trợ sự phát triển của một nền kinh tế số năng động và đổi mới sáng tạo.

Chủ Quyền Dữ Liệu Quốc Gia

Hồ Sơ Chính Sách của dự án Luật An ninh dữ liệu định hướng áp dụng mô hình quản trị dựa trên rủi ro và phân lớp bảo vệ nhằm xây dựng một "hệ sinh thái tự chủ, tự cường" theo đó: (1) đối với nhóm Dữ Liệu Cốt Lõi thì yêu cầu phải sử dụng mật mã nội địa và hạ tầng dùng riêng (air-gapped); (2) đối với nhóm Dữ Liệu

[1] Để biết thêm thông tin về Liên minh Dữ liệu Toàn cầu, vui lòng truy cập www.globaldataalliance.org

[2] *Xem* Liên minh Dữ liệu Toàn cầu, Góp ý của GDA cho Chính phủ Việt Nam (2020 – 2025), at: https://globaldataalliance.org/resources-results/?pub_type=resource-filings&location=loc-vietnam&sector=&language=&posts_filtered=1

Quan Trọng thì yêu cầu phải lưu trữ dữ liệu "gốc" tại Việt Nam; và (3) đối với nhóm dữ liệu còn lại được phép "lưu thông linh hoạt" sử dụng cơ chế quản lý bằng "hậu kiểm" và tuân theo tiêu chuẩn an toàn thông lệ quốc tế. Theo Hồ Sơ Chính Sách, điều này cho phép Việt Nam giữ vững được độc lập tự chủ trên không gian mạng, giữ vững được chủ quyền số song không bị tụt hậu trong cuộc đua kinh tế toàn cầu.

Hồ Sơ Chính Sách đồng thời đề ra các bước thực thi dưới đây để đảm bảo chủ quyền số:

- Xây dựng danh mục dữ liệu quốc gia, phân loại rõ ràng các nhóm dữ liệu để áp dụng cấp độ bảo vệ tương ứng, tránh đánh đồng dữ liệu kinh doanh với dữ liệu an ninh.
- Thiết lập "biên giới số" thông minh: vận hành đơn vị quản trị an ninh dữ liệu quốc gia để theo dõi dòng chảy dữ liệu tự động 24/7, phát hiện bất thường và không cần đọc nội dung dữ liệu của doanh nghiệp.
- Làm chủ hạ tầng lưu trữ: ban hành các quy chuẩn kỹ thuật bắt buộc để các nhà cung cấp dịch vụ hạ tầng trong nước đạt tiêu chuẩn bảo vệ dữ liệu.
- Có thể nghiên cứu cơ chế "hậu kiểm kỹ thuật số", thay thế giấy phép bằng việc giám sát trực tuyến và thanh tra dựa trên dấu hiệu vi phạm.

GDA ủng hộ mục tiêu của Việt Nam trong việc nâng cao năng lực tự cường, tạo lập niềm tin và thúc đẩy đổi mới, sáng tạo. Tuy nhiên, không thể đạt được chủ quyền số thiết thực thông qua việc hạn chế hợp tác toàn cầu hay giới hạn các lựa chọn về công nghệ. Chủ quyền số cần được xây dựng dựa trên các tiêu chuẩn được quốc tế công nhận, quản trị minh bạch và khả năng vận hành một cách vững chắc trong một hệ sinh thái số mở và có tính kết nối. Thách thức đối với các nhà lập pháp là phải dung hoà được mong muốn kiểm soát chính đáng của Việt Nam với thực tiễn của một nền kinh tế số toàn cầu vốn phụ thuộc lẫn nhau.

Khuyến nghị: Các cơ chế kiểm soát liên quan đến chủ quyền chỉ nên được áp dụng theo mức độ rủi ro, trên cơ sở cân nhắc toàn diện các hệ quả đi kèm, ví dụ như khả năng đổi mới, sáng tạo, an ninh mạng và mức độ khả dụng của các tính năng dịch vụ. Suy cho cùng, từng tổ chức riêng biệt – tùy thuộc vào mức độ rủi ro và tác động tiềm tàng, và dù là cơ quan nhà nước hay đơn vị vận hành hạ tầng trọng yếu – phải là chủ thể tự quyết định phạm vi áp dụng các biện pháp quản lý và phương án cân đối các rủi ro và hệ quả ảnh hưởng này.

Bảo Đảm An Ninh Dữ Liệu

Luật An ninh dữ liệu đề xuất bảo đảm an ninh dữ liệu dựa trên cơ chế phân loại 04 cấp độ rủi ro, cụ thể:

- Cấp độ 1: Dữ liệu tác động trực tiếp đến độc lập, chủ quyền, quốc phòng, an ninh và sự ổn định của chế độ. Dữ liệu Cấp độ 1 đồng thời được xem là Dữ Liệu Cốt Lõi.
- Cấp độ 2: Dữ liệu tác động trực tiếp đến sự vận hành của hạ tầng thông tin quốc gia, trật tự an toàn xã hội và nền kinh tế vĩ mô.
- Cấp độ 3: Dữ liệu tác động đến quyền riêng tư, danh dự của công dân và lợi ích hợp pháp của tổ chức trên quy mô lớn.
- Cấp độ 4: Các loại dữ liệu công khai, thương mại có mức độ ảnh hưởng thấp nhưng vẫn phải được quản lý, bảo vệ theo quy định của pháp luật.

Cấp độ 1 và 2 yêu cầu áp dụng biện pháp kỹ thuật đặc biệt, bao gồm bắt buộc áp dụng công nghệ "lá chắn dữ liệu", cô lập vật lý đối với dữ liệu tuyệt mật và kiểm soát quyền truy cập dựa trên định danh sinh trắc học quốc gia. Đối với cấp độ 1 và 2 thì phải sử dụng hạ tầng dùng riêng, mật mã nội địa và kiểm soát truy cập đa nhân tố đặc biệt. Cấp độ 3 và 4 sẽ sử dụng hạ tầng dùng chung có tính linh hoạt cao, ưu tiên tốc độ kết nối và chia sẻ. Hồ Sơ Chính Sách đề cập rằng "[p]hân thành 4 cấp độ giúp dữ liệu cấp độ 3, 4 được lưu thông cực nhanh, thúc đẩy xã hội số, kinh tế số". Thêm vào đó, Luật An ninh dữ liệu hướng tới việc ưu

tiên sử dụng các giải pháp phần cứng, phần mềm và mật mã nội địa để loại bỏ nguy cơ "cửa sau" từ các nhà cung cấp nước ngoài.

Nếu một lượng lớn dữ liệu do các tổ chức thuộc khu vực tư nhân nắm giữ bị phân loại vào Cấp độ 1 hoặc Cấp độ 2, ví dụ như dữ liệu trong lĩnh vực tài chính hoặc y tế, việc chuyển và sử dụng dữ liệu này có thể gặp điểm nghẽn; làm chậm lại các hoạt động thương mại, giảm khả năng bảo mật và ảnh hưởng đến quá trình đổi mới sáng tạo.

Việt Nam đã ban hành Luật Dữ liệu theo đó phân loại dữ liệu thành ba nhóm: Dữ Liệu Cốt Lõi, Dữ Liệu Quan Trọng và Dữ liệu khác. Luật An ninh dữ liệu cần làm rõ mối tương quan giữa các nhóm dữ liệu theo Luật Dữ liệu và đề xuất phân loại theo hệ thống bốn cấp theo Luật An ninh dữ liệu. Để tránh nguy cơ chồng chéo pháp luật, Việt Nam nên xem xét sửa đổi, bổ sung các luật hiện hành thay vì ban hành một Luật An ninh dữ liệu riêng rẽ. Phương án này sẽ giúp hợp lý hóa các quy định quản trị dữ liệu hiện tại, loại bỏ các nghĩa vụ trùng lặp cho doanh nghiệp, đồng thời hình thành một hành lang pháp lý đồng bộ, nhất quán về phân loại, bảo vệ và chuyển dữ liệu xuyên biên giới.

Khuyến nghị: Để tránh tình trạng phân loại quá mức gây cản trở cho các hoạt động kinh tế, Luật An ninh dữ liệu cần thu hẹp phạm vi và áp dụng phương thức tiếp cận dựa trên mức độ rủi ro. Theo đó, dữ liệu Cấp độ 1 và Cấp độ 2 cần được định nghĩa rõ ràng và chủ yếu giới hạn đối với dữ liệu thuộc quyền sở hữu hoặc kiểm soát của Nhà nước mà có ảnh hưởng trực tiếp đến quốc phòng, an ninh quốc gia, an toàn công cộng, hoặc sự vận hành của các hạ tầng trọng yếu quốc gia. Các nhóm dữ liệu phổ biến ở khu vực tư nhân như dữ liệu tài chính hoặc dữ liệu y tế không đương nhiên bị phân loại là dữ liệu Cấp độ 1 hoặc Cấp độ 2. Dữ liệu cũng không nên bị phân loại là dữ liệu cốt lõi hoặc dữ liệu quan trọng khi chỉ dựa trên quy mô hoặc khối lượng dữ liệu. Việc phân loại một cách bao quát toàn bộ các ngành hoặc bao gồm cả các bộ dữ liệu thông thường thuộc nhóm thương mại, vận hành hay khách hàng là dữ liệu Cấp độ 1 và 2 sẽ tạo ra chính các điểm nghẽn dữ liệu mà Hồ Sơ Chính Sách muốn tránh. Thêm vào đó, chúng tôi kiến nghị thu hẹp phạm vi của dữ liệu Cấp độ 1 và 2, ví dụ như định nghĩa dữ liệu Cấp độ 1 là dữ liệu có liên quan trực tiếp đến các vấn đề quân sự hoặc các vấn đề nhạy cảm về an ninh quốc gia, đồng thời loại bỏ các khái niệm mang nghĩa rộng như "độc lập" và "trật tự an toàn xã hội".

Khuyến nghị: Luật An ninh dữ liệu không nên quy định rõ việc ưu tiên sử dụng phần cứng và phần mềm nội địa vì điều này sẽ làm hạn chế khả năng tiếp cận của các tổ chức tại Việt Nam đối với các giải pháp công nghệ tiên tiến hàng đầu trên thế giới, bao gồm các công nghệ bảo mật hiện đại, đồng thời cản trở khả năng hội nhập liền mạch của các tổ chức Việt Nam vào nền kinh tế số toàn cầu. Thay vào đó, Luật An ninh dữ liệu nên ưu tiên áp dụng các tiêu chuẩn quốc tế được công nhận rộng rãi, bảo đảm mức độ cao về khả năng tương thích, liên thông giữa các hệ thống cũng như an toàn, an ninh dữ liệu.

Đảm Bảo An Ninh trong Chuyển Dữ Liệu Xuyên Biên Giới

Hồ Sơ Chính Sách nhấn mạnh mục tiêu chính sách bao gồm việc thực thi chủ quyền số và bảo đảm an ninh quốc gia, đồng thời làm rõ yêu cầu lưu trữ dữ liệu nhạy cảm tại Việt Nam "đảm bảo rằng cơ quan quản lý luôn có khả năng tiếp cận, kiểm soát và bảo vệ tài nguyên này trước các nguy cơ can thiệp hoặc cấm vận từ bên ngoài". Hồ Sơ Chính Sách cũng nêu mục tiêu thiết lập cơ chế quản trị dòng chảy dữ liệu "mở có kiểm soát" và chuyển đổi từ tư duy "cấm đoán" sang "điều phối dựa trên rủi ro". Hồ Sơ Chính Sách hướng tới việc tạo ra các "luồng xanh" cho dữ liệu thông thường để phát triển kinh tế, đồng thời thiết lập các "luồng đỏ" kiểm soát chặt chẽ dữ liệu cốt lõi và quan trọng, điều này sẽ tạo sự linh hoạt cho nền kinh tế dữ liệu nhưng không đánh đổi an ninh quốc gia. Tuy nhiên, các hạn chế đối với dòng chảy dữ liệu và chuyển dữ liệu có thể vô tình làm giảm hiệu quả của các cơ chế dự phòng hệ thống được tích hợp trong các dịch vụ điện toán đám mây tiên tiến, hệ quả là, dữ liệu quan trọng có thể đối mặt với rủi ro mất mát lớn

hơn trong trường hợp xảy ra các sự cố hoặc tình huống ngoài dự kiến[3] ảnh hưởng đến các hệ thống lưu trữ dữ liệu được yêu cầu đặt tại địa phương.

Chúng tôi đánh giá cao việc Bộ Công an tập trung vào việc thúc đẩy hội nhập và tương thích quốc tế như nội luật hóa các cam kết quốc tế về Dòng Chảy Dữ Liệu Tự Do Có Tin Cậy (**Data Free Flow with Trust – DFFT**) và các hiệp định thương mại tự do thế hệ mới như Hiệp định Đối tác Toàn diện và Tiến bộ xuyên Thái Bình Dương (**Comprehensive and Progressive Agreement for Trans-Pacific Partnership – CPTPP**), Hiệp định Thương mại Tự do Liên minh châu Âu – Việt Nam (**EU-Vietnam Free Trade Agreement – EVFTA**); và Hiệp định Khung về Kinh tế số ASEAN (**ASEAN Digital Economy Framework Agreement – DEFA**).

Mặc dù chúng tôi thừa nhận một số lợi ích của cơ chế "danh sách trắng" (danh sách các quốc gia/tổ chức có hệ thống pháp luật bảo vệ dữ liệu tương đương Việt Nam, doanh nghiệp chuyển dữ liệu sang các đối tượng này chỉ cần thông báo, không cần xin phép với cơ quan nhà nước), chúng tôi vẫn có những quan ngại liên quan đến nghĩa vụ thông báo cho cơ quan nhà nước, quy trình lập danh sách được chấp thuận cũng như cách thức quản lý đối với các chủ thể không nằm trong danh sách này. Chẳng hạn, nếu yêu cầu thông báo cho cơ quan nhà nước vẫn kéo theo nghĩa vụ nộp các bộ hồ sơ phức tạp như các yêu cầu hiện hành theo Luật Bảo vệ dữ liệu cá nhân và Luật Dữ liệu, thì cơ chế danh sách trắng sẽ khó đạt được mục tiêu mong muốn là giảm gánh nặng tuân thủ cho doanh nghiệp. Tương tự, nếu quy trình đưa các quốc gia hoặc tổ chức vào danh sách được chấp thuận mang tính hạn chế quá mức hoặc mất nhiều thời gian, thì cách tiếp cận này trên thực tế có thể tạo ra nhiều rào cản đối với hoạt động chuyển dữ liệu xuyên biên giới hơn mức cần thiết.

Việt Nam cũng đang xem xét chuyển đổi từ "tiền kiểm" sang "hậu kiểm" số bằng cách giới thiệu "Điều Khoản Hợp Đồng Mẫu" cho doanh nghiệp và cơ chế liên thông quốc tế như Hệ Thống Quy Tắc Bảo Mật Xuyên Biên Giới Toàn Cầu (**Global Cross-Border Privacy Rules System – Global CBPR**) mà theo đó dữ liệu Việt Nam có thể lưu chuyển trong các khối liên minh kinh tế mà không cần đàm phán lại từ đầu. Tương tự, nếu doanh nghiệp vẫn bị yêu cầu thực hiện lập và nộp các bộ hồ sơ chi tiết đối với từng lần chuyển dữ liệu, thì các mục tiêu đặt ra sẽ khó có thể đạt được.

GDA ủng hộ mạnh mẽ việc tạo điều kiện thuận lợi cho hoạt động chuyển dữ liệu xuyên biên giới, bao gồm cả dữ liệu cá nhân. Chúng tôi ghi nhận và đánh giá cao việc cả Hồ sơ Dự thảo Báo Cáo Đánh Giá Tác Động Chính Sách và Dự thảo Báo cáo thực trạng bảo vệ dữ liệu cá nhân đều thừa nhận tầm quan trọng của hoạt động chuyển dữ liệu quốc tế, bao gồm trong bối cảnh thực hiện các cam kết của Việt Nam theo CPTPP và EVFTA.

Khuyến nghị: Chúng tôi đặc biệt khuyến nghị Luật An ninh dữ liệu không nên đặt ra bất kỳ yêu cầu mới nào đối với hoạt động chuyển dữ liệu xuyên biên giới. Thay vào đó, Luật An ninh dữ liệu nên được xem là cơ hội để rà soát, hợp lý hóa và thống nhất các nghĩa vụ liên quan đến việc chuyển dữ liệu hiện đang tồn tại và có sự chồng chéo giữa Luật Bảo vệ dữ liệu cá nhân và Luật Dữ liệu. Luật An ninh dữ liệu theo đó cần thiết lập một khuôn khổ pháp lý thống nhất, đồng bộ thay vì bổ sung thêm một tầng nghĩa vụ tuân thủ mới. Hồ Sơ Chính Sách đã xác định tình trạng phân mảnh pháp lý và chồng chéo nghĩa vụ là “một trong những hạn chế lớn nhất” của khuôn khổ quản trị dữ liệu hiện nay. Việc đưa ra thêm những yêu cầu về chuyển giao – ngay cả khi chỉ là những điều chỉnh để hoàn thiện – cũng làm gia tăng rủi ro làm phân mảnh nghĩa vụ mà Luật An ninh dữ liệu đang muốn khắc phục. Doanh nghiệp đã đầu tư nguồn lực để xây dựng hệ thống tuân thủ đối với hoạt động chuyển dữ liệu theo Luật Bảo vệ dữ liệu cá nhân không nên phải đối mặt với một hệ thống nghĩa vụ thứ hai có khả năng chồng chéo hoặc mâu thuẫn đối với cùng một loại hoạt động là chuyển dữ liệu.

[3] Tham khảo thêm ví dụ tại: https://www.straitstimes.com/asia/east-asia/up-in-smoke-work-documents-of-191000-civil-servants-lost-in-data-centre-fire-in-south-korea

Luật An ninh dữ liệu cần làm rõ rằng việc dữ liệu chỉ được định tuyến về mặt kỹ thuật hoặc được xử lý tạm thời thông qua hạ tầng đặt ngoài lãnh thổ Việt Nam, tự thân nó không được xem là hoạt động chuyển dữ liệu xuyên biên giới thuộc phạm vi điều chỉnh của pháp luật. Luật An ninh dữ liệu cũng cần quy định rằng không bắt buộc phải thực hiện hoạt động xử lý dữ liệu gốc trên lãnh thổ Việt Nam nếu việc truy cập từ xa đối với dữ liệu nhạy cảm vẫn có thể đáp ứng các mục tiêu chính sách của Việt Nam về bảo đảm chủ quyền số và an ninh quốc gia. Ngoài ra, trong trường hợp việc đánh giá tác động đối với hoạt động xử lý và chuyển dữ liệu xuyên biên giới được yêu cầu áp dụng trong những hoàn cảnh cụ thể, các báo cáo đánh giá này chỉ nên phải nộp cho Bộ Công an khi có yêu cầu thay vì bắt buộc phải nộp trong mọi trường hợp. Cách tiếp cận này phù hợp với thông lệ quốc tế và sẽ giúp cả doanh nghiệp lẫn cơ quan quản lý tập trung nguồn lực hiệu quả hơn vào các trường hợp thực sự cần được xem xét và quản lý.

Đây là thời điểm vàng để Việt Nam công nhận và áp dụng các cơ chế chuyển dữ liệu cá nhân được quốc tế công nhận mà không áp đặt thêm các yêu cầu tuân thủ bổ sung, chẳng hạn như nghĩa vụ thực hiện Đánh Giá Tác Động Chuyển Dữ Liệu Cá Nhân theo Luật Bảo vệ dữ liệu cá nhân. Những cơ chế này bao gồm Điều Khoản Hợp Đồng Chuẩn của Liên minh Châu Âu (**EU Standard Contractual Clauses – EU SCCs**), Điều Khoản Hợp Đồng Mẫu của Hiệp hội các quốc gia Đông Nam Á (**ASEAN Model Contractual Clauses – ASEAN MCCs**), và Global CBPR. Việc công nhận các cơ chế này sẽ góp phần giảm gánh nặng quản lý và tuân thủ cho cả doanh nghiệp và cơ quan quản lý nhà nước, tạo thuận lợi cho dòng chảy dữ liệu xuyên biên giới đáng tin cậy, đồng thời thúc đẩy các mục tiêu của Việt Nam về hội nhập quốc tế và phát triển kinh tế số.

Trong trường hợp Việt Nam không lựa chọn cách tiếp cận này, thì cũng cần loại bỏ các yêu cầu báo cáo trùng lặp và tránh bổ sung thêm các nghĩa vụ báo cáo mới đối với hoạt động chuyển dữ liệu xuyên biên giới. Điều này dẫn đến sự chồng chéo không cần thiết và làm gia tăng gánh nặng tuân thủ mà không mang lại lợi ích tương ứng về an ninh, an toàn dữ liệu. Luật An ninh dữ liệu cần bổ sung một quy định rõ ràng về nguyên tắc không trùng lặp, theo đó, trong trường hợp một hoạt động chuyển dữ liệu đã thuộc phạm vi điều chỉnh của các yêu cầu theo Luật Bảo vệ dữ liệu cá nhân, Luật Dữ liệu hoặc bất kỳ văn bản pháp luật nào khác, thì chỉ cần thực hiện một lần báo cáo đối với hoạt động chuyển dữ liệu này.

Kết luận

GDA trân trọng cảm ơn cơ hội được đóng góp các ý kiến này. Hồ Sơ Chính Sách của Luật An ninh dữ liệu đã thể hiện một số nguyên tắc tích cực, bao gồm cách tiếp cận phân loại dữ liệu dựa trên mức độ rủi ro, cam kết tạo thuận lợi cho dòng chảy dữ liệu thương mại thông thường và ghi nhận các cam kết thương mại quốc tế của Việt Nam. GDA khuyến nghị Việt Nam triển khai đầy đủ và nhất quán các nguyên tắc này trong dự thảo luật cũng như các văn bản hướng dẫn thi hành chi tiết.

Nếu Quý cơ quan có bất kỳ câu hỏi nào liên quan đến bản góp ý này, xin vui lòng liên hệ với chúng tôi.

Xin trân trọng cảm ơn Quý cơ quan đã tạo điều kiện để chúng tôi tham gia góp ý.

Trân trọng,

Joseph P. Whitlock
Giám đốc Điều hành
Liên minh Dữ liệu Toàn cầu
josephw@bsa.org