Business Software Alliance

Réponse au groupe de travail sur la souveraineté numérique

Consultation des parties prenantes sur la souveraineté numérique

Juin 2026

À propos de la BSA

La Business Software Alliance (www.bsa.org) est l'association professionnelle mondiale du secteur des logiciels d'entreprise, représentant des entreprises leaders en matière d'intelligence artificielle, de cybersécurité, d'informatique en nuage et d'autres technologies de pointe. Nous opérons dans plus de 20 marchés aux États-Unis, en Europe et en Asie, en plaidant pour des politiques qui renforcent la confiance dans la technologie afin que chaque secteur industriel et le grand public puissent bénéficier de l'innovation.

Les membres[1] de la BSA sont des entreprises mondiales dont le siège social est établi aux États-Unis, au Canada, en Europe, en Asie-Pacifique et au-delà, opérant à l'avant-garde de la transformation numérique de l'Europe.

Position générale de la BSA

La BSA salue les travaux du groupe de travail franco-allemand sur la souveraineté numérique et soutient l'ambition de l'UE de renforcer sa résilience, sa compétitivité et ses capacités technologiques. Les préoccupations qui sous-tendent cette consultation sont légitimes : des dépendances à l'égard d'un petit nombre de fournisseurs, indépendamment de leur nationalité ou de leur lieu d'établissement, créent des risques

[1] *Les membres de la BSA comprennent : Adobe, Akamai, Alteryx, Amadeus, Asana, Atlassian, Autodesk, Avalara, Bentley Systems, Box, Cisco, Cloudflare, Cohere, Cohesity, Dassault Systèmes, Databricks, DocuSign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Trend Micro, TriNet, Veeam, Workday, Zendesk et Zoom Communications Inc.*

réels — non seulement pour les administrations publiques, mais pour l'ensemble de l'économie, étant donné qu'une grande partie de la législation en discussion s'appliquera bien plus largement.

La manière dont l'Europe répond à ces préoccupations, et les critères concrets qu'elle retient pour définir la souveraineté, revêtent une importance capitale. La BSA estime que la souveraineté numérique s'obtient avant tout par l'ouverture, la confiance et des normes solides — et non par l'isolement, l'exclusion géographique ou des exigences fondées sur l'origine. Comme le souligne le document de la BSA de novembre 2025 intitulé "Keeping the Door Open: The EU's Path to Digital Sovereignty", ce qui importe pour la souveraineté de l'Europe, c'est la capacité à gouverner, à auditer et à atténuer les risques, et non l'origine géographique. La position de la BSA est alignée sur les conclusions récentes du Conseil européen des transports, des télécommunications et de l'énergie du 5 décembre 2025, dont la section V est intitulée « Renforcer la souveraineté numérique de manière ouverte », soulignant la nécessité d'une « coopération étroite avec (...) des partenaires internationaux (...) pour garantir des chaînes d'approvisionnement numériques diversifiées, sécurisées, résilientes et fiables ». Enfin, les positions de la BSA sont alignées sur la Déclaration pour la souveraineté numérique européenne issue du sommet franco-allemand du 18 novembre 2025, qui stipule que « la souveraineté numérique ne signifie pas l'isolement ou le protectionnisme ; elle signifie garantir que l'Europe peut agir de manière indépendante et autodéterminée sur la base du droit international, de ses propres lois, valeurs et intérêts en matière de sécurité, tout en aspirant à la coopération internationale avec ses partenaires qui partagent les valeurs et principes européens ».

La BSA invite donc le groupe de travail à adopter un modèle fondé sur la confiance et sur les risques, qui récompense la sécurité, l'interopérabilité et la responsabilité, tout en reconnaissant les garanties techniques, contractuelles et organisationnelles comme des moyens valables de gérer les dépendances.

Section 1 : Dimensions de la souveraineté numérique

1. Capacité d'exécution (Q1–Q2)

Évaluation de la BSA : Partiellement appropriée

La BSA soutient le principe selon lequel les organismes publics et les organisations doivent pouvoir superviser leurs dépendances numériques. Toutefois, les approches en matière d'exécution doivent être fondées sur les risques et la proportionnalité, et non sur une exclusion juridictionnelle générale.

- Les exigences de transparence juridictionnelle sont une mesure raisonnable et réalisable, à condition qu'elles soient proportionnées et n'imposent pas une charge administrative excessive aux fournisseurs ou aux acheteurs.
- Les interdictions générales d'accès aux données sensibles pour les pays tiers risquent de confondre souveraineté et isolement. L'UE devrait plutôt s'appuyer sur des garanties contractuelles, techniques et juridiques solides — telles que le chiffrement et les contrôles d'accès — plutôt que sur l'exclusion géographique.
- Les membres de la BSA respectent le RGPD, NIS2, le Data Act et d'autres cadres réglementaires qui prévoient des mécanismes d'exécution robustes. Nous estimons que les outils existants devraient être mobilisés avant d'imposer de nouvelles exigences, au risque d'aboutir à des doublons.
- Les cadres de régulation relatifs à la souveraineté numérique devraient définir avec précision le périmètre du terme « données ».
    - Dans les services SaaS modernes, le contenu des clients, les données d'identité, les métadonnées, les journaux d'entrées, la télémétrie, les données d'assistance, les sauvegardes et les données de traitement liées à l'IA servent tous des finalités différentes et présentent des profils de risque différents.
    - Toute exigence en matière de localisation des données devrait précisément identifier les catégories de données, les activités de traitement, les restrictions d'accès, les délais de conservation et les limitations applicables aux sous-traitants concernés.

2. Capacité à concevoir, déployer et utiliser les technologies (Q3–Q4)

Évaluation de la BSA : Partiellement appropriée, avec des réserves importantes

La BSA soutient fermement les investissements dans les capacités numériques européennes, notamment dans l'IA, l'informatique en nuage, la cybersécurité et l'informatique quantique. Toutefois, la "maîtrise" des technologies ne devrait pas être comprise comme l'obligation, pour l'Europe, de développer ou de déployer uniquement des solutions européennes.

- Les entreprises mondiales de logiciels sont des partenaires essentiels de la transformation numérique de l'Europe. Les membres de la BSA investissent massivement dans les centres de données européens, emploient des milliers de professionnels du numérique dans les États membres et dispensent des programmes de formation en cybersécurité, en informatique en nuage et en IA. Les solutions numériques que ces entreprises proposent soutiennent la compétitivité des entreprises européennes et la réalisation des objectifs

européens en matière d'environnement, d'infrastructures, d'eau et d'industries manufacturières, entre autres.

- Exiger des organisations qu'elles adoptent exclusivement des technologies européennes est irréalisable, coûteux et risquerait de nuire à la sécurité et à l'innovation. Par ailleurs, si l'open source est un outil précieux, il ne devrait pas être imposé comme solution par défaut.
- Les politiques publiques devraient se concentrer sur le développement des capacités, de l'échelle et du choix, et non sur la restriction de l'origine des technologies déployées.

3. Capacité et aptitude à la création de valeur économique (Q5–Q6)

Évaluation de la BSA : Partiellement appropriée — préoccupations importantes quant à la mise en œuvre

La BSA partage l'ambition de l'UE de développer une économie numérique européenne compétitive. Comme le souligne le rapport Draghi, accélérer l'adoption de l'IA et de l'informatique en nuage dans l'industrie européenne est essentiel à la compétitivité. Toutefois, la BSA nourrit des préoccupations importantes concernant l'approche proposée.

- Lier les évaluations de souveraineté à l'ancrage territorial de la création de valeur — notamment la part de l'emploi dans l'UE et la localisation de la R&D — risque de fonctionner comme une obligation d'achat européen déguisée. Cela nuirait à la concurrence, augmenterait les coûts pour les administrations publiques et réduirait, de fait, les choix disponibles.
- Les membres de la BSA réalisent des investissements considérables en Europe. Beaucoup de nos membres exploitent d'importants centres de données européens, disposent d'effectifs importants basés dans l'UE et contribuent aux écosystèmes industriels et économiques locaux. Ces investissements sont réalisés parce que l'Europe est un marché attractif, et non en raison d'une obligation. Cette attractivité doit être préservée.
- Les cadres des marchés publics devraient être conçus en fonction des résultats — sécurité, performance, interopérabilité, rapport qualité-prix — et non de l'origine géographique des prestataires de services ou de la localisation du siège social des entreprises.
- Documenter et rendre compte de la part de la valeur ajoutée générée dans l'UE par produit ou service technologique mondial est complexe, voire impossible, sur le plan opérationnel. Isoler et attribuer la création de valeur au niveau territorial générerait des charges de conformité disproportionnées, en particulier

pour les entreprises qui contribuent déjà massivement à l'économie numérique européenne.

4. Protection des données (Q7)

Évaluation de la BSA : Partiellement appropriée, à condition que la mise en œuvre soit fondée sur les risques et technologiquement neutre

La BSA soutient fermement des normes élevées de protection des données pour les données sensibles. L'UE dispose déjà du cadre de protection des données le plus complet au monde, et les membres de la BSA respectent le RGPD, NIS2 et les obligations connexes.

- Les mesures techniques et organisationnelles — chiffrement, pseudonymisation, contrôles d'accès, garanties contractuelles et options de localisation des données — sont des outils efficaces et proportionnés pour gérer les risques extraterritoriaux.
- Le recours obligatoire à des technologies spécifiques de protection de la vie privée doit être envisagé avec prudence : imposer des solutions techniques particulières peut créer un effet de verrouillage, réduire la flexibilité et devenir rapidement obsolète à mesure que la technologie évolue.
- La confiance se construit par la responsabilité et la transparence, et non par la nationalité. La protection contre l'accès extraterritorial peut être efficacement assurée par des garanties contractuelles, juridiques et techniques solides, appliquées de manière proportionnée en fonction de la sensibilité des données. Il serait préférable de permettre aux entreprises européennes d'adopter des contrôles renforcés lorsque les risques le justifient, plutôt que d'imposer à l'ensemble des entreprises, y compris les fournisseurs SaaS, le modèle le plus coûteux et lourd par défaut.

5. Substituabilité et interopérabilité des systèmes (Q9–Q10)

Évaluation de la BSA : Particulièrement appropriée — il s'agit du levier le plus efficace pour la souveraineté

La BSA considère l'interopérabilité et les normes ouvertes comme la pierre angulaire de la véritable souveraineté numérique. Les exigences dans ce domaine s'attaquent directement aux risques de verrouillage et permettent aux utilisateurs d'exercer un choix libre.

- L'UE devrait promouvoir des normes techniques ouvertes, reconnues au niveau international — telles qu'ISO 27001 — plutôt que de développer des cadres

européens parallèles ou exclusifs. Ces normes renforcent la souveraineté tout en maintenant la connectivité mondiale.

- Les architectures de systèmes modulaires et les nomenclatures logicielles documentées sont des mesures pratiques et efficaces que les membres de la BSA peuvent aider à mettre en œuvre et soutenir.
- Les solutions open source ont un rôle important à jouer, mais ne devraient pas être imposées. L'essentiel est que les systèmes soient conçus pour éviter les dépendances unilatérales et le verrouillage par les fournisseurs (par exemple dans des environnements multicloud) — cela peut être réalisé par des normes ouvertes, des droits de changement de fournisseur contractuels, ainsi que des exigences d'interopérabilité et de portabilité techniques.
- La coopération en matière de normalisation avec des partenaires mondiaux — via l'ISO, l'IEC et d'autres organismes internationaux — devrait être une priorité afin de prévenir la fragmentation et de garantir que les normes européennes aient un poids mondial.

6. Résilience des infrastructures (Q11–Q12)

Évaluation de la BSA : Appropriée, à condition que les « partenaires internationaux de confiance » soient définis de manière large et sur la base de critères de risque.

La BSA soutient le développement d'infrastructures informatiques critiques résilientes et fiables. Néanmoins, c'est par la diversité et la redondance, et non par des restrictions géographiques, que l'on parvient le mieux à garantir la résilience.

- Les approches multicloud et hybrides, qui associent des fournisseurs européens et internationaux dans un cadre de gouvernance clair, offrent une protection et une résilience plus robustes que le principe d'exclusivité géographique. Une infrastructure cloud européenne unique présenterait un risque de concentration dangereux.
- Les critères définissant les « partenaires internationaux de confiance » devraient reposer sur des normes de sécurité vérifiables, des garanties juridiques, des engagements contractuels et des mesures techniques — et non sur le pays d'origine du fournisseur.
- Les membres de la BSA qui construisent et exploitent des centres de données européens et des points de présence distribués contribuent déjà directement à la résilience des infrastructures européennes. Cet investissement est plus efficace lorsqu'il s'effectue dans un marché compétitif et ouvert.

Critères supplémentaires et remarques (Q13)

La BSA souhaite mettre en avant les considérations supplémentaires suivantes :

- Cohérence réglementaire et simplicité : L'agenda de souveraineté numérique doit s'inscrire dans la continuité de l'agenda de simplification de l'UE — les deux vont actuellement dans des directions opposées. Le cadre réglementaire existant — RGPD, NIS2, l'AI Act, le Cyber Resilience Act — offre déjà une base solide pour protéger la vie privée et la sécurité. Les nouvelles exigences de souveraineté devraient s'appuyer sur ces bases plutôt que de les dupliquer ou d'entrer en conflit avec elles. Les cadres de souveraineté trop complexes, coûteux ou incohérents avec les règles existantes réduisent les choix, augmentent les coûts de conformité et détournent les investissements de la croissance et de l'innovation. Le prochain paquet de souveraineté technologique devrait donc être conçu autour des principes fondamentaux de simplicité et de proportionnalité.
- Compétences numériques : La souveraineté à long terme de l'Europe dépend autant des personnes que de la technologie. L'investissement dans les compétences numériques — notamment en cybersécurité, en informatique en nuage et en IA — doit être un pilier central de tout cadre de souveraineté.
- Alignement international : Sans une certaine convergence au niveau international, le risque est de se retrouver face à une mosaïque d'exigences sur mesure qui augmente les coûts et, en fin de compte, ne profite à personne. Le groupe de travail devrait examiner la manière dont ses propositions interagissent avec les engagements commerciaux internationaux et les cadres normatifs mondiaux.

Section 2 : Focus sur les indicateurs de création de valeur économique

La BSA émet d'importantes réserves concernant cette partie de la consultation. Bien que présentés comme axés sur la « création de valeur économique » plutôt que sur l'origine du capital ou la propriété, les indicateurs envisagés fonctionneraient en pratique comme d'indicateurs indirects de l'origine des entreprises, ce qui désavantagerait de fait les prestataires non européens, indépendamment de la qualité, de la sécurité ou de la compétitivité de leurs services.

Q1–2 : Pertinence des indicateurs

La BSA reconnaît l'intérêt d'évaluer les contributions aux écosystèmes locaux, au développement technologique et à l'emploi qualifié en tant qu'indicateurs de valeur économique. Toutefois, ceux-ci devraient être utilisés comme indicateurs positifs de contribution, et non comme seuils d'exclusion.

Parmi les indicateurs supplémentaires que la BSA considérerait comme pertinents, on peut citer :

- La conformité aux cadres réglementaires de l'UE, le statut de certification de sécurité et la capacité avérée à fournir des services sécurisés, fiables et évolutifs conformément aux règles et valeurs de l'UE, y compris les engagements contractuels en matière d'accès aux données, de portabilité et de droits de changement de fournisseur ;
- L'investissement dans l'innovation, la cybersécurité, les capacités en matière d'IA et les infrastructures résilientes, notamment par le biais de partenariats avec des universités, des centres de recherche et des entreprises technologiques de l'UE, et par des programmes de développement des compétences, des apprentissages et des partenariats éducatifs qui renforcent les capacités numériques de l'UE à grande échelle ;
- L'effet multiplicateur de l'écosystème : l'activité économique générée au sein de l'UE par l'écosystème de partenaires et de revendeurs du fournisseur, qui dans de nombreux cas dépasse significativement l'empreinte directe en termes d'emploi du fournisseur ;
- La participation aux écosystèmes mondiaux de recherche, d'open source et d'innovation ;
- La résilience et la diversification de la chaîne d'approvisionnement.
- Le cadre d'évaluation devrait rester neutre sur le plan technologique et éviter les approches susceptibles de fragmenter les marchés, de réduire l'interopérabilité ou de limiter l'accès à des technologies et expertises compétitives à l'échelle mondiale.

Q3–4 : Localisation du siège social et hébergement des données

La BSA ne considère pas que la localisation du siège social d'une entreprise soit un indicateur pertinent ou approprié en matière de souveraineté. L'écosystème technologique est fondamentalement mondial et interconnecté, de nombreuses solutions technologiques étant conçues, développées, produites et livrées à travers des chaînes de valeur complexes impliquant de multiples pays et régions. L'essentiel est la conformité au droit de l'UE, les normes de sécurité technique et la capacité concrète

des clients à exercer un contrôle sur leurs données — aucun de ces éléments n'étant déterminé par le lieu d'incorporation d'une entreprise.

La localisation de l'hébergement des données peut être un facteur pertinent pour des cas d'utilisation spécifiques à haute sensibilité, mais ne devrait pas être appliquée comme une exigence générale. La localisation obligatoire des données dans l'UE pour tous les services fragmenterait le marché unique numérique, nuirait à la cybersécurité (en éliminant la redondance géographique) et affaiblirait la portée mondiale des entreprises européennes. De plus, les exigences imposant la localisation des données uniquement pour des raisons de proximité physique peuvent nuire à la cybersécurité et à la résilience opérationnelle. Elles pourraient entraver le partage transfrontalier de renseignements sur les menaces, augmenter les coûts de maintenance de solutions de sécurité de pointe et affaiblir la résilience et les capacités de basculement en limitant les possibilités de stockage alternatif ou de récupération rapide en cas de pannes, d'incidents cybernétiques ou de pertes de données.

Q5–11 : Seuils pour la main-d'œuvre, la R&D et la sous-traitance

La BSA recommande la plus grande prudence dans la conception de ces indicateurs. Fixer des seuils minimaux pour l'emploi dans l'UE, le personnel de R&D ou les dépenses de sous-traitance comme conditions d'éligibilité aux marchés publics constituerait une restriction, de fait, fondée sur l'origine, quelle que soit la manière dont elle est formulée.

De tels seuils risquent d'être incompatibles avec les engagements commerciaux internationaux de l'UE, notamment dans le cadre de l'Accord sur les marchés publics de l'OMC.

Ils réduiraient la concurrence, augmenteraient les coûts pour les administrations publiques et pourraient réduire la sécurité plutôt que la renforcer, en limitant l'accès aux solutions les plus performantes au niveau mondial.

Si des indicateurs de cette nature devaient être utilisés, ils ne devraient l'être qu'en tant que critères positifs dans la notation des marchés — jamais en tant que seuils d'éligibilité — et uniquement lorsqu'ils sont véritablement pertinents au regard du profil de sensibilité et de risque du marché spécifique. Ils devraient également éviter de créer des charges administratives inutiles pour les entreprises en Europe, notamment en s'abstenant d'introduire des critères trop détaillés concernant le produit ou la solution.

Plus précisément, pour chacune des questions :

(Q5) La présence sur le territoire européen de fonctions support critiques telles que la maintenance, les opérations ou le support de niveau 3 peut constituer un indicateur pertinent pour certains cas d'utilisation hautement sensibles ou critiques, où les utilisateurs requièrent de fortes garanties concernant la continuité du service, le

contrôle opérationnel et la réactivité. Dans ces contextes, les utilisateurs peuvent s'attendre non seulement à des technologies sécurisées et fiables, mais aussi à la transparence, à des garanties de gouvernance et à des garanties d'exécution concernant la continuité du service. Toutefois, la localisation des fonctions de support seule ne devrait pas être traitée comme un critère autonome pour mesurer la valeur ajoutée technologique ou la souveraineté numérique. Le plus important est de savoir si les fournisseurs peuvent garantir des services résilients, sécurisés et fiables grâce à des garanties techniques, contractuelles et opérationnelles objectives.

(Q6) Aucun seuil minimum spécifique ne devrait être imposé. La localisation des employés seule n'est pas une mesure suffisante de création de valeur technologique en Europe, en particulier dans un écosystème technologique mondialement interconnecté.

(Q7) Aucun seuil minimum spécifique ne devrait être imposé. La R&D et l'innovation reposent de plus en plus sur la collaboration mondiale et l'accès à l'expertise internationale. L'essentiel réside dans la qualité de l'innovation et la contribution aux capacités technologiques de l'Europe.

(Q8) Aucun seuil minimum spécifique ne devrait être imposé. Les technologies de base sont de plus en plus développées à travers des écosystèmes mondiaux et collaboratifs, notamment en IA, en informatique en nuage, en cybersécurité et dans les logiciels open source. Des exigences de localisation risquent de décourager l'investissement et de limiter l'accès à une expertise et une innovation de confiance. La souveraineté technologique devrait plutôt viser à renforcer la résilience, les capacités et la compétitivité de l'Europe sans créer de charges de conformité inutiles, ni d'obstacles à la croissance.

(Q9) La localisation des équipes d'ingénierie dans l'UE ne devrait pas, en elle-même, être considérée comme un indicateur déterminant de création de valeur technologique ou de souveraineté numérique. L'économie numérique est mondiale, et les entreprises ont besoin d'accéder à des talents et à une expertise internationale pour innover et être compétitives. Des exigences générales de localisation risquent de limiter l'accès aux compétences critiques et ainsi de réduire la compétitivité. Lorsque les critères de souveraineté sont justifiés, ils ne devraient s'appliquer qu'aux cas d'usage les plus sensibles ou stratégiques. Le plus important est la manière dont les logiciels et les services numériques sont développés, sécurisés, gouvernés et maintenus, ainsi que la poursuite des investissements dans l'écosystème de compétences et d'innovation de l'Europe.

(Q10) Aucun pourcentage minimum spécifique ne devrait déterminer si un service numérique contribue de manière significative à la création de valeur ajoutée technologique en Europe. Un seuil quantitatif fondé sur la localisation ou la structure

de propriété des sous-traitants de premier rang ne refléterait pas fidèlement les réalités de l'écosystème technologique mondial et interconnecté, et ne conduirait pas non plus à de meilleurs résultats en matière de cybersécurité, de résilience ou d'innovation. L'évaluation devrait plutôt porter sur la capacité des fournisseurs à faire preuve d'une gouvernance, d'une surveillance et d'une gestion des risques tout au long de leurs chaînes d'approvisionnement, indépendamment du lieu où les activités de sous-traitance spécifiques sont réalisées.

(Q11) La BSA ne considère pas que l'obligation d'adopter des licences open source soit un indicateur pertinent de souveraineté. L'open source peut contribuer à la transparence et à la vérifiabilité, mais la sécurité et la fiabilité reposent sur des processus rigoureux, la certification et la responsabilité — et non sur des modèles de licence. Les logiciels open source reflètent également la nature mondiale et collaborative de l'économie numérique. Des contributeurs du monde entier développent, testent, maintiennent et améliorent en permanence des technologies largement utilisées, apportant une expertise plus étendue, un examen par les pairs plus solide et une identification et une correction plus rapides des vulnérabilités. Ce qui importe n'est donc pas l'emplacement des contributeurs, mais la manière dont les logiciels sont développés, sécurisés, gouvernés et maintenus.

Conclusion

La BSA est prête à collaborer de manière constructive avec le groupe de travail sur la souveraineté numérique pour développer un cadre de souveraineté ambitieux, cohérent et praticable. La BSA soutient pleinement la Déclaration pour la souveraineté numérique européenne issue du sommet franco-allemand du 18 novembre 2025, qui stipule que « la souveraineté numérique ne signifie pas l'isolement ou le protectionnisme ; elle signifie garantir que l'Europe peut agir de manière indépendante et autodéterminée sur la base du droit international, de ses propres lois, valeurs et intérêts en matière de sécurité, tout en aspirant à la coopération internationale avec ses partenaires qui partagent les valeurs et principes européens ».

À cet égard, nous estimons que la souveraineté numérique de l'Europe devrait être assurée par :

- Des normes et exigences d'interopérabilité solides, reconnues au niveau international ;
- Une réglementation fondée sur les risques et neutre sur le plan technologique qui récompense la sécurité et la responsabilité avérées ;
- Des cadres de marchés publics conçus autour des performances, et non de l'origine géographique ;

- Un partenariat entre les institutions européennes et les entreprises technologiques mondiales qui investissent déjà activement dans l'avenir numérique de l'Europe ;
- La coopération internationale pour prévenir la fragmentation et garantir que les normes européennes exercent une influence mondiale.

La plus grande force de l'Europe a toujours résidé dans sa capacité à établir des normes élevées que les autres choisissent de suivre. Le groupe de travail a l'opportunité de construire un cadre de souveraineté que le monde regardera comme un modèle — ouvert, fiable et véritablement résilient.

* * *

Pour plus d'informations, contactez
Thomas Boué : thomas@bsa.org