December 6, 2021

National Institute of Standards and Technology
US Department of Commerce
100 Bureau Drive
Gaithersburg, MD 20899
Attn: David F. Alderman, Standards Services Division

BSA | The Software Alliance makes the following submission in response to the public solicitation of comments[1] by the National Institute of Standards and Technology (NIST) regarding the policies and influence of China in the development of international standards for emerging technologies.

A. Ensuring Non-Discrimination and Procedural Fairness in International Standards Development Processes

In emerging technologies, China and other governments are increasingly applying standards-based or technical regulatory governance approaches to advance policies relating to cybersecurity, artificial intelligence (AI), or industrial policy. These approaches often transpose tools traditionally used to regulate goods – such as standards development practices, mandatory certification, conformity assessment, labeling, or other technical requirements ("technical requirements or standards") – to emerging technologies. These technologies include payments-, cloud-, AI-, and over-the-top (OTT)-related services, as well as digital technologies embedded in industrial, vehicular, consumer, and other IoT devices.

Standards development processes are well-suited to emerging technologies when they are international, voluntary, industry-driven, and do not discriminate against non-national persons, technologies, or services. These processes shall comport with requirements in the World Trade Organization (WTO) Agreement on Technical Barriers to Trade (TBT) that require technical regulations to be based on international standards[2] and that encourage interoperability among different countries' technical regulations. These and other TBT provisions facilitate regulatory compatibility and reduce barriers to trade, especially when requirements are based on open, consensus-based standards development processes.

Additionally, international, voluntary, industry-driven standards have for many years informed policymakers' development of interoperable technical regulatory requirements and guidelines that can offer industry a clear avenue to demonstrate regulatory compliance. Such standards not only generate efficiencies of scale and can speed the development and distribution of new innovations, but they can also provide the basis for beneficial technical regulations that are neither discriminatory nor unnecessarily restrictive.

B. Distortions to International Standards Development Processes and/or Deviations from on International Standards

When governments mandate compliance with country- or region-unique technical requirements or standards, they create the risk of discrimination, non-tariff barriers to trade, and unnecessary regulatory divergence and incompatibility.[3] There is growing concern that these types of outcomes are becoming

increasingly prevalent, including in the context of China's standards-related activities in national and international fora.

Regulatory reliance on either market-specific standards or a limited subset of international standards is suboptimal as it often leads to regulatory divergence and market fragmentation, often manifested in new non-tariff barriers to trade, product safety or reliability issues, or other challenges. The ICT goods space is instructive in this regard: over 80 countries have technical regulations for safety, electromagnetic interference, and telecommunications; some base requirements unfortunately still on national standards that deviate from international standards.[4]

In view of the sheer magnitude of Chinese standard-setting activities relating to cybersecurity, encryption, industrial IoT, enterprise software, and other emerging technologies, there is concern that a similar outcome could befall these emerging technologies. Moreover, to the extent forthcoming certification and/or conformity assessment requirements for emerging technologies are not grounded in international standards, there is a risk of technical disruption (i.e., impact on product safety, impact on the ability of firms to deliver secure goods and services), which fall most heavily on SMEs. Finally, country- or region-unique technical requirements or standards development often lacks the transparency and due process associated with open, international standards development processes.

C. Specific Areas of Concern

Such technical requirements are more likely to result in regulatory divergence and incompatibility – with attendant security, trade, and economic implications – whether in the same country or across international borders. Broadly speaking, examples of problematic measures and processes include:

- Multi-stakeholder groups that are tasked with establishing technical requirements or standards for particular technologies in the absence of due process safeguards typically built into international standards development;
- Measures requiring the adoption of unique certification requirements or encryption standards that do not align with IEC, ISO, ITU and well-established international standards; and
- Frameworks to regulate or establish procurement criteria for emerging technologies, such as AI, Blockchain, or cloud computing, that would mandate preferences for or reliance on one country or region's domestic technical requirements, standards, local testing bodies, or technology, services and/or suppliers.

A non-exhaustive list of specific examples follows.

1. Cybersecurity Classified Protection Scheme

In May 2020, China posted the final version of the Cybersecurity Classified Protection Scheme (CCPS),[5] a de facto cybersecurity protection baseline for network operators and a universal compliance framework for the CSL. The CCPS is a continuation of the Multi-level Protection Scheme (MLPS).[6] Like the MLPS, the CCPS ranks the importance of network and information systems, based on – among other things – their importance to China's national security, social order, public interests — constituting a significant point of concern for the industry at large. The Government of China continues to release supporting standards and guidance on implementing the CCPS. For example, the September 22, 2020 "*Guiding Opinions on Implementing CCPS and CII Protection Scheme*"[7] which includes new concepts such as supply chain security and applies the CCPS to critical infrastructure protection. The CCPS came into effect on November 1, 2020.

2. Encryption

The China National Information Security Standards Technical Committee (TC-260) continues to release a myriad of draft cybersecurity standards involving encryption for public comment. A consistent and worrying trend exhibited by these standards is the extent to which they create a basis for favoring locally

developed products over those developed outside of China. Such changes to algorithms or encryption mechanisms create technical barriers to trade and undermine interoperability.

In late 2019, the Government of China enacted the Cryptography Law.[8] There are several concerns with the law: First, while the updated Law states that commercial cryptography would not be subject to import licensing or export controls, the subsequent draft implementation regulations released suggest otherwise. Certification requirements for commercial cryptography are also being introduced. This overall regulatory framework could potentially restrict foreign participation in commercial cryptographic products. In implementation, it will also be important to avoid unwarranted source code disclosure requirements and to ensure that safeguards protect any trade secrets or other proprietary information.

D. Specific Recommendations

A concerted US government strategy, coordinated with like-minded countries, can help: (1) improve processes and outputs in standards development organizations; (2) address concerns about the influence of dominant non-market economies in those organizations; and (3) limit the risk of global regulatory fragmentation (i.e., divergent requirements between jurisdictions) that may result from distortions in standards development processes. BSA recommends that the US government:

1. In coordination with interested private sector participants, develop and execute upon a strategy (drawing upon elements outlined in the Appendix to this submission) designed to increase the beneficial influence of US or US industry participation in standards development organizations. Several of the tasks below are more appropriately performed by private sector participants, but the United States could nevertheless engage with stakeholders on these issues.

    a. Direct strategies include: (1) participating in voting processes; (2) consistently attending and contributing to standards committee meetings; (3) submitting written contributions/comments that are accepted as proposed or in principle; (4) identifying relevant standards essential patents; (5) proposing standards projects that are approved and ultimately published; and (6) contributing early in the project's development cycle, where such participation shapes the proposal's scope or general direction of the project.
    b. Indirect strategies include: (1) asking other members to support the same voting or substantive position through their written comments; (2) asking the leading experts/voices in a standards committee to support key position in meetings; (3) serving as a leading expert/'trusted voice' in a standards committee to influence meeting participants; and (4) serving as a chair of a committee or as a lead editor

2. Allocate necessary and additional funding to ensure that US government representatives from the Departments of State and Commerce (including NIST) and the Office of the US Trade Representative (among others) are able to travel and participate more fully in standards-development organizations that are open to governmental involvement, and to communicate with US private sector participants in relation to key standards-development processes.

3. Develop a proactive workplan (including cleared talking points, model written interventions, etc.) to ensure that standards-development organizations eschew discriminatory, unnecessary, and/or non-transparent requirements or standards relating to emerging technologies, especially where such requirements or standards would distort conditions of competition based on the origin/nationality of the technologies, products, services, or entities involved;

4. Develop a proactive workplan to ensure that emerging technologies benefit from greater regulatory interoperability and compatibility, based on a broad international commitment to the open, voluntary, and industry-driven development of technical requirements or standards;

5. Consider developing with like-minded countries joint statements, principles, memoranda of understanding, compilations of best practices, international regulatory roadmaps, or other outcomes referencing IEC, ISO, ITU standards. Such outcomes could be formulated in for a including TTC, APEC, the OECD, the G7 or other international organizations.

6. In the context of President Biden's recently announced Indo-Pacific Economic Framework and Trade & Technology Council (TTC), ensure that all negotiating partners agree to a legal clarification that explicitly extends application of all existing WTO TBT-related disciplines to emerging technologies broadly.

Thank you for the opportunity to present these views. Please feel free to direct any views to Joseph Whitlock, Director, Policy at BSA | The Software Alliance. (josephw@bsa.org)

Appendix

While membership and processes vary across standards organizations, there are ways that a stakeholder can typically influence the content of a standard. Below we summarize these as direct and indirect ways to influence standards development.

Direct (roughly in order of increasing influence)	**Indirect** (roughly in order of increasing influence)
1. Vote – The influence of an organization's vote varies by a committee's rules on what constitutes a member. It can by individual expert, organization, and/or country. 2. Consistently attend and participate in the standards committee meetings. (This also supports indirect influence "C.") 3. Send in written contributions/comments that are accepted as proposed or in principle. For certain technologies, a standards essential patent is another indicator of influence. 4. Propose a standards project that gets approved and ultimately published. 5. Contribute early in the project's development cycle, where such participation shapes the proposal's scope or general direction of the project.	A. Ask other members to support the same voting or substantive position through their written comments. B. Ask the leading experts/voices in a standards committee to support your position in meetings. C. Be a leading expert/'trusted voice' in a standards committee to influence meeting participants. D. Serve as a chair of a committee or as a lead editor.

The column of direct ways to influence a standard can generally be observed by standards committee managers (and members). But three of the four indirect ways are difficult to measure since the information for A and B will only be known to limited parties, and C is subjective.

Chairs and editors roles' vary, but they do not provide a way to directly influence the content of standards. These positions are used to manage and lead members to arrive at consensus-based decisions. Note that committee managers and secretariats are not included in either list.

We therefore advise that any recommendations on how the United States can take steps to influence (or mitigate the influence of others) in international standards-development bodies be based on factors detailed above and discourage using what is easier to count or measure.

---

[1] National Institute of Standards and Technology, *Study on People's Republic of China (PRC) Policies and Influence in the Development of International Standards for Emerging Technologies*, Docket Number 211026–0219, 86 Fed. Reg. 60801 (Nov. 4, 2021).

[2] *i.e.*, All those developed in accordance with Annex 2 to Part 1 (Decision of the Committee on Principles for the Development of International Standards, Guides and Recommendations with relation to Articles 2, 5 and Annex 3 of the Agreement) in the Decisions and Recommendations adopted by the WTO Committee on Technical Barriers to Trade Since 1 January 1995 (G/TBT/1/Rev.13), as may be revised, issued by the WTO Committee on Technical Barriers to Trade.

[3] BSA agrees with NIST that, "[i]nternational standards allow regulators and governments to improve trade policies and develop better regulations. International standards developed in a process consistent with the World Trade Organization's Technical Barriers to Trade Agreement provide an ideal tool to support trade agreements, and to provide confidence that requirements for products and testing have global relevance and are accepted worldwide. … International standards need to be relevant and to effectively respond to regulatory and market needs, as well as scientific and technological developments in various countries. They should not distort the global market, have adverse effects on fair competition, or stifle innovation and technological development. In addition, they should not

give preference to the characteristics or requirements of specific countries or regions when different needs or interests exist in other countries or regions. Whenever possible, international standards should be performance based rather than based on design or descriptive characteristics." *See* 86 Fed. Reg. 60801.

[4] ITI (2016), "Localized Standards and Regulatory Requirements: Don't Reinvent the Wheel," *TechWonk Blog*, https://www.itic.org/news-events/techwonk-blog/localized-standards-and-regulatory-requirements-dont-reinvent-the-wheel

[5] *Cybersecurity Classified Protection Regulations (Draft for Comment)*, June 27, 2018 (CCPS) (Chinese), at: http://www.mps.gov.cn/n2254536/n4904355/c6159136/content.html?from=timeline&isappinstalled=0.

[6] *Administrative Measures for the Multi-level Protection Scheme of Information Security*, June 22, 2007 (MLPS) (Chinese), at: http://www.mps.gov.cn/n2254314/n2254409/n2254431/n2254438/c3697388/content.html.

[7] *Guiding Opinions on Implementing CCPS and CII Protection Scheme,* September 2020 (English) at: https://www.mps.gov.cn/n6557558/c7369310/content.html.

[8] *The Cryptography Law of the People's Republic of China*, December 2020 (Chinese), at: http://www.npc.gov.cn/npc/c30834/201910/6f7be7dd5ae5459a8de8baf36296bc74.shtml; *China's New Cryptography Law – Still No Place to Hide,* December 2020, at: https://www.chinalawblog.com/2019/11/chinas-new-cryptography-law-still-no-place-to-hide.html#:~:text=The%20PRC%20National%20People%27s%20Congress,effect%20on%20January%201%2C%202020.&text=The%20Law%20provides%20that%20it%20welcomes%20foreign%20providers%20of%20commercial%20encryption.