U.S. Chamber of Commerce International Affairs | U.S.-Japan Business Council | JUBC Japan-U.S. Business Council

Digital Economy

In April 2024, President Joe Biden and Prime Minister Fumio Kishida agreed to strengthen U.S.-Japan cooperation on critical and emerging technologies, with a focus on cybersecurity, AI, quantum, and semiconductors. The U.S.-Japan Business Council and the Japan-U.S. Business Council ("the Councils") welcome a joint technology agenda for closer semiconductor cooperation bilaterally and with like-minded countries to strengthen global semiconductor supply chains, recognizing the importance of semiconductors to various industries and national security. In a similar vein, given the ever-growing importance of cybersecurity to national security as evidenced by the updated national security strategies of both countries, we commend the bilateral commitment to establish a new cybersecurity working group that will develop an action plan for mutual recognition of cybersecurity labeling schemes with input from relevant experts. In addition, continued emphasis should be placed on the promotion of strong digital trade rules, such as those enshrined in the U.S.-Japan Digital Trade Agreement, and the free flow of data, a key pillar of the global digital economy. As our two countries work to address societal concerns and facilitate sustainable growth via our deep partnership across the digital economy, we recommend that the governments consider the following policy recommendations:

1. Enshrine cross-border data flows in trade and digital agreements.

The digital economy remains a major driver of economic growth around the world, and organizations of all sizes and industries rely on the movement of data to thrive. This need for efficient and effective cross-border data flows will only accelerate in the era of AI and as other innovations emerge. However, some governments have called for a policy of data localization based on a misguided belief that keeping data onshore will provide better security and protection. In reality, data localization increases compliance costs, weakens security, creates new areas of cybersecurity vulnerability, and impedes the openness and accessibility of the global Internet.

The Councils urge the U.S. and Japanese governments to push back against efforts that promote data localization and undermine open cross-border data flows by advancing shared principles for responsible data management and cybersecurity, such as through the Data Free Flow with Trust ("DFFT") initiative and implementing the 2023 G7 digital commitments. We strongly encourage the two governments to continue to uphold the free flow of data in multilateral fora, such as the G20, OECD, APEC, and the WTO, and to promote these principles through established mechanisms, such as the APEC Cross-Border Privacy Rules ("CBPR") System, the Global CBPR Forum, and the workstreams under the OECD DFFT Experts Community. The Councils urge the Biden administration to restore U.S. leadership on digital trade policy and work closely with partners like Japan to reinforce strong digital trade rules that facilitate data flows, protect intellectual property, and prevent discriminatory treatment of businesses based on nationality. The Councils also recognize the importance of digital governance, such as privacy, data protection, and trustworthiness, to further promote the digital transformation of society, however these policy objectives are consistent with, not hindered by, our trade obligations.

2. Bolster U.S.-Japan leadership in critical and emerging technologies.

Semiconductors are strategically important to economic and national security given their essential role in digitizing the world and powering nearly all industries. Notably, chips are necessary for advanced information and communications technology ("ICT") sectors, which are critical to secure supply chains. As such, close coordination between the U.S. and Japan is required not only to fill critical gaps in the semiconductor supply chain, but also to reinforce supply chain resilience throughout the entire semiconductor ecosystem. As the U.S. and Japan seek to

strengthen their role as global leaders in the development and protection of this critical technology, the two allies should develop a bilateral mechanism involving the U.S. Department of Commerce, Japan's Ministry of Economy, Trade and Industry, and the private sector of both countries. Building on the U.S.-Japan Competitiveness and Resilience ("CoRe") Partnership launched in April 2021, this initiative should complement multilateral supply chain strengthening efforts under the Indo-Pacific Economic Framework for Prosperity ("IPEF"). A formal public-private dialogue would help prepare both countries for supply chain disruptions. As part of this regular exchange, the Councils encourage both governments to continue to ensure that their respective semiconductor incentive programs are open to both U.S. and Japanese companies and joint ventures. Additionally, these incentive programs should support R&D, design, and production of the full range of semiconductor technologies.

The Councils urge the two governments to accelerate the implementation of cutting-edge quantum technology, in areas including quantum computers, quantum secure communications, and quantum networking, and the implementation of demonstration schemes and joint development based on the CoRe Partnership. In addition, both countries should work to identify and protect rule-based standards for development processes, secure the supply chain for critical inputs necessary for quantum technology, and implement approaches that bolster industry capacity in key standard-setting processes for emerging and critical technologies, including quantum technology.

3. Promote trustworthy AI and empower the workforce with 21st-century digital skills.

As technology innovation advances rapidly, it is crucial to develop and utilize AI not only for consumers but also for industrial use to enhance economic productivity and achieve a resilient and efficient society. It is also essential to develop human-centric and trustworthy AI to maximize social benefits of the technology. As discussions on AI regulations continue globally, the Councils recognize the importance of ensuring that AI governance keeps up with the rapid pace of technological innovation while ensuring that innovation can take place in an interoperable environment of rules and standards to properly utilize AI on a global scale. We urge the two governments to lead in achieving these goals while cooperating with relevant stakeholders, including industry. To this end, the Councils welcome the leaders' commitment to further advance the Hiroshima AI Process and strengthen collaboration between the U.S. and Japanese AI Safety Institutes. We believe establishing trust is foundational for the successful and secure deployment of AI. We encourage the two governments to work toward adoption of practices that enable the use of trusted vendors, support trusted enterprises, and build trusted governments.

Additionally, to ensure the responsible development and use of AI across all players in the AI ecosystem, it is essential to endorse transparent, multi-stakeholder approaches to AI governance that are informed by internationally recognized standards and frameworks. This includes developing voluntary standards, frameworks, and codes of practice that can bridge the gap between AI principles and implementation. Multi-stakeholder initiatives have the greatest potential to identify gaps and mobilize AI actors to address them. The United States' National Institute of Standards and Technology's ("NIST") Artificial Intelligence Risk Management Framework ("AI RMF") and Japan's Ministry of Economy, Trade and Industry ("METI") AI Governance Framework offer a good basis to coordinate on bilateral interoperability of AI governance, given their shared emphasis on agile governance, a risk-based approach, promoting safety, transparency, and accountability while fostering innovation, making both suitable models for broader inspiration and adoption. We welcome the launch of the AI Safety Institute (AISI) by the Government of Japan in February 2024 and call on the two governments to accelerate cooperation between the AISIs to establish interoperable AI safety assessments.

With businesses looking at upskilling employees on AI, there is an urgency, particularly in Japan, to empower the workforce with basic digital skills and specialist trainings. Both the public and private sectors should invest in programs that help ease worker transitions and improve incentives for businesses to invest in training. Education systems must also adapt through policy reform to better prepare students in both the K-12 and higher education systems for developing AI and machine learning systems. And through these efforts, we should address the digital divide. Collaboration between governments and businesses is vital, as businesses' access to a global skilled workforce will be critical to its ability to succeed across borders. Additionally, both governments should raise public awareness regarding the innovation and benefits of AI across the economy and society to help the public better understand how to maximize its use in their daily lives. When using AI technologies, it is important to respect and safeguard the

intellectual property ("IP") rights of creators and owners. Governments must provide clear and predictable standards that ensure full respect for IP protection and enforcement with respect to AI, including through patents, trademarks, and copyrights.

AI and other technologies can also be used to support climate resilience and the green transition by enabling existing technology to operate more efficiently. For example, AI models can enable better balancing of the electrical grid by providing grid managers with more accurate demand forecasts. Meanwhile, the Councils recognize the exciting potential for data centers to drive innovation in energy by considering their environmental impacts thoughtfully and collaborating with new and existing energy providers to meet their power needs. Optimizing data center energy efficiency through energy-saving innovations, such as next generation semiconductor technologies including high-density integration, optoelectronic integration, silicon carbide materials, power devices, cooling systems, thoughtful water use policies, and energy management, will be crucial to realizing sustainable development objectives with AI.

4. Develop and promote a resilient and reliable next-generation ICT infrastructure.

The Councils believe that secure and trusted next-generation telecommunications infrastructure will enable innovation and new opportunities across all industries by accelerating digitalization of wireless infrastructure. We believe that governments should seek an all-of-the-above solution to advance communications infrastructure including fiber, wireless, fixed wireless, and satellite. In the wireless space, we believe that an open, interoperable architecture can help enhance economic security by expanding options for selecting trusted vendors and diversifying supply chains. Based on the U.S.-Japan Global Digital Connectivity Partnership launched in May 2021, we urge both governments to continue to establish clear, secure, and trusted information and communications technology ("ICT") 5G technology public policies to accelerate development and voluntary adoption, as well as the use of virtual, open, interoperable, and standards-based network technologies and solutions including those for radio access networks ("RANs"), optical transport, and network management both domestically and internationally. It is also important to strengthen cooperation between both governments in 6G, next-generation radio communication technology beyond 5G. While the private sector is driving the development of 6G, both governments can play an important role in realizing the promise of 6G through research and development, bilateral and multilateral cooperation, and standards development.

Further, sound spectrum policy should be a key goal of both governments. A sound spectrum policy is critical to the business community and its consumers, as well as to fulfilling important national objectives including national and homeland security, job creation and economic growth. Both governments should focus on developing modern spectrum pipelines that consider all spectrum access models, engage in long-term spectrum planning, investment in spectrum research and development, and ensure coordination on spectrum policy across each government.

Finally, we encourage the two governments to take initiative in accelerating the adoption of these technologies by implementing their commitments to invest in research, development, testing and deployment. We recognize that it is important to develop, build, and maintain a multi-layered network consisting of not only terrestrial networks, but also non-terrestrial networks and submarine cables among others, to bolster the reliability and strength of the overall information and communications network. From this viewpoint, we call on both governments to continuously strive to further collaborate with like-minded partners, including those in the Global South, to build a highly reliable and strong network by leveraging the international communications infrastructure (such as transoceanic submarine cables), thus bolstering global connectivity. We encourage coordination between likeminded governments to spur advances in next generation foundational technology (e.g., chip development, quantum, and AI) through active and robust participation in standards development organizations.

5. Leverage cybersecurity to deploy a safe and secure infrastructure.

The Councils recognize that effective cybersecurity risk management, especially regarding critical infrastructure, is vital to the economic and national security of both countries. Given the evolution of cybersecurity threats and their increased frequency and sophistication, use of digital technologies to bolster infrastructure resilience will be key to

managing risks. Moreover, the Councils recognize that a risk-based approach is more effective for managing cyber risk than prescriptive regulation. As such, we encourage both governments to discuss current and anticipated cyber regulation, balancing the need for safety and innovation while ensuring harmonization of regulation and standards to maximize cross-border value creation. The use of outdated digital devices that are no longer supported by their manufacturers can pose security risks to critical networks and information systems. Both governments should consider ways for critical infrastructure owners or operators to address these risks when such devices are beyond their supported lifecycles.

As the U.S. and Japan take steps to strengthen cybersecurity across government, critical infrastructure, and supply chains, approaches to cybersecurity should adhere to internationally recognized cyber risk management frameworks that are relevant across sectors that businesses can utilize to enhance their security over time. Allowing industry to combat evolving cyber threats with evolving best practices and globally recognized standards, such as the NIST Cybersecurity Framework, permits a more flexible, current, and risk-based cybersecurity approach. Furthermore, increasing the use of cloud and AI as essential enablers of cybersecurity capabilities as well as enabling the rapid sharing of cybersecurity vulnerability and threat information between countries and critical industry will be key to strengthening cyber capacity and resilience. A more aligned international approach to cyber policymaking also streamlines the process for SMEs that need to strengthen their cybersecurity capabilities to integrate into global supply chains. The Councils urge the U.S. and Japanese governments to lead in enhancing cybersecurity cooperation for critical infrastructure in the G7 and the Global South.

The international approach should include continued efforts toward mutual recognition of Internet of Things (“IoT”) cybersecurity labeling program and agreement on the key elements of the Secure Software Development Framework (“SSDF”) and the software bill of materials (“SBOM”) to ensure interoperability of policies for secure IoT and software development.

We encourage the two governments to include the U.S.-Japan Digital Trade Agreement’s cybersecurity provisions in future trade agreements, including the WTO joint initiative on e-commerce and the trade pillar of IPEF.