

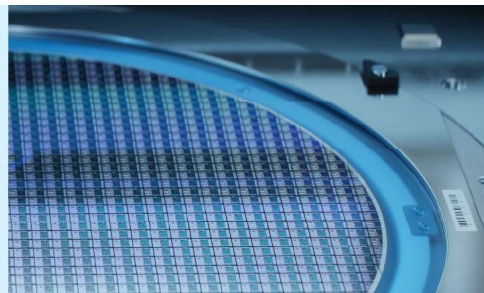


U.S. Chamber of Commerce
International Affairs
Asia

U.S.-Japan
Business Council



Digital Economy



Cutting-edge digital technologies play a central role across all industries in today's economy. The development of open, secure, trusted, interoperable, and resilient digital infrastructure is essential to economic growth and national security. The Japan-U.S. Business Council and the U.S.-Japan Business Council (the "Councils") urge policymakers to consider the following recommendations.

1. Advance the Implementation of Trusted AI

AI Governance and Security: The U.S. and Japan should build a trusted AI ecosystem using best practices from the U.S. National Institute of Standards and Technology's (NIST), AI Risk Management Framework (AI RMF), Japan's AI Guidelines for Business, and the Hiroshima AI Process. Both governments should promote interoperable, internationally recognized standards, norms, testing methods, and assurance frameworks for agentic AI.

Governance frameworks should be risk-calibrated—accounting for each system's materiality, degree of autonomy, customer impact, and access to sensitive data, while avoiding fragmented, duplicative evaluations and regulations. Frameworks should also ensure the safe and responsible use of AI models broadly and protect the integrity of AI and data supply chains. As frontier AI models develop capabilities for autonomous vulnerability discovery, both governments should work together to ensure that legitimate research, red-teaming and defensive vulnerability discovery are preserved, and that model-level safeguards do not impede defenders while leaving adversaries unconstrained.

AI Workforce Development: Workforce development should prioritize reskilling, upskilling, and expanded AI and machine-learning education at K–12 and higher-education levels. Governments should invest in structured partnerships between industry and academia, including collaborative research programs, apprenticeship and internship pipelines, and AI ethics training for responsible development and use of AI. Both countries should also support industry-led public awareness initiatives that address misinformation, disinformation, AI system vulnerabilities, and regulatory compliance to build trust and security in AI.

Energy-Efficient AI Infrastructure: The U.S. and Japan should promote investment in data centers and broadband infrastructure with affordable, reliable, and energy-efficient technology and power sources. Both governments should encourage the development of sustainable and renewable energy sources to support the entire AI ecosystem. To promote sustainable AI development, both countries should work towards optimizing the full AI stack through energy-saving innovations—including next-generation semiconductors and processors, advanced materials and filtration technologies, and efficient cooling technologies.

Physical AI: Physical AI and robotics are becoming strategic technologies by building upon cyber-physical systems that integrate sensing, perception, and control. Both governments should advance common approaches to safety, reliability, interoperability, and testing. Support for testbeds, regulatory sandboxes, and standards development will accelerate responsible deployment.

Given the critical importance of hardware-software integration, both countries should pursue an open and collaborative approach that leverages best-in-class international technologies while strengthening the resilience of critical capabilities domestically and among trusted partners.

In addition, both governments must strengthen research and development and enhance supply chain resilience for

all underlying technologies, enabling physical deployment. They should also encourage the participation of small and medium-sized enterprises (SMEs) to promote the broader deployment of these technologies.

2. Promote Trustworthy, Free Data Flows

Trusted Cross-Border Data Flows: Both governments should support trusted cross-border data flows and avoid unnecessary or discriminatory data localization requirements, including requirements affecting AI services that rely on data across jurisdictions. Both countries should work toward mutually recognized personal data regulations and R&D efforts that protect sensitive data while enabling responsible data use, research, and cross-border collaboration.

Internationally Recognized Standards: Both governments should advance data interoperability using best practices and market-oriented operational rules established by the Global Cross-Border Privacy Rules Forum, APEC, and the OECD's "Data Free Flow with Trust" Expert Community.

Industrial Data Spaces: Japan and the U.S. should advance trusted, interoperable Industrial Data Spaces as a foundation for secure data sharing as outlined in Japan's Ouranos Ecosystem initiative. Such cooperation would support the advancement of innovative technologies and supply chain security, allowing for a secure operational technology and manufacturing data ecosystem to accelerate Physical AI innovation.

3. Strengthen U.S.-Japan Leadership in Emerging Technologies

Semiconductors: Given the strategic importance of all types of semiconductors, the U.S. and Japan must work together to secure the entire semiconductor supply chain—from raw materials and specialty inputs to device fabrication and advanced packaging—through diversification, international cooperation, joint funding, and R&D. Joint development projects that engage all parts of the supply chain can increase competitiveness and overcome current supply chain insecurity.

Both countries must also reduce trade barriers and promote transparent policies that promote trade in semiconductor materials, equipment, and related technology inputs, while reducing tariff and non-tariff barriers that increase costs for advanced manufacturing supply chains.

Quantum Technology: Both governments should advance collaborative quantum technology development, focusing on the practical implementation of quantum networks and computing systems. Quantum computing also presents a strategic cybersecurity challenge for both the U.S. and Japan, as it could undermine encryption protecting digital economies. As quantum systems near practical deployment, both countries should emphasize their use to enhance industrial competitiveness and recognize quantum risk as a systemic issue of national and economic security with steps to guide organizations to transition to quantum-resistant encryption algorithms, including post-quantum cryptography, while advancing quantum-secure communications.

The Councils also request government support in securing supply chains for essential materials and collaborating with industry on internationally recognized standards for interoperability.

R&D and Innovation Policy: Both governments should foster a policy environment that rewards sustained investment in research and development, including through competitive tax incentives, streamlined permitting for advanced manufacturing facilities, and stable funding for public-private R&D partnerships. Policies that encourage long-term capital investment in next-generation process technologies and materials science are essential to maintaining U.S.-Japan technological leadership. They should also pursue mutual recognition agreements and harmonized regulatory standards that facilitate the free flow of critical technology goods and services between the two countries.

4. Develop a Resilient Next-Generation ICT Infrastructure

Open Technologies for Connectivity: The U.S. and Japan should promote safe, trusted digital connectivity and advance policies that foster clear, secure ICT connectivity solutions—encouraging virtual, open, interoperable, and

standards-based network technologies, including for Radio Access Networks (RANs), Radio Local Area Networks (RLANs), optical transport, network management, and technologies that enable more efficient use of radio spectrum, such as Dynamic Spectrum Access (DSA), and automated frequency coordination (AFC).. Interoperable architecture expands trusted vendor selection

and diversifies supply chains. For 6G development, both countries must coordinate on transparent rulemaking to continue these interoperable efforts.

Multilayered Networks: Both countries should take a multi-layered approach to international communications, integrating submarine cables and non-terrestrial systems, such as Low Earth Orbit (LEO) satellite constellations, to improve disaster resilience and enhance coverage in remote areas. Governments should also support the private sector in securing funding for third-country submarine cable projects with trusted suppliers.

5. Strengthen Cybersecurity for Resilient Infrastructure

AI-Powered Threat Mitigation: The U.S. and Japan must develop secure AI systems and cybersecurity solutions that address professional shortages while mitigating AI risks. Infrastructure resilience must integrate technology, policy, and international cooperation through a risk-based approach. Cybersecurity frameworks—such as the NIST Cybersecurity Framework—should be used across governments, critical infrastructure, and supply chains. Both countries should lead on promoting standards such as the Software Bill of Materials, IoT cybersecurity labeling, and the Secure Software Development Framework. Both governments should modernize vulnerability management frameworks to enable rapid patch deployment from vendors with mature remediation practices, accelerate the retirement of end-of-life technology through government procurement and incentive funding, and incentivize AI-powered compensatory controls to protect systems that cannot be patched or taken offline without disrupting critical operations. Governments should also align incident reporting timelines and avoid mandating the disclosure of unremediated vulnerabilities outside coordinated vulnerability disclosure practices.

International Cooperation: To counter cyberattacks leveraging advanced technology, joint initiatives should include: developing AI-based cyberattack detection models integrating machine learning and deepfake detection; sharing cyber threat intelligence; and co-developing quantum-secure communication systems with joint technology standards and pilot projects.

The Councils commend the intent behind Japan's active cyber defense legislation and call for continued close public-private collaboration through dialogues, such as the U.S.-Japan Cyber Dialogue Track 1.5, in shaping its implementation regulations, ensuring transparency, proportionality and the avoidance of prescriptive design mandates on ICT vendors.

6. Strengthen Strategic Cooperation on Dual-Use Technologies

As the boundary between civilian and national-security applications continues to blur in physical AI, robotics, advanced ICT, semiconductors, and quantum technologies, the U.S. and Japan should promote risk-based, transparent governance frameworks that protect security while preserving innovation.

Priority areas include clearer technology classification, greater transparency and alignment in export controls and investment screenings, stronger research-security and IP protection, and trusted talent collaboration among industry, academia, and government—improving predictability for businesses and avoiding unnecessary barriers to legitimate commercial and research cooperation.