The text of the following statement was released by the Government of the United States of America and the Kingdom of Spain on the occasion of the second U.S.-Spain Cyber and Digital Dialogue:

The United States and Spain held their second bilateral Cyber and Digital Dialogue on June 6, 2024, in Washington, D.C.

Representatives of the Unites States and Spain noted their will to foster the bilateral cooperation to promote security and stability on cyberspace and digital policy issues. Both sides reiterated their commitment to promote and preserve the rules-based international order, a secure, stable, accessible, and peaceful cyberspace, and to protect and respect human rights online.

Both sides continue to be strongly committed to implementing and advancing the UN framework of responsible state behavior in cyberspace, grounded in the application of international law to cyberspace, adherence to established norms of responsible state behavior, and implementation of practical cyber confidence building measures. The United States and Spain continue to work toward the establishment of the UN Cyber Programme of Action, which gives States a permanent, action-oriented mechanism for multilateral cyber discussions under the auspices of the UN. As a priority, the United States and Spain reaffirmed their strong commitment to digital solidarity, to further enhance global cyber resilience, and to implement cyber capacity building supporting partners including but not limited to those in the Western Hemisphere. The United States and Spain discussed addressing cybersecurity challenges related to the protection of critical infrastructure, emerging technologies, and combatting cybercrime.

U.S. and Spanish officials exchanged views on the importance of strengthening the security of the ICT ecosystem and protecting privacy, intellectual property rights,-and respect for international human rights. This includes promoting the investment in and the development and deployment of secure and trustworthy fifth generation (5G), next generation networks, and other ICT in infrastructure in advanced and emerging economies.

Both sides stressed the importance of information integrity and exchanged views on how best to advance it, especially when facing the challenge posed by cross-border dis- and misinformation in the Spanish language. The sides intend to address the challenge of disinformation through implementing the Memorandum of Understanding signed by their foreign ministers on behalf of their foreign ministries in May 2024. Officials also noted the importance of promoting rights-respecting, safe, secure, and trustworthy artificial intelligence systems to accelerate progress towards the full realization of the 2030 Agenda for Sustainable Development.

Ambassador-at-Large Nathaniel Fick opened the consultation, which was chaired by Deputy Assistant Secretary for International Cyberspace Security Liesyl Franz and Ambassador Steve Lang, Deputy Assistant Secretary for International Information and Communications Policy for the U.S. Department of State's Bureau of Cyberspace and Digital Policy. The United States was also represented by the Department of Homeland Security (the Cybersecurity and Infrastructure Security Agency, Homeland Security Investigations), the Federal Bureau of Investigation, the Office of the National Cyber Director, the National Institute of Standards and Technology, the Federal Communications Commission, the National Telecommunications and the Department of Defense. José Miguel Corvinos, Ambassador-at-Large for Digital Transformation and Hybrid Threats, led the Spanish interagency delegation, which included representatives from the Prime Minister’s Office (the Department of National Security), the Ministry of Defense (the Joint Cyberspace Command and the National Cryptologic Center), the Ministry of Interior (the Cybersecurity Coordination Center), and the Ministry of Digital Transformation (the State Secretariat for Digitalization and Artificial Intelligence, the State Secretariat for Telecommunications, and the National Cybersecurity Institute).