



Report to Congress on An Update on Securing Digital Infrastructure in Developing Countries Financed by the PRC

Section 7019(e) of the National Security, Department of State, and Related Programs Appropriations Act, 2026 (Div. F, P.L. 119-75) and House Report 119-217.

Advancement of a country's digital ecosystem, spanning physical infrastructure, cybersecurity, and sound data and technology policy, drives economic development, stability, and security. Investments in the responsible adoption of artificial intelligence, secure cloud services, and robust cybersecurity capabilities create lasting, positive effects for generations. These investments connect end users to modern commerce and the global information space while enabling advancements in critical infrastructure such as transportation, the internet of things, healthcare, education, cross-border digital trade, and resilient cyber defenses. Increasingly, these choices have implications for broader market access for U.S. companies depending upon if a country chooses interoperable U.S. or allied technology, or the technology stack of competitors like China. In low and middle income countries especially, the Chinese government, through companies like Huawei and ZTE, uses non-market practices to undercut the price of trusted suppliers with financing terms that entice these countries to select Chinese

technology, thereby locking them into the Chinese tech stock and locking U.S. companies out of that market.

The Department of State's Approach

The Bureau of Cyberspace and Digital Policy (CDP), established in 2022, leads the Department of State's efforts to promote U.S. science, technology, and innovation; advance U.S. prosperity and security; and ensure the United States wins the race in the next generation of critical and emerging technology. Through the Artificial Intelligence (AI) Action Plan, launched in 2025, CDP works to promote adoption of U.S. AI technology globally.

The AI revolution and the need to secure global supply chains fundamentally represent an opportunity to deepen our partnerships with countries in every layer of the tech stack and in all areas of the supply chain. The Administration has made clear that it will pursue an economic foreign policy and national security policy that promotes U.S. technologies, standards, and governance models worldwide to strengthen relationships with our partners and secure our continued technological dominance and critical global supply chains.

CDP strategically deploys a toolkit of targeted, agile, and tailored technical assistance programs across the full technology stack to secure U.S. technological leadership and ensure technology adoption transforms economies while protecting against authoritarian threats. Our work shapes other nations' technology policies to expand markets for U.S. companies and reduce security and economic vulnerabilities posed by malicious state and non-state actors in cyberspace. Following the 2025 creation of the Bureau of Emerging Threats (ET) that now leads the Department of State's cybersecurity and defense functions, CDP has worked with ET on programming related to protecting cybersecurity,

critical and digital infrastructure from adversary threats. Moving forward, ET will assume responsibility for those specific programs.

Leveraging the Digital Connectivity and Cybersecurity Partnership (DCCP) to Advance Secure Digital Infrastructure

As the U.S. government (USG) lead for the DCCP initiated under the first Trump administration, CDP also coordinates USG agencies on cyber, digital, and emerging technology issues. In addition to USG agencies, CDP works with other allied governments, the private sector, multilateral organizations, academia, and U.S. federally funded research and development centers to achieve U.S. policy goals.

In working with partner agencies such as the U.S. Trade and Development Agency, the Department of Commerce's Commercial Law Development Program (CLDP), and in alignment with the Office of the Partnership for Global Infrastructure and Investment in the Bureau of Economic, Energy and Business Affairs (EEB/PGI), CDP can design and fund foreign assistance programming that supports secure and trusted digital ecosystems on a variety of fronts. These engagements raise awareness about security and reliability risks of untrusted information and communications technology (ICT) suppliers with the goal of deploying secure and trusted ICT across the globe.

CDP has added the following programmatic options to advance digital and cyber policy goals, including:

- Developing fit-for-purpose, rapid cyber incident response.
- Facilitating the adoption of secure and trusted technology solutions in international markets.

- Directing investments in trusted undersea cable infrastructure.
- Assisting partners to enact policies that counter commercial spyware.
- Strengthening partner capacity to engage in ICT standards development.
- Supporting establishment of legal frameworks for data privacy, cross-border data flows, and digital trade.
- Advancing cloud-based digital security and disaster recovery solutions.
- Promoting responsible AI development and governance.

To date, there have been several examples of coordinated USG engagements that have been effective in mitigating the adoption of untrusted suppliers while advancing critical foreign policy objectives.

Colombia Asserts National Position on International Law in Cyberspace

As a result of CDP capacity building, Colombia's National computer security incident response team (CSIRT) successfully acceded to the Forum of Incident Response and Security Teams (FIRST) in June 2025, marking a significant step in the country's cybersecurity strength. Joining means the national CSIRT could demonstrate core incident response competencies and has aligned its policies and procedures with international best practices. CDP also funded training and workshops to Colombian officials, which resulted in the publishing of a national position on the applicability of international law in cyberspace, enabling more meaningful engagement in multilateral discussions and countering adversarial states' push for restrictive treaties.

Promoting American Approaches to Digital Trade in Africa

From 2023-2025, CDP embedded a digital trade advisor to help the African Continental Free Trade Area Secretariat draft a digital trade protocol. The protocol includes provisions for data governance and cross-border data flows that counter malign actors and align with U.S. policy objectives. The U.S. advisor helped negotiate finalization of the protocol among African Union member states, which was adopted in February 2024. The advisor also helped build consensus among member states around eight annexes governing critical elements of the digital trade ecosystem such as intellectual property rights, cross-border payments and data flows, and emerging technologies that are critical for continued market expansion of the U.S. tech industry in Africa. The annexes were successfully adopted in February 2025.

Bangladesh Drafting Personal Data Protection Law

Supported by CDP, CLDP conducted a series of workshops, meetings, and interventions with Bangladeshi officials starting in 2021 to encourage the adoption of less restrictive, pro-investment data protection legislation and use of the Global CBPR system. In 2025, Bangladesh's interim government introduced a Personal Data Protection Ordinance that allows for CBPR adoption and does not include criminal penalties or other anti-investment provisions such as a requirement for U.S. firms to have local offices.

Strengthened Albanian Cybersecurity Thwarts Iranian Attacks

The United States responded to a 2022 Iranian-backed cyberattack against Albania with a \$25 million multi-year cybersecurity assistance package. In early 2023, U.S. consultation and training led to the Government of Albania's development of strategic cybersecurity goals, and by April 2024, Albania passed a cybersecurity law and established national cyber and information agencies. While continued support is needed to build experience, Albania now operates an

effective Government Security Operations Center (SOC) dedicated to protecting government networks, as well as a national SOC focused on safeguarding critical infrastructure networks. Both centers serve as vital early-warning partners, enhancing U.S. cybersecurity and Iranian threat awareness. The Government of Albania's response to two recent incidents demonstrated the profound impact of U.S. assistance. The government quickly and effectively responded to contain and limit the damage of an October 2024 incident affecting a major Albanian hospital and a June 2025 attack against Tirana's municipal government networks.

Increased Adoption of NIST Cybersecurity Framework

Ransomware is a global threat affecting individual users, small businesses, large corporations, and government entities. In 2025, CDP supported multinational counter ransomware exercises that applied the U.S. NIST Cybersecurity Framework. This resulted in diplomatic breakthroughs with 11 additional nations expressing their intent to join the International Counter Ransomware Initiative, which now has 74 members from every region in the world. All participants developed plans to advance their cybersecurity informed by U.S. guidelines. Every nation sharing the burden of acting to counter ransomware is one less way for ransomware to threaten the United States.

Eleven Countries Join the Forum of Incident Response and Security Teams

Through its work with the Software Engineering Institute, CDP assistance has resulted in the CSIRTs from 11 nations gaining entry to FIRST between 2016-2025, including:

- Armenia,
- Albania,
- The Bahamas,

- Colombia,
- Costa Rica,
- Cote d'Ivoire,
- Ghana,
- North Macedonia,
- Panama,
- Serbia,
- and Vietnam.

More nations engaging in FIRST benefits the United States and overall international cyberspace security through:

- Providing a picture of global cybersecurity needs that U.S. tech companies can meet with their goods and services.
- Information-sharing and coordination between various countries' CSIRTs and their U.S. counterparts.
- Early detection and prevention for threats that could affect U.S. national security.

The nations we supported in gaining membership have since sponsored membership in FIRST for 25 other teams, demonstrating a sustained return that goes beyond CDP's initial investment.

Conclusion

Countries around the world are prioritizing secure digital infrastructure to safeguard critical investments that protect their national security. These investments also bring reliable connectivity to rural communities, accelerate

innovation in new industries, and build a strong foundation for future economic growth. The Department of State remains firmly committed to working closely with partners across the U.S. interagency, as well as with Congress, toward these goals.