USAID FROM THE AMERICAN PEOPLE | DAI Shaping a more livable world.

DIGITAL CONNECTIVITY AND CYBERSECURITY PARTNERSHIP (DCCP)

USAID Activities

AS THE ADOPTION OF DIGITAL TECHNOLOGIES rapidly advances across the globe and increasing economic prosperity in many countries becomes intricately linked to Internet connectivity, we face a dilemma. How do we ensure that this digital transformation is built on technology that is open and secure, promotes inclusive growth, fosters resilient and democratic societies, and empowers all, including the most vulnerable? In other words, how do we make sure that technology isn't used to monitor populations, restrict citizens' access to information, and exploit the vulnerability of a workforce not trained to combat data breaches and cyber attacks?

Launched in July 2018 by Secretary of State Michael Pompeo, the Digital Connectivity and Cybersecurity Partnership (DCCP) is a whole-of-government initiative that aims to:

- *Expand and increase secure Internet access in targeted emerging markets by enabling market entry (or expanded market access) for U.S. or like-minded technology companies*
- *Promote exports of U.S. Information and Communications Technology (ICT) goods and services and increase U.S. company market share in targeted markets*
- *Increase adoption of policies and regulatory positions that encourage open, interoperable, reliable, and secure digital infrastructure*
- *Increase adoption of cybersecurity best practices in targeted countries.*

Chaired by the U.S. Agency for International Development (USAID) and the U.S. Department of State, DCCP works with partner countries to support the development of communications infrastructure; promote transparent regulatory policies for open, competitive markets; and build partners' cybersecurity capacity to address shared threats through engagement with the private sector, government, and civil society.

> "We do this because we recognize the tremendous economic and social benefits that come with an open, secure, and reliable internet." – *Remarks by Mike Pompeo, Secretary of State, at the DCCP launch.*

WHY CONNECTIVITY AND CYBERSECURITY?

The rapid development and adoption of digital technology holds the promise of a new digitally-enabled global society, with the potential to spur economic growth, improve development outcomes, and lift millions out of poverty. However, the emergence and adoption of digital technology also introduces risks. Digital tools and services, built on unsecure communications infrastructure, may be captured by malign actors to advance divisive messaging, crime, illicit finance, and cyber attacks that can have devastating consequences on our partners and beneficiaries.

The U.S. Government is working with partner governments and the private sector to promote informed investments in the development of communications infrastructure and digital markets. In developing their communications infrastructure, countries are at risk from authoritarian regimes that seek to dominate the telecommunications industry and control digital tools or services that increase censorship and repression. Through DCCP, the U.S. Government provides technical assistance to partner governments to counter these attempts by supporting initiatives that promote an open, interoperable, reliable, and secure Internet.

As networks expand, there are intrinsically greater cybersecurity risks that can jeopardize a country's infrastructure and services. The frontline of defense against cyber threats and data breaches (and often the most vulnerable point) is a country's workforce of

engineers, bank managers, government officials, or development practitioners. Because of the critical role these professionals play in maintaining cybersecurity and recovering from cyber attacks, they require adequate digital skills and training; the right processes, policies, or systems; and an appropriately protective legal and regulatory environment. To address this risk, DCCP is building the cyber capacity of partner country governments, industry, and civil society; promoting regulations and laws that protect privacy and freedom of expression; uniting industry and government to develop a highly qualified cybersecurity workforce; and increasing the digital literacy and digital security of citizens.

OUR WORK

USAID is implementing multiple DCCP activities through Digital Frontiers, a five-year (2017-2022) cooperative agreement administered by USAID's Center for Digital Development (CDD). Current activities include:

- ***Digital Asia Accelerator Support (DAA)*** — Serves as a vehicle for citizens and small businesses to become more digitally savvy and cyber-safe by increasing public awareness of digital safety issues, providing digital and cybersecurity upskilling for small and medium-sized enterprises (SMEs) and civil society, and providing opportunities to engage on digital policy issues across Southeast Asia.
- ***Promoting American Approaches to ICT Policy and Regulation (ProICT)*** — Through ProICT, USAID provides dedicated technical assistance, including embedded experts, for receptive host country ministries and regulatory bodies to assist in the design, development, and implementation of ICT policies.
- ***South Asia Regional Digital Initiative (SARDI)*** — Works toward improving digital connectivity in the South Asia region and strengthening the private sector and civil society's digital capacity and their ability to engage on digital and ICT policy issues.
- ***Advancing Timor-Leste's Autonomous Telecommunications Landscape (ATLATL)*** — Develops Timor-Leste's ICT policy while engaging the private sector to catalyze infrastructure investment.
- ***Cross-Border Privacy Rules (CBPR)*** — Socializes, increases knowledge of, and builds capacity and improved environments for the Asia-Pacific Economic Cooperation (APEC) Cross-border Privacy Rules System (CBPRs) with both APEC and non-APEC economies.

These activities work to advance DCCP's goals through engagement at multiple levels– from a grassroots level, providing cybersecurity upskilling to citizens and civil society organizations, to regulatory and policy support and technical assistance, to host country governments. In this way, USAID can support and secure communications infrastructure, Internet governance, and cyber resilience at all touchpoints of the digital ecosystem.

Working together with our partners, we can ensure that the Internet remains an open, interoperable, safe, reliable, and secure space while advancing U.S. economic prosperity and preserving the agency and security of citizens.

CONTACT US/LEARN MORE

KOMAL BAZAZ SMITH ▸ TEL: 301-771-7337 | EMAIL: Komal_BazazSmith@dai.com
Digital Connectivity & Cybersecurity Partnership (DCCP) Project Director, Digital Frontiers

TOM KOUTSKY ▸ TEL: 703-395-7117 | EMAIL: tkoutsky@usaid.gov
Senior Connectivity Program Coordinator, USAID