USAID
FROM THE AMERICAN PEOPLE

USAID DIGITAL STRATEGY

Photo: Raz Jahanpour for USAID/Digital Development Communications

USAID'S FIRST-EVER DIGITAL STRATEGY CHARTS AN AGENCY-WIDE VISION for development and humanitarian assistance in the world's rapidly evolving digital landscape.

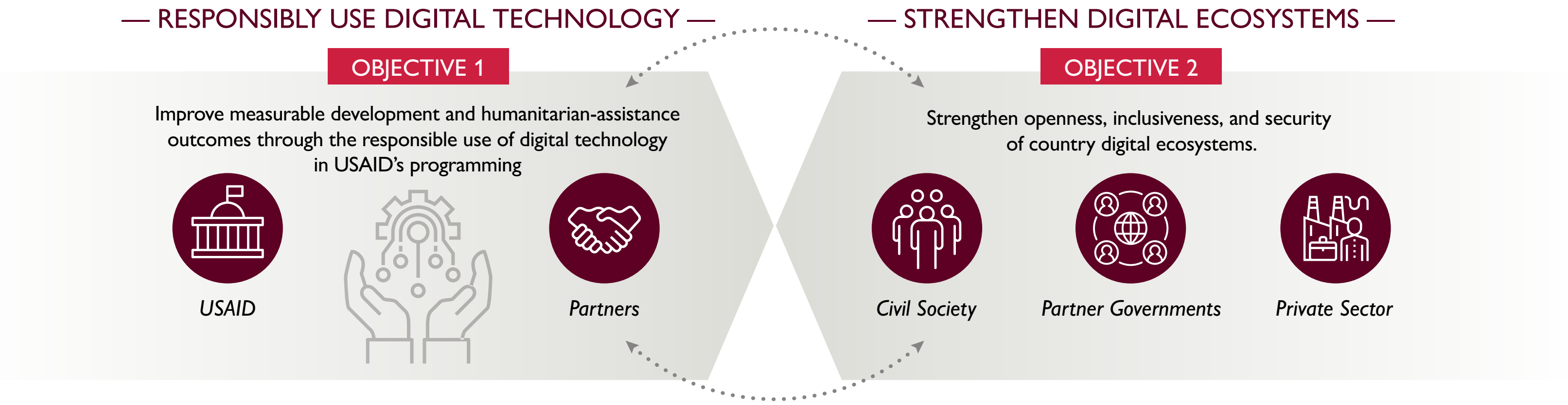
THE DIGITAL REVOLUTION has given way to the promise of a digital world that spurs economic growth, improves health outcomes, and lifts millions out of poverty using new technologies and services. While digital tools present immense potential to advance freedom and transparency, generate shared prosperity, strengthen inclusion, and inspire innovation, it also presents significant risks to privacy and security through competing models of Internet freedom.

STRATEGY GOAL

To achieve and sustain open, secure, and inclusive digital ecosystems that contribute to broad-based, measurable development and humanitarian-assistance outcomes and increase self-reliance in emerging market countries.

The *Digital Strategy* includes two core, mutually reinforcing objectives:

DIGITAL ECOSYSTEM: *stakeholders, systems, and enabling environments that together empower people and communities to use digital technology to gain access to services, engage with each other, or pursue economic opportunities.*



— RESPONSIBLY USE DIGITAL TECHNOLOGY —

OBJECTIVE 1

Improve measurable development and humanitarian-assistance outcomes through the responsible use of digital technology in USAID's programming

USAID

Partners

— STRENGTHEN DIGITAL ECOSYSTEMS —

OBJECTIVE 2

Strengthen openness, inclusiveness, and security of country digital ecosystems.

Civil Society

Partner Governments

Private Sector

To achieve the overall goal of the *Strategy*, these objectives will be executed through four tracks:

TRACK 1: ADOPT AN ECOSYSTEM APPROACH ▸ **Develop tools and resources** necessary to deliver development and humanitarian assistance effectively in a digital age

TRACK 2: HELP PARTNERS NAVIGATE RISK AND REWARDS ▸ **Build capacity of our partners** to navigate the unique opportunities and risks that digital technology presents across USAID's Program Cycle

TRACK 3: SHIFT TO "DIGITAL BY DEFAULT ▸ **Support implementing partners** in adoption of digital operations

TRACK 4: BUILD THE USAID OF TOMORROW ▸ **Invest in our human capital** to guide the Agency through the digital age

USAID
FROM THE AMERICAN PEOPLE

TRACK 2: HELP PARTNERS NAVIGATE RISK AND REWARDS: CONSIDERATIONS FOR COVID-19 RESPONSE

CYBERSECURITY

USAID's first-ever Digital Strategy outlines a path to strengthen open, inclusive, and secure digital ecosystems in all partner countries, and calls on the Agency to "expand our capacity to help governments, the private sector, civil society, and citizens in partner countries to mitigate harm through cybersecurity programming."

CYBERSECURITY IMPLICATIONS FOR COVID-19 AND DEVELOPMENT

Cyber attacks on health systems, the media, civil society, small and medium size businesses, and development and humanitarian programs have significantly increased during the COVID-19 pandemic.[1] Tech firms have identified COVID-19 as the biggest topic ever used as bait for phishing attacks, with a near 700 percent increase in attacks since the pandemic started.[2]

Nation states and cybercriminals regularly use times of crisis to launch attacks, taking advantage of associated fear and confusion. Disinformation about the pandemic is prevalent and often includes hyperlinks used to spread malware and facilitate further hacking efforts. For example, in Ukraine violent protests broke out after hackers sought to sow public fear by spreading false information through a spoofed mass email that appeared to be from Ukraine's health ministry.[3]

The cybersecurity risks emerging during the global pandemic could both undermine response efforts and the long-term resilience and health of the digital ecosystem in developing countries.

CYBERSECURITY IN DEVELOPMENT

Cybersecurity for development can be understood as identifying, protecting, detecting, responding, and recovering from threats and risks in a digital environment. For USAID programs this includes the policies, regulations, processes, and technical standards for the security of programs operating in an online or digital world, and also the security and stability of the digital infrastructure and systems—in the places we work—that are critical to attaining development objectives.

KEY CONSIDERATIONS FOR CYBERSECURITY IN COVID-19 RESPONSE PROGRAMMING

Increased cyber threats require improved cybersecurity awareness across COVID-19 responses in all sectors and dedicated support to build the cyber capacity and resilience of our partner countries, institutions and citizens. When designing programs or working with external partners and stakeholders to implement COVID-19 response activities, these considerations can provide guidance.

Just as hand washing is critical to stopping the spread of the virus, the basics of cyber hygiene are now more important than ever and are the best place to start. There are practical steps that can help mitigate cyber risks in COVID-19 response programming.

- Have basic cyber hygiene practices been defined for programs and are they being followed by your implementing partners and beneficiaries?
- Are implementing partner and beneficiary staff now working from home? What measures have organizations taken to mitigate related threats?

[1] https://www.devex.com/news/covid-19-brings-wave-of-cyberattacks-against-ngos-96934
[2] https://www.bbc.com/news/technology-52319093
[3] https://www.cnbc.com/2020/02/21/coronavirus-ukraine-protesters-attack-buses-carrying-china-evacuees.html

Practical steps that can help mitigate cyber risks in COVID-19 response programming (continued):

- If implementing partners or beneficiaries become the victim of a ransomware attack, do they have a planned response? Best practices for responding to cyber incidents can be found here.
- How would programs be affected if data was lost or compromised due to ransomware or other attack? Is critical data being regularly backed up and secured through multiple copies that are stored in separate virtual locations?

For these kinds of challenges, USAID has a new mechanism called Digital Apex, that is designed to help USAID partners and non-governmental beneficiaries improve their cybersecurity practices. Missions can also explore what capable and trusted local cybersecurity companies are available to help partners and beneficiaries prepare for and respond to cyber attacks.

IMMEDIATE RISKS:

Increasing **cyber threats have the potential to cause significant disruption** across sectors, further exacerbating the impacts of the COVID-19 crisis and limiting response efforts. What cybersecurity threats are happening in your country?

- Explore where you can learn about phishing, disinformation and misinformation trends occurring locally. Is there a local civil society organization, local cyber firm, or government ministry tracking cyberattacks and sharing information about risk? Can you access that information to share with partners and beneficiaries?
- Are the government's critical infrastructure systems, such as healthcare, financial services, communications (including Internet and social media), and energy, being hit with cyber attacks? If these systems were to shut down temporarily due to an attack, how would it affect programs?
- To the extent they exist, has there been an increase in public digital surveillance operations since the start of the pandemic? If so, how could it impact USAID programs or beneficiaries? What steps, if any, are beneficiaries or partners taking to mitigate concerns?

FUTURE RISKS:

Strengthening the cyber capacity and resilience of governments, civil society, private sector and citizens is crucial for supporting social and economic recovery over the coming years. These are some questions you can ask to better understand the cybersecurity landscape in your country and identify possible areas for programming:

- What is the capacity of the partner country to assess and address cybersecurity vulnerabilities of essential government services and critical infrastructure?
- What systems are in place to detect and deter cyber attacks in the organizations and institutions with which we are working?
- Is there an adequately skilled cybersecurity workforce?
- What are the basic levels of digital literacy and cyber security awareness of citizens?
- Has a partner country developed its own cybersecurity framework? Has it developed effective regulations to deal with cyberthreats?

OPPORTUNITIES

USAID programming can help address immediate cyber risks related to the pandemic and identify ways to engage host country governments and institutions to build cyber capacity and resilience. Talk with your host government counterparts to understand their cybersecurity needs and capabilities and identify where USAID can provide support.

USAID's Center for Digital Development has technical expertise available to help assess and design cybersecurity programming, and manages Digital Frontiers, a buy-in mechanism that works with USAID, the private sector, and international and local development organizations to identify successful and sustainable digital approaches and scale their impact globally.

Resources and contact information

For more information on cybersecurity, please contact digitaldevelopment@usaid.gov.