

[DRAFT - 5.23.24]

USAID Digital Policy

2024 - 2034

Table of Contents

Vision & Purpose: Development in a Digital Age	2
Background	4
Goals	6
Principles	11
Learning Agenda	17
Policy into Practice	18
Conclusion	21
Annex I - Brief History of Digital at USAID	22
Key Terms	23

Vision & Purpose: Development in a Digital Age

USAID envisions a world where open, inclusive, secure, and rights-respecting digital ecosystems enable people everywhere to thrive.

In today's digitally-connected world, there is a growing recognition that open, inclusive, secure, and rights-respecting digital ecosystems—and the life-enhancing and life-saving services they enable—are fundamental. We turn to digital tools for effective democratic governance; improved health, educational, and humanitarian outcomes; food security; national, global, and regional security; trade; and broad-based economic growth. Cutting across every sector, geography, and demographic, digital technologies and cybersecurity are fundamental components of international development and humanitarian assistance. Digital technologies have become central to the development journeys of our partner countries and are increasingly central to driving, managing, and stabilizing conflicts and crises. As USAID looks to the next decade and beyond, we are redoubling our efforts to meet the greatest challenges of our time by innovating boldly, embracing responsibility and accountability, generating reliable and usable evidence, and launching dynamic partnerships that enhance security, human rights, and economic prosperity for people everywhere.

CALL OUT BOX: Digital Ecosystem: The stakeholders, systems, and enabling environment that together empower people and communities to use digital technology to gain access to services, engage with each other, or pursue economic opportunities. A digital ecosystem is conceptually similar to, but broader than, a digital economy. Although certain aspects of the digital ecosystem have country-wide reach, other features differ across geographies or communities. The critical aspects of a digital ecosystem include the following: (1) sound enabling environment and policy commitment; (2) robust and resilient digital infrastructure; (3) capable digital service-providers and workforce (e.g., both public and private institutions); and, (4) empowered end-users of digitally enabled services.

The digital landscape has shifted significantly in the past decade as internet usage in low- and middle-income countries has roughly doubled. Internet platform companies now dominate the technology space, smart device adoption has proliferated globally, and most recently the rise of generative artificial intelligence (AI) models¹ is reshaping the way people do work, access information, and engage with one another. USAID faces critical development challenges related to technological change. Globally, more men continue to have access to the internet than women, but nowhere is this divide more stark than in South Asia (41%) and Sub-Saharan Africa (36%), where almost two thirds of women in low- and middle-income countries who are not using mobile internet live.² Increased access and use of technology have come with a dramatic increase in technology-facilitated gender-based violence (TFGBV). Information integrity, which is needed to protect democratic institutions, such as free and fair elections, are more at risk than ever. Governments, businesses, civil society organizations, media outlets, and individual citizens are at risk of malicious cyber activity. While most people now live in a digital world, billions are still locked out of it.

Technology is an arena of geostrategic competition; USAID must consider geopolitical realities as we advance cybersecurity and digital programming in emerging economies. Some competitors, including the

¹ For more information on USAID's programmatic work on AI and machine learning, visit <https://www.usaid.gov/digital-development/artificial-intelligence>

² GSMA: <https://www.gsma.com/r/gender-gap/>

People’s Republic of China (PRC) and Russia, are using their technological capacity and increasing influence over international institutions to create more permissive conditions for repressive and authoritarian practices. Authoritarian regimes are shifting from reactive to proactive measures to guard against perceived threats from civil society through censorship, information manipulation, mass surveillance, and commercial spyware which enhance state control over domestic and transnational political and social debate.

As part of its role on the Principals Committee of the National Security Council (NSC), USAID is at the forefront of advancing democratic, secure, interoperable, and open alternatives to the digital authoritarian models that feature state control, censorship, and violations of individual privacy. As a development and humanitarian agency, USAID brings an important and unique perspective to the national security discourse, particularly in regards to cybersecurity and digital technologies, as we focus on how we can support our Missions to better collaborate with partner governments in their digital transformations. The countries in which USAID works are at an inflection point with regards to technology. Today’s decisions about rules, standards, norms, and infrastructure will shape digital ecosystems for years to come. At the same time, these countries are being actively courted by digital authoritarians. USAID’s programmatic and policy leadership is an indispensable part of the U.S. Government’s efforts to reinforce an open, inclusive, secure, and rights-respecting internet and digital economy for all.

The next ten years promise to be no less dramatic than the past ten – as access continues to broaden, many countries will undergo “twin transitions”³ and many more will adopt Digital Public Infrastructure (DPI) approaches to their government systems. Advances will be made in AI, extended reality (XR), and quantum computing, and entirely new technology areas will reshape digital ecosystems. The children and youth of today – who make up the largest portion of internet users – are the first “digital native” generation, and their current experiences and engagements with digital technologies will have huge impacts on future economies and societies. Given these realities, the Agency must continue to embrace and harness the opportunities that digital technologies present to our partner communities, and mitigate the risks that are inherent in their use. We must work to make everyone a part of this new digital world. Building on the 2020 Digital Strategy and the body of digital development work that USAID has invested in over the past 28 years, the USAID Digital Policy⁴ will embrace the use of digital technologies more intentionally, and will support and guide USAID’s work for the next decade.

This Policy, and USAID’s approach to achieving it, supports the goals and principles outlined in other key USG policy documents, including the USAID Policy Framework; the USAID AI Action Plan; [the USAID Information Technology Strategic Plan](#); [the USAID Advancing Protection and Care for Children in Adversity Strategy](#); the Department of State-USAID Joint Strategic Plan; [the United States International Cyberspace and Digital Policy Strategy](#); the U.S. Strategy on Women, Peace, and Security; the [Rule of Law](#)

³ World Economic Forum: <https://www.weforum.org/agenda/2022/10/twin-transition-playbook-3-phases-to-accelerate-sustainable-digitization/>

⁴ The USAID Digital Policy is a development and humanitarian assistance policy document focused on the promotion of open, inclusive, secure, and rights-respecting digital ecosystems and the programmatic use of digital technology in the Agency’s development and humanitarian assistance programming, which we commonly refer to as “digital development.” While the Digital Policy primarily focuses on enhancing USAID’s programmatic activities, USAID’s operational components (enterprise architecture and systems) are crucial to executing the Policy. This Policy is a complement to the authorities and responsibilities of these operational entities, including the Bureau for Management (e.g., the Office of the Chief Information Officer [M/CIO], and the Office of Acquisition and Assistance [M/OAA], and the Responsibility, Safeguarding, and Compliance Division [M/MPBP/RSC]); the Office of Human Capital and Talent Management (HCTM); and the Office of the General Counsel (GC), and the Agency’s Regional and Pillar Bureaus will execute it in partnership with them. The implementation of the Strategy will be consistent with all applicable laws, including, but not limited to, the Clinger-Cohen Act of 1996, Electronic Government (eGov) Act of 2002/The Federal Information Security Management Act (FISMA) of 2002, the Federal Information Security Modernization Act of 2014, the Federal Information Technology Acquisition Reform Act of 2015, the Foundations for Evidence-Based Policymaking Act (Evidence Act), and the Grants Oversight and New Efficiency Act.

[Policy; U.S. Government Strategy on International Basic Education 2024 - 2029](#); the 2023 Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence; and the U.S. National Cyber, National Security, and Counterterrorism Strategies.

Background

USAID's programming integrates digital technologies and tools that enable and catalyze development and humanitarian outcomes. USAID's efforts generally fall into two main areas: integrating digital technologies responsibly across the practice of development and humanitarian assistance, and building open, inclusive, secure, and rights-respecting digital ecosystems and the capacity of people everywhere to use technology responsibly. The Agency is working towards a future where digital technology promotes inclusive growth, fosters resilient and democratic societies, advances human rights, and empowers all, including the most vulnerable. We must meaningfully institutionalize the use of secure, sustainable digital technologies into all aspects of our development work, business processes, and outlook.

As early as the 1990s, USAID began investing in the digital transformation of partner countries with the Leland Initiative (1996) to improve internet connectivity in Africa and CSPro (1998), a digital census survey data-collection tool now used in 193 countries. The first digitally-focused team at USAID was created in 2010 to harness the use of mobile money to spur economic advancements. Throughout the 2010s, USAID continued to elevate the importance of digital technologies in the development agenda. Investments in digital programming were incorporated across every sector at the Agency, and were brought to bear during critical moments, such as the 2014 Ebola pandemic in West Africa. USAID also embraced a multilateral approach to digital investments, creating digitally-focused alliances and joint programming partnerships, such as with GSMA on the Connect Women program.

In April 2020, USAID launched the [Digital Strategy](#), charting an Agency-wide vision for development and humanitarian assistance in the world's rapidly evolving digital landscape. It set a path to equip the USAID workforce, empower partners, and shape effective programming that supports partner countries on their digital transformation journeys. The Strategy reinforced USAID's deliberate and holistic commitment to improve development and humanitarian assistance outcomes through the use of digital technologies to strengthen open, inclusive, secure, and rights-respecting digital ecosystems. In doing so, the Strategy outlined how USAID would change the way we did development – including embracing digital technologies by default – in a manner that reflected evidence, local context, and best practice.

During the years of the Strategy implementation, USAID accelerated digital programming. Thirty-seven Missions conducted [Digital Ecosystem Country Assessments](#) (DECAs) and 18 completed digital agriculture assessments to better understand the opportunities and impacts of digital technologies within their programming; five Bureaus and Operating Units completed Digital Strategy Action Plans to guide their digital programming; and the Agency released pivotal policy documents related to digital, including an [AI Action Plan](#), the first-ever [Geospatial Strategy](#) and [Digital Health Vision](#), a [Cybersecurity Primer](#), and a [Gender Digital Divide Primer](#). USAID took a leadership role in multilateral fora, co-creating the [Charter for Digital Public Goods](#) and the [Donor Principles for Human Rights in the Digital Age](#). The Agency provided cybersecurity and rapid response support to 200 partners in 20 countries through the Digital APEX mechanism; supported the creation of the World Health Organization's SMART guidelines to establish normative guidelines that are accurately represented in software systems countries adopt; created a Digital Youth Council to provide a platform for children and youth from around the world to

better access key digital ecosystem stakeholders and decision makers; and at the 2021 Summit for Democracy, USAID announced the [Advancing Digital Democracy Initiative](#), aimed at promoting democratic values and human rights, while also addressing geopolitical competition and the malign use of technology. The White House announced the [Women in the Digital Economy Fund](#) (WiDEF), a joint effort between USAID and the Bill & Melinda Gates Foundation to accelerate progress on closing the gender digital divide. And when Russia invaded Ukraine in 2022, USAID supported the expanded use of the country's mobile application and online government portal, [Diia](#), to support Ukrainians during wartime, such as registering displaced persons and disbursing reimbursements for damaged property. Diia is so successful that, together with USAID, Ukraine is now sharing this technology with other countries.

USAID achieved all of these things (and more) since 2020, despite also facing a worldwide pandemic. When COVID-19 emerged, the world largely shut down and shifted to remote communications to turn the tide of the outbreak. The pandemic reinforced why it was so essential for USAID to embrace digital technologies throughout its programming. Many organizations and governments around the world had a similar experience, leveraging existing capabilities and rapidly adopting new tools to digitize healthcare, education, government services, and business. At the same time, the COVID-19 pandemic highlighted digital divides and inequality, as many individuals and communities found themselves left out of a world that had suddenly gone virtual. Harmful and incorrect information, particularly regarding public health, surged online, dividing societies and weakening pandemic response. Cybercrime became an increasingly profitable industry impacting critical infrastructure key to development, with the annual global cost of these attacks ballooning from \$1.16 trillion in 2019 to \$2.95 trillion in 2020 alone.⁵ Post-pandemic, many of these harms have persisted or grown: the overall cost of cybercrime has skyrocketed to \$8.15 trillion in 2023, and a troubling trend of democratic backsliding around the world has been accelerated by online information manipulation campaigns, often targeting marginalized groups, including LGBTQI+ communities.⁶

Another challenge USAID now faces is a changing geopolitical context, increasingly shaped by strategic competition, emerging technologies, and cyberspace. Because digital technologies are so transformative, building digital ecosystems in developing countries is an area of intense competition. Over the past decade, U.S. strategic competitors have emerged as major sources of technology transformation funding, epitomized by the PRC's 2013 Belt and Road Initiative (BRI) and 2015 Digital Silk Road Initiative. Even with changing economic conditions, the BRI has evolved towards smaller, more targeted projects⁷ with digital infrastructure remaining a major focus. At the same time, reliance on PRC-based funding and infrastructure development has often been accompanied by democratic backsliding and an embrace of digital repression. The Digital Policy will inform USAID's efforts to respond to this challenge with more than rhetoric. A combination of cutting-edge technical support, mobilization of private capital, and an inclusive approach to project co-creation will enable the U.S. to partner with developing countries to advance an affirmative vision for the digital future.

CALL-OUT BOX: Focus Topic: Digital Transformation with Africa

The Digital Transformation with Africa (DTA) initiative aims to expand digital access in Africa, increase commercial engagement between U.S. and African companies, enhance digital skillings across the

⁵ Statista: <https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/>

⁶ Often these online information manipulation campaigns have offline, real-world consequences. For example, in 26 countries, computational propaganda is being used as a tool of information control to suppress fundamental human rights, discredit political opponents, and drown out dissent. The same report found that a handful of sophisticated state actors use computational propaganda for foreign influence operations.

⁷ East Asia Forum: <https://eastasiaforum.org/2022/05/24/making-the-belt-and-road-initiative-small-and-beautiful/>

continent and support best practices in the digital ecosystems. DTA will foster an inclusive, resilient, and secure African digital ecosystem, led by African communities and supported by the U.S. and like-minded allies. Since its launch in 2022, the DTA initiative has mobilized an array of tools and capabilities across the USG and U.S. private sector to advance the initiative’s objectives: increasing access to the digital economy and infrastructure; strengthening human capital; and reinforcing the digital enabling environment.

The past decades of innovation and investment in technology for development and humanitarian work at USAID have already had a tremendous impact. However, technology has only become more pervasive in the lives of USAID’s partners and stakeholders, and more indispensable in achieving USAID’s mission to save lives, reduce poverty, strengthen democratic governance, and help people progress beyond assistance. Technology is always changing (far more rapidly than progress in development is typically made), and USAID must continuously relearn and reimagine our work to keep pace. While USAID has achieved a great deal, thoughtful use of digital technologies needs to be further integrated throughout all programs. To be successful in an increasingly connected age, development is now digital.

Goals

The Digital Policy aims to prepare USAID and our partners around the world to keep pace with rapid change, adopt digital technologies responsibly, embrace democratic values, bolster information integrity and resilience, engage in strategic competition to counter authoritarianism, and decisively accelerate development progress and humanitarian response using digital technologies. The ubiquitous, networked, artificially-intelligent technologies of tomorrow will require us to adapt our ways of working and acting in the world. At the same time, the core concerns of digital development will remain unchanged: bridging inequities, broadening inclusion, protecting human rights, and safeguarding human dignity through the incorporation of sound data governance and cybersecurity practices in an era of digital transformation.

As such, the Digital Policy will pursue three key goals:

1. **BUILD:** Propel development and humanitarian outcomes through an infrastructural approach to digital technology and services.
2. **TRANSFORM:** Evolve USAID’s digital approach through proactive improvement of our knowledge, skills, policies, and technology.
3. **PROTECT:** Promote safety, security, and fairness in USAID programming and across the broader digital context.

BUILD: Propel development and humanitarian outcomes through an infrastructural approach to digital technology and services

Going forward, digital technologies and services will permeate existing economic, social, and cultural systems to the extent that digital development will become a default mode of working – not a false choice between “digital” and “development.” In some sectors, the digital development community has already moved to an architecture-driven approach with a focus on mature applications and interoperable data systems. Yet, there are still too many instances of unsustainable pilots in development and humanitarian programming. Over the period of the Digital Policy, our programs will mature to embrace integrated, interoperable approaches in all sectors. While many technology actors pursue a vision of unified “killer apps” with massive scale and global reach, this approach often fails marginalized

communities. USAID’s technology approach will be grounded in local realities, leveraging the experience and perspectives of local actors to build and deploy technology that works in context. Leveraging innovations from the private sector in new and creative ways can help us to accelerate development outcomes. A focus on open standards, interoperability, and open source (where appropriate) will help us to place the proper emphasis on architectures, processes, and systems – not unsustainable pilots and flashy mobile applications.

USAID will:

- Look beyond technology to holistic investments in the people and processes needed for positive development impact across sectors.
- Apply USAID’s expertise in sectors including health, agriculture, education, gender, child protection, peacebuilding, climate, disaster assistance, and locally-led development to build digital tools that strengthen existing systems and institutions.
- Continue to support and leverage global goods, digital public goods, and digital public infrastructure and promote innovation that enhances and builds on these fundamental platforms.
- Work with the designers of digital platforms, tools, and services to foster inclusion by tailoring their offerings for marginalized and isolated populations including rural communities; racial, ethnic, religious, and linguistic minorities; LGBTQI+ individuals; and persons with disabilities.
- Strengthen the capacity of local business owners, content creators, activists, and technologists to advance digital innovation.
- Partner with local innovators to build the data resources, workforce, and computational infrastructure needed for locally-appropriate AI applications
- Support businesses and facilitate trade by promoting good regulatory practices to support open, transparent, and accountable regulatory frameworks.
- Advance U.S. national security by strengthening open, inclusive, and rights-respecting digital ecosystems.

CALL-OUT BOX: Focus Topic: Artificial Intelligence (AI)

USAID/India’s Transformative Research and AI Capacity for Elimination of TB (TRACE-TB) activity exemplifies this architecture-led approach to digital development programming. The project was implemented by Wadhvani AI, a Mumbai-based technology nonprofit, in partnership with Nikshay, the Indian Ministry of Health’s system for tuberculosis case management. The partnership with Nikshay offered nationally-representative data and a clear path to integration with existing public health systems, while Wadhvani AI offered innovative new technology approaches. Rather than just “making an app”, TRACE-TB took a broad-based approach to reforming and streamlining data systems and creating a pipeline of AI applications that would build on digital public infrastructure used in India’s health system, rather than a series of short-lived pilots.

TRANSFORM: Evolve USAID’s digital approach through proactive improvement of our knowledge, skills, policies, and technology

Digital transformation involves mutually-reinforcing elements of workforce training, technology application, policy reform, and thought leadership. In the past, USAID’s digital transformation efforts have focused on upskilling our workforce through dedicated training and hiring specialists, such as Digital Development Advisors. In the next stage of USAID’s digital transformation, we will continue these efforts while enhancing our organizational capacity to act as a high-value partner, effectively supporting the

digital journeys of governments, civil society, and the private sector. USAID will emphasize accountability and transparency, working with external thought partners to benchmark and track progress and regularly sharing our status and future plans with our workforce, host-country partners, and the public. We will identify key areas of opportunity and ally with host-country governments, local organizations, civil society actors, academic institutions, and private enterprises who share our vision of an inclusive, equitable, and just digital future. We can make use of the innovation capacity of our own staff by encouraging, identifying, and scaling new approaches that reduce burdens and improve our work. USAID staff will grow in their capacity for participatory and human-centered design (HCD), as they work to strengthen digital development capacity across a wide range of different partners. Becoming a stronger partner will require building systems, safeguards, and culture that embody the advice we provide to others.

CALL-OUT BOX: Focus Topic: Working with the Private Sector

The Alliance for eTrade Development II ("eTrade Alliance") is a Global Development Alliance between USAID and 15 leading private sector partners to support MSME cross-border e-commerce development. The eTrade Alliance works to expand trade and further inclusive growth for micro-, small- and medium-sized enterprises (MSMEs) in developing countries by piloting solutions and models that can help MSMEs engage with ecommerce and conduct digital trade at scale. It co-invests with partners to implement activities that support MSME digital development and contribute to partners' business interests, fostering increased engagement in local ecommerce ecosystems and providing learnings that help companies and public sector stakeholders more effectively implement ecommerce development activities globally. In the policy area, the Alliance's work has ranged from large-scale stakeholder discussions on e-commerce broadly to targeted technical dialogues aimed at specific policy improvements. In 2024, the Alliance led and participated in digital trade policy dialogues and capacity-building efforts for countries negotiating the historic African Continental Free Trade Agreement (AfCFTA) Digital Protocol and the Association of Southeast Asian National (ASEAN) Digital Economy Framework Agreement (DEFA). This combined approach to capacity building and policy reform will be a key piece of USAID's future approach to growing digital economies -- fostering deeper partnerships and building critical guardrails for effective and principled private-sector engagement.

USAID will:

- Build a digital cadre⁸ with a workforce of digitally-fluent development experts that can support upskilling across the Agency to use technology responsibly and effectively.
- Invest in our workforce's capabilities to design and manage digital programming through peer-to-peer connections, executive fellowships, and training opportunities.
- Prioritize the creation of new roles for technology experts at USAID so that we are at the cutting-edge of technology use for development objectives.
- Develop tools and metrics to understand strengths and gaps in USAID's digital transformation, including a system for tracking digital activities across the Agency.
- Continuously formulate and update plans to leverage strengths and improve areas of weakness.
- Apply particular care to the deployment of technology in humanitarian contexts, where privacy and security concerns are often more acute.
- Work with humanitarian professionals both within the Agency and without to improve coordination and collaborate on the uses of digital technology in crisis response.

⁸ [Link to internal Digital Cadre page]

- Leverage USAID’s interagency and international development policy leadership to advance U.S. national security and safeguard an open, inclusive, secure, and trustworthy internet.
- Support partner governments and local and international fora in the development of policies, strategies, and regulations around technology areas such as AI, XR, and IoT.
- Work with governments and telecommunications providers to improve access and affordability and close digital divides related to gender, geography, disability, age, and other societal inequities.
- Use research and assessments as an opportunity to collaborate and amplify the voices of local partners.
- Mobilize open innovation and local technology talent to drive results in USAID’s key strategic priority areas (climate, health, humanitarian assistance, etc.).

CALL-OUT BOX: Focus Topic: Geostrategic Competition

As countries around the world seek to build much-needed digital infrastructure, there are growing concerns that the government of the PRC is distorting markets to advantage PRC-based hardware, software, and services suppliers, hampering competition and innovation and compromising the security of suppliers.

The Promoting American Approaches to ICT Policy and Regulation (ProICT) activity, under the interagency Digital Connectivity and Cybersecurity Partnership (DCCP), provides technical assistance and capacity-building to help developing country governments establish ICT policy and regulatory frameworks that will enable open, secure, interoperable, and reliable digital ecosystems. In Colombia, in the wake of an early-2023 DCCP/CLDP interagency workshop regarding trusted vendor requirements and after months of DCCP/ProICT engagement with the GOC on a number of spectrum policy issues, Colombia held its first successful 5G spectrum auction. The auction attracted bids totalling \$380 million from four private operators. These spectrum licenses are anticipated to open the door for large-scale private-sector 5G deployment in Colombia and attract an estimated \$28 billion in investment over the next 10 years. ProICT’s ability to build on existing dialogues and nimbly respond to the needs of Colombian regulators have helped position the U.S. as a valued and trusted partner, while allowing Colombian regulators to design and implement an auction that was consistent with Colombian telecommunications law. USAID Mission staff played an active role in designing and coordinating delivery of critical spectrum policy expertise. This pattern of both building and leveraging the knowledge, skills, and professional connections of USAID Mission-based digital experts is both an advantage and a benefit of the ProICT approach.

PROTECT: Promote safety, security and fairness in USAID programming and across the broader digital context

Not all impacts of digital technology are good. USAID’s digital programs have demonstrated our ability to mitigate digital-related harms including mental health impacts, cybercrime, and technology-facilitated gender-based violence (TFGBV). Going forward, our technology approach will evolve beyond a focus on programs, building a culture of equity, inclusion, and risk management. Digital harms exist on a spectrum that includes physical threats, and require attention to intersecting patterns of violence, repression, and social exclusion. Many of these risks can be exploited to undermine the stability and security of our partner countries, particularly through threats to critical infrastructure. Children, youth, and women in all their diversity are exposed to heightened risks of digital harm and require dedicated focus. Mitigating

these risks cannot be an afterthought -- as development becomes more digital, every activity will need to advance an affirmative vision of safe, secure, and rights-respecting technology.

CALL-OUT BOX: Focus Topic: Information Integrity and Resilience

In Indonesia, USAID's Media Literacy for New Digital Arrivals activity aims to improve digital literacy among Indonesians who are coming online for the first time. Part of the project's success has come from its deep engagement with local stakeholders and content creators, including by producing videos in consultation with Indonesian digital literacy experts and collaborating with local organizations to share best practices for strengthening information integrity and resilience. Another key tool in strengthening the information environment online has been the Misinformation Early Warning System, a cutting-edge AI tool that is used to identify altered and manipulated online content. Looking ahead, initiatives such as the Media Literacy for New Digital Arrivals can help us strengthen the digital ecosystem and the integrity of the information landscape across all sectors of development.

USAID will:

- Strengthen U.S. national security by building the cyber resilience of partner governments through safeguarding measures, cybersecurity and risk mitigation.
- Work with local organizations, civil society, donors, and partner governments to address information manipulation and bolster healthy information ecosystems.
- Leverage tools such as the NIST AI Risk Management Framework to ensure that USAID's investments in AI and other new technologies align with our commitment to respect human rights and safeguard all people.
- Work with Indigenous and other communities to develop resilient and forward-leaning models of data ownership that recognize the value of traditional knowledge and share its benefits equitably.
- Ensure partner compliance with existing requirements related to safeguarding participants and their communities from harm, and support capacity-building so that partners are better able to prevent, detect, and respond to incidents of digital harm.
- Complement our partnerships with the private sector with robust attention to consumer protection.
- Provide targeted training for journalists, human rights defenders, and others working in contexts with a high risk of malicious cyber activity, including the misuse of commercial spyware.
- Partner with local organizations to address individual-level harms such as TFGBV, mental health impacts⁹, online scams, and privacy breaches.

CALL-OUT BOX: Focus Topic: Information Integrity and COVID-19

In countries around the world, the COVID-19 pandemic was accompanied by an "infodemic" - an overwhelming influx of accurate and inaccurate information. USAID/Bangladesh responded to this challenge through the Bangladesh Digital Ecosystem Activity (BDEA) for COVID-19 Rapid Response. USAID partnered with BRAC to strengthen the digital space to provide reliable and accurate information for the Bangladeshi public. Through this activity, BRAC developed a digital application to identify rumors that were circulating among the general public, and created and implemented a mass communication campaign to counteract those rumors. For example, misleading online rumors claimed that COVID-19 could be prevented by regularly rubbing saline in the nose or applying alcohol all over the body. A social media campaign and offline activities were able to reach more than 44 million

⁹ USAID Mental Health guidance: <https://www.usaid.gov/inclusivedevelopment/mental-health>

Bangladeshis with science-based health messages designed to counter common narratives. This activity is an example of how information integrity and resilience can be a key part of development programming in many other sectors.

Principles

The principles laid out in this Policy will drive decision-making at USAID in support of the vision that digital transformation must enable well-being for all. Through these principles, USAID reaffirms the values of established principles that USAID has endorsed.

CALL OUT BOX: Principles USAID has Endorsed:

- [Principles for Digital Development](#)
- [Principles for Donor Alignment in Digital Health](#)
- [Digital ID Principles](#)
- [Donor Principles for Human Rights in the Digital Age](#)
- Digital Democracy Principles

To achieve the Digital Policy vision and goals, USAID will operate by the following Digital Policy principles:

1. **Understand the Digital Ecosystem**
2. **Put People First and Respect Human Rights**
3. **Strengthen Local Digital Capacity, Infrastructure, and Partnerships**
4. **Embrace Innovation and Adaptation**

UNDERSTAND THE DIGITAL ECOSYSTEM

For USAID to successfully address development challenges in today's world, the Agency must understand each country and region's digital ecosystems, and the unique political, social, cultural, economic, and environmental conditions that shape them. Understanding the digital ecosystem helps us plan how to reach development goals and helps us prevent unintended consequences in our programming.¹⁰ The history of development is littered with wasteful and sometimes catastrophic results of technology deployment in which donors, program designers, and technologists have ignored the local context. It is worth investing the time to understand local conditions, including national strategies; supply and demand-side constraints; and the knowledge, experiences, challenges, and capabilities of local actors. It means approaching local stakeholders as full partners and integrating their priorities into our own.

CALL-OUT BOX: DECA Impacts

The DECA is a useful tool that helps Missions understand the state of the local digital ecosystem, as well as identifying some opportunities for Missions to integrate digital technologies into their programming to create better outcomes for their communities. In Colombia, eight months after receiving a draft version of their DECA report, USAID had started to apply 8 of the 12 recommendations. The Mission included digital as a cross-cutting theme in their CDCS (Country

¹⁰ Principles for Digital Development: <https://digitalprinciples.org/>

Development Cooperation Strategy) and is focusing on digital as an integrated approach. One example is the recommendation to "promote digital security for civil society"; the Mission began working with Digital APEX¹¹ which supported training and cybersecurity assessments for USAID/Colombia Implementing Partners.

Understanding the digital ecosystem also requires being knowledgeable about how the larger global geopolitical context influences local conditions. Global influences can include standards and best practices, as well as harmful crossborder influences from criminals or digital authoritarians such as hacking, ransomware, and information manipulation. A deep understanding of digital ecosystems – and the factors that shape them – will be key to USAID’s ability to make informed and strategic choices, partner wisely, and respond to the needs of the people and communities we support.

USAID will fulfill this principle by:

1. Understanding and incorporating local actors’ priorities, visions, and strategies into our strategies and programming to draw upon their knowledge and evidence.
2. Investing in assessments such as the Digital Ecosystem Country Assessments (DECAs), sectoral assessments, and issue-specific assessments (such as cybersecurity or information manipulation) to understand the context for digital technologies in countries where we work and incorporating findings into our work. This includes investing in evidence that can be reused by multiple stakeholders, when possible.
3. Analyzing the impact of the wider geopolitical context on local digital programming by using a political economy lens to understand the motivations, incentives, and constraints of global actors.

PUT PEOPLE FIRST AND RESPECT HUMAN RIGHTS

USAID supports digital transformation that puts *people* first. Adopting new technologies without addressing existing power structures entrenches the status quo, often further harming the most marginalized. Careless digitalization can negatively impact economies, livelihoods, social structures, the environment, and democratic institutions. As technology advances, so does the risk of cybersecurity attacks, the challenge of information integrity, and the complexity and scope of digital threats. USAID will place “do no harm” principles and respect for people’s dignity and human rights at the forefront of the design and management of digital services and the governance of data.

People should be placed at the heart of the design and governance of digital technologies and data. This goes beyond consulting with the target audience expected to make use of a system (the “users”) during the design phase¹². It involves considering *whose* problems are being prioritized in the first place – and whose are neglected. Technology discussions often privilege the perspectives of those who already have power at the expense of those who are marginalized due to their gender identity, age, marital status, class, ethnicity, race, disability status, geographic location, or sexual orientation. Exclusion can be even more acute for individuals who experience intersecting marginalized identities and overlapping inequities.¹³ USAID recognizes the value of integrating diverse perspectives in digital programming. The people who will use or be affected by a technology policy, solution, or system should be engaged

¹¹ For more information on Digital APEX, visit: <https://www.usaid.gov/digital-development/cybersecurity>

¹² This is often referred to as human centered (or user centered) design and is a necessary – but not sufficient – part of implementing new technology.

¹³ See USAID/REFS’ Intersectional Identities Digital Design Toolkit for more resources:

<https://www.athenainfonomics.com/resources/inclusive-digital-design-toolkit-practical-guidance-for-feed-the-future-activities>

throughout the processes of design, deployment, and governance. Technology and data should be applied and managed in a manner that is open, sustainable, secure, and respectful of democratic values and human rights.¹⁴

Digital technologies have been misused to undermine human rights protections and democratic institutions, processes, and norms. These range from individual violations such as TFGBV, doxxing, and misuse of commercial spyware to systemic abuses such as surveillance, information manipulation, and the disruption of essential services through ransomware attacks. Harms have been acutely felt by those in the Global Majority, and especially persons in vulnerable situations¹⁵ who have limited influence over how decisions are made about technologies' development, deployment, governance, and use.¹⁶ These harms can be perpetrated by many entities: from malicious individuals, to organized criminal groups, to nation-state competitors. USAID must be prepared to address and mitigate the consequences of strategic rivals employing technology tools to deepen polarization and undermine democracies. USAID is committed to taking a proactive approach to understand risks associated with technology use and address them by encouraging the development of open, inclusive, secure, and rights-respecting digital ecosystems.

USAID has a variety of options to address these threats. One (as detailed above in the "PROTECT" goal) is to promote safety, security, and fairness in all our digital development and humanitarian programming, and work to enshrine these principles in development practice. By advancing an affirmative vision of open, inclusive, secure, and rights-respecting digital ecosystems, we can shrink the space within which malign actors can operate. Consultation with local stakeholders can help reduce the potential for unintended harm resulting from our development and humanitarian work. We can work with partners to make systems secure by design, mitigate bias, protect individuals' data and privacy, and plan for sustainable maintenance and security after project completion. Throughout any project's lifecycle, USAID and our partners should monitor for and address unintended negative consequences. Beyond our own programs, we can work with partner governments to establish legal and regulatory frameworks that support data protection, digital democracy, and human rights.

USAID will fulfill this principle by:

1. Engaging communities and civil society organizations that will be impacted by our programming in the design, implementation, and evaluation of digital initiatives. Participatory approaches are key for surfacing local knowledge, concerns, and priorities to inform risk mitigation strategies.
2. Elevating the lived experience of individuals and embracing the concept of "nothing about us, without us" by engaging marginalized and underrepresented communities as we endeavor to close digital divides and promote dignity and well-being for all.
3. Leveraging our digital diplomacy role to work with partners, including private sector technology companies, to embrace rights-respecting and safety-focused designs. This will necessarily include working with partners to advance privacy, cybersecurity, safety, and fairness, in line with existing USAID guidance. At times, this may also mean not collecting monitoring data that can put people at risk.¹⁷

¹⁴ In accordance with responsible data use and data governance, open data may not be possible in certain contexts. A responsible approach to data governance is one that addresses the underlying values driving data governance decisions—such as an individual's right to privacy—as well as broader commitments to inclusion, participation, and transparency. (USAID's Responsible Data Governance for Digital Development - add link in design)

¹⁵ Examples of persons in vulnerable situations can include: children and youth, women and girls, persons with disabilities, LGBTQI+ individuals, religious, ethnic, racial, and linguistic minorities, Indigenous peoples, human rights activists and other underrepresented groups.

¹⁶ From the Donor Principles for Human Rights in the Digital Age

¹⁷ Considerations for Using Data Responsibly at USAID: <https://www.usaid.gov/sites/default/files/2023-03/USAID-UsingDataResponsibly.pdf>

4. Integrating safeguarding measures and human-rights approaches into digitally-enabled programming and strengthening staff capacity to effectively identify and address human rights risks in the digital age. This process will allow us to assess the impact of new technology systems on human rights and democratic institutions, and build the capacity of partner governments to conduct technology risk assessments, including the implications from use of products from digital authoritarians.

STRENGTHEN LOCAL DIGITAL CAPACITY, INFRASTRUCTURE, AND PARTNERSHIPS

As USAID works to improve and reinforce digital ecosystems, several ingredients are key. First, our investments should be designed to improve local capacity (human and institutional) to effectively govern, manage, and use digital technologies and data systems.¹⁸ USAID will think beyond sectoral silos to focus on strengthening the system as a whole, including foundational aspects of technical standards and good regulatory practices.

A second key aspect of ecosystem strengthening is attention to infrastructure. As described in the “BUILD” goal, an infrastructural approach is about more than just technology – it requires investment in people and processes, with an eye to integration, interoperability, and inclusion.

CALL-OUT BOX: Focus Topic: Digital Public Infrastructure

Ukraine's Diia (Дія) app is widely hailed as an example of effective government services in the digital age. Diia is an implementation of Ukraine's "State in the Smartphone" policy initiative, supported through a joint USAID-UKAid activity, Transparency and Accountability in Public Administration and Services (TAPAS), which seeks to reduce corruption through e-procurement, open data, and the use of online services. Diia currently provides over 20 million Ukrainians with one-stop access to more than 120 government services such as paying taxes, registering businesses, applying for support to rebuild damaged homes, and even displaying a valid passport on their phones.

Portals like Diia do not appear overnight. The app sits on top of a range of long-term strategic investments in digitalization across a wide number of government services, processes and people. More than just an app, Diia is the user-focused layer of robust digital public infrastructure, which includes long-term investments in foundational digital infrastructure such as digital identity, digital payments and mobile banking, cross-border data exchange, cybersecurity and data privacy, and records management. As USAID aims to help our partner governments deliver services more equitably and effectively, the same sorts of foundational "data plumbing" will be essential for success.

The third major piece of USAID's ecosystem-strengthening approach is partnerships. As in any other area of development, USAID cannot make real progress alone. With strong and inclusive partnerships, clear standards, effective governance, and investment in both digital public goods (DPGs) and the distinct paths toward digital transformation in each of our partner countries, we have the potential to harness emerging technologies, such as AI, to revolutionize digital health care, revitalize and build the resilience of economies, optimize disaster response, and dramatically improve people's lives and livelihoods in many other ways. To successfully cultivate ecosystems that do not rely on foreign assistance, USAID must elevate the practice of digital diplomacy, deepening engagements across the U.S. Government and with other donors, responsible private sector companies, and other relevant organizations. USAID will cultivate current partnerships and build new partnerships around open, inclusive, secure, and

¹⁸ Language inspired from Digital Health Vision technical guidance note 1: https://www.usaid.gov/sites/default/files/2023-06/FINAL_USAID_DHV_TGN1_508_06232023.pdf.

rights-respecting digital ecosystems. This will include pursuing adoption and deployment of secure digital infrastructure and fostering stronger partner and country technical capacities and technological capabilities for digital transformation. Our success will be greatest when we approach local actors as partners, not beneficiaries, pooling resources and expertise to advance a locally-led agenda. USAID will rely on the advice of local stakeholders who are often the best guides to what skills or resources, if any, are required from external partners, and what groups are the best collaborators. We will work to create more equitable power dynamics in our partnerships with local actors and between implementing partners – whether local or international – and communities, to support power shifting and sharing.

Engaging in responsible partnerships requires working effectively with a wide range of partners including governments, local technologists and innovators, global and national businesses, advocates and civil society organizations, other donors, local and global private sector actors, and academics. It also involves working across different scales, from local town halls to multilateral convenings.

USAID will fulfill this principle by:

1. Investing in local capabilities to design and manage digital technologies and their regulatory systems (including those connected to technical standards) through peer-to-peer connections, in-service training and skill building, and embedded technical assistance.
2. Drawing on USAID's thought leadership and digital diplomacy capabilities to shape technology's global governance, including standards setting and safeguarding, by deepening engagement in key multilateral and international fora. Supporting local stakeholders to increase their influence in technical, engineering, and standards bodies will better ensure that technical standards reflect human rights and democratic values.¹⁹
3. Recognizing, mapping, and planning holistically with local systems to involve the private sector, community organizations, youth organizations, faith-based organizations, governments, other donors, educational institutions, and people in digital initiatives.

EMBRACE INNOVATION AND ADAPTATION

Digital transformation is changing lives around the world, and USAID needs to evolve as well. This principle promotes a spirit of innovation, while encouraging a responsible approach to deploying technology. There are multiple ways to pursue innovation, and while USAID's development and humanitarian mission calls for big ideas and bold new approaches, it also requires us to prioritize intentionality over speed. Rather than "moving fast and breaking things," USAID's approach to innovation emphasizes bringing in new people, ideas, and ways of solving development challenges, and then using evidence to identify and refine the most promising solutions to continually find ways to reach development objectives more effectively and sustainably. We will work with partners to discern what type of technology is appropriate in a given context, how it can prioritize locally-led efforts and strengthen existing systems, and what type of future our technology interventions are encouraging.

Innovation can involve new technology, but just as often it means creatively applying existing technologies. USAID will continue to encourage new ideas and approaches to addressing development challenges as technology continues to evolve, especially in the adaptation of those technologies to local stakeholder contexts. We will support partners to build, reuse, improve, and strengthen the systems and data that help people create positive impacts. As we work to strengthen USAID's internal digital capacity, we will unlock the innovative potential of our own staff through training, upskilling, and the removal of

¹⁹ Examples include the International Telecommunication Union (ITU), the Internet Governance Forum (IGF), Internet Corporation for Assigned Names and Numbers (ICANN), Internet Engineering Task Force (IETF), Telecommunications Industry Association, 3rd Generation Partnership Project, American National Standards Institute, and the Institute of Electrical and Electronics Engineers (IEEE).

administrative barriers to innovation. Responsible innovation will require investments in digital literacy and capacity strengthening of local stakeholders, so that they too can take advantage of the positive impacts of digital technologies.

CALL-OUT BOX: Focus Topic: Innovation in Artificial Intelligence

AI has the potential for transformative impact in many areas of development, and recent advances have put AI tool development within reach for many of USAID's partners. Consistent with the overall U.S. government approach, USAID is actively encouraging innovation in AI.²⁰ At the same time, we must manage risks that can stem from reckless adoption and inflated expectations. Working together with partners, USAID will leverage a combination of technological acumen and development expertise to promote AI innovation at a safe speed and in a pro-development direction. Continuous adaptation will help us to learn from deployment experiences and research advances, and adjust our approach accordingly. A balanced approach, grounded in the *USAID AI Action Plan*,²¹ the *AI Risk Management Framework*,²² and evolving U.S. policy around AI, will emphasize human rights impact analysis, careful monitoring of performance and accuracy, and strengthening ecosystems for responsible innovation.

Digital ecosystems are constantly changing; USAID and our partners must learn, adapt, and check our assumptions on an ongoing basis. USAID will embrace intentional adaptation to these changes through a commitment to learning. We will continuously improve our work through evaluations of our programs and upskilling of our staff. Intentional learning and adaptation will also help us to be responsive to the needs of our partner countries as they navigate the changing technology landscape.

Data and knowledge management are at the core of intentional adaptation. We will collect the data we need to learn from our digital development experiences, and share findings across USAID, the U.S. government, and the broader development community.

USAID will fulfill this principle by:

1. Removing barriers to innovation by reducing unnecessary administrative burdens on our partners and staff. Simplified and accessible procurement and partnership models will enable us to work with a wider range of innovators and take smart bets on new ideas. Flexible planning can free up the innovation capacity of our partners through intentional adaptation and agile activity management.
2. Erecting clear guardrails that distinguish exploratory, experimental work from deployment and essential service delivery. Experiments are a critical tool for evidence generation, but we will always approach affected populations as partners and co-investigators, not test subjects.
3. Doing our best to understand and knowledgeably assess the hype around new and emerging technologies. Without shying away from potential innovations, we should avoid both extremes of blindly adopting or uncritically dismissing new technologies in favor of an approach that is patient, empirical, and risk-aware.

²⁰ Executive Order 14110 "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence": <https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence>

²¹ USAID AI Action Plan: <https://www.usaid.gov/digital-development/artificial-intelligence-action-plan/>

²² NIST AI Risk Management Framework: <https://www.nist.gov/itl/ai-risk-management-framework>

Learning Agenda

To support the rapid development and adoption of digital technology, USAID will employ a continuous learning agenda for its Digital Policy to adapt implementation, keep the policy current, and ensure its implementation is reflective of actual conditions as documented in annual and other reporting. In doing so it asks an overarching learning question based on the Digital Policy Vision Statement:

How can USAID support global actors, partner countries, and local leaders in creating “a world where open, secure, and rights-respecting digital ecosystems enable people everywhere to thrive”?

LINKAGES TO THE USAID AGENCY-WIDE LEARNING AGENDA

USAID’s Digital Policy Learning Agenda addresses the operational learning needs of Missions, Bureaus, and Independent Offices as they respond to the [USAID Agency Learning Agenda](#) and report their digital activities. Missions are encouraged to use a variety of research and evaluation methods such as user feedback, developmental evaluation, AI-powered analysis, impact evaluation, and cost- effectiveness analysis to adapt digital technology and cyber tools and approaches to operating unit needs and to meet our vision. Furthermore, the Agency Learning Agenda serves as a link between the Digital Policy and other whole-of-agency policies such as Localization, Gender, and others.

EVIDENCE GAPS

The Digital Policy Learning Agenda links to the Digital Policy goals and identifies priority evidence gaps. Addressing these gaps will help us understand how to achieve the Digital Policy Vision. The following evidence gaps are starting points rather than exhaustive. USAID will use evidence gathered through research and learning activities to design and adaptively manage USAID activities, while contributing to the broader knowledge and evidence bases on digital development.

GOAL	EVIDENCE GAPS
<p>BUILD: Propel development and humanitarian outcomes through an infrastructural approach to digital technology and services.</p>	<p>How can USAID best facilitate open, interoperable approaches to digital technology and services that benefit local communities, especially marginalized groups?</p> <p>What elements of the enabling environment enhance the purposeful construction of digital ecosystems that align with USAID and partner values and capabilities?</p>
<p>TRANSFORM: Evolve USAID’s digital approach through proactive improvement of our knowledge, skills, policies, and technology.</p>	<p>What is the best way for USAID to identify, train, and equip diverse adaptive-management oriented staff to keep pace with the scale and pace of change in digital technology and cybersecurity?</p> <p>What adaptations are needed to allow staff to address the most critical digital needs of stakeholders – civil society organizations, implementing partners, and other groups, especially those least empowered?</p>

<p>PROTECT: Promote safety, security, and fairness in USAID programming and across the broader digital context.</p>	<p>How does USAID’s commitment to democratic and inclusive governance serve as a comparative advantage relative to rivals and how does this commitment contribute to desired outcomes for digital development and economic benefit?</p>
--	---

LEARNING AGENDA ACTIVITY GUIDANCE

USAID Digital Policy Learning Agenda offers guidance for learning over the lifespan of the policy to address our evidence gaps, unintended consequences, and progress. USAID will:

- Use existing learning tools, indicators, and methods as appropriate and adapt these as needed. Embrace innovative tools such as AI and other approaches when these enhance organizational learning and adaptation;
- Harmonize metrics and goals with partners and other stakeholders to build a broad knowledge base that describes and analyzes national, regional, and global patterns of digital technology as part of development and humanitarian efforts; and,
- Commit to rigorous and continuous evaluation and assessment, including an externally executed mid-course policy assessment supported by frequent, low-lift portfolio reviews.

Policy into Practice

Requirements and recommendations for the Digital Policy focus on three areas: programs (development outcomes), people (capacity and skills), and learning (evidence).

PROGRAMS

Digital Assessments – Requirement:

- **Missions, Regionals Missions, and Country Offices:** Missions, Regional Missions, and Country Offices need a comprehensive understanding of relevant aspects of the digital ecosystem as it relates to their programming. Missions and Country Offices that have not already conducted a Digital Ecosystem Country Assessments (DECA)²³ or Digital Ecosystem Regional Assessment (DERA) must complete one within 18 months from the date the Policy is released and integrate DECA and DERA findings and recommendations into their R/CDCSs, Project Development Documents and Activity Approval Memoranda. DECA and DERAs can provide the evidence base to formulate digital strategies for the Mission and guide projects and activities. It is encouraged that Missions, Regional Missions, and Country Offices update their assessments periodically to remain informed on changes in their digital ecosystem.
 - **Recommendation:** Missions, Regional Missions, and Country Offices with dedicated sectoral funding are encouraged to undertake sectoral digital assessments, such as in digital agriculture or digital health, to better design programming to advance the digital ecosystem in these areas.

²³ The DECA Toolkit is designed to help guide Missions to conduct a DECA with an implementer of their choice: <https://www.usaid.gov/digital-development/deca-toolkit>

- **Washington Pillar and Regional Bureaus:** Pillar and Regional Bureaus must prepare Digital Action Plans²⁴ with the participation of relevant Regional Platforms, Missions, and Pillar Bureaus that articulate regional priorities and opportunities. Technical Centers in the IPI Bureau must also develop Digital Action Plans for core technical areas that would benefit from an in-depth analysis of sector-specific technology and digital approaches. These Action Plans must be completed within 18 months from the date the Policy is released.
 - **Recommendation:** Bilateral programs should refer to these regional and Pillar Digital Action Plans as they develop their own strategies and project/activity designs while Regional and Pillar Bureaus should refer to relevant country-level DECAs and DERAs.

Mission Orders – Recommendation: All Missions, Regional Missions, and Country Offices are encouraged to adopt or update a Mission Order (MO) on Digital Development within one year of the release of this policy and every five years thereafter.²⁵

PEOPLE

Digital-focused Positions – Requirement

- **Missions, Regionals Missions, and Country Offices:** Priority Missions, Regional Missions, and Country Offices must hire, contract, or appoint a **Digital Development Advisor (DDA)** or a **Digital Specialist** with a majority allocation of their overall time (i.e., level of effort [LOE]) dedicated to work on digital and cybersecurity programming,²⁶ determined by their annual program budget. DDAs and Digital Specialists must have the necessary technical skills, competencies, and experience, with responsibilities explicitly included in their job descriptions. *(NOTE: Priority Missions will have 18 months from the date the Policy is released to meet the LOE requirements for Digital Advisors. To alleviate the administrative burden of every Mission determining the roles, responsibilities, and qualifications of DDAs, HCTM has pre-classified three [Standard Position Descriptions](#) for DDAs at the FSN-10, -11, and -12 levels, which are available on ProgramNet and on HCTMs SPD page with a guidance document. OUs will have three years from the date the Policy is released to meet the minimum LOE requirements for DDAs and Digital Specialists.)*
 - **Recommendation:** It is recommended that Missions, Regional Missions, and Country Offices not included on the priority list hire, contract, or appoint a Digital Development Advisor (DDA) or a Digital Specialist with an allocation of their overall time (i.e., level of effort [LOE]) dedicated to work on digital and cybersecurity programming, determined by their annual program budget.
- **Washington Pillar and Regional Bureaus:** All Pillar and Regional Bureaus must hire, contract, or appoint a Digital Advisor with a majority allocation of their overall time (i.e., level of effort [LOE]) dedicated to work on digital and cybersecurity programming,²⁷ tiered by the annual program budget of the Bureau. Digital Advisors can be hired through any hiring mechanism (FSO, CS, ISC, etc). Digital Advisors must have the necessary technical skills, competencies, and experience,

²⁴ The Digital Action Plan Guide is available to support the creation of Digital Action Plans:

<https://my.usaid.gov/IPI/DigitalStrategy/articles/digital-strategy-action-plan-guide>

²⁵ Digital Development Mission Order template is available on ProgramNet:

<https://programnet.usaid.gov/resource/digital-development-mission-order-template>

²⁶ This is different from the role of the EXO and IT support staff, and should not focus on internal Agency systems or those operated on behalf of the agency, which are overseen by M/CIO. This role should be program-focused. It is possible that an IT specialist at a small Mission could serve as a part-time DDA, but the distinction between the two roles still stands. “Digital programming” can refer to general digital programming work, or sector-specific digital programming work, such as digital health.

²⁷ This is different from the role of M/CIO, and should not focus on internal Agency systems, which are overseen by M/CIO. This role should be program-focused.

with responsibilities explicitly included in their job descriptions. (NOTE: OUs will have 18 months from the date the Policy is released to meet the LOE requirements for Digital Advisors. A repository of Position Descriptions in Washington and at Missions can be found on the Digital Cadre page on MyUSAID).²⁸

Policy Implementation Training – Requirement: The Agency workforce, including all hiring and contracting mechanisms, must complete the Digital Policy 101 training course,²⁹ an introductory online course on the role of digital technologies in USAID’s development and humanitarian programming, within two years of the release of this Policy, and new hires within a year of start date.

Digital Competencies³⁰ – Recommendation: In line with existing Executive Orders and National Security Memoranda on USG technology policies, for every OU position and role inclusive of all hiring mechanisms and sectors:

- **Existing Skills** - staff should identify and managers should validate position digital development competencies (baseline data) and manage competencies development progress (performance management);
- **New Skills** - staff should identify OU skills gaps to inform Agency workforce planning and OU hiring justifications; and
- **Positions** - managers should incorporate digital development skills in position descriptions, such as artificial intelligence (AI), data science, cybersecurity, geospatial and other digital development skills to achieve development and humanitarian objectives.

Additional Training – Recommendation

- **Technical Digital Trainings:**³¹ It is recommended that the Agency workforce, including all hiring and contracting mechanisms, complete the Digital Development 101 (in-person or [online](#)), Responsible Artificial Intelligence in International Development,³² Gender Digital Divide, Cybersecurity in Programming, Digital Literacy, and any other sectoral digital training, such as the Digital Health: Planning National Systems course, within three years of the release of this Policy.
- **Additional Training:** Missions, Bureaus, and Independent Offices should incorporate specific content on digital development (or approaches), inclusive of technologies, AI, cybersecurity, and other topics, into broader technical or sectoral training they manage. IPI/ITR/T can provide technical support to MBIOS in this process. It is recommended that all OUs incorporate digital and cybersecurity into training plans annually and to complete learning across diverse topics, such as geospatial, data science, AI, cybersecurity, digital ecosystems, and more to stay current on changing dynamics in digital development and industry technologies impacting development.

LEARNING

GLAAS Tag – Requirement: All Missions, Bureaus, and Independent Offices (MBIOS) must identify obligations made to digital and cybersecurity programming in the Global Acquisition and Assistance System (GLAAS) using the “digital development” tag.

²⁸ Digital Cadre page on MyUSAID: <https://my.usaid.gov/IPI/ITR/Digital/digital-cadre-development>

²⁹ To-be developed upon finalization of this Policy

³⁰ Digital Skills can be added to all positions via Launchpad. Under your profile, select “My Skills”, then “Browse Skills Catalog”. 205 digital skills are available to add to your work profile.

³¹ Additional skills building resources for USAID workforce are available at: Digital Cadre Development Intranet

³² Available through USAID University:

<https://workplace-usaid.csod.com/ui/lms-learning-details/app/event/37dce6f0-fc12-4cfc-9743-7f8a07d68e4d>

Reporting – Requirement: All MBIOs must also attribute funding in each fiscal year to all applicable **OP Plan Key Issues** (“Digital Technology” and “Cyber”). All MBIOs must work with implementing partners to collect data as part of their regular program reporting and report on all applicable standard indicators that cover digital programming and cybersecurity in the OP Plan and annual **Performance Plan and Report (PPR)**.

MEL Indicators – Recommendation: All OUs should adapt targets and indicators for tracking and measuring progress toward the four Policy objectives during strategic planning and project design at all geographic levels. All OUs should develop custom digital and cybersecurity indicators with implementing partners that provide the quality and range of information necessary to thoroughly assess progress and impact of digital technologies on development and humanitarian programming. Furthermore, USAID will explore adopting standard outcome indicators related to digital and cybersecurity.

Conclusion

For nearly 30 years, USAID has been a leader in supporting digital transformation around the world. This policy will now set the course for USAID to continue advancing development and humanitarian outcomes in an ever-accelerating digital age. The Agency will strive to improve our ability to meet the needs of our partner countries, to transform USAID’s digital approach as technology continues to evolve, and protect the communities we serve from harm within these new and evolving contexts. To achieve the Digital Policy vision and goals, USAID is committed to fostering innovative and adaptive approaches to advance open, inclusive, secure, and rights-respecting digital ecosystems in the countries where we work, put people first and respect the human rights of the populations in the countries we work in, and strengthen local digital capacity, infrastructure, and partnerships. Through collaboration with our global partners, continual evolution of our current digital approach, and collective dedication to our mission and vision, we will contribute to a more inclusive digital world for all.

Annex I - Brief History of Digital at USAID

While USAID began investing in digital transformation in the late 1990s, it was the Haiti Earthquake in 2010 that spurred USAID to more intentionally embrace digital technologies by creating the Mobile Money team, the first digitally-focused team in the Agency. During the Haiti response, USAID also began leveraging geospatial analysis to “crisis-map” the impact of the earthquake and determine how best to direct support, as well as the Agency’s first public-private partnership focused exclusively on digital technologies, specifically closing the gender digital divide. Throughout the early 2010s, USAID ramped up investments in digital health and electronic supply chain solutions; put digital tools in the hands of farmers, educators, students and many others; launched the GeoCenter to institutionalize the use of geospatial data at the Agency; supported broadband and mobile network expansions; and created or joined international alliances to advance the adoption of digital technologies in developing countries, such as the Better than Cash Alliance, the E-Trade Alliance, and the Alliance for Affordable Internet.

Throughout the 2010s, USAID continued to elevate the importance of digital technologies in the development agenda, co-creating the [Principles for Digital Development](#) and leading a global endorsement campaign for their adoption, and later partnering with other leading global health funders to create the [Principles for Donor Alignment in Digital Health](#). During the Ebola epidemic in West Africa, the Agency invested heavily in information systems that supported real-time decision making which enabled health workers to respond to the outbreak more effectively.³³ In 2016, USAID co-founded the [Digital Impact Alliance](#) along with the Bill and Melinda Gates Foundation, Sweden’s Sida agency, and the UK’s Foreign, Commonwealth, and Development Office (FCDO). The following year, the Agency also co-founded [Digital Square](#), an organization focused on strengthening country efforts to develop national digital health infrastructure.

Also in the mid-2010s, the GeoCenter launched the YouthMappers program, creating partnerships with universities all over the world to help young people map their communities and use geospatial data to inform local policies. The Agency partnered with GSMA to create the Connect Women program, and later launched the WomenConnect Challenge, working to close the gender digital divide by bringing women and girls online. USAID also launched the [All Children Reading](#) Grand Challenge, which advanced EdTech innovation and research to improve reading outcomes for marginalized children in low-resource contexts. And as the adoption of technology swelled in the late 2010s, the Agency published technical papers on [responsible data](#) use, [digital identity](#), [artificial intelligence](#), and [blockchain](#) use in development, launched the Fall Armyworm Tech Prize, issued a Procurement Executive Bulletin on the use of digital payments in USAID programs, and created the Digital Development Advisors program.

After the USAID Digital Strategy was released in April 2020, the pace of USAID’s investments in technology accelerated. The background section of this Policy documents achievements over the last five years, and establishes the foundation for the next decade of digital programming at USAID.

³³ USAID’s Fighting Ebola with Information report: <https://www.usaid.gov/document/fighting-ebola-information>

Key Terms

ADOPTION: The widespread use of an innovation or technology at the desired scale and sustained by the relevant ecosystem of actors, once that innovation or technology has proven its ability.³⁴

ARCHITECTURE (SYSTEMS): Systems architecture is a conceptual model that defines the structure and behavior of a digital system and its components. A system architecture can include multiple hardware and software elements that interoperate to achieve the system goals.³⁵

ARTIFICIAL INTELLIGENCE (AI): The science and technology of creating intelligent systems. Machine learning (ML) often enables AI systems, which apply data-derived predictions to automate decisions. While ML focuses on learning and prediction, AI applications often create, plan, or do something in the real world.³⁶ Automated decisions might be directly implemented (e.g., in robotics) or suggested to a human decision maker (e.g., product recommendations in online shopping).

BLOCKCHAIN (DISTRIBUTED LEDGER TECHNOLOGY): An example of a distributed ledger technology (DLT), which is a type of shared, peer-to-peer computer database that enables all network participants to agree on a set of facts or events without needing to rely on a single, centralized, or fully trusted intermediary party. Blockchains are the most common form of DLT, and require data on the “chain” to be structured in linked, sequential “blocks.”³⁷

CENSORSHIP: The suppression of free speech by governments or private institutions based on the assumption that said speech is objectionable or offensive. In addition to hard forms of censorship (handed down officially through laws and regulations), soft forms of censorship exist (applied through financial and/or reputational pressure).³⁸

CIVIL SOCIETY ORGANIZATIONS: Organizations including formal non-government organizations (NGOs) as well as formal and informal membership associations (labor unions, business and professional associations, farmers’ organizations and cooperatives, and women’s groups). CSOs articulate and represent the interests of their members, engage in analysis and advocacy, and conduct oversight of government actions and policies.³⁹

CYBER ATTACK: According to NIST, a cyber attack is “an attack, via cyberspace, targeting an enterprise’s use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.”⁴⁰

CYBER THREATS: According to NIST’s Computer Security Resource Center, a cyber threat is “any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of

³⁴ From the IPI/ITR Innovation Division definition.

³⁵ Adapted from Interview Bit, “System Architecture - Detailed Explanation”, June 22, 2023: <https://www.interviewbit.com/blog/system-architecture/>

³⁶ Adapted from Amy Paul, Craig Jolley, and Aubra Anthony, “Reflecting the Past, Shaping the Future: Making AI Work for International Development,” USAID (September 2018): <https://www.usaid.gov/digital-development/machine-learning/AI-ML-in-development/>

³⁷ USAID DECA Toolkit: <https://www.usaid.gov/digital-development/deca-toolkit>

³⁸ Ibid.

³⁹ Ibid.

⁴⁰ USAID Cybersecurity Primer: <https://www.usaid.gov/digital-development/usaid-cybersecurity-primer>

service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.”⁴¹

CYBERCRIME: According to Interpol, cybercrime “refers to crimes against computers and information systems, where the aim is to gain unauthorized access to a device or deny access to a legitimate user.”⁴²

CYBERSECURITY: The prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.⁴³ As the Cybersecurity Strategy of the U.S. Department of Homeland Security (DHS) emphasizes: “Cybersecurity is not an end unto itself, and efforts to mitigate cybersecurity risks must also support international commerce, strengthen international security, and foster free expression and innovation.”⁴⁴

DATA GOVERNANCE: The people, policies, and processes that provide direction, goals, and oversight into how data are used and decisions are made.

DATA MANAGEMENT: The execution of day-to-day management tasks regarding data within an organization. Sometimes also referred to as data processing.⁴⁵

DATA PRIVACY: The right of an individual or group to maintain control over, and the confidentiality of, information about themselves, especially when that intrusion results from undue or illegal gathering and use of data about that individual or group.⁴⁶

DIGITIZATION: The act of converting analog data or documents into digital data or documents.

DIGITALIZATION: The use of digital technologies to change a process or provide value-producing opportunities.

DIGITAL AUTHORITARIANISM: The use of digital information technology by authoritarian regimes to surveil, repress, and manipulate domestic and foreign populations.⁴⁷ This term describes governments that use digital technologies such as social media, AI-powered surveillance systems, and big data collection and analysis capabilities for repression and social control.⁴⁸

DIGITAL DEMOCRACY: A context in which digital technology and data systems are designed, developed, deployed, used, and governed in alignment with human rights and democratic values. This is in opposition to digital authoritarianism or digital repression, where technologies are used to repress, control, censor, and surveil people.⁴⁹

DIGITAL DEVELOPMENT: Development programming focused on building and expanding secure, open,

⁴¹ Ibid.

⁴² Ibid.

⁴³ National Institute of Standards and Technology (NIST), U.S. Department of Commerce “Cybersecurity,” accessed November 2019: <https://csrc.nist.gov/glossary/term/cybersecurity>

⁴⁴ U.S. Department of Homeland Security, Cybersecurity Strategy (2018): <https://www.dhs.gov/publication/dhs-cybersecurity-strategy>

⁴⁵ USAID, [Forthcoming] Responsible Data Governance for Digital Development Reference Sheet, 2024.

⁴⁶ Adapted from NIST Computer Security Resource Center, “Privacy,” accessed December 2019: <https://csrc.nist.gov/glossary/term/privacy>; USAID DECA Toolkit: <https://www.usaid.gov/digital-development/deca-toolkit>

⁴⁷ Brookings: https://www.brookings.edu/wp-content/uploads/2019/08/fp_20190826_digital_authoritarianism_polyakova_meserole.pdf

⁴⁸ Adapted from Geneva Centre for Security Policy:

<https://www.gcsp.ch/publications/digital-authoritarianism-how-digital-technologies-can-empower-authoritarianism-and>; USAID Digital Strategy 2020-2024: <https://www.usaid.gov/digital-development/digital-strategy>

⁴⁹ USAID, [Forthcoming] Democracy, Human Rights and Governance (DRG) Policy, December 2023.

and inclusive country-level digital ecosystems and the programmatic use of digital technology in development and humanitarian assistance.⁵⁰

DIGITAL DIPLOMACY: This term describes the intersection of diplomacy and digital policies. In the context of foreign policy and international development, digital diplomacy is the work done to advance U.S. interests while leveraging digital technologies. An example of digital diplomacy is U.S. investment in a country’s connectivity infrastructure by funding the upgrade from 2G to 5G wireless. Another example is the work the U.S. does to advance democratic regulations of digital technologies in international fora.⁵¹

DIGITAL DIVIDE: The gap between those who have access and can use digital products and services and those who are excluded from them. It often results in, and is simultaneously exacerbated by, low digital literacy, prohibitive access costs, strict social norms, and minimal available or relevant content in local languages. The digital divide often stems from the intersection of gender, economic status, geography, age, and many other factors.⁵²

DIGITAL ECONOMY: The use of digital and internet infrastructure by individuals, businesses, and government(s) to interact with each other, engage in economic activity, and access both digital and non-digital goods and services. As the ecosystem supporting it matures, the digital economy might grow to encompass all sectors of the economy—a transformation driven by both the rise of new services and entrants, as well as backward linkages with the traditional, pre-digital economy. A diverse array of technologies and platforms facilitate activity in the digital economy; however, much activity relies in some measure on the Internet, mobile phones, digital data, and digital payments.⁵³

DIGITAL ECOSYSTEM: The stakeholders, systems, and enabling environment that together empower people and communities to use digital technology to gain access to services, engage with each other, or pursue economic opportunities. A digital ecosystem is conceptually similar to, but broader than, a digital economy. Although certain aspects of the digital ecosystem have country-wide reach, other features differ across geographies or communities. The critical pillars of a digital ecosystem include the following: (1) sound enabling environment and policy commitment; (2) robust and resilient digital infrastructure; (3) capable digital service-providers and workforce (e.g., both public and private institutions); and, (4) empowered end-users of digitally enabled services.⁵⁴

DIGITAL ECOSYSTEM COUNTRY ASSESSMENT: The Digital Ecosystem Country Assessment (DECA), a flagship initiative of the Digital Strategy, identifies opportunities and risks in a country’s digital ecosystem to help the development, design, and implementation of USAID’s strategies, projects, and activities. It informs USAID Missions and other key decision-makers about how to better understand, work with, and support a country’s digital ecosystem.⁵⁵

DIGITAL IDENTITY: The widely accepted Principles on Identification define identity as “a set of attributes that uniquely describes an individual or entity.” Digital identification (ID) systems often require registering individuals onto a computerized database and providing certain credentials (e.g., identifying numbers, cards, digital certificates, etc.) as proof of identity. Government actors can set up these

⁵⁰ USAID Digital Strategy 2020-2024: <https://www.usaid.gov/digital-development/digital-strategy>

⁵¹ Adapted from “The Evolving Landscape of Digital International Relations”, Stratheia Margalla Policy Digest, Dr. Sahibzada Muhammad Usman and Fatime Mehdi, October 26, 2023: <https://stratheia.com/the-evolving-landscape-of-digital-international-relations/#:~:text=At%20its%20core%2C%20digital%20diplomacy%20is%20the,digital%20platforms%20that%20foster%20communication%20and%20collaboration>

⁵² USAID Connectivity Primer: <https://www.usaid.gov/digital-development/connectivity-primer>

⁵³ USAID DECA Toolkit: <https://www.usaid.gov/digital-development/deca-toolkit>

⁵⁴ Ibid.

⁵⁵ USAID Digital Ecosystem Country Assessment (DECA) Factsheet: <https://www.usaid.gov/digital-development/deca-factsheet>

systems to create foundational, national ID programs, or donors or non-governmental organizations (NGOs) for functional purposes to identify beneficiaries, e.g., for humanitarian assistance and service-delivery.⁵⁶ Digital ID is considered a foundational DPI.

DIGITAL LITERACY: The ability to “access, manage, understand, integrate, communicate, evaluate, and create information safely and appropriately through digital devices and networked technologies for participation in economic and social life. This may include competencies that are variously referred to as computer literacy, information and communications technology (ICT) literacy, information literacy, and media literacy.”⁵⁷

DIGITAL PUBLIC GOODS (DPGs): Open source software, open data, open artificial intelligence (AI) models, open standards and open content that adhere to privacy and other international and domestic applicable laws, standards and best practices, do no harm, and help attain the Sustainable Development Goals (SDGs).⁵⁸

DIGITAL PUBLIC GOOD STANDARD: A set of nine indicators maintained by the Digital Public Good Alliance that are used to determine whether or not open-source software, open data, open AI systems, and open content collections are digital public goods. Those meeting the standards criteria are then listed in the DPG Registry.⁵⁹

DIGITAL PUBLIC INFRASTRUCTURE: DPI is an architectural approach for government systems that uses a combination of technology building blocks, governance, and multi-stakeholder engagement to provide foundational digital services available for use by a broad variety of actors. These foundational digital services include, but are not limited to, data exchanges, digital identification, and payments rails that are intended to provide broad public benefit and are open to many different actors and uses. DPI investments are rarely “end to end” solutions but rather essential and reusable building blocks that allow a variety of innovations to be developed faster, cheaper, and safer. A DPI investment is not solely a software investment; it is a digital services solution that may include different software and hardware components as well as the associated governance and community engagement elements required for the public benefit from these investments.⁶⁰

DIGITAL REPRESSION: The intentional use of digital tools and technology to suppress or violate human rights.

DIGITAL REVOLUTION: The Digital Revolution is a term commonly used to describe the development of digital technology, moving from mechanical and analog systems and processes to digital ones. This period encompasses the Information Age (mid-twentieth century to the early twenty-first century) when digital computers and digital record keeping became the norm.

⁵⁶ USAID Digital Strategy 2020-2024: <https://www.usaid.gov/digital-development/digital-strategy>

⁵⁷ Adapted from UNESCO, “A Global Framework of Reference on Digital Literacy Skills for Indicator 4.4.2,” (June 2018): <http://uis.unesco.org/sites/default/files/documents/ip51-global-framework-reference-digital-literacy-skills-2018-en.pdf>

⁵⁸ Digital Public Goods Alliance (DPGA), Roadmap to Digital Cooperation: https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf

⁵⁹ Digital Public Goods Alliance: <https://digitalpublicgoods.net/digital-public-goods/>

⁶⁰ UNDP: <https://www.undp.org/digital/digital-public-infrastructure#:~:text=DPI%20is%20an%20evolving%20concept,innovation%2C%20especially%20across%20public%20programmes>

DIGITAL SURVEILLANCE: Refers to the use of digital technology to monitor the behavior or movement of people in public and private places. Governments, private companies, and other organizations can use it to target, intimidate, or otherwise influence individuals or groups.⁶¹

DIGITAL TECHNOLOGY: This Policy uses the term “digital technology” not only to describe a type of technology but also to refer to the platforms, processes, and range of technologies that underpin modern ICT, including the internet and mobile-phone platforms, as well as advanced data infrastructure and analytical approaches.⁶²

DIGITAL TRANSFORMATION: The innovation and adoption of digital products, services, and processes to disrupt, transform, and improve the ways in which economies, governments, and societies function.⁶³

DISINFORMATION: A piece of information that is intentionally false or misleading and deliberately used by the producer to achieve a specific social, economic, and/or political objective. Disinformation is often confused with misinformation, which is false or misleading information shared by error or mistake.⁶⁴

DO NO HARM: Consciously looks for and seeks to avoid or mitigate negative impacts on conflict dynamics (the context in which tensions exist in a given setting)—for example, unintentionally worsening divisions among identity groups or reinforcing structural or systemic marginalization.⁶⁵

ENABLING ENVIRONMENT: Refers to the conditions that must be in place for robust access to and use of digital technologies to take place. Fundamentally, this includes meaningful connectivity, i.e., when access to the internet and connected devices is affordable and reliably available. Other foundational enablers include digital literacy (when people have knowledge of how to access and use digital technologies and devices for their benefit) and rights-respecting regulations of digital environments that increase inclusivity, rather than diminish it. A skilled workforce, business-friendly practices, adequate higher education opportunities, and open and inclusive government policies are also key enablers for the uptake and adoption of digital technologies.

EXTENDED REALITY: Extended reality (XR) is an umbrella term for any technology that alters reality by adding digital elements to the physical or real-world environment to any extent and includes but is not limited to, augmented reality (which overlays perceptual information on top of real-world environments), mixed reality (which allows real and virtual elements to interact in an environment) and virtual reality (in which users experience wholly virtual immersive environments).⁶⁶ XR broadens digital interfaces beyond traditional screen-based devices to include headsets, eyeglasses, and other wearable devices (e.g., Pokémon Go, or Apple Vision).

GLOBAL MAJORITY: The group of people in the world who do not consider themselves or are not considered to be white.⁶⁷

⁶¹ USAID Cybersecurity Primer: https://www.usaid.gov/sites/default/files/2022-05/10-26-21_EXTERNAL_CyberPrimer-CLEARED-accessible.pdf

⁶² USAID Digital Strategy 2020-2024: <https://www.usaid.gov/digital-development/digital-strategy>

⁶³ FCDO Digital Strategy, 2024-2030:

<https://assets.publishing.service.gov.uk/media/6613e7f7c4c84d4b31346a68/FCDO-Digital-Development-Strategy-2024-2030.pdf>

⁶⁴ Adapted from Caroline Jack, “Lexicon of Lies: Terms for Problematic Information,” Data and Society Research Institute, (n/d):

https://datasociety.net/pubs/oh/DataAndSociety_LexiconofLies.pdf; USAID Digital Strategy 2020-2024:

<https://www.usaid.gov/digital-development/digital-strategy>

⁶⁵ “Responsible Development: A Note on Conflict Sensitivity from USAID’s Center for Conflict and Violence Prevention”, (December 2020):

https://pdf.usaid.gov/pdf_docs/PA00XCZ1.pdf

⁶⁶ Adapted from Interaction Design Foundation: <https://www.interaction-design.org/literature/topics/extended-reality-xr>

⁶⁷ Cambridge Dictionary definition

GOVERNANCE (DATA): Data governance refers to the people, policies, and processes that provide both direction and oversight into how and why decisions about data are made. These decisions are executed via day-to-day management of the data lifecycle—steps and stages that include planning, acquiring, processing, analyzing, curating, publishing, and sharing data. Unlike data management, data governance considers the strategic, legal and regulatory frameworks needed to minimize risks, promote accountability and optimize data assets within and across data ecosystems. In the context of digital development, data governance deploys data to unlock social and economic opportunities while minimizing risk and harm.⁶⁸

GOVERNANCE (DIGITAL): Digital Governance refers to the act or process of governing or overseeing the control and direction of systems and processes used to manage our digital presence, including:

- Establishing clear operating rules
- Defining responsibilities and lines of authority
- Creating mechanisms to ensure those rules and authorities are followed

Digital governance clarifies who's responsible for the management and operation of digital services. It includes content, design, technical infrastructure, security, funding, and product, project, and program management.⁶⁹

GOVERNANCE (INTERNET): Internet governance refers to the rules, policies, standards and practices that coordinate and shape the internet. These include management of global data communication protocols, such as Internet protocol, Transmission Control Protocol (TCP), Domain Name System (DNS), and Border Gateway Protocol (BGP).⁷⁰

HUMAN-CENTERED DESIGN (HCD): Human-centered design, also referred to as “user-centered design,” is a methodology that incorporates feedback from the people for whom one is designing throughout the design process. The goal of human-centered design is to end up with a solution that is tailored to meet people's needs, with little wasted effort and reduced risk.⁷¹

HUMAN RIGHTS: A set of rights inherent to all people regardless of place of birth, nationality, and/or citizenship, as defined by the Universal Declaration of Human Rights, including the rights to life, liberty, and security of person; freedom from slavery and torture; freedom of expression, association, and peaceful assembly; as well as the right to access work and education.⁷²

INFORMATION INTEGRITY: The accuracy, consistency, and reliability of information.⁷³

INFORMATION MANIPULATION: A set of tactics that alter, modify, or mischaracterize data to shape public opinion, undermine trust in the authenticity of information, or disrupt democratic decision making. The U.S. government prefers the use of “information manipulation” over terms such as “disinformation” or “misinformation.” Information manipulation broadly encapsulates these other terms.⁷⁴

⁶⁸USAID [Forthcoming] Responsible Data Governance for Digital Development Reference Sheet, 2024.

⁶⁹ Adapted from Digital.gov: <https://digital.gov/resources/an-introduction-to-digital-governance/#fn1>

⁷⁰ Internet Governance Project: <https://www.internetgovernance.org/what-is-internet-governance/>

⁷¹ Adapted from 18F

⁷² Adapted from United Nations “Universal Declaration of Human Rights,” (December 10, 1948):

<https://www.un.org/en/universal-declaration-human-rights/>

⁷³ United Nations: <https://www.un.org/sites/un2.un.org/files/our-common-agenda-policy-brief-information-integrity-en.pdf>

⁷⁴ Intelligence Community Lexicon for Foreign Malign Influence:

https://drive.google.com/file/d/1iGv_qSIXuhYCiwlmBK4V7IcreROkm4v6/view?usp=sharing

INNOVATION: Novel business or organizational models, operational or production processes, or products or services that lead to substantial improvements (not incremental “next steps”) in addressing development challenges. Innovation may incorporate science and technology but is often broader, to include new processes or business models.⁷⁵

INTERNET OF THINGS: The Internet of Things (IoT) refers to a network of physical devices, vehicles, appliances, and other physical objects that are embedded with sensors, software, and network connectivity, allowing them to collect and share data.⁷⁶ IoT forms a global infrastructure for the information society that enables advanced services by interconnecting physical and virtual things based on existing and evolving interoperable information and communication technologies.⁷⁷

INTEROPERABILITY: The ability of data to be exchanged, combined, and layered on top of each other. Interoperability can refer to:

- Technological: computer systems or software are able exchange and make use of data from other systems in automated ways, such as using an API or exchange layer.
- Semantic: data sets use the similar enough definitions, data formats, taxonomies, and classifications - i.e. dates come in date formats, indicators are measured the same way, groups are aggregated in the same groupings.
- Syntactic: data sets use similar enough data formats - i.e. spreadsheets use Excel, CSV, or Sheets, images use PNG, JPEG, or GIF.
- Operational: data sets meet expected data structures, quality, and completeness expectations for specific operational usage - for example, interoperable payment systems allow digital transfers of money between different financial service providers. Each player in the system has a specific operational role in the data being exchanged, which is reflected in how the data is recorded and shared.

KILLER APPS: A term originally coined in the late 1980s, a “killer app” is an application or technology product that is considered indispensable or is the default for a particular category of product for a period of time. For example, Microsoft Excel or Word for Windows were killer apps in the 1980s and 1990s; they were present and necessary on all personal computers. More recent “killer apps” include Amazon, Gmail, Twitter, Facebook, and WhatsApp, mainly due to their ubiquity globally and brand recognition.⁷⁸

LGBTQI+: Lesbian, gay, bisexual, transgender, queer, and intersex people. The “+” in LGBTQI+ represents additional sexual orientations, gender identities, gender expressions, and sex characteristics (SOGIESC) that do not fit within the “LGBTQI” identity labels.⁷⁹

LOCALIZATION (DATA): A term referring to legal requirements or policy preferences for data to be hosted locally (i.e. not in a Cloud server hosted in a different country).⁸⁰

⁷⁵ From IPI/ITR Innovation Division’s definition

⁷⁶ IBM:

[https://www.ibm.com/topics/internet-of-things#:~:text=The%20Internet%20of%20Things%20\(IoT\)%20refers%20to%20a%20network%20of%20to%20collect%20and%20share%20data](https://www.ibm.com/topics/internet-of-things#:~:text=The%20Internet%20of%20Things%20(IoT)%20refers%20to%20a%20network%20of%20to%20collect%20and%20share%20data)

⁷⁷ International Telecommunications Union, “Overview of the Internet of Things,” accessed November 2019:

<https://www.itu.int/rec/T-REC-Y.2060-201206-1/en>

⁷⁸ Adapted from The 25 Killer Apps of All Time | Channel Insider; The Investopedia. “Killer Application: What It Means, How It Works, Value.” Investopedia. Accessed May 15, 2024: <https://www.investopedia.com/terms/k/killerapplication.asp>

⁷⁹ LGBTQI+ Inclusive Development Policy: <https://www.usaid.gov/policy/lgbtqi>

⁸⁰ Adapted from Kiteworks, “What is Data Localization?”:

<https://www.kiteworks.com/risk-compliance-glossary/data-localization/#:~:text=Data%20Localization%20refers%20to%20the%20strategy%20that%20requires%20all%20data,this%20concept%20one%20step%20further>

LOCALIZATION (DEVELOPMENT): The set of internal reforms, actions, and behavior changes that we are undertaking to ensure our work puts local actors in the lead, strengthens local systems, and is responsive to local communities.⁸¹

MACHINE LEARNING (ML): A set of methods that train computers to learn from data, where “learning” generally amounts to the detection of patterns or structures in data. ML approaches begin by finding patterns in a subset of existing data and use them to make predictions for new, unseen data.⁸²

MARGINALIZED GROUPS: Marginalized groups may include, but are certainly not limited to, women; youth; children in adversity and their families; older persons; persons with disabilities; LGBTQI+ people; displaced persons; migrants; Indigenous Peoples and communities; non-dominant religious, racial, and ethnic groups; people of castes traditionally considered lower; people of lower socioeconomic status; and people with unmet mental health needs.⁸³

PARTNER: An organization or individual with which/whom the U.S. Agency for International Development collaborates to achieve mutually agreed upon objectives and to secure the participation of ultimate customers. Partners include host-country governments, private voluntary organizations, local and international non-governmental organizations, faith-based organizations, universities, other U.S. Government Departments and Agencies, the United Nations and other multilateral organizations, professional and business associations, and private businesses and individuals.⁸⁴

PHISHING: According to CISA, “phishing attacks use email or malicious websites to infect your machine with malware and viruses in order to collect personal and financial information.” An ODNI factsheet has more information, as does this Stop, Think, Connect campaign video.⁸⁵

PLATFORM: A group of technologies used as a base upon which other technologies can be built or applications and services run. For example, the internet is a platform that enables web applications and services.⁸⁶

QUANTUM COMPUTING: An alternative method of computation that exploits the laws of quantum physics to efficiently solve some problems that are difficult to solve with classical computing.⁸⁷

RANSOMWARE: Ransomware is an ever-evolving form of malware used to elicit a ransom. The malware itself is designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid.⁸⁸

RESPONSIBLE PARTNERSHIP: A partner engagement that aligns to the Agency’s values and mission, democratic principles, and respects human rights. In practice, this can mean USAID choosing partners to work on a given program who best-fit the needs and context of that program.

⁸¹ USAID, Localization, Accessed April 2, 2024: <https://www.usaid.gov/localization>

⁸² Adapted from Amy Paul, Craig Jolley, and Aubra Anthony, “Reflecting the Past, Shaping the Future: Making AI Work for International Development,” USAID (September 2018): <https://www.usaid.gov/digital-development/machine-learning/AI-ML-in-development>; USAID Digital Strategy 2020-2024: <https://www.usaid.gov/digital-development/digital-strategy>

⁸³ ADS 201: https://www.usaid.gov/sites/default/files/2023-10/USAID-ID-Hub_ADS-201-AH-Documents_Oct-2023_1.pdf

⁸⁴ USAID, “Glossary of ADS Terms,” accessed November 2019: <https://www.usaid.gov/who-we-are/agency-policy/glossary-ads-terms>

⁸⁵ USAID Cybersecurity Primer: <https://www.usaid.gov/digital-development/usaid-cybersecurity-primer>

⁸⁶ USAID Digital Strategy 2020-2024: <https://www.usaid.gov/digital-development/digital-strategy>

⁸⁷ Quantum Futures: International Development and the Quantum Computing Transition: <https://www.usaid.gov/sites/default/files/2023-08/USAID%20Quantum%20Computing%20Report.pdf>

⁸⁸ CISA: <https://www.cisa.gov/stopransomware/ransomware-faqs>

RESPONSIBLE DATA: The term is used to describe a number of specific practices in data management, including collection, storage, analysis, sharing, and usage. Using data responsibly in development programs ultimately requires balancing prioritization of three broad thematic areas: data use, privacy and security, and transparency and accountability. These three areas are frequently in tension with one another; improved data precision for better analysis can create privacy risks and increase security needs while transparency and accountability often relies on retaining a lot of - often sensitive - data. Understanding these tensions and working to balance them based on specific contexts can help development practitioners work responsibly and highlight questions about risk and benefit surrounding data.⁸⁹

RESPONSIBLE DATA GOVERNANCE: This term refers to the application of responsible data principles and development values such as transparent, rights-respecting, and inclusive data oversight (i.e. traditional data governance systems and practices) to improve development outcomes and reduce the risk of data misuse and harms.⁹⁰

RIGHTS-RESPECTING: This term is adapted from the longer phrase of “respecting human rights”. Respecting human rights in the design, development, deployment, use and governance of digital technologies and data requires conducting due diligence to avoid adversely impacting human rights. This includes establishing policies and systems to identify, avoid, mitigate and manage potential or actual adverse human rights impacts.⁹¹ Rights-respecting digital systems and data-driven technologies are those that are developed, implemented, managed, and governed in a way that respects the fundamental human rights of persons and societies. Governance regimes for rights-respecting digital systems and data driven technologies can be contrasted with authoritarian governance regimes.

SAFEGUARDING: Safeguarding is the implementation of preventative, protection, and compliance measures for populations who may be at an increased risk from harm across an organization’s operations, for the purposes of preventing harm, including but not limited to exploitation, abuse, and violence.⁹² Digital systems and data-driven technologies developed, designed, deployed, used and governed in accordance with safeguards that conform to accepted international standards can be referred to as “rights-respecting” as described above.

STAKEHOLDERS: Individuals and groups that have an interest or equity in the work of USAID. This can include government representatives, civil society organizations, the private sector, industry, academia, faith-based organizations, multilateral organizations, government donors, and philanthropy organizations, or distinct people groups such as youth, LGBTQIA+, persons with disabilities, ethnic minorities, and women as well as individuals who are directly or indirectly impacted by USAID’s work. Key stakeholders are determined based on the context of work being done and will look different project-to-project.⁹³

TECHNOLOGY-FACILITATED GENDER-BASED VIOLENCE (TFGBV): TFGBV A threat or act of violence committed, assisted, aggravated, and amplified in part or fully by using information and communication technologies or digital media that is disproportionately targeted at women, girls, and gender

⁸⁹ USAID Considerations for Using Data Responsibly at USAID: <https://www.usaid.gov/sites/default/files/2022-12/USAID-UsingDataResponsibly.pdf>

⁹⁰ USAID [Forthcoming] Responsible Data Governance for Digital Development Reference Sheet, 2024.

⁹¹ See the UN Guiding Principles on Business and Human Rights for more guidance on the role of government and businesses in managing potential and actual human rights risks.

⁹² ADS 113mab

⁹³ Adapted from “Considerations for using data responsibly at USAID”: <https://www.usaid.gov/sites/default/files/2022-12/USAID-UsingDataResponsibly.pdf>

non-conforming individuals. It is a continuum of multiple, recurring, and interrelated forms of gender-based violence that takes place both online and offline. Examples can include online harassment and abuse; non-consensual distribution of intimate digital images; cyberstalking; sextortion; doxing; malicious deep fakes; livestreamed sexual violence of children, youth, and adults; rape and death threats; disinformation; intimate partner violence; and recruitment into trafficking and abusive labor.⁹⁴

TWIN TRANSITION: This term is used to refer to the huge and largely untapped opportunity for technology and data to drive sustainability goals, especially as they relate to the environment. Rather than treating digital and sustainability in isolation, a twin transition combines these critical functions to unlock benefits in terms of efficiency and productivity. A twin transition can make a positive impact by ‘greening’ technology, data assets, and infrastructure while accelerating sustainability.⁹⁵

USER (END): Individuals who interact directly with the final software application, hardware device, or digital service, utilizing its features and functionalities to meet their specific needs or requirements.⁹⁶

USER-CENTERED DESIGN: User centered design refers to design approaches and tools that center the user experience. This iterative process focuses on users and their needs at every stage in the design and implementation process, with different forms of user testing and analytics integrated into the development work plan.⁹⁷

⁹⁴ Department of State: <https://www.state.gov/reports/united-states-strategy-to-prevent-and-respond-to-gender-based-violence-globally-2022/>

⁹⁵ World Economic Forum:

<https://www.weforum.org/agenda/2022/10/twin-transition-playbook-3-phases-to-accelerate-sustainable-digitization/>

⁹⁶ Adapted from “End User: Definition, Examples, Vs. Customer”, Investopedia. Accessed May 16, 2024:

<https://www.investopedia.com/terms/e/end-user.asp&sa=D&source=docs&ust=1715807604739348&usg=AOvVaw2YZpggD3H5nsr56R7d0xP8>

⁹⁷ IxDF (interaction-design.org): <https://www.interaction-design.org/literature/topics/user-centered-design>