USAID
FROM THE AMERICAN PEOPLE

Source: USAID North Macedonia

DIGITAL GOVERNMENT MODEL

Acknowledgements

This document was prepared by the Digital Societies and Governments team in the Technology Division of the Innovation, Technology, and Research (ITR) Hub of the Bureau for Inclusive Growth, Partnerships, and Innovation (IPI), in consultation with USAID's Bureau for Democracy, Human Rights, and Governance (DRG Bureau) and with input from select Missions and implementing partners. The development of this document was led by Laura Sigelmann and Jaclyn Carlsen from USAID's ITR Hub, Matthew Laird from USAID's DRG, Chrissy Martin Meier consulting for DAI, and Anand Varghese and Talia Dweck from DAI's Center for Digital Acceleration with support from Priya Sethi and Alin Hannessian from DAI's Digital Frontiers project. Drafting of the document was led by Chrissy Martin Meier. Special thanks to Stefan Peterson and Digital Frontiers for design and graphics. Additional thanks to the Digital Societies and Governments Team for their contributions: Rebecca Saxton-Fox, Njemile Davis, Mikael Baker, Taylor Braun-Dorrell, and to Siobhan Green, Kendra Grimes, and Beth Hain for their continued support. This document was revised in December 2023. Special thanks to Priya Sethi, Jeremy Schmidt, Deepika Ramachandran, and Carlos Saavedra from DAI's Digital Frontiers project for facilitating the revision process.

Source: Jim Huylebroek for Creative Associates International

This report is made possible by the generous support of the American people through the United States Agency for International Development. The contents are the responsibility of the authors and do not necessarily reflect the views of USAID or the United States Government. This publication was produced by the Digital Frontiers Project under Cooperative Agreement AID-OAA-A-17-0003 under the Digital Societies and Governments team and in alignment with the Digital Strategy.

Background:

WHY USE A MODEL TO DESCRIBE DIGITAL GOVERNMENT?


Source: USAID

USAID's Digital Strategy charts an Agency-wide vision for equipping staff and partners to adapt development and humanitarian assistance to the opportunities and risks resulting from the proliferation of digital technology.

Digital technology has transformed most aspects of public and private lives. It is also driving immense change for governments. More governments are using digital technologies to set measurable administrative goals, improve public service delivery, make data-driven decisions, enact evidence-based policies, ensure greater accountability and transparency, and engage with the public.

USAID and its development partners are increasingly looking to support countries in the process of adopting technologies to create public value[1] while mitigating and avoiding significant risks. These opportunities and risks have become even more evident in the face of global challenges such as climate change, conflict and unrest, and global pandemics. Governments with digital systems, processes, and infrastructure in place are better able to quickly bring to scale emergency response assistance, communications, and payments. At the same time, rapid digitalization has accelerated many risks associated with digital tools, as state and non-state actors spread mis- and disinformation, exploit personal data, and use new technology to increase surveillance and social control.

What Is Digital Government?[2]

"Digital government" is the use of digital technologies as an integrated part of government strategies. The term describes how governments use technology to provide access to data, services, and content for other government actors, non-governmental organizations, businesses, civil society, and individuals. Broadly, governments use digital technology to ***manage*** *internal systems and processes,* ***deliver*** *government services, and* ***engage*** *stakeholders.*[3]

1 Public value describes the value that an organization or activity contributes to society.

2 USAID uses the term digital government over the alternatives since it appears most frequently in the literature. As the UN e-Government Development Index states, in some cases, "reference is made to digital government as the next phase of e-government." Thus, as this landscape aims to be comprehensive, the broader term was chosen.

3 Definition of digital government is adapted from the USAID Digital Ecosystem Framework. Originally adapted from OECD (2014), Recommendation of the Council on Digital Government Strategies, OECD/LEGAL/0406. Available at: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0406.

This document provides a descriptive model as the basis for a shared understanding and vocabulary of the key components of digital government. It builds on and is informed by existing frameworks for digital or e-government.[4] This model is not intended to be prescriptive, nor is it intended to replace existing reference frameworks and documents already in use by partners. The model is a living document intended to evolve over time and complements the strong base of existing work on digital development and governance. (Please refer to the Complementary Resources box.)

There is no common definition of digital government in the development community, nor is there agreement on its principal components.[5] It is sometimes referred to as e-government. This model describes what governments are currently investing in but does not describe what they should invest in.

By suggesting a common vocabulary, this document sets the stage across USAID for future research and technical assistance on digital government under the Digital Strategy.

The Technology Division of the USAID Innovation, Technology, and Research Hub (ITR) in the Bureau for Inclusive Growth, Partnerships, and Innovation (IPI) led the development of this model in consultation with USAID's Bureau for Democracy, Human Rights, and Governance (DRG), with input and feedback from select Missions and implementing partners.

Source: USAID

COMPLEMENTARY RESOURCES

Principles for Digital Development

Country-specific digital strategies

USAID Democracy, Human Rights, and Governance Strategy

USAID Digital Strategy

USAID Digital Visions and Digital Strategy Action Plans

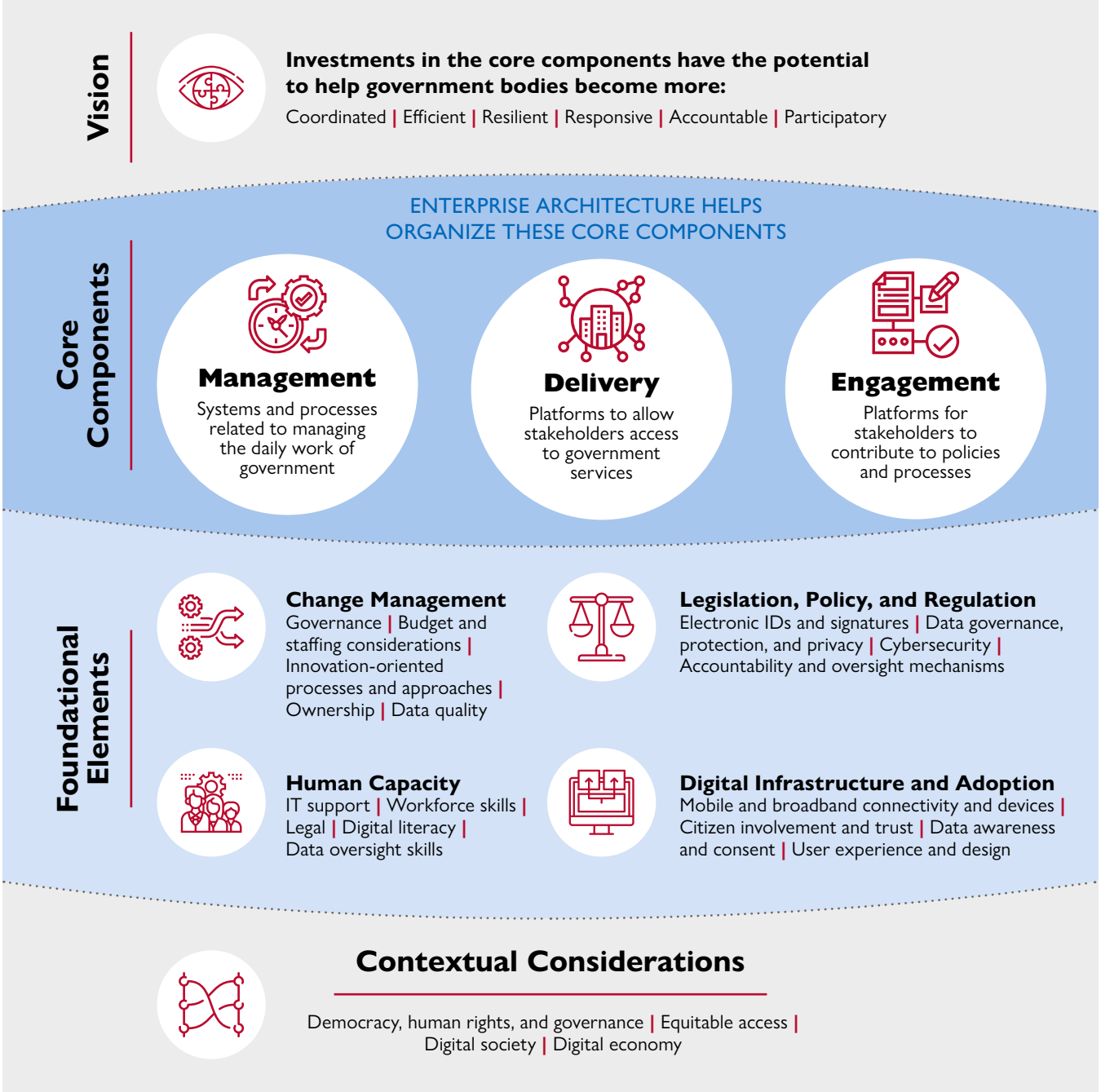
USAID Digital Ecosystem Country Assessments (DECAs)

4 Frameworks from the following organizations were reviewed in preparing this USAID model: Deloitte, Estonia e-Governance Academy (eGA), Future State, International Telecommunications Union (ITU), OECD, PwC, UNDP, World Bank.

5 How Can Digital Government Advance Global Development and Democracy? https://www.brookings.edu/blog/up-front/2021/12/15/how-can-digital-government-advance-global-development-and-democracy/

The Model

Digital government is the use of digital technologies as an integrated part of government strategies. This includes three core components: i) management of internal government systems and processes; ii) delivery of government services; and iii) engagement with stakeholders. The core components rely on a set of foundational elements and contextual considerations that influence the success of digital government investments.[6]



6 All examples under the foundational elements (e.g., governance, ownership, data quality) are illustrative, and are not intended as an exhaustive list.

Vision:

WHAT CAN AND SHOULD DIGITAL GOVERNMENT STRATEGIES AND INVESTMENT AIM TO ACHIEVE?

Donors and partners invest substantial funding and human resources in digital government initiatives with the hope that such initiatives will improve governance and service delivery. However, "getting digital government right is not just about digital, it is also about companion analog processes, including strengthening government institutions and democratic norms and processes."[7]

Vision

Investments in the core components have the potential to help government bodies become more:

Coordinated | Efficient | Resilient | Responsive | Accountable | Participatory

Investments in digital government *have the potential* to help government become more:

- **Coordinated,** by providing the systems and tools necessary for government bodies to work together across ministries and levels (e.g., national, provincial, municipal);
- **Efficient,** by achieving fiscal savings and allowing for innovation by decreasing the time spent on administration;
- **Resilient,** by supporting response to and recovery from natural disasters or other sudden social and economic changes;
- **Responsive,** by increasing the ability to anticipate and respond to a range of stakeholder needs from individuals, the private sector, and civil society actors;
- **Accountable,** by reducing opportunities for corruption and providing tools for collaborative, inclusive, accessible, and transparent policy design and service delivery; and
- **Participatory,** by creating systems and tools that enable citizens and civil society to engage with governments.


Source: Panos

The extent to which these outcomes are possible depends largely on the enabling environment, which includes democratic norms and institutional capacity, among other factors. Digital initiatives undertaken by a government are part of the broader political, economic, and social context. The same digital investments that support democratic institutions,

7 George Ingram and Meagan Dooley, Digital government: Foundations for global development and democracy, Center for Sustainable Development at Brookings, https://www.brookings.edu/wp-content/uploads/2021/12/Digital-government.pdf

rights-respecting government bodies, and open societies in one context can be used to suppress political dissent, quash individual freedoms and rights, and limit competition in the marketplace. When digital government investments are undertaken by authoritarian governments in countries affected by democratic backsliding[8] or by malign actors, those investments can serve as agents of repression and restriction.

Investments in digital government carry risks, including:

- **Repression and restriction,** by using technology to surveil, censor, persecute, and socially manipulate individuals. Digital repression can also create barriers to technology access.
- **Exclusion,** by shifting interaction with governments to digital channels that are difficult to use or not available to all segments of society.
- **Technology overdependence** on brittle, inflexible, and overly complex systems, specific technology vendors, or specific platforms, hardware, and software.
- **Inadequate data protection and data governance** can make it difficult for individuals to understand when and how their data is being used, or to have autonomy over their data.
- **Cyber attacks** against digital government technology can cause an array of harms to governments and citizens, such as data leaks, lapses in crucial services, and high costs to bring systems back online.

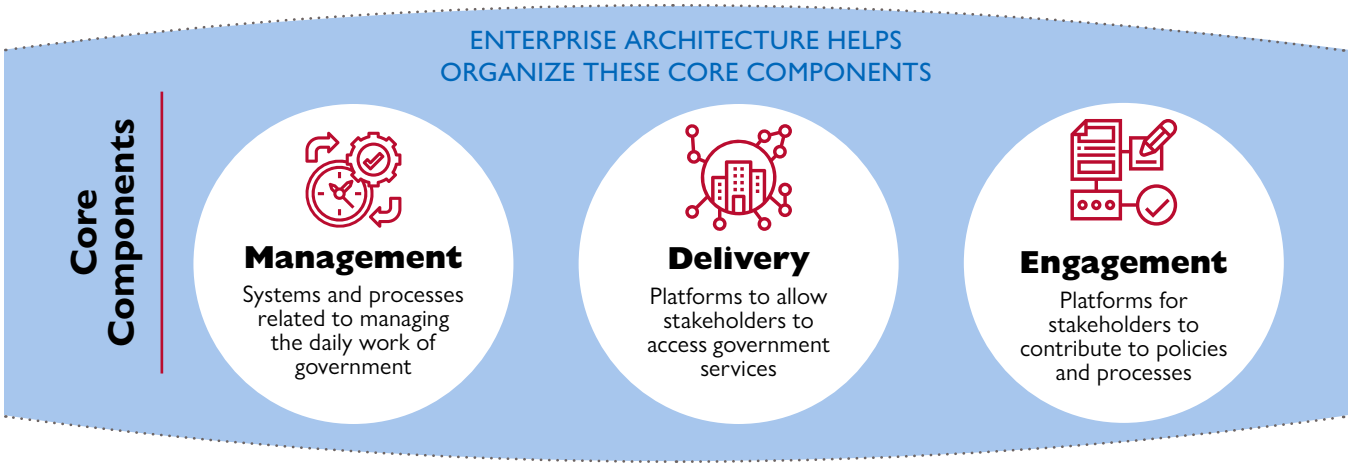
Source: USAID

8 For more information, refer to V-Dem

Core Components:

WHAT ARE THE TANGIBLE, VISIBLE COMPONENTS THAT COMPRISE DIGITAL GOVERNMENT?

USAID defines digital government broadly, looking across the functions of government to understand the impact digital tools have on the work of governments. This model uses three categories to describe the components of digital government: management, delivery, and engagement.



These three categories provide an expansive definition of how technology is changing government across its various functions. Regardless of category, digital government investments must be *sustainable*, supporting government policy planning, operations, and services with data and information over the long term, and must be *integrated* into broader efforts to improve governance.

The core components of digital government are:

Management, or e-administration, includes the digitalization of internal government processes and systems. Examples include:

- Digital databases which store data in a digital format for easier reference and data analysis;
- Data storage solutions that allow for data to be securely stored and protected;
- Management information systems (MIS) which are information systems used for decision-making, and for the coordination, control, analysis, and visualization of information; and
- E-procurement systems which enable a more efficient and transparent exchange of information and transactions between government and suppliers of goods and services.

Delivery, or e-service delivery, includes the digitalization of government service provision. Examples include:

- Government portals including mobile apps which provide access to information and services and the ability for stakeholders to carry out administrative procedures online;
- Digital payments which can help governments improve public financial management and increase the efficiency and transparency of payments to and from government bodies; and
- Digital identification (ID) systems which can potentially provide the means for individuals to securely prove their identity and provide a unique ID number that facilitates data exchange across government systems. Digital ID systems must be secured; must be designed to be broadly inclusive and with meaningful consent processes; and must be implemented in countries with robust data protection, privacy regulations and policies, consistent enforcement of these regulations and policies, and independent oversight and grievance redress mechanism.[9]

Engagement, or e-participation, includes digital channels and platforms through which stakeholders can collaborate with and influence government agencies and policies. Examples include:

- Citizen and voter education that are provided through accessible channels;
- Government-supported incubation hubs which engage the private sector in creating tools and systems to meet the specific needs of governments;
- Open data portals which allow citizens and businesses to use government data for innovation, services, and accountability;
- Political participation mechanisms which offer stakeholders access to direct lines of communication with local representatives to raise questions and concerns, and which provide an easy way for representatives to respond; and
- Citizen science initiatives, wherein the public voluntarily participates in the scientific process to help address real-world problems.

Enterprise Architecture refers to the standardized processes, protocols, and policies that enable governments to coordinate across digital government systems. Comprehensive enterprise architecture enables the integration of systems and shared services across government agencies. This requires robust connectivity infrastructure and devices across government bodies operating at the national, regional, and local levels.

9 For more on inclusive, secure, and appropriate digital ID systems, refer to the Principles on Identification for Sustainable Development (2021). https://documents.worldbank.org/en/publication/documents-reports/documentdetail/213581486378184357/principles-on-identification-for-sustainable-development-toward-the-digital-age and the Good ID Movement https://cyber.harvard.edu/story/2021-11/incorporating-good-id

Foundational Elements:

WHAT ARE THE LESS TANGIBLE, CRITICAL FACTORS THAT DETERMINE IF THE CORE COMPONENTS LEAD TO POSITIVE DEVELOPMENT OUTCOMES?

To achieve this vision, initiatives that focus on the core *management, delivery, and engagement* components must be met with investments in foundational elements. Foundational elements include: change management; human capacity; legislation, policy, and regulation; and digital infrastructure and adoption.

Foundational Elements

Change Management
Governance | Budget and staffing considerations | Innovation-oriented processes and approaches | Ownership | Data quality

Legislation, Policy, and Regulation
Electronic IDs and signatures | Data governance, protection, and privacy | Cybersecurity | Accountability and oversight mechanisms

Human Capacity
IT support | Workforce skills | Legal | Digital literacy | Data oversight skills

Digital Infrastructure and Adoption
Mobile and broadband connectivity and devices | Citizen involvement and trust | Data awareness and consent | User experience and design

Change management considerations:

- Planning for the long-term governance of digital systems, which includes identifying the agency and staff members who will be responsible for sustaining digital systems;
- Planning for ongoing costs and required personnel by considering long-term budget and staffing needs early on;
- Integrating innovation-oriented processes into government standard operating procedures, such as agile techniques and human-centered, rights-respecting design processes;
- Planning for the ownership of business processes and the responsibility for their development, modification, and simplification;
- Ensuring data quality by consistently cleaning and checking data sets for errors and biases as data is entered into digital government databases and used for analysis; and
- Ensuring ongoing data security by monitoring cybersecurity threats, potential changes in administration, and risks of democratic backsliding.


Source: Morgana Wingard

Human capacity across government staff, the private sector, and individuals:

- IT support to maintain, update, and troubleshoot systems either through internal government hiring or outsourcing to external support entities;
- Workforce skills to ensure that government staff are willing and able to use software, reimagine business processes, analyze data, adapt to new technology, and proactively address downstream impacts of data and technology;
- Capacity among regulators, judges, and lawyers to design, implement, and litigate underlying policies and frameworks;
- Digital literacy at all levels to support stakeholders who are asked to engage with the government in new and technology-driven ways, to play a role in securing their own data and ensuring that their rights are respected, and to protect themselves against cybersecurity threats; and
- Data oversight skills to ensure that data is collected, stored, and shared in line with respect for human rights and democratic values.

Legislation, policy, and regulation adoption and implementation:

- Legal recognition of electronic signatures and IDs to allow for digital transactions and services;
- Data governance, protection, and privacy measures to avoid misuse of data, including personal information for profit, surveillance, or other malintent by current or future internal government actors and their private sector data-sharing partners;
- Cybersecurity legislation to designate responsibility for managing cyber incidents, to combat cyber crime, and to increase awareness of common cybersecurity risks among government staff and the general public; and
- Accountability and oversight mechanisms, such as ombudsmen, national human rights institutions, reporting mechanisms for corruption and discrimination by government officials, and publicly accessible information on laws, compensation, grievance procedures, and rights.[10]

Digital infrastructure, access, and use considerations:

- Affordable and accessible mobile and broadband connectivity and devices underpinning the core components. Geographic network coverage, network performance, Internet bandwidth, access to connected devices, and spectrum allocation affect who will and will not be reached by digital government initiatives;
- Citizen involvement and trust must be nurtured at all stages of digital government initiatives, through transparent and inclusive implementation that takes into account the views and concerns of key stakeholders;
- Data awareness and consent, when actively fostered, can help individuals understand and make informed decisions about how their data is being used, thereby encouraging participation; and
- User experience and use of design principles[11] can facilitate trust, inclusion, access, and use by making digital government tools simple and intuitive for all types of stakeholders (including marginalized groups and individuals with specific access needs, such as persons with disabilities).

10 For general guidance on oversight, refer to https://ctb.ku.edu/en/table-of-contents/maintain/maintain-quality-performance/establishing-oversight-mechanisms/main

11 Refer to the Principles for Digital Development (https://digitalprinciples.org/) and the Universal Design principles, https://universaldesign.ie/what-is-universal-design/the-7-principles/

Contextual Considerations:

WHICH OTHER FACTORS WILL DETERMINE IF DIGITAL GOVERNMENT INVESTMENTS WORK TOWARD THE VISION?

Contextual Considerations

Democracy, human rights, and governance | Equitable access | Digital society | Digital economy

Digital government investments are influenced by broader **democracy, human rights, and governance** considerations. Such considerations include:

- The presence—or lack of—participatory, representative, and inclusive political processes and government institutions;
- The protection and promotion of universally recognized human rights;
- Freedom of the press;
- A strong civil society; and
- Legal and judicial systems to foster greater accountability by institutions and leaders to citizens and the law.

Additionally, **equitable access to platforms and services** is vital to successful digital engagement strategies. Engaging youth, women, and marginalized or underrepresented groups[12] in digitalization initiatives is key to addressing and closing the digital divide.

Digital government investments influence and are influenced by all aspects of the digital ecosystem as articulated in the three pillars of USAID's Digital Ecosystem Framework. The first pillar is **digital infrastructure and adoption**, one of the foundational elements, which includes the resources that make digital systems possible. The second pillar is **digital society, rights, and governance**, which includes digital interactions between government, media, and civil society. The third pillar of the digital ecosystem is the **digital economy**, which is defined by factors such as digital financial services, e-commerce, the tech start-up environment, and the digital talent pool.

Digital technology has transformed public and private life, including government operations. It has influenced how governments manage their operations, deliver services, and engage with stakeholders. This model can help USAID operating units think beyond sectors and understand the components that are required in digital government transformation. The model is intended to spark conversations about what must be considered in USAID's digital government programming and how USAID can support partner governments in navigating the complex landscape of digitalization. The risks are considerable. Together with our partners we aim to learn and adapt so that technology ultimately creates better public value.

12 Such groups may include, but are not limited to, women and girls, persons with disabilities, LGBTQI+ people, displaced persons, migrants, Indigenous Peoples and communities, youth, older persons, religious minorities, ethnic and racial groups, people in lower castes, and people of diverse economic class and political opinions. These groups often suffer from discrimination in the application of laws and policy and in access to resources, services, and social protection, and may be subject to persecution, harassment, and/or violence.

Under the Digital Strategy, USAID's Technology Division in the Innovation, Technology, and Research Hub (ITR), with support from the Bureau for Democracy, Human Rights, and Governance (DRG), is providing technical assistance, resources, and workshops on digital government. If you are interested in learning more about these initiatives, please reach out to the Digital Societies and Governments team at digitalsocieties@usaid.gov.

USAID
FROM THE AMERICAN PEOPLE