Photo: USAID Energy

Environment, Energy, and Infrastructure (EEI)

Digital Literacy[1] and EEI

Digital literacy is an important prerequisite for expanding the use of digital technologies in USAID's environment, energy, and infrastructure (EEI) portfolio, which helps tackle global challenges like climate change, energy and water services insecurity, and access to sustainable infrastructure. In addition to increasing the use of digital tools across this sector, incorporating digital literacy into EEI programming can also help ensure that USAID stakeholders create an enabling environment for digitalization to thrive. However, because the implementation of digital tools in the EEI sector can have significant legal implications (for example, when they are utilized for land tenure registries or as anti-wildlife trafficking tools) and has the potential to impact daily lives (i.e., in the event of a malfunctioning digital operating system for a wastewater utility), cyber safety is a particularly critical digital literacy competency.

What is Digital Literacy?

USAID—building on UNESCO's definition of the term—defines digital literacy as "*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, social, and political life.*"

[1] Unless otherwise cited, all information in this sectoral brief comes from USAID's Digital Literacy Primer. Full citation: "Digital Literacy Primer: How to Build Digital Literacy into USAID Programming" (USAID, 2022), https://www.usaid.gov/digital-development/digital-literacy-primer.

USAID's Digital Literacy Framework

To effectively and equitably achieve digital access, USAID's approach to digital programming must extend beyond infrastructure and devices to ensure that users possess a nuanced set of skills to meaningfully, responsibly, and safely participate in digital ecosystems. Two pillars underpin USAID's definition of digital literacy: capacity and safety.

» **Capacity** refers to the technical knowledge and skills required to use digital devices and services such as mobile phones; tablets and computers; the Internet; messaging and social media platforms such as WhatsApp, Twitter, and Facebook; and audio and visual tools.

» **Safety** refers to the skills and awareness required to use digital tools carefully while navigating potential harms and cyber threats successfully. This pillar includes, but is not limited to, strategies for strengthening cyber hygiene[2] and countering mis- and disinformation.

As explained in the Digital Literacy Primer, USAID takes two primary approaches for incorporating digital literacy into program design:

» **Foundational** digital literacy activities build digital literacy skills applicable to all aspects of users' economic, social, and personal lives—a goal in and of itself.

» **Tactical** digital literacy activities prepare target populations to use digital tools to ensure that a specific digital intervention is effective in a particular sector (this category may also include activities that do not have digital literacy as their singular goal).

Digital Literacy in USAID's EEI Portfolio

Given the variety of target users within the EEI sector—ranging from wildlife rangers to critical infrastructure operators—key stakeholders possess different digital literacy levels and experience different barriers that limit their uptake of digital literacy competencies. Digital literacy interventions in the EEI sector therefore target **three main levels of users: (1) individuals and communities; (2) EEI-focused civil society organizations (CSOs); and (3) utilities, manufacturing and private companies, and national and local government agencies**.

Building **digital literacy among individuals and communities** (including cultivating trust in digital tools) is a prerequisite for the mass adoption of digital tools that advance environmental objectives like climate change mitigation and adaptation, promoting adoption of renewable energy, enhancing green infrastructure solutions, protecting biodiversity, and supporting smart city solutions. For example, citizens may need support in learning how to use digital financial services to pay their energy bills, crowdfund sustainable transport projects, or use a smartphone app to access a flood early warning system.

Photo: FAIDA

USAID supports **EEI-focused CSOs and companies** to understand the impact that new digital technologies can have on their work, including cybersecurity-related implications. By training and encouraging decision-makers to evaluate their standards, procurement processes, and supply chain management approaches, USAID can help energy and infrastructure companies critically assess their grids and other infrastructure modernization needs and implement solutions that digitally upskill their workforce.

[2] Cyber hygiene is defined as the practices and steps that users of computers and other devices take to maintain system health and improve online security. These practices are often part of a routine to ensure the safety of identity and other details that could be stolen or corrupted.

Photo: Riaz Jahanpour for USAID / Digital Development Communications

An important corollary is to develop digital interventions that are appropriate to the target user's digital literacy level. For example, USAID's Wildlife Asia Activity conducted research in 2018 showing that people in Thailand frequently used Google to search for information about illegal wildlife products. To deter consumers from purchasing these products, the Activity launched a seven-month digital deterrence pilot that used Google deterrence ads to educate people searching for these products about the impacts of the illegal wildlife trade. The pilot was effective; the ads were shown over 550,000 times, and the campaign's cost per thousand ad impressions (CPM) was less than half of the average in Thailand ($14.33 CPM compared to the Thailand average of $30–$40).

At the operational level, USAID activities also build the digital skills of private sector partners and CSOs to increase their use of digital tools. For example, with funding from USAID's Higher Education Solutions Network, the AidData Center for Development Policy—alongside local civil society organizations like the Center for Environmental and Agricultural Policy—conducted a five-day ArcGIS workshop in Nepal to help local institutions use geospatial data and tools to visualize development problems and projects.

Activities targeting **national and local government agencies** often aim to improve the digital literacy of policymakers, their staff, and other government employees. For example, as part of USAID's support to Tanzania's National and Transnational Serious Crimes Investigative Unit to improve its anti-poaching capabilities, the Agency's Promoting Tanzania's Environment, Conservation, and Tourism (PROTECT) project provided the Unit's staff members with software, systems to institutionalize these digital tools, and a long-term training plan which increased the staff's political will to use this software in their work.

USAID also supports the adoption of improved policies to ensure that EEI-related digital literacy and cybersecurity-related initiatives are codified into laws, regulations, and standards. For example, USAID's Cybersecurity for Critical Infrastructure in Ukraine Activity supported the inclusion of cybersecurity-related inputs in Ukraine's new 2021 law on critical infrastructure, aligned with Ukraine's National Cybersecurity Strategy.

Key Considerations

Digital literacy among target users is becoming increasingly important when implementing successful digital technology-related interventions in the EEI sector. Further, cybersecurity measures, which are crucial in bolstering economic resilience and national security, must therefore be an integral part of digital literacy from the start of new EEI programs. Specific areas of opportunity to build digital literacy within USAID's EEI portfolio include:

» **FOR ALL DIGITAL LITERACY INTERVENTIONS IN THE EEI SECTOR:**

Assess the current digital literacy levels of the intervention's target audience, then customize the intervention accordingly.

- This typically requires interviewing or surveying the target audience about which devices, platforms, and digital tools—and the specific functionalities of which—they use, if any.
- If the target audience's digital literacy levels are highly variable, segment the intervention into different levels.

Institutionalize longer-term digital capacity-building (not only digital literacy training) when delivering digital technology-related interventions. Incorporating mentoring, coaching, or long-term technical assistance provides longer-term support than one-off training or training series alone, increasing the likelihood that the target audience will apply their new digital knowledge.

Incorporate cybersecurity and cyber hygiene protections into all digital literacy interventions. This is especially critical for the EEI sector because of the degree of sensitivity—including potential national security implications—around critical infrastructure like water services and energy.

» AT THE INDIVIDUAL AND COMMUNITY LEVEL:

Design and conduct digital-focused interventions that incorporate digital tools and technologies that the target audience already uses, then build public outreach campaigns to raise users' awareness of the benefits. This increases the likelihood that the target audience will continue using these tools after the activity ends.

» AT THE EEI-FOCUSED CSO AND COMPANY LEVEL:

To upskill staff, add additional training or capacity modules into all digital-focused interventions—i.e., the introduction of a new wildlife management application—to promote digital literacy capacity-building. After assessing the staff's digital literacy levels, ensure that the intervention builds on their current levels of digital knowledge.

Enhance the ability of energy and water services utilities—including all actors along the supply chain—to identify, prevent, and respond to cyberattacks. This includes keepin. special cybersecurity bodies, like Information Sharing and Analysis Centers (ISACs), informed on the status and parameters of the intervention.

Promote the adoption of relevant ISO 27000[3] series and NIST standards,[4] (like NIST's Cybersecurity Framework) for information security management.

» AT THE NATIONAL AND LOCAL GOVERNMENT LEVEL:

At the policymaking level, work with government ministries and agencies to institutionalize best practices for cybersecurity into their standards, procurement processes, and supply chain management approaches, especially for critical infrastructure.

At the institutional level, embed digital literacy and capacity-building into existing structures, such as Agency training units.

At the government personnel level, expand awareness of and strengthen the capacity of EEI decision-makers and operational staff in digital literacy, particularly with regards to responding to cyber threats. This aligns with the emphasis on developing human capacity in USAID's Digital Government Model.

- At the executive level: Engage senior leaders in the public and private sector in digital literacy activities to help influence their teams to take up informed and effective digital literacy practices.
- At the mid- and junior levels:
  - To avoid losing institutional knowledge on cybersecurity, include deputies and other mid- or low-level staff in training and other digital literacy interventions, as they will be responsible for operationalizing new strategies.
  - Develop and maintain reference documents that will help future employees learn how to operationalize digital literacy practices.

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

[3] Also known as the ISO 27000 Family of Standards, this is a series of information security standards that provide a global framework for information security management practices. They are published and developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

[4] NIST develops and disseminates the standards that allow technology to work seamlessly and business to operate smoothly.

USAID'S DIGITAL STRATEGY

USAID's Digital Strategy was launched in April 2020 with the goal of supporting USAID partner countries through their digital transformations. It aims to improve measurable development and humanitarian assistance outcomes through the responsible use of digital technology and to strengthen the openness, inclusiveness, and security of partner country digital ecosystems.