The United States Has an Opportunity to Lead in Digital Development

By Daniel F. Runde, Romina Bandura, & Sundar Ramanujam

Introduction

Despite the significant global economic and social progress achieved in the past 30 years, many countries in the developing world are grappling with financial inclusion challenges (see Appendix A). Technology-enabled strategies can address challenges such as the two billion adults who still transact on a cash basis, the 35 percent of women globally excluded from the formal financial system, and the $110 billion in tax revenue losses incurred by governments annually. Moreover, many of these economies have high levels of informality, with millions of people operating outside of formal regulations and tax structures, lacking official identification (ID), and being excluded from the financial system writ large. Regulatory challenges, weak governance, lack of access to digital infrastructure, and other structural and sociocultural barriers explain the global gaps in this space (Figure 1).

Figure 1: Elements of the Digital Financial Inclusion Ecosystem

Source: Author’s own analysis.
As the fourth industrial revolution continues to unfold, developing digital payments and digital ID infrastructure (e.g., real-time retail payment systems, inclusive ID systems, credit information, and internet and mobile access) can help address the structural problems of financial exclusion and informality. One area where significant investments are needed is digital infrastructure. Even though developing countries have made progress in providing access to mobile telephony, according to the Global System for Mobile Association (GSMA), only 40 percent of the population in developing countries (2.6 billion people) is connected in terms of mobile internet, compared to almost 75 percent in advanced economies. Even then, women are 14 percent less likely to own mobile phones than men. Moreover, four billion people in developing countries have no access to the Internet, and 789 million have no electricity access. A digital-first financial inclusion strategy—cloud-powered, data-driven, and built on greater access to reliable high-speed internet—can help countries take steps to formalize their economies and help citizens become economically empowered, paving the way to building more inclusive societies.

The unforeseen devastation caused by the Covid-19 pandemic has highlighted the importance of digital payments and digital ID infrastructure for mitigating socioeconomic challenges. Consider countries like India, whose government over the past decade has made a strong push to implement a universal digital ID, an interoperable digital payment system, and near-universal bank account access. Currently, India is in a position to quickly distribute funds to hundreds of millions of low-income households. The system has been in use since 2013, long before the pandemic struck, when the Indian government converted its US$8 billion domestic cooking fuel subsidy program into direct cash transfers to the bank accounts of beneficiaries—verified by its unique biometric identification system.

Even before the global Covid-19 pandemic pushed the world to adopt digital solutions, the digital revolution was rapidly transforming how global markets and economies function. From healthcare and education to retail and public service delivery, digital technologies—and the internet in particular—have become as essential a service in modern households as electricity and water supply. Unsurprisingly, digital infrastructure has joined the ranks of the “commanding heights” of any economy, that is, an essential sector for economic growth. In response, developing countries are seeking investments from abroad to help solve their digital infrastructure needs.

**Digital ID, digital payments, and data governance are each important individually. Together, they add up to a powerful public good. This combination is as crucial to today’s economies as roads and railways were to those of the twentieth century.**

— World Economic Forum

Without significant leadership and investment from the United States, low- and lower-middle-income countries find themselves drawn toward alternative digital models offered by China and other more authoritarian-minded actors. These models subvert civil liberties such as the rights to privacy and free expression, undermine the rule of law, and enable social oppression. Moreover, these forms of digital infrastructure often come with strings attached, which not only undermines the sovereignty of countries but also incentivizes them to pursue a model of development that does not serve the strategic and security interests of the United States and its allies. The United States has an opportunity to engage in—even lead—the digital financial and ID infrastructure space, helping countries unlock their full economic and...
social potential. At the same time, investments abroad can help the United States achieve its own national security priorities while creating new markets for U.S. goods and services.

**Global Benefits of Investing in Digital Financial and ID Infrastructure Systems**

Investing in safe and secure digital financial and digital ID infrastructure can have substantial positive economic and social impacts in the developing world. As the world becomes increasingly digital, secure infrastructure can significantly expand access to capital and information, both of which are critical for the sustained growth of markets. It will also be catalytic in achieving the United Nations’ [Sustainable Development Goals (SDGs)](https://www.un.org/sustainabledevelopment/) by 2030.

Digital financial tools, in particular, can create new avenues for accessing international markets and building economic resiliency, in turn spurring job creation (SDG #8) and reducing inequalities (SDG #10). Moreover, in societies with more restrictive or orthodox value systems, digital technologies can also help democratize the financial sector, empowering women to overcome structural and sociocultural barriers and encouraging gender equality (SDG #5) in financial and economic systems. Specifically, digital financial tools have an immense potential to close the 9 percent gender gap in developing countries’ financial inclusion through access to formal credit, financial literacy, and autonomy over financial decisions. They also eliminate the need to physically travel to banks (often an improbable feat in specific socioeconomic contexts) and provide verifiable risk assessment tools for new lending and investment in women-owned enterprises.

More importantly, closing the gender gap will require a coordinated and gender-intentional approach to the design of regulatory frameworks. Scaling up existing infrastructure could potentially exacerbate current inequities. For instance, women and other marginalized populations often need and value aspects like digital privacy more than others in society, as they are more likely to be subject to violence, harassment, or exploitation should their data become public. Similarly, in countries where social norms or legal barriers limit women’s economic engagement, digital financial tools can actually make the existing gender gap worse by facilitating rapid adoption by men and limited adoption by women. For example, many women around the world are “invisible”: they lack proper identification, which acts a significant barrier to their engagement in society, government, and the economy. Women living in low-income countries (LICs) are particularly disadvantaged in accessing a national ID (see Figure 2). Still, policymakers and development partners continue to explore how such considerations can be at the heart of a digital strategy that seeks to support the development of digital financial and ID systems.

**Figure 2: Gender Gaps in ID Access**


With more than 1 billion people in the world lacking formal identification (ID) and another 3.4 billion people having some form of ID but limited ability to use it in the digital world, expanding these systems can profoundly impact citizens and economies. Within SDG #16, target 16.9 specifically addresses this “identity gap,” stating that by 2030 countries should “Provide legal identity for all, including birth registration.” ID enables individuals to get a job, build their credit, and access other public services.

In this regard, advances in technology can help countries circumvent paper-based IDs to instead focus on digitally-based IDs. These digital IDs, in turn, facilitate the achievement of other critical SDGs—for instance the more targeted distribution of welfare benefits, particularly for those at the brink of abject poverty (SDG #1); food and nutrition subsidies that will eliminate hunger (SDG #2) and ensure food security; universal access to healthcare (SDG #3); and access to quality education (SDG #4) through increased school enrollment of youth. The use of this digital ID system creates a reservoir of data and metrics that can subsequently be used by the state to assess the impact of its programs while also creating accountability within the system.

Investment in secure digital financial systems and digital ID infrastructure can create many benefits for governments, civil society, and the private sector, ultimately fostering sustainable and equitable development. However, the biggest challenges in implementing digital financial infrastructure involve obtaining enough financing to close the investments gaps, implementing transparent and democratic regulatory and legal frameworks to govern these systems, and guarding these systems against cyber intrusions.

Why Should the United States Invest and Engage in Digital Financial and ID Infrastructure?

Developing countries are increasingly coming under pressure to modernize their economies and invest in digital solutions, with the Covid-19 pandemic only compounding this challenge. In response to these pressures, developing countries seek infrastructure investments and technological partnerships from abroad. As the digital revolution continues to disrupt the global landscape, nations such as China and Russia are asserting their influence in geopolitics using digital investments that threaten Western values rooted in democratic traditions of individual liberties and dignity.

In the absence of a democratic values-based alternative, countries are left to engage with authoritarian-minded actors to meet their digital infrastructure needs. These digital infrastructure formats contain severe security and privacy vulnerabilities, which may then be exploited by political actors—both in the investing country and the recipient countries. These efforts can subvert civil liberties such as the rights to privacy and free expression, undermine the rule of law, and increase oppression in the affected countries.

As the 2018 National Cyber Strategy informs, from a U.S. national security perspective, yielding the design and development of global digital infrastructure to more authoritarian-minded actors would compromise U.S. strategic interests and the nation’s ability to maintain the liberal and democratic international order from which it has benefitted for over a half-century. The Bush administration’s National Security Strategy (2006) brought to prominence the concept of a “3D” security framework (i.e., tying national security to defense, development, and diplomacy) to enable a holistic response to complex global existential threats like terrorism, climate change, and pandemics. Today, the challenges posed by authoritarian alternatives to digital financial and identity systems also warrant a holistic response from the U.S. government, grounded on a “3D” framework.
INVESTING IN DIGITAL FINANCIAL INCLUSION AND DIGITAL ID HAS U.S. NATIONAL SECURITY IMPLICATIONS

A first national security consideration is maintaining the role of the U.S. dollar as the de facto global reserve currency, since it has given the United States unprecedented influence over the international financial system. The United States has leveraged the dollar’s status to enforce international sanctions on human rights violators and terrorist groups. With the vast majority of global banking functions conducted in USD, the U.S. Department of Treasury has become a critical player in developing and enforcing U.S. national security policy, wielding its sanction powers in pursuit of U.S. strategic interests. Suppose alternative digital financial systems—powered by authoritarian actors—can capture the market. In that case, sanctions will become less impactful, which will hurt U.S. influence in combatting transnational security threats. On a fundamental level, a values-based design and implementation of the digital payment and ID infrastructures could strengthen financial integrity by reducing informal and illegal transactions and ensuring the ability to identify individuals and trace payments.

A second national security consideration surrounds the standards involved in developing critical digital infrastructure. Experts and analysts have raised concerns about the integrity of the systems developed by non-democratic sponsors and their vulnerabilities to exploitation by leaders with authoritarian tendencies. Specifically, concerns around data privacy, surveillance, espionage, and intellectual property theft elevate any discussion around global digital infrastructure investment to the national security space. China leads these digital authoritarianism efforts and has been leveraging technologies to engage in cyberattacks and espionage. Malicious cyber activity in 2016, including business disruptions and theft of proprietary information, cost the U.S. economy $109 billion. These efforts are amplified when quasi-commercial enterprises (such as Huawei) successfully expand their global footprint and influence technological platforms’ development, including the design of infrastructure and regulations for digital finance and ID in developing countries. China has markedly increased foreign direct investment and infrastructure projects in Africa, particularly in the digital space (dubbed the “Digital Silk Road”) while simultaneously growing its surveillance capacity in the region. Currently, 70 percent of the 4G networks in Africa are built by Huawei. Meanwhile, the Chinese telecom company will likely look to build up 5G on the continent. Chinese technology companies offer cheap and attractive products and services. The United States and allies must compete at the procurement table regarding digital projects.

A third national security implication relates to the evolution of global internet governance. The current model, built on Western values, has long protected an open and secure internet that has allowed civil society to thrive in oppressed regimes. This multistakeholder model has enabled the internet to expand at an unprecedented pace, generating business opportunities and wealth worth billions of dollars. Alternatives to this multistakeholder model would result in the internet’s fragmentation, giving way to governments to exercise unrestricted control over the content flows in its digital space. This lack of accountability could foster author-
itarianism and extremism and boost the prospects of illicit economic actors, undermining existing security and development efforts. Additionally, a fragmented internet would also hurt global technology companies, as protectionist sentiments can be expressed by blocking content and platforms built or used in other countries. U.S. leadership will be vital in stopping efforts to move away from the existing multistakeholder model of global internet governance.

In sum, preserving U.S. influence in this space will be critical for any U.S. national security strategy. As a result, disengaging from the global digital infrastructure development race will only reduce U.S. influence and hurt the nation’s ability to protect its security interests while allowing strategic competitors to fill the vacuum.

INVESTING IN DIGITAL FINANCIAL INCLUSION AND DIGITAL ID HAS U.S. DIPLOMATIC AND COMMERCIAL IMPLICATIONS

In addition to national security consequences, a lack of U.S. investment and leadership in this area would also have long-term diplomatic and commercial implications. As evidenced by the space exploration race of the 1960s and the telecom revolution of the early 2000s, U.S. supremacy in digital infrastructure offers a first-mover advantage to shape and influence the broader ecosystem for decades. With close to one billion people without electricity access, half of the world still unconnected to the internet, and more than 1.7 billion persons unbanked, there is a real opportunity for private investors to benefit from closing these digital and financial inclusion gaps.

U.S. businesses—retail, fintech, and others—have much to gain from the development of digital infrastructure that facilitates widespread e-commerce adoption. An estimated 1.9 billion people purchased goods online in 2018. E-commerce and related sectors have only continued to grow since, particularly in large emerging markets in Africa, Asia, and the Americas, amounting to approximately $3.5 trillion in 2019. As the middle class expands worldwide, there should be little doubt that early intervention by the U.S. private sector in global digital development will create long-term and sustainable economic partnerships that benefit the United States and developing economies alike: a win-win strategy. In 2020, the global digital payments market hit $5.4 trillion dollars in transaction value. Currently, China leads this market, with Chinese firms generating $2.9 trillion of all value. U.S. digital payments firms trail behind, generating only $1.26 trillion in value in 2020—less than half the size of the Chinese industry. That said, between 2019 and 2020, the U.S. digital payments industry grew at a faster rate of 23 percent, compared to the 17 percent growth enjoyed by Chinese digital payment firms during that same period.

To remain competitive, the United States needs to increase its investments in digital financial infrastructure—and more specifically, in retail payment systems and financial technology and services, which include e-payments, savings, remittances, and insurance. Following the Covid-19 pandemic, countries have a unique opportunity to build the infrastructure and tools necessary to establish interoperable systems founded on U.S. technology. To accomplish this, U.S. private sector engagement is equally important. Supporting the private sector will foster innovation and increase U.S. products, services, and influence in global digital development, and it will provide alternatives to e-payment platforms such as the Chinese Ali-pay.

INVESTING IN DIGITAL FINANCIAL INCLUSION AND DIGITAL ID HAS DEVELOPMENT IMPLICATIONS THAT ALIGN WITH U.S. FOREIGN POLICY GOALS

As already discussed, investing in digital financial inclusion and ID infrastructure can yield many development benefits. Expanding access to financial products and services for low-income people, women, and other excluded groups has the ability to produce significant economic and social results,
including the ability to improve income-generating opportunities, smooth consumption, increase savings, manage financial risks, and advance women’s economic empowerment. Moreover, strengthening governments’ digital systems can enable them to deliver payments and services more efficiently, cost-effectively, and equitably.

Yet, the development benefits of digital financial inclusion and ID infrastructure are not limited to these benefits. They are broader in nature and well-aligned with the U.S. foreign policy goals laid out in the U.S. Department of State and the U.S. Agency for International Development (USAID) Joint Strategic Plan (2018–2022) and USAID’s “Journey to Self-Reliance,” which seeks to promote countries’ ability to graduate from foreign aid. These more nuanced benefits include: (1) for citizens and business, the ability to participate more formally in an economy and create employment; (2) for governments, the capacity to expand taxation and reduce waste; and (3) for economies, the propensity to increase cross-border trade and reduce fraud.

First, increased digitalization can lead to more economic formalization by allowing citizens and businesses to perform essential functions like registration, taxation, contracts, and social insurance. For example, in July 2014, Estonia launched its electronic register for tax and customs, which saw more than 70,000 companies and over 600,000 employees register in just under four months (by November 2014), resulting in increased labor tax declarations amounting to $6 million, as well as 9,000 new taxpayers. Similarly, Peru’s electronic payroll system, established in 2006, helped increase registered and formal employment, and improved direct communication with more businesses. The system includes the T-Registro system, which serves as a worker registry, and the Monthly Payroll (PLAME), which tracks time worked, tax deductions, and worker income. From 2002 to 2011, registered employment in businesses with greater than four workers increased from 930,000 to 2.4 million.

At the same time, the use of digital technologies can help close the gender divide and increase economic productivity by targeting the untapped potential of women entrepreneurs and workers, as evidenced by U.S. development programs like USAID’s WomenConnect Challenge. This program funds women-driven technology initiatives—such as in the Dominican Republic, where using mobile phones to test new credit score models helps women access loans, and in Senegal, Morocco, Kenya, and Namibia, where rural women are getting support to run local internet service providers.

Second, digital technologies are also critical for e-governance initiatives that can transform developing countries’ domestic resource mobilization (i.e., tax collection and savings) and public finance capabilities. Specifically, governments can enhance their ability to collect taxes, make their public procurement process more transparent, and eliminate leakages in welfare distribution systems. These benefits can be seen in a number of ongoing development investments and programs. The Better Than Cash Alliance, a 75-member global coalition of development actors (including USAID), found that a 2010 Budget Decree requiring all federal agencies to switch to digital payments (rather than cash) has helped the Mexican government save nearly $1.3 billion (or 3.3 percent of its expenditure on wages, pensions, and social transfers) annually. This was achieved through legal, infrastructure, and business processes changes which were digitized, centralized, streamlined, and reliably accounted for payments. USAID has also supported digital transformation of the Filipino tax administration system, which helped drastically increase its e-filing rates from 8 to 80 percent between 2013 and 2019. As a consequence, the government of the Philippines was able to generate $3.5 billion in additional tax revenue in 2018 that was then used to fund infrastructure and other public investments.
Third, digitalization can also enable **cross-border trade** by increasing transparency and boosting overall customs management. This reduces costs, expands trade portfolios, helps establish connections between businesses making supply chains more efficient, and curbs illegal smuggling. According to the World Trade Organization, mainstreaming digital technologies in global trade could reduce costs by an **average of 14.3 percent while boosting trade by over $1 trillion**. In the case of the European Union, the International Monetary Fund found a positive association between **increased digitalization of trade and reduced cases of fraud** in 28 countries. Similarly, in Costa Rica, after implementing the $1.7 million electronic single window system, **exports** increased by 2 percent annually between 2007 and 2013. Coupled with the reduction in overhead administrative costs, Costa Rica saw a sixteen-fold return to every dollar it invested in this system.

**What Should the Biden Administration Prioritize?**

The United States government remains active in the digital space and has recently enacted a series of related strategies and policies. The past Trump administration launched a series of strategies and policy documents addressing global digital infrastructure, including the U.S. National Cyber Strategy (2018), National Security Strategy (2017), and National Strategy for Counterterrorism (2018). In the development and diplomacy fields, relevant documents include the Department of State-USAID Joint Strategic Plan (2018–2022), USAID Policy Framework (2019), and USAID’s Digital Strategy 2020–2024 (see Appendix B). The United States also participates in many international commitments (see Appendix C). Although data on U.S. digital investments and commitments is not readily available, a preliminary survey of key digital development initiatives conducted by CSIS found that the U.S. government had committed a minimum of $10 billion since 2014, funding initiatives from the State Department, USAID, the Millennium Challenge Corporation, and the Development Finance Corporation (DFC) (formerly known as the Overseas Private Investment Corporation). These investments supported a wide range of initiatives that CSIS has deemed to be critical for sustained digital development (see Box 1).

As the pace of digital development accelerates, the United States will need to increase its engagement and investments in digital financial inclusion to remain competitive and lead the field. The Biden administration has an opportunity to increase its engagement, but it will need to be strategic in its approach.

In a now-famous *Foreign Affairs* article, President Biden highlighted the various opportunities for the United States to lead the quality- and standard-setting charge for the global digital revolution and acknowledged the dangers of the United States abdicating its responsibilities in leading the liberal international order. Consistent with his policy objectives, the Biden administration should approach digital financial inclusion and ID infrastructure on three main fronts:

**CRAFTING A COMPREHENSIVE U.S. DIGITAL STRATEGY**

Since 9/11, every U.S. administration has put forth cybersecurity strategies that have committed to securing U.S. digital infrastructure. Given that we live in an age of an interconnected world, and given the nature of the digital ecosystem, efforts to secure our digital assets also require timely and significant interventions and investments abroad. Recognizing this, USAID launched its first-ever **digital strategy in 2020**, which laid out how the agency would adapt its foreign assistance programs and operations to the age of technological revolution while advancing core democratic principles.
Although these represent significant efforts, the United States needs to develop a more comprehensive strategy that ties all these different elements together and provides an interagency approach. The development of a comprehensive U.S. digital strategy that addresses both domestic and foreign engagement should begin with a review of past strategies that map out various agencies’ interests and equities concerning digital finance and digital identity systems. In carrying out this exercise, the new strategy should identify the lessons learned from past strategies and pursue a more coordinated approach across the U.S. government. U.S. bilateral development aid agencies such as USAID, the DFC, and the United States Trade and Development Agency (USTDA) should be part of the process alongside the Department of Defense and State Department. Foreign aid and development finance tools are critical in combatting digital authoritarianism’s growing menace and in building U.S. global leadership.

**LEVERAGING PUBLIC-PRIVATE PARTNERSHIP**

Second, the administration should consider partnering with the U.S. private sector, which is willing and eager to expand its role and its market in developing the infrastructure for digital finance and identity. The Biden administration should leverage one of the United States’ most prominent assets: an innovative and
The resilient private sector that can mobilize hundreds of billions of dollars in investment capital. This will require a regulatory framework that considers security and economic stability to facilitate greater market access for technology firms while also providing the guardrails to preserve democratic norms and values in the digital ecosystem. The framework can also facilitate interoperability across platforms offered by different firms so long as they are consistent in safeguarding digital rights such as privacy and data security. At a time when other governments and supranational entities (such as the European Union) are developing more regressive regulatory safeguards, a partnership allows the business sector to engage closely with the U.S. government and ensure that global standards are adopted.

Partnerships with the private sector can take various other forms. Without resorting to a statist intervention for the digital industry that resembles industrial policies in the mid-twentieth century, the Biden administration should recognize the opportunity for the U.S. government to provide short-term subsidies that will generate long-term benefits in the form of national security and stable commercial partnerships. Examples include offering grants for pilot projects to advance research, development, and innovation; subsidizing critical infrastructure platforms; and using tools like guarantees to underwrite risks for investments of strategic significance.

REIN VIGOR ATING U.S. ALLIANCES AND LEADING IN THE MULTILATERAL SYSTEM
Third, the United States needs to reinvigorate its alliances and lead various multilateral fora to ensure that standards (developed through stakeholder consultations) are adopted and enforced internationally. Multilateral engagement will be necessary to execute any U.S. digital strategy at the international level. Along with the multilateral system, the United States and its allies can work together to create a regulatory framework around digital development that protects human rights and freedoms and promotes digital inclusion worldwide. Specifically, the United States should build off initiatives such as the Digital Connectivity and Cybersecurity Partnership (DCCP) and the Digital Single Market and set universal standards and international law around data privacy, digital trade, cybersecurity, localization, digital ID, and systems interoperability.

Restoring the multilateral system’s role and relevance has been the single and most identifiable hallmark of President Biden’s foreign policy campaign strategy. However, realizing this goal will require meticulous diplomatic lobbying and the bringing together of allies, friends, and partners who have diverging interests in the digital communications and infrastructure sector. The administration can begin these efforts by taking advantage of the 2021 G20 and G7 Summits, led by Italy and Britain (respectively). Policy dialogues around the digital revolution will be prominent. By coordinating closely, President Biden’s diplomatic team can ensure that the United States is closely aligning itself with like-minded democratic countries’ interests at both summits. The G7 Summit is of particular significance, given member states’ commitment to addressing the “frictions in existing digital payment systems,” including strengthening the sector’s integrity, improving its efficiency, and lowering costs for consumers. Other opportunities include the Britain-backed “D10,” which would effectively add three democracies (Australia, India, and South Korea) to the G7 as a club of the 10 largest democratic economies with shared interests and which can tackle common challenges. Of course, the administration does not need to limit itself to the 10-member limit, considering how other economies like Israel, Estonia, and Finland share the D10’s commitments for a principles-based global digital payments system.

Beyond the opportunities at annual diplomatic summits, key officials in the administration should be competing in leadership elections at valuable standard-setting bodies (such as the International Telecommunications Union and the World Intellectual Property Organization) within the UN system. Without
adequate planning or timely action, the United States can suffer long-term consequences to its leadership and ability to set global standards if such elections end up elevating officials nominated by adversarial powers like Russia and China. As President Biden and his foreign policy advisors consider appointments to the State Department, particular attention should be paid to the Bureau of International Organization Affairs. They will be charged with setting U.S. policy toward these bodies.

**Conclusion**

The change in administration is an opportunity for the United States to lead in the development of digital financial and ID infrastructure globally. This will not only yield benefits to the United States in terms of national security, diplomacy, and commercial interests; it will also strengthen developing countries’ capacity to address the structural problems of financial exclusion and informality, help people become economically empowered, and pave the way to building more inclusive and resilient societies. By contrast, failure of the United States to lead would result in a fragmented internet, less secure and more opaque digital transactions, and a weakened liberal international order. Investing in digital infrastructure and demonstrating leadership in developing the norms and standards governing the global digital landscape will have long-term implications for the United States and its partner countries that share common aspirations.

Daniel F. Runde is senior vice president, director of the Project on Prosperity and Development (PPD), and holds the William A. Schreyer Chair in Global Analysis at the Center for Strategic and International Studies (CSIS) in Washington, D.C. Romina Bandura is a senior fellow with PPD and the Project on Leadership in Development at CSIS. Sundar Ramanujam is a research associate with PPD at CSIS.

Support for this publication was provided by the Bill & Melinda Gates Foundation. The views expressed here do not necessarily reflect the views of the Gates Foundation.

This report is produced by the Center for Strategic and International Studies (CSIS), a private, tax-exempt institution focusing on international public policy issues. Its research is nonpartisan and nonproprietary. CSIS does not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s).

© 2021 by the Center for Strategic and International Studies. All rights reserved.
### Appendix A

**Definitions**

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FINANCIAL INCLUSION</strong></td>
<td>Individuals and businesses that have access to useful and affordable financial products and services that meet their needs—transactions, payments, savings, credit, and insurance—delivered responsibly and sustainably. (<em>World Bank</em>)</td>
</tr>
<tr>
<td><strong>DIGITAL TECHNOLOGIES</strong></td>
<td>Platforms, processes, and a range of technologies that underpin modern information and communications technologies (ICT), including the internet and mobile phone platforms, as well as advanced data infrastructure and analytic approaches. (<em>USAID</em>)</td>
</tr>
<tr>
<td><strong>DIGITAL FINANCIAL INCLUSION</strong></td>
<td>Digital access to and use of formal financial services by excluded and underserved populations. Such services should be suited to the customers’ needs and delivered responsibly, at a cost both affordable to customers and sustainable for providers. (<em>CGAP</em>)</td>
</tr>
<tr>
<td><strong>DIGITAL IDENTITY</strong></td>
<td>A set of electronically captured and stored attributes and/or credentials that uniquely identify a person. (<em>World Bank</em>)</td>
</tr>
<tr>
<td><strong>DIGITAL ID SYSTEMS</strong></td>
<td>A technology-enabled platform that establishes formal identification for populations to increase civic, economic, political, and social participation and provide community benefits. It also helps governments deliver necessary citizen services (e.g., welfare programs, voter registration, licenses, and certifications). Specific systems currently vary in model, level of digital integration, trust and transparency, and registration. (<em>USAID</em>)</td>
</tr>
<tr>
<td><strong>DIGITAL FINANCIAL INFRASTRUCTURE</strong></td>
<td>The necessary physical and digital components—such as broadband, mobile networks, or POS terminals—critical to facilitating digital financial services and resources. This includes financial technology that services transactions, payments, credit, savings, remittances, and insurance. (<em>OECD</em>)</td>
</tr>
</tbody>
</table>
Appendix B
Current U.S. Strategies on Digital Development

NATIONAL SECURITY STRATEGY (2017)
The 2017 National Security Strategy underscores that the United States will need to increase its competitiveness to counter Chinese and Russian strategic actions and malign actors. The digital aspects of the National Security Strategy include protecting infrastructure and building up cybersecurity strategies, promoting U.S. prosperity, and advancing U.S. influence through renewing U.S. competitive advantages and capabilities in cyberspace. The document identifies the following as priority actions that would strengthen the United States’ cyber defense capabilities:

- identifying and prioritizing risk
- building defensible government networks
- deterring malicious cyber actors
- improving interoperability
- deploying layered defenses

The strategy also aims to increase research in science and technology, promote U.S. innovation and exports, and protect U.S. inventions and ideas through methods such as intellectual property rights and digital security infrastructure. Overall, the United States should lead in cutting-edge technologies and cyberspace to facilitate foreign policy initiatives (i.e., information statecraft) and promote U.S. national security.

NATIONAL CYBERSECURITY STRATEGY (2018)
The 2018 National Cybersecurity Strategy proposes a whole-of-government approach to effectively implement cybersecurity strategies and advance national security interests. Four pillars are identified as cybersecurity priorities:

I. Protect networks, systems functions, and data for national security
II. Promote U.S. prosperity by helping build a digital economy and advancing U.S. technological innovation
III. Preserve peace and security
IV. Increase U.S. global influence and ensure an open, interoperable, secure internet and digital space

Pillar I underscores the importance of increasing government oversight of digital activities to counter threats and of improving upon digital risk management systems to better protect supply chains and defense efforts. Additionally, the U.S. government should lead in cyber strategies. These efforts should help identify risks to the United States and preserve democratic institutions. Pillar II focuses on fostering economic growth, innovation, and the efficiency of digital networks and systems through resilient cyberspace. This includes expanding broadband and network infrastructure, continuing U.S. leadership in emerging technologies (artificial intelligence, machine learning, blockchain), maintaining intellectual property rights protections, building a cybersecurity workforce, and advancing U.S. economic interests. Pillar III seeks to preserve peace by countering malign actors in cyberspace, setting universal cyber norms, and encouraging adherence to these norms in the international community. Lastly, Pillar IV aims to use digital technologies
to advance U.S. influence and secure open digital space. Priority actions include securing internet freedom, working with allies to advance digital technologies and U.S. priorities, helping build infrastructure globally to increase opportunities for U.S. actors, and promoting the use of U.S. technologies and digital services. Additionally, it emphasizes the importance of building cyber capacity to counter threats to digital systems.

**NATIONAL STRATEGY FOR COUNTERTERRORISM (2018)**

The 2018 National Strategy for Counterterrorism aims to protect U.S. citizens and interests, both in the United States and abroad. The strategy seeks to increase U.S. capacity to address threats, learn from the past, and reduce terrorism globally. The strategy includes modernizing U.S. counterterrorism tools to build up defense agencies’ cyber capacities and resources. The United States will look to work with allies to reduce terrorist cyber capabilities and cyberattacks. Strategies to protect U.S. infrastructure and resilience will also require secure digital systems.


The Joint Strategic Plan developed by the State Department and USAID for fiscal years 2018 to 2022 outlines the United States’ foreign policy priorities to “lead . . . and unit[e] the free world around American values to uphold liberty,” including countering bad actors, increasing economic opportunities for U.S. businesses, investing in U.S. innovation, and private sector engagement. The plan identifies how these priorities can maintain an open and free digital economy and global environment. For example, these can be achieved through establishing cybersecurity initiatives, increasing U.S. digital exports and services (e.g., data flows and operating systems), and promoting technology businesses. The State Department and USAID also plan to increase digital literacy programs, invest in digital infrastructure development to foster digital access and entrepreneurship, implement U.S. digital ID systems in partner countries, and increase access to cloud systems and business data to facilitate economic activity.

**U.S. AGENCY FOR INTERNATIONAL DEVELOPMENT DIGITAL STRATEGY (2020–2024)**

USAID launched its first-ever Digital Strategy (for fiscal years 2020 to 2024) to facilitate global digital transformations in industry, government, economy, and society, with the aim to achieve greater resiliency, reduced inequality, better digital ecosystems, and improved development in emerging countries. Through their various operating units (OUs) and strategic objectives, USAID’s programs aim to increase digital service access, thereby helping partner countries implement digital resources to complement government, social, and economic activities. USAID’s strategic objectives include using digital tools and resources in USAID development and assistance programming to increase digital inclusion and digital infrastructure in partner countries. Improving digital ecosystems increases government, citizen, economic, and civil society capacity and enables development efforts. USAID digital programs include increasing government accountability and transparency, facilitating economic and e-commerce activities, empowering youth leadership, improving land titling systems, increasing access to data and information, and using cutting-edge strategies to help design and implement projects and systems (e.g., artificial intelligence and machine learning). USAID strategies also aim to counter threats created in the digital space, including risks to privacy and security, online extremism, misinformation and disinformation, and digital resource exclusion. USAID will use digital tools to make foreign aid more effective and efficient, implement a monitoring and evaluation system to improve upon its efforts, and work in conjunction with partner country governments and civil society to guide its development assistance efforts across USAID program cycles. USAID will also work with other U.S. agencies to take a whole-of-government approach to digital development and inclusion.
U.S. DEPARTMENT OF STATE DIGITAL CONNECTIVITY AND CYBERSECURITY PARTNERSHIP

The Digital Connectivity and Cybersecurity Partnership (DCCP) is a whole-of-government effort to promote open networks, expand secure access to the internet in developing countries, promote U.S. innovation and exports, and enhance cybersecurity globally and in the United States. The DCCP was established in July 2018 with a $25 million investment and will contribute to digital connectivity, ICT development, technical assistance and public-private partnerships, economic and commercial opportunities for U.S. companies, digital regulatory policies, and cybersecurity capacity. Each U.S. agency incorporates DCCP objectives into their priorities and harnesses their respective capabilities to promote the initiative. For example, USTDA helps develop projects to support open, interoperable, reliable, and secure communications and internet through partnerships with the private sector and investors. Additionally, USAID has improved technical assistance in partner countries to better advance initiatives. Under the DCCP, USAID will help strengthen domestic self-reliance in partner countries to monitor ICT infrastructure, expand digital economic opportunities, increase digital technology use in government and business, and empower civil society through a free internet and access to resources. In the Indo-Pacific, the DCCP works in partnership with ASEAN and helps build ICT, connectivity, emergency communications, cybersecurity, and “smart city” capacities.
Appendix C

Key Multilateral Initiatives on Digital Development

ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT (OECD)

As demand for digital tools and network connectivity increases, the global digital divide remains large. The OECD Going Digital Project looks to support a global digital transformation by increasing the openness of access, use, innovation, trust, jobs, society, and markets through digital strategies. Although digital integration and innovation provide many social and economic benefits, a careful regulatory policy should be constructed to prevent technological abuse and exclusion. The OECD has identified potential policy recommendations and analysis to help understand the drivers of digital transformation and to identify how governments, businesses, and organizations can harness digital resources for development. The Going Digital Project argues that countries should increase access to communication infrastructure, services, and data; build capacity to effectively use digital technologies and data; invest in data-driven and digital innovation across sectors; increase digital literacy and training to ensure job opportunities; regulate and increase access to online digital platforms; combat digital misinformation and disinformation campaigns; build trust and consumer data protection guarantees; and facilitate transactions in an open digital market. Digital policies will need to be comprehensive, integrated, coordinated, compatible, and transparent in all policy areas in order to be effective and to develop digital capacity across sectors.

G20 PRINCIPLES ON FINANCIAL INCLUSION

The Toronto G20, held on January 27, 2010, established the G20 Principles for Innovative Financial Inclusion. These principles stem from a combination of G20 members’ and global policymakers’ experience and expertise in financial inclusion strategies. The nine principles are leadership, diversity, innovation, protection, empowerment, cooperation, knowledge, proportionality, and framework. Governments should help increase access to and usage of financial services, promote technological and digital strategies to improve access and infrastructure (e.g., mobile networks), implement financial literacy programs, monitor projects, and develop a regulatory framework that is compatible with digital solutions. The Principles are meant to serve as a guide for policymakers in a variety of country contexts to increase innovative financial inclusion and protect citizens’ and consumers’ financial stability.

THE WORLD BANK’S PRINCIPLES ON IDENTIFICATION FOR SUSTAINABLE DEVELOPMENT

The World Bank’s Principles on Identification for Sustainable Development include three broad categories: (1) inclusion (universal coverage and accessibility); (2) design (robust, secure, responsive, and sustainable); and (3) governance (building trust by protecting privacy and user rights). The principles align with and help achieve the UN Sustainable Development Goals, helping to empower individuals and promote economic growth, public services, and human rights. Currently, 1.5 billion people in the developing world lack an official and verifiable identity document, which creates enormous economic, political, and social challenges for communities and countries. Lacking an ID can prevent individuals from participating in the formal economy; accessing financial, health, and government services; and enrolling in education programs. ID systems can help strengthen the efficacy and capacity of governments, the private sector, multilateral organizations, and development institutions to implement development and capacity-building programs. ID systems can also help further development efforts by accelerating the digital transformation and providing more opportunities in society and in the economy for citizens. Building off international norms, the Principles on Identification aim to encourage multilateral and governmental collaboration and participation, with the goal of helping to create a more inclusive and integrated world.
THE WORLD BANK’S IDENTITY FOR DEVELOPMENT (ID4D)

Identity for Development (ID4D) is a World Bank initiative that helps countries build more inclusive digital ID systems that can increase financial inclusion, health service benefits, social protection, and economic empowerment of women and girls. Currently, about 40 percent of adults in low-income countries lack an official form of identification, and there is a significant gender disparity in ID distribution, with 45 percent of women not having an ID compared to 30 percent of men. ID4D provides analytics, assessments, and financing capabilities to run country diagnostics, technical assistance, and advisory services relating to the design, implementation, regulation, integration, evaluation, and engagement of digital ID systems. The initiative has identified digital ID systems as a crucial foundational element for realizing the UN’s Sustainable Development Goals and works across the World Bank Group, multilateral organizations, governments, private sector, and non-profit organizations to promote and accelerate ID4D’s work. The initiative prioritizes advocacy and strategic discussion, in-country implementation support, and local in-person support to facilitate the development and implementation of digital ID systems.

AFRICA DIGITAL FINANCIAL INCLUSION FACILITY (ADFI)

The Africa Digital Financial Inclusion Facility (ADFI) is an initiative housed by the African Development Bank (AfDB) focused on improving digital financial inclusion in Africa. The project builds on the Central Bank of Western African States’ (BCEAO) interoperability project, which has enhanced digital payment systems and use. The ADFI will focus on improvements to infrastructure, payment systems, capacity building, digital products, innovation, and policy and regulatory reform and interoperability. The ADFI specifically aims to increase connectivity for 332 million people—60 percent of which are women—and to grant them access to the formal digital economy. Digital financial inclusion is an ever-increasing priority for equitable development and economic growth. E-commerce, e-government, e-payment systems, and digital solutions can enable better access to services and resources. Digital transformation of economies and societies can significantly enhance economic output, government capacity, and individual prosperity. With a large youth population with enormous economic potential, harnessing digital tools and ensuring widespread access will be crucial to sharing and reaping the economic and social benefits of digital technologies in Africa. The ADFI is a blended financial vehicle that is supported by multiple donors, including the AfDB, the Bill and Melinda Gates Foundation, the government of Luxembourg, and the Agence Française de Développement. Currently, the ADFI has an investment horizon of approximately 10 years, a special fund investment term of 15 years, and a target fund size of $100 million.