In 2021 the new Administration and Congress will be managing through one of the most difficult challenges that the United States has faced in its history. The COVID-19 global pandemic has demonstrated the resiliency and ingenuity of our country’s technology and innovation base, but it has also shined a spotlight on the persistent digital divide, the lack of consistent consumer privacy protections, and the critical need for domestic and international leadership to strengthen U.S. technology and innovation leadership to combat the virus and ensure a rapid and robust recovery. The COVID-19 crisis further exacerbated existing disparities that cut across the country’s social and economic fabric, underscoring the need for a comprehensive and inclusive strategy for investing in the future.

In defeating the virus and revitalizing American economic growth, the United States can also reinvigorate American ingenuity by expanding participation in and access to the innovation economy at home, re-engaging with global partners, pursuing cybersecurity imperatives, and reinvesting in the fundamental drivers of American innovation.

The CEOs of the Business Roundtable urge the incoming Administration and Congress to take up and advance the following policies and urgent strategic priorities over the course of 2021:

1. **Bridge the digital divide.** *(pg. 2)*
2. **Protect consumer data privacy.** *(pg. 3)*
3. **Fortify U.S. cyber defenses and trust in information and communications technology (ICT) supply chains.** *(pg. 5)*
4. **Strengthen U.S. global leadership on data and technology policy.** *(pg. 7)*
5. **Bolster federal research and development (R&D) programs.** *(pg. 9)*
6. **Support access to and retention of global talent.** *(pg. 10)*

The following sections outline key policy recommendations that the Biden Administration and Congress can act on quickly to advance these urgent strategic priorities. We cannot afford further delay or failure to act to revitalize American leadership in technology and innovation.
BRIDGE THE DIGITAL DIVIDE

COVID-19 has shifted many aspects of everyday life online. From work to education to health care, access to broadband internet and reliable devices is more critical than ever. The digital divide across socioeconomic, racial and geographic communities is exacerbating gaps in educational achievement as students shift to distance learning and in health outcomes as telehealth becomes critical for many patients to access care.

The broadband provisions included in the December 2020 COVID relief package represent meaningful progress toward addressing and closing the digital divide during the pandemic. But the digital divide predated the pandemic and will outlive it in the absence of longer-term, sustainable policy solutions.

The federal government should take action to promote broadband deployment and develop a sustainable low-income connectivity program to make sure all Americans can stay connected to their communities, schools, critical services, health care providers and workplaces. While targeting connectivity gaps, care should be taken not to undermine the incentives that have encouraged tremendous private sector investment in robust and resilient networks.

1. Expand and modernize support for low-income households to purchase broadband.

The Emergency Broadband Benefit Program will provide additional assistance during the pandemic, but it is a temporary program. Given the ongoing need to address the digital divide, Congress should adopt a new long-term program that is designed to help the most vulnerable consumers purchase broadband and devices. The modernized program should:

a. Be supported by a sustainable, appropriated, long-term federal funding stream;

b. Provide the subsidy directly to low-income beneficiaries in the form of an electronic voucher or debit card to give them the flexibility to choose the provider and service that best fits their needs;

c. Eliminate the Eligible Telecommunications Carrier (ETC) requirement to encourage broad provider participation;

d. Increase efficiency and prevent waste, fraud and abuse by having the government handle all eligibility verification; and

e. Be designed so that it is easy for eligible users to apply for and receive the benefit. In doing so, the federal government should explore ways to leverage participation in other existing programs where feasible to boost participation in this new program.

2. Clarify and expand the E-Rate program to provide critical resources to meet student and teacher connectivity needs for e-learning.

Congress should clarify and expand the E-Rate program to ensure that students and teachers can fully participate in virtual classrooms and distance learning. To do so, Congress should:

a. Clarify that E-Rate can be used to reimburse the costs of internet service for e-learning to support student and teacher connectivity needs for educational purposes during the COVID-19 public health emergency;
b. Clarify the Federal Communications Commission’s (FCC) authority to expand its definition of a school campus in the context of distance learning throughout the COVID-19 public health emergency;

c. Direct the FCC to coordinate any E-Rate provisions with the Department of Education and any federal low-income broadband programs to ensure efficient use of funds; and

d. Ensure that students and teachers can rapidly obtain broadband service by directing the FCC to streamline E-Rate administrative procedures.

3. Fund the purchase of connected devices for use in e-learning.

Congress should establish and fund a program to support purchases of equipment for students and teachers in low-income communities and households engaged in distance learning. Funding for such a program should be channeled through states to school districts through block grants or other grant-in-aid programs, while using existing eligibility criteria (e.g., from the E-Rate program).

4. Accelerate broadband buildout in unserved areas of the country.

Congress should make the needed investments to bring high-speed internet to unserved parts of the country by taking the following actions:

a. Make the necessary funding consistently and reliably available to the FCC to support the buildout of broadband infrastructure to help close broadband coverage gaps. Investments should be based on technology-neutral criteria to support a mix of solutions that can be rapidly deployed.

b. Work with state and local governments to support the adoption of uniform timeframes with streamlined permitting processes for reviewing broadband deployment applications.

c. Accelerate the distribution of FCC funding for high-speed internet projects as the agency improves its broadband maps.

5. Support access to online health care services.

Congress should permanently remove geographic and site restrictions on Medicare telehealth benefits. Additionally, the Centers for Medicare and Medicaid Services should maintain and expand its waiver authorities that expanded the availability and flexibility of benefits during the pandemic.

PROTECT CONSUMER DATA PRIVACY

Consumers should have meaningful rights over their personal information, and companies that access this information should be held consistently accountable under a comprehensive federal consumer data privacy law. The absence of a U.S. federal privacy law contributes to an increasingly fragmented and complex regulatory landscape across the country. It also threatens U.S. leadership in technology globally and undermines efforts to establish globally interoperable privacy regimes that facilitate the protected transfer of data.
1. Pass federal consumer privacy legislation.

Congress should pass and the President should sign into a law federal consumer data privacy legislation that provides strong and consistent privacy protections for consumers and establishes a national privacy framework to enable continued innovation and growth in the U.S. digital economy. This federal privacy legislation should accomplish the following objectives:

   a. **Champion consumer privacy and establish accountability.** The legislation should include strong protections for personal data that enhance consumer trust and demonstrate U.S. leadership as a champion for privacy by including clear and comprehensive obligations regarding the collection, use and sharing of personal data as well as accountability measures to ensure that those obligations are met.

   b. **Foster innovation and competitiveness.** The legislation should be technology neutral and take a principles-based approach so organizations can adopt privacy protections that are appropriate to specific risks, such as the sensitivity of the data, as well as provide for continued innovation and economic competitiveness in a dynamic and constantly evolving technology landscape.

   c. **Harmonize privacy protections through a strong national framework.** The legislation should establish a coherent framework for consumer privacy protection across federal and state jurisdictions through a comprehensive national law. The law should build upon the global standards for privacy protection and avoid the potential for conflicting state approaches that would confuse consumers and create a challenging patchwork of compliance requirements.

   d. **Achieve greater global interoperability.** The legislation also should facilitate international transfers of personal data and e-commerce. It should further promote consumer privacy regimes that are interoperable on a global basis, meaning the legislation should support consumer privacy while also respecting and bridging differences between U.S. and foreign privacy regimes (e.g., the European Union's [EU] General Data Protection Regulation).

Business Roundtable's [framework for privacy legislation](https://www.businessroundtable.org) proposes a strong and comprehensive consumer data privacy law to establish a set of core individual rights that we believe consumers should have over their data. Additionally, Business Roundtable has outlined [principles to protect the privacy and security of personal COVID-19 data](https://www.businessroundtable.org).

2. Finalize a new privacy framework for EU-U.S. cross-border data flows.

The Administration should prioritize continued, constructive engagement with their European counterparts that helps ensure the ability of U.S. companies to efficiently conduct cross-border data transfers between the EU and United States in light of the Court of Justice of the European Union's (CJEU) invalidation of the Privacy Shield Framework in its Schrems II decision and the underlying concerns it raised in that case.

To secure an agreement, the U.S. government must take action to address the issues raised by the CJEU around providing Europeans with more information and an ability to seek redress in association with
Fortify U.S. Cyber Defenses and Trust in ICT Supply Chains

The United States is engaged in an ongoing and escalating struggle against persistent, agile and well-funded cyber adversaries. To succeed in this fight, the federal government needs to improve its defenses against sophisticated and determined cyber threats with a coordinated, multilayered and cutting-edge cyber defense strategy. Significant investments in updating and securing federal government networks to prevent, detect, mitigate and remediate cyber intrusions are a key component of a successful strategy, as well as investments in a robust and active partnership with the private sector to ensure a resilient and adaptive defense of critical infrastructure and government systems.

To that end, the federal government should enhance collaboration between the public and private sectors to detect, deter and respond to malicious activity in cyberspace. The Administration should renew its cyber deterrence frameworks and leadership of global efforts to combat cyber threats.

1. Invest in and modernize U.S. government cyber defenses.

The federal government should make significant investments to secure and modernize its information technology (IT) systems and cyber defense capabilities, particularly across civilian federal government agencies. This work includes taking the following actions:

   a. Modernize federal IT systems, with a particular focus on those protecting civilian and regulatory agencies. Additionally, the government should improve efforts to recruit and retain the cybersecurity talent needed to develop and maintain these systems.

   b. Increase the use of secure, cloud-based computing architecture among government agencies and their vendors.

   c. Partner with state, local, tribal and territorial governments; law enforcement; and citizen services bodies to dramatically improve their cybersecurity posture.

   d. Ensure that the Office of National Cyber Director has the resources, the authorities and a clear mandate to lead the federal government’s engagement with private industry and coordinate a whole-of-government approach to partnership with critical infrastructure operators.

2. Operationalize cyber defense collaboration between private and government entities.

The federal government should continue to focus on encouraging and amplifying bidirectional communication between the public and private sectors to eliminate cyber threat intelligence silos, particularly given the private sector’s role in operating critical infrastructure in the United States. Clear,
available fora for public-private information sharing are necessary to ensure that both industry and government have up-to-date information on emerging and increasingly multifaceted threats. The 2015 Cybersecurity Information Sharing Act established a statutory framework around information sharing, but there continue to be gaps in implementation where information is not shared between agencies, is not shared on a timely basis with the private sector or lacks actionable context. To operationalize public-private cyber defense collaboration between, the federal government should:

a. Enhance existing information-sharing platforms to facilitate the secure exchange of real-time threat data between public and private entities;

b. Systematize a regular process to review cyber intrusions into public and private systems to capture and share lessons learned with the private sector;

c. Expand and build upon the use of mission accelerators to allow the private sector to collaborate with the government on emerging cybersecurity threats;

d. Provide resources and authorities for U.S. agencies with significant cybersecurity capabilities to collaborate actively with the private sector to help reduce systemic cyber risk; and

e. Resource national security agencies to develop programmatic support for critical infrastructure cybersecurity and recognize designated critical infrastructure as intelligence customers.

3. Improve the resiliency and transparency of ICT supply chains.

The federal government should continue to work collaboratively with the private sector to enhance the trust in and security of ICT supply chains. Specifically, the federal government should:

a. Promote the adoption of best practices for secure software development, distribution and testing and support continued development for software assurance programs such as the early-stage National Telecommunications and Information Administration’s Software Bill of Materials Project;

b. Combine, streamline and expand on work already underway to enhance supply chain security, such as the Department of Homeland Security ICT Supply Chain Risk Management Task Force and the Department of Defense Cybersecurity Maturity Model Certification program;

c. Partner with critical infrastructure supply chain entities (owners, operators, suppliers and manufacturers) to identify and remediate policy, legal and technical barriers to security testing for critical hardware and software components; and

d. Support the continued advancement of responsible and coordinated approaches to the management and disclosure of security vulnerabilities. The federal government should work with the private sector to update guidance and frameworks for vulnerability management, including disclosure and patching.

4. Invest in building a deeper pool of highly qualified and diverse cybersecurity talent.

Current pathways for training, recruiting and retaining cybersecurity personnel are inadequate to meet the demand for cybersecurity talent. The government should build partnerships with academia and industry to deepen the pool of qualified candidates for critical cybersecurity jobs, including by taking the following actions:
a. Expand current pathways into government cybersecurity roles by utilizing apprenticeship and externship programs, increasing the funding available to the CyberCorps program, and investing in upskilling programs for current federal employees.

b. Work with colleges and universities to fund and develop cybersecurity training programs for high-demand cyber skills, such as secure software development and penetration testing.

5. Promote global cooperation on cyber threat deterrence.

In addition to advancing norms for responsible behavior in cyberspace, the federal government should re-engage with partners and allies and take the lead in building a robust transnational cybersecurity alliance against threat actors that coordinates responses and legal remedies to deter malicious cyber activity.

STRENGTHEN U.S. GLOBAL LEADERSHIP ON DATA AND TECHNOLOGY POLICY

Increasing levels of technology protectionism and digital nationalism threaten to balkanize technology, data and internet policies around the world with negative impacts for U.S. innovation leadership and competitiveness. At the same time, countries are grappling with legitimate concerns regarding the security of data and supply chains, responsible uses of technology, and potential employment and economic disruptions from innovation and automation. These developments threaten to disrupt the flow of ideas, people and capital that have historically defined and fueled U.S. dynamism on the global stage.

International leadership in technology and innovation is a core American strength — a driver of prosperity and catalyst of opportunity. The Administration can advance U.S. interests by reinvigorating global engagement to set global data and technology policy standards and by reinvesting in the fundamentals of inclusion, access and collaboration that drive innovation at home.

The benefits of enhancing American innovation fully materialize at home when key foreign markets are open to U.S. products and services and legitimate policy concerns such as data security are effectively addressed by governments without interfering unnecessarily with the responsible uses of technology. To fuel American jobs and prosperity, our domestic strengths in innovation and technology policy leadership should be exercised through multilateral cooperation and sustained engagement with key partners around the world. U.S. leadership to advance global data and technology governance policies that are consistent with democratic values will accelerate innovation and promote shared prosperity through a fair, democratic and flourishing global innovation landscape.

1. Work to establish global consensus on governance of data and technology.

The U.S. government should increase engagement and collaboration with key allies and other partners while strengthening U.S. leadership on global data and technology policies. This work includes taking the following actions:
a. Establish new, dedicated coalitions with like-minded countries to prioritize and sustain free cross-border data flows, promote the economic and societal value of data and digital trade, foster digital ethics, and actively address key concerns about data governance.

b. Establish and support international partnerships to promote joint research collaboration to advance U.S. technology and innovation priorities, such as COVID-19 recovery, global climate change, artificial intelligence, cybersecurity, supply chain resilience and other research fields.

c. Partner with U.S. industry stakeholders to enhance U.S. participation in international technology standards-setting bodies (e.g., the 3rd Generation Partnership Project, International Telecommunication Union, International Organization for Standardization) and continue to support a strong, private-sector-led presence in these bodies.

d. Work with allies to implement a funding mechanism to support the deployment of open and interoperable network infrastructures and fund capacity-building in developing countries and regions where connectivity is poised to rapidly expand.

2. Establish and strengthen international agreements around digital trade.

The U.S. government should engage in multilateral and bilateral negotiations with trading partners to set the rules of digital trade and enforce international commitments. The U.S. government should leverage the high-standard digital commitments in the U.S.-Mexico-Canada Agreement (USMCA) as a model to facilitate the movement of data and address data localization measures and other market access barriers to support continued U.S. innovation leadership. This work includes taking the following actions:

a. Negotiate bilateral and multilateral commitments that protect cross-border data flows, prevent data localization requirements, support cooperation on the development and deployment of new and emerging technologies, and protect intellectual property rights.

b. Continue leadership in multilateral negotiations, including World Trade Organization e-commerce negotiations, to establish and enforce rules and norms that promote an open internet, open markets and tariff-free nondiscriminatory digital trade.

c. Support Trade Promotion Authority policy priorities and negotiating objectives to prevent data localization and onshore data storage requirements and support cross-border data flows modeled on the USMCA, while exploring additional avenues to promote trade in and use of emerging technologies as well as responsible use of technology through trade agreements.

3. Work multilaterally to ensure that export controls on technology that is essential to national security are effective and support U.S. innovation leadership.

The U.S. government should use export controls in ways that are consistent with the policies and provisions in the Export Control Reform Act of 2018, including by prioritizing the use of multilateral controls and ensuring their targeted use for chokepoint technologies of concern that are not widely available outside of the United States. To ensure that current and new export controls advance national security and preserve U.S. economic competitiveness and innovation leadership, use of export controls should be consistent with the following principles:
a. Multilateral export controls improve efficacy, reduce enforcement costs and prevent technology leakage to countries of concern.
   i. Unilateral export controls over widely available commercial items harm the U.S. industrial base and are not effective at preventing the proliferation of controlled items to countries of concern. Investment in and the development of such technologies simply migrates from the United States to other countries, which then supply the technologies to countries of concern.
   ii. Unilateral export controls on well-established and widely used categories of technology could significantly and negatively affect U.S. national security by undermining American research, commercial and service industries and placing them at a disadvantage to their foreign counterparts.

b. Controls tailored to end uses and end users of concern are preferable to controls over entire categories of technologies because they allow continued development with trusted partners and export for beneficial uses.

c. To address the challenges of scaling export controls around the world, new technologies may help to make end-use and end-user controls more effective, more dynamic and more comprehensive while preserving U.S. technological leadership, especially when exporting products and technology to allies. These technologies could include software- and hardware-based tools to enforce and monitor government-imposed restrictions on users and uses and to secure the infrastructure surrounding these technologies.

**BOLSTER FEDERAL R&D PROGRAMS**

The United States has built and sustained a competitive edge across key technology areas, lending it a unique and powerful source of credibility and a prominent platform on the world stage. A robust R&D landscape has been a key driver of this competitive edge for decades. While the United States still leads the world in R&D investment, U.S. primacy is dwindling as federal funding slows. Meanwhile, the global R&D ecosystem has evolved, and the United States now plays a very different role compared to its historical position. Federal support for R&D should reflect this reality and focus on partnerships and other linkages that help advance research at different stages in the R&D pipeline.

1. **Increase federal investment in R&D.**

The federal government should recommit itself to innovation leadership by substantially boosting spending on R&D, including but not limited to early-stage, basic R&D and technologies that are integral to continued U.S. competitiveness, such as advanced materials, quantum computing, semiconductor manufacturing and artificial intelligence. Specifically, Congress should pass and the President should sign legislation such as the Endless Frontier Act that significantly boosts R&D spending on key strategic technologies for U.S. innovation leadership.
2. Support collaborative research partnerships.

The federal government should coordinate and invest in collaborations of academic institutions, national labs and private industry to fully leverage research capabilities across the R&D pipeline and spur national innovative capacity. This work includes taking the following actions:

a. Expand the scope and funding for existing research programs that are collaborations of the private sector, academic and research institutions, federal agencies, and national labs (e.g., the National Science Foundation’s Engineering Research Centers, Industry-University Cooperative Research Centers, Manufacturing Institutes & Manufacturing Extension Partnerships, National AI Research Institutes Program, and National Quantum Initiative).

b. Designate a portion of federal R&D funding to support and facilitate technology transfer and commercialization activity and ensure that collaborative research and manufacturing programs play a productive role in facilitating and coordinating the commercialization of innovation and intellectual property.

c. Establish translational research centers to support the commercialization of advanced manufacturing technologies and expand collaboration between domestic manufacturers and research universities while advancing a strategic, long-term approach to supporting an innovative domestic manufacturing base.

SUPPORT ACCESS TO AND RETENTION OF GLOBAL TALENT

U.S. innovative capacity and global competitiveness attract, and are reinforced by, the knowledge and contributions of global talent, particularly in critical high-tech fields such as 5G, cybersecurity, quantum computing and artificial intelligence. Against this backdrop, pursuing steps to better leverage and retain global talent, while ensuring that key national security safeguards remain in place, is critical. At the same time, the federal government should work to ensure that the U.S. innovation economy is benefiting from the full potential of a world-class domestic workforce while creating pathways to broaden participation in innovation-intensive sectors. This work entails supporting and investing in workers to equip them with the skills to respond and adapt to new opportunities, while expanding and modernizing pathways toward digitally resilient jobs.

1. Support systems to leverage global talent.

The federal government should modernize our U.S. system to allow U.S. employers to access and retain global talent. This work includes taking the following actions:

a. Improve the H-1B system for skilled workers in innovation-intensive fields and allow the employment of H-4 dependent spouses.
b. Maintain authorization for the Optional Practical Training period for visas held by students in qualifying science, technology, engineering and math (STEM) fields to retain foreign students after graduation.

c. Provide a new, streamlined path to a green card for graduates in advanced STEM fields and exempt individuals with special skills (e.g., STEM-related skillsets) from the visa cap.

d. Eliminate the per-country cap on employment-based immigrant visas.

e. Transition to a digital and predictable system to process immigration benefits.