An American Competitiveness Agenda

IBM

As the 118th Congress settles in and tackles a new policy agenda, our nation's leaders should focus on bipartisan measures that advance America's economic competitiveness and national security.

At a time of international uncertainty and intense competition, it is imperative to advance a bipartisan agenda that supports innovation, supply chain resiliency, cybersecurity, trusted technology, and a workforce skilled for the jobs of this new era.

For more than a century, IBM has sought to promote thoughtful, bipartisan public policy solutions that bring people together and help solve tomorrow's problems today.

Below are five priorities that IBM believes the new Congress and the Biden Administration should prioritize to strengthen America's global competitiveness in 2023 and beyond:

1.
Accelerate American Innovation and Discovery

Investments in America's ability to innovate and create entirely new industries lead to jobs and opportunities at home and a stronger and more resilient economy that is prepared to compete globally in cutting-edge technologies.

The CHIPS and Science Act is an excellent example of how the nation can promote vitally important technology research in the United States. A supply chain crisis was the forcing function that underscored the urgency of building and designing semiconductors in America.

We should act in other equally essential technology areas before the next crisis, and IBM calls on Congress and the Administration to do this by:

- **Fully implementing the CHIPS Act and funding the Science Title** as authorized by Congress, including funding for the National Science Foundation to build the Technology, Innovation, and Partnerships (TIP) Directorate focusing on emerging technologies and scale a highly skilled workforce. The administration should also expeditiously build the National Semiconductor Technology Center (NSTC) as provided for in the Act.

- **Accelerating American R&D** through initiatives like the National Artificial Intelligence Research Resource (NAIRR), which would build a data and computing superstructure that allows government, industry, and academia to accelerate AI R&D.

- **Prioritizing investments in Quantum Computing**, because we should not wait for another crisis to focus on our technological leadership. In recent years Congress has passed bipartisan legislation to support quantum R&D and workforce building, including the National Quantum Initiative Act — which must be reauthorized in 2023 — and the QUEST Act and the Networking Act that will both need to be funded as part of CHIPS.

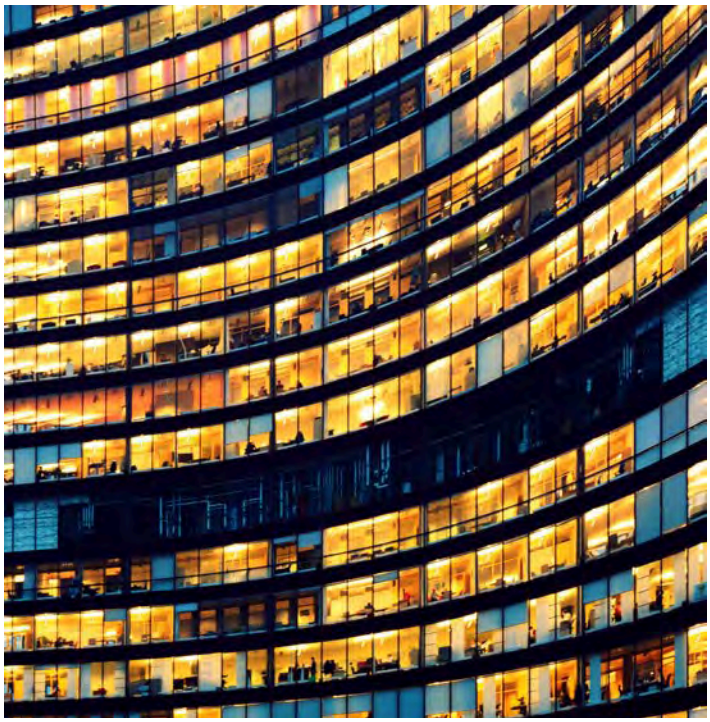
  We must continue to prioritize these investments that will spur public-private partnerships and ensure that America remains the unquestioned leader in this game-changing technology — and that we are prepared to address the security implications and threats that will be posed by our adversaries

- **Enacting R&D expensing**, so innovative companies do not face cash flow issues from current laws that require capitalization over time and can instead focus on creating jobs and bolstering American economic prosperity and security.

2.
Build a More Resilient, Secure, and Modern Government

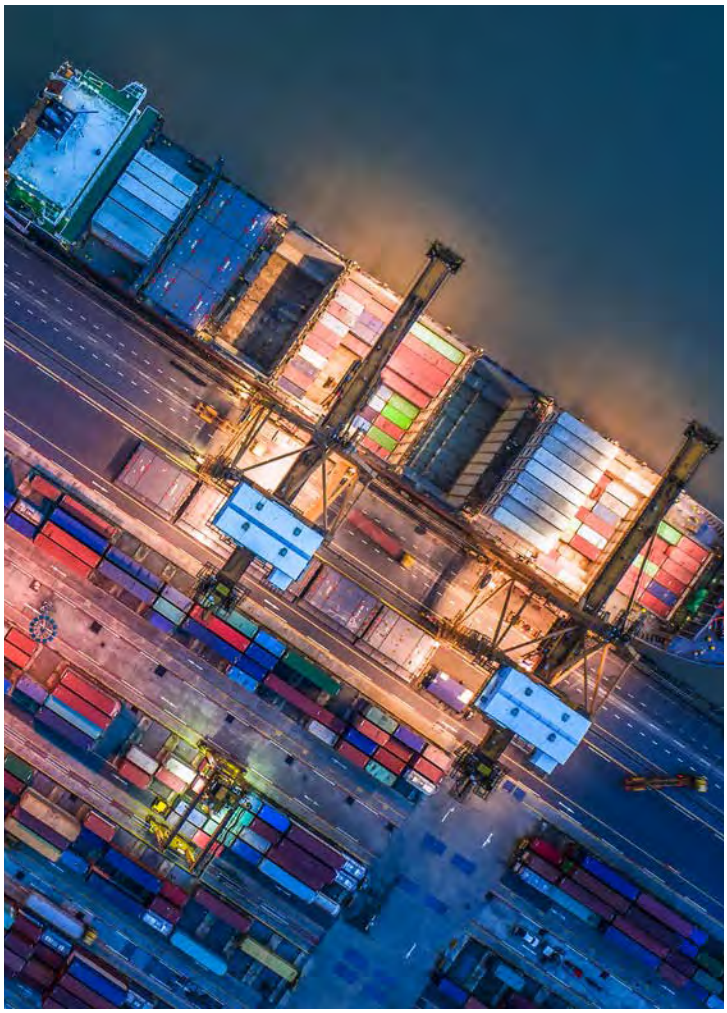
At a time of conflict and uncertainty, it is more important than ever to fortify government IT systems, so they are robust, resilient, and well-defended against cyberattacks by hostile actors. In any IT system, overreliance on a single technology exposes a single vector of attack. It then is harder to react to surges in demand and may lead to over-customization, making updates difficult and costly.

Congress and the Administration should prioritize investments in technological resiliency. Our leaders can make investments now to ensure federal agencies' IT propels the country forward by:



- **Continuing to invest in modern, secure, and resilient government IT,** like hybrid cloud technology, which is inherently a more secure and flexible infrastructure for our critical missions including military readiness and modern customer service. It avoids the pitfall of a single point of attack, and provides flexible, cutting-edge tech capabilities everywhere from Washington, D.C to Washington state and to places worldwide where American forces are deployed.
- **Fully implementing the recently passed FedRAMP Authorization Act** with a particular focus on ensuring reciprocity and streamlining the authorization process.
- **Focusing on IT that improves the government customer experience.** Modern, secure, digital citizen services are paramount to a competitive society, especially when it comes to things like, administering student loans, processing Veterans' benefits, modernizing FEMA flood maps, or delivering programs that serve under-served communities.

  IBM urges agencies to adopt a hybrid cloud strategy that allows them to integrate the best available commercial platforms to enable modern, digital operations that enhance customer service and provide tools available to accomplish the mission.



3. Strengthen and Diversify the Supply Chain

A country's economic stability is only as strong as its supply chain. The recent baby formula shortage in the U.S. is a stark reminder that investing in and maintaining a diverse supply chain is critical to American security and success.

However, the key to supply chain security is to use intelligent, targeted policies that protect national security, not overly broad or cumbersome rules that hurt only American firms while foreign competitors capture markets. IBM calls for "Precision Regulation" of the supply chain by:

- **Implementing precision export controls,** in partnership with global allies, on new technologies like quantum computing, so we can protect our national security without hindering innovation.
- **Establishing tools for resilient and responsive software supply chains** that provide greater security through understanding and insight into the foundational elements that comprise software (sometimes called a “software bill of materials”) used in critical infrastructure.

  These tools enable companies and organizations to understand what makes up their code to reach risk-informed decisions about software supply chains and if their software is affected by new vulnerabilities enabling the quick mitigation of any security risks.

4.
Build, Train, and Retain a Diverse Workforce

American competitiveness relies on a highly skilled and diverse workforce, where a traditional bachelor's or postgraduate degree is not the only pathway to a well-paying career.

Our workforce is essential to supporting, developing, and creating the technology solutions that will solve our society's most pressing problems. We can develop and grow a diverse workplace by:

- **Ensuring the Americans behind American innovation are supported** by aligning key federal programs to focus on retraining and new job-relevant skills acquisition and making existing federal student aid funding and programs available for targeted learning opportunities such as apprenticeships, internships, or technology certificate programs, and for workers in retraining or upskilling programs.
- **Increasing job opportunities for more high skilled workers** for more high skilled workers by reducing college degree mandates imposed on federal contractors.
- **Investing in workforce development,** particularly through the regional technology hubs authorized in the CHIPS and Science Act, to expand the innovation economy beyond the coasts and increase career-enhancing experiential learning through programs that help train a skilled and diverse STEM workforce.

5.
Strengthen Trust in Technology

We must also strengthen societal trust in technology to create a competitive technological economy. Consumers are understandably concerned about the use of today's rapidly changing technologies and the data that feeds into them. Still, we can drive progress and enhance consumer protections and business innovation by:

- **Advancing national privacy legislation** that provides strong consistent consumer data protection through pre-emption of state laws and common-sense national privacy standards that enable beneficial use of data.
- **Avoiding provisions like a private right of action** that creates uncertainty among consumers and businesses without creating strong consumer protection and that undermines the predictability of a national privacy standard. People, not plaintiff's attorneys, should benefit most from a national privacy law.
- **Continuing collaboration with Europe and other like-minded governments** on targeted, risk-based regulation of technology like artificial intelligence that differentiates between software that automates everyday tasks and software that advises humans in sensitive areas like healthcare, finance, or safety, and placing robust regulations on those use cases of AI with the most potential to cause societal harm.