March 7, 2023

Lael Brainard
Director of the National Economic Council
Eisenhower Executive Office Building
1650 17th St NW
Washington, D.C. 20500

Jake Sullivan
National Security Advisor to the President
The White House
1600 Pennsylvania Ave NW
Washington, D.C. 20500

Dr. Arati Prabhakar
Director of the Office of Science and Technology Policy
Eisenhower Executive Office Building
725 17th Street NW
Washington, D.C. 20500

Dear Co-Chairs of the CHIPS Implementation Steering Council:

We applaud Congress and the Administration for passing and signing the CHIPS Act into law, which will invest $54 billion in the semiconductor industry. With the many natural calamities and societal tensions in our world today, it is difficult to find areas of broad agreement and we recognize this important step forward.

Now that we are committed to bringing semiconductor manufacturing back home, we need to establish the basic benchmarks that keep chips safe, reliable, and secure. The government has a primary role here, because it can require that the chips used in critical infrastructure and the defense industrial base meet these standards. Like other consumer protections, such as seatbelts in cars and labels on foods, the government can establish guidelines that industry must follow to keep our citizens safe. Nowhere is this more important than in the information technology sector. And semiconductors are the foundation of it all.

Protecting chips is an achievable goal. We can circumvent and avoid the cybersecurity hacks that have exfiltrated our finances, our medical records, our personnel records, the blueprints of our most sophisticated fighter jets and shut down critical infrastructure. Those were network breaches, and the security holes were plugged with software. But if a bad actor hijacks a chip, there is no software that can stop them. This is why we have to pay attention now, before we produce the next generation of devices that will be even-more ubiquitous, from biological implants to autonomous drones.

There are two challenges; both are surmountable.

First, cybersecurity defenses must remember every known attack, discover every possible vulnerability, and anticipate every move. This is the inherent asymmetry that offensive intruders enjoy: they have all the time in the world to explore and exploit weaknesses. Because the perverted incentives are so lucrative there are more hackers than ever before, and they only need to be successful once.

The second challenge is that we need to be able to see and detect inevitable intrusions. Renowned cybersecurity expert Dan Geer describes this as the “no unmitigable surprise” approach to information security. This is why our bodies have immune systems. We need, and could affordably build, an immune system in every single semiconductor device.

The technical solutions are nascent but effective. They rely on recent advances in applied mathematics, our practical knowledge of what has gone wrong and what could go wrong, and our new ability to “see inside” the chip even during normal operation, even in the field. For most manufacturers, however, incorporating these innovations in their devices may involve new incremental cost of production

If this Steering Council were to require minimal standards of chip integrity and security, we could start erecting technical roadblocks for our nation’s adversaries and establishing on-chip checkpoints that are convenient, affordable, and incredibly effective. Our adversaries may still find a way in over time, but we must make it much harder for them to corrupt our chips.

In order to secure the future of America’s devices, we call on the CHIPS Implementation Steering Council to take two actions today:

- Require all chips used in our national security and critical infrastructure be certified against attack by 2026

- Require a portion of the $11 billion allocated for research and development be targeted to technologies that accomplish this goal

The work of this Steering Council is among the most consequential policy opportunities for ensuring our nation’s economic security into the 21st century. We applaud your efforts in expanding chip production and call on your collaboration with industry to harden our nation’s technological defenses and preserve our way of life.

Respectfully,

Ron Black
Chief Executive Officer, Codasip

Niall Brennan
Retired FBI Supervisory Special Agent; former Legal Attaché to France and Monaco

Terry Burruss
Former Senior Intelligence Cyber Leader

Mark D. Cheng
Former Executive Director, President's Intelligence Advisory Board

Richard M. Frankel
Retired FBI Special Agent in Charge, Department of Justice; Former Associate Director of National Intelligence, Office of the Director of National Intelligence

Brian P. Hale
Former Senior U.S. Intelligence Official

Peter L. Levin
Former Chief Technology Officer, U.S. Veterans Affairs; Co-Founder & CEO, Amida Technology Solutions

Michael Lumpkin
Former Under Secretary of Defense for Policy, U.S Department of Defense

Doug Smith
Former Assistant Secretary for Private Sector, Department of Homeland Security

Leo Taddeo
Former FBI Special Agent in Charge, Department of Justice; CEO of Appgate