We Make Scientific Breakthroughs Possible

Restoring U.S. Primacy in Microelectronics by Establishing a Dedicated Federally Funded Research and Development Center (FFRDC)

Background

Microelectronics are central to our national security apparatus, but the global industry that supports their development is oriented toward commercial needs and permeable to foreign adversaries. Strengthening America's capacity to produce trusted information and communications technologies (ICT) through innovation and industry partnerships is paramount if the U.S. is to confront this national and economic security grand challenge.

The Centrality of Microelectronics in an Increasingly Competitive World

Microelectronics underpin every military platform, intelligence apparatus, and critical infrastructure network and provide secure communications, electronic warfare capabilities, and cryptographic applications, among others. Important national security technologies have performance goals that can only be met by the most sophisticated semiconductor devices. However, U.S. national security is precariously dependent on the integrity of commercial suppliers for those microchips. Most of these companies are optimized to meet commercial—not national security— specifications, and the global commercial supply chain is widely permeable to potential adversaries.

Increased attention has – rightly – been paid to the threat China poses to U.S. semiconductor industries and its covert and overt methods to steal or buy U.S.- developed technologies. Russia has demonstrated similar persistent, advanced, and ever-improving capabilities, including through automated means, the penetration of industrial control systems. Other countries exploit the weakness of the microelectronics we use, and continue to exhibit advanced hacking capabilities to conduct espionage and destroy information held by U.S. organizations and industry. In addition, malefactors routinely commit cybercrimes and threaten the stability of weak nations, which provides incentive for DOD to continually look for and mitigate vulnerabilities.

Policymakers have begun to respond to these threats through legislation and top-down coordination initiatives. However, there is not a strategic, whole-of-government approach aimed at solving a multilayered issue with impacts

Contact Us

2650 Park Tower Drive
Vienna, VA 22180

(202) 462-1676

info@aui.edu

www.adi.edu

View Document Online

on regulatory frameworks, acquisition policies, research and development (R&D) investments, and government standards. Recent efforts to address this challenge have also been stymied by a fragmented and entrenched bureaucracy. Resources intended to promote a unified federal response, support vulnerable state and local government systems, and sustain at-risk industries are scattered across mission-driven, parochial, and inward-looking elements of the national security apparatus. Naturally, each component of the fragmented response promotes solutions that advance its narrow mission and resists attempts to elevate resources that could enable the U.S. to mount an effective, innovative, and unrelenting response. Absent a paradigmatic shift, the Nation will fail to reclaim its sovereignty over the design, production, and distribution of ICT hardware and software that promotes resilience and reinforces a strong national security posture towards our adversaries.

A Holistic Solution for a Complex Problem

Only a whole-of-government, multi-pronged initiative can effectively address these current challenges and provide for the design, manufacture, delivery, and maintenance of technologies foundational to U.S. national and economic security. The following are key recommendations towards achieving this:

Elevating Solutions

Action to eliminate or discourage entrenched parochial thinking must be initiated and attended to from the Executive Office of the President. Specifically, the president should establish an office led by an individual who sits on the National Security Council (NSC), Domestic Policy Council (DPC), and other multi- agency and Executive Branch policymaking bodies. This office would be responsible for implementing and overseeing a top-down federal initiative aimed at ensuring validation of security standards across the entire supply chain while supporting a research, development, test, and evaluation (RDT&E) activity to advance semiconductor manufacturing, robustness and resilience, system-on-chip design, and cybersecurity.

This office would be served by an ICT Advisory Council (ICTAC) charged with guiding the implementation and contributing to the development of recommendations for export controls, industry support, and compliance with International Traffic in Arms Regulation. Membership on the advisory body would include federal officials, industry representatives, and academic researchers to broaden perspectives and maximize multi-sectoral interaction.

Independence & Security Through Innovation

DOD would be best equipped to lead agency-level execution of this initiative given its centrality to the national security ICT market, its access to secure labs and other research infrastructure, and its vast existing RDT&E enterprise. In particular, the Office of the Secretary of Defense (OSD) could coordinate efforts across the agency with involvement from both the Office of the Under Secretary of Defense for Research and Engineering and the Office of the Under Secretary of Defense for Acquisition and Sustainment. Doing so will enable DOD to strengthen the ICT sector holistically, from early stage research to acquisition and deployment.

Supporting America's Industrial Base

An important element of the ICT initiative will be supporting the national security industrial base through close collaboration with the business and academic sectors. This would specifically be manifested in the involvement

of ICT companies and academic institutions in the initiative's planning and execution, including through their representation on the ICTAC. This would help align the federal ICT initiative with the needs and capabilities of industry, foster collaboration with researchers at the leading edge of ICT, and strengthen the ICT workforce development pipeline. In addition, a primary function of the FFRDC/consortium noted above would be the validation and certification of ICT components. This would enable ICT companies to demonstrate the security of their products and the financial returns of selecting them over others' non-certified products. Together, these activities serve to strengthen the domestic ICT industry while enabling it to meet national security needs.

Recommendation

Establish a federally funded research and development center (FFRDC)[1] with an initial estimated budget of $30M/year in service of this initiative. Through a combination of licensed technology and evaluation fees, the FFRDC could be self-sustaining within five years. Amid an environment with only a handful of global suppliers, an FFRDC can serve as a trusted and objective agent of the government to faithfully execute the mandates of a White House ICT strategy with added flexibility and agility around hiring, procurement, and operations. Specifically, this entity would be responsible for independently testing and verifying ICT technologies to assure systems security, helping ICT manufacturers repatriate production, and coordinating and conducting leading-edge research internally and with trusted partners. The latter would include DOD efforts within the Defense Microelectronics Activity, which supports semiconductor R&D, as well as other federal agencies and activities at U.S. research institutions. Finally, this entity would have the flexibility to conduct classified research with national security experts while also working in open environments with industry and academia to identify new technologies and promulgate security standards for ICT trust and assurance.

[1]A master list of existing FFRDCs can be found at https://www.nsf.gov/statistics/ffrdclist/#ffrdc.