Trusted Access to Microelectronics: Addressing DoD's Unique Issues of Accessibility, Integrity, and Confidentiality of Microelectronics

Ted Glum

STEPS: SCIENCE, TECHNOLOGY, ENGINEERING, AND POLICY STUDIES

ISSUE 9, 2024

STEPS (Print) ISSN 2158-3854
STEPS (Online) ISSN 2153-3679

Ted Glum. "Trusted Access to Microelectronics: Addressing DoD's Unique Issues of Accessibility, Integrity, and Confidentiality of Microelectronics," *STEPS* 9 (2024): 39-46.

POTOMAC INSTITUTE PRESS

STEPS: Science, Technology, Engineering, and Policy Studies
is published by Potomac Institute Press of the
Potomac Institute for Policy Studies.

Access to *STEPS* is available free online at:
www.potomacinstitute.org/steps.

TRUSTED ACCESS TO MICROELECTRONICS

Addressing DoD's Unique Issues of Accessibility, Integrity, and Confidentiality of Microelectronics

Ted Glum, Member of the Board of Directors,
Potomac Institute for Policy Studies

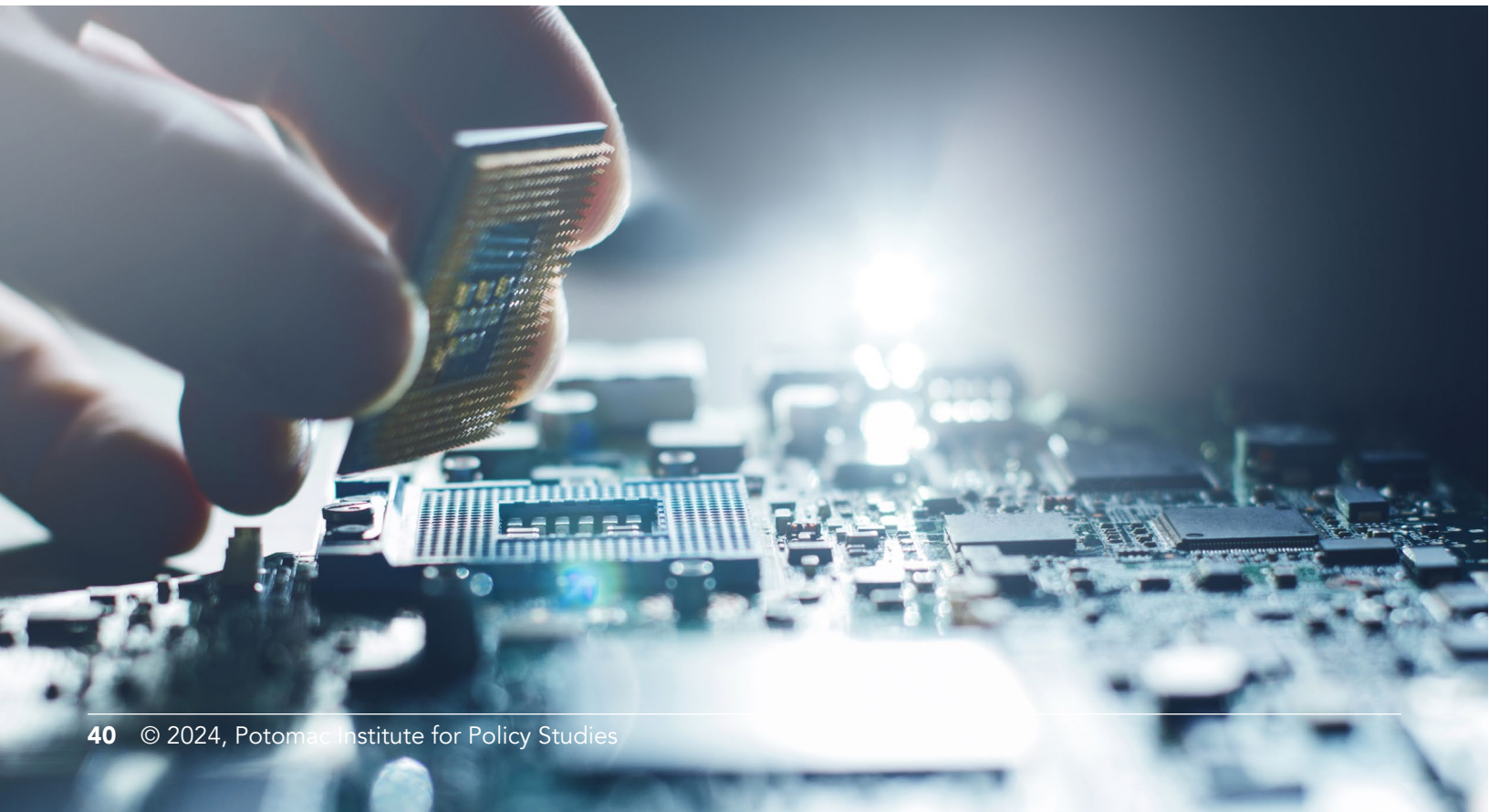
With all the current emphasis on the supply chain issues for microelectronics, as well as the CHIPS Act's attempt to re-shore production, it is worth considering the unique needs of the US Department of Defense (DoD). The DoD needs access to both commercial-off-the-shelf (COTS) microelectronics and trustworthy devices for its weapon systems and operations. The US military has long depended on electronics, and modern defense systems increasingly rely on the superior performance of microelectronics to sense, decide, adjust, control, and act.[1] Whereas in the past, the best defense was to have the most firepower and best armor, now a modern defense depends on superior microelectronics.

This dependence is why the US DoD has long been concerned with "trusted access" to microelectronics. Trust means different things in different contexts, but here we adopt an inclusive understanding of trusted access in three dimensions:

- **Accessibility** refers to the ability to obtain and use the required microelectronics when needed. For example, in wartime, the Department might need to produce many weapon systems rapidly. Production delays due to microelectronics supply limitations would operationally compromise the military.
- **Integrity** refers to the trust that the microelectronics serve their intended functions and that no other functionality such as a kill switch, backdoor, or data capture was inserted covertly.
- **Confidentiality** of the microelectronics relates to trust that competitors and adversaries cannot glean information to compete with or defeat a system based on their knowledge of the design or type of microelectronics. This dimension of trust includes security against major vulnerabilities such as rival access to proprietary or classified knowledge of a microelectronic part's intended use (or even the customized design of those parts).

Critical infrastructure industries, such as companies involved in the electric power grid, cloud services, and banking, are concerned with trusted microelectronics to ensure the integrity and reliability of their systems. Producers and consumers of commercial products, such as automobiles, similarly have an interest in the accessibility and integrity of their constituent electronics, if not also confidentiality. But the military has a particular interest in a high level of trust across all three dimensions because adversaries are motivated to attack these attributes. Thus, microelectronics used in all these areas need reliable access to trusted parts with the assurance of some degree of accessibility, integrity, and confidentiality of the supply.

The COVID pandemic highlighted the vast regional concentration of microelectronics production in Asia, exposed the fragility of the microelectronics supply chain, and revealed the vulnerability of microelectronics parts to malicious intent.[2] Recently, there has been much focus on the fact



that a large percentage of the microelectronics used in the US, including by the DoD, are manufactured, assembled, and tested overseas. While the CHIPS portion of the CHIPS and Science Act of 2022 will attempt to re-shore American microelectronics manufacturing, it will not automatically guarantee access to trusted microelectronics. American fabrication alone will not ensure that microelectronics are free of defects, malware, inserts, or spyware.

The Department has a long history of providing support and services to DoD industrial suppliers to ensure that microelectronics are trusted, as defined in this paper. The program, generally known as the **Trusted Foundry** program, has evolved over time, addressing the issue of trust for parts over the entire range of the microelectronic supply chain (design, fabrication, packaging, and testing) to include guaranteed access, integrity, and confidentiality.[3] The program's name, the Trusted Foundry program, is a misnomer because the program goes far beyond foundry services and has led to confusion over what this program provides and the gaps (including those in the CHIPS Act) that it hopes to fill.

DOD ACQUISITION OF MICROELECTRONICS

The US DoD accesses a wide variety of microelectronic parts for use in defense systems through its many contractors and suppliers. Defense needs include new and emerging technologies (e.g., silicon photonics), state-of-the-art (SOTA) technologies (currently 7nm and smaller), state-of-the-practice (SOTP) mature microelectronics (typically 28 to 45nm), and legacy technologies (nodes greater than 45nm or other parts no longer in production or readily available for purchase). In addition, the DoD requires that parts satisfy significant qualification criteria against unique operational demands, such as challenging battlefield conditions and radiation hardening for space applications.

State-of-the-Art (SOTA)	Currently 7nm or less
State-of-the-Practice (SOTP)	Typically, 28 to 45nm
Legacy parts	Larger than 45nm, sometimes microns, generally no longer in production

DoD programs generally have lifetimes far outlasting the life cycle times of typical commercial microelectronics parts. Sustainment cannot be based on the assumption that subsequent generations of parts will enable backward compatibility. Access to parts no longer in production (legacy parts) is an all-too-common problem for the DoD who generally rely on prime contractors and their subcontractors to ensure long-term access to needed microelectronics for their systems. Primes and their subcontractors must worry about when manufacturing sources have been discontinued or have moved on to new generations of electronics. This process is called "Diminishing Manufacturing Sources and Material Shortages Management"—or "DMSMS management." Mitigation of microelectronics DMSMS is a particularly vexing problem for the DoD.

When the parts become outdated, systems must still be maintained as originally designed. Upgrades involving tech redesign are extremely costly. Given the pace of microelectronic advancements, the cost of redesigning based upon the constant evolution of each type of microelectronic device used in a system is not budgetarily feasible. In addition, each redesign must proceed through a systematic progression of time-consuming systems testing and re-qualification. In short, although redesigns are beneficial by using newer technology, these redesigns must be programmed, budgeted, and scheduled for testing and integration into operations. These block cycle upgrades could be shortened and cycled more often using digital engineering and open system architectures. However, in systems highly populated with microelectronics, these cycles should be generated from a managed upgrade plan and sustainment practices, not from a reaction to a single DMSMS notice.

DMSMS mitigation of every single device in every system is not practical. Therefore, each new system requires a plan for long-term sustainment to include a long-term supply of devices as originally designed and a plan for tech insertion via programmed redesigns.

Acquisition of microelectronic parts that are currently in production (i.e., state of the art—SOTA and state of the practice—SOTP) can also present issues for the DoD. Suppliers delay or fail to fulfill orders for parts due to the low volumes DoD requires for production. Commercial orders involve much larger volumes, so it is generally not economical for a commercial microelectronics supplier to process low-volume orders.

Export control compliance and International Trafficking in Arms Regulations (ITAR) further complicate procurement due to the need to provide specifications for required parts. Regulations may prohibit companies from providing

explicit requirements, so companies must find alternate sources or hide intended end-use through multiple layers of obfuscated procurement companies. Export control regulations sometimes inflict net harm on systems procurement instead of providing the protections the regulations were meant to provide.[4]

Regardless of the reason, DoD and the Defense Industry has very little insight into its systems' entire microelectronics supply chain. Subassemblies, constituent parts, and manufacturing steps can be five to twenty tiers below the prime contractor, and all the various sources can be impossible to track.

The result is great uncertainty about the integrity and long-term supply needs of microelectronics for the DoD, whether for legacy or currently produced parts. The DoD and the intelligence community (IC), in particular, require access to parts that provide high assurance that neither the design nor the purpose is revealed to potential adversaries. Ensuring this level of integrity and confidentiality requires extraordinary caution and chain of custody oversight.

HISTORY OF TRUSTED ACQUISITION OF MICROELECTRONICS

Decades ago, the government set up its own microelectronics fabrication facility (a "fab"), run by National Semiconductor, located on secured federal property, and dedicated to specific microelectronics production for government purposes. This dedicated fab eventually shut down because it was too expensive to continue to operate and upgrade without commercial use and because the facility became obsolete. In 2004, a new program called "Trusted Foundry" was initiated by the intelligence community (IC) to provide both guaranteed access to a then-state-of-the-art US fab at IBM along with a high degree of security. The **Trusted Foundry Program** was managed by an organization internal to the IC called the **Trusted Access Program Office** (TAPO). IBM was compensated with two contracts—one for access and multi-project wafer runs and the other for security services. While the TAPO organization managed these contracts, the costs were split between the IC and DoD offices in the Pentagon. The Defense Microelectronics Activity (DMEA) based in Sacramento was made the DoD program manager and funded to provide the DoD portion of the funding.

Around 2007, DMEA expanded the DoD portion of the program, still called the "Trusted Foundry Program" to include formal accreditation and audits of other fabs and services needed to create an entire ecosystem of microelectronics suppliers with a high level of trust. These services included design, fabrication, assembly, and testing. The trusted set of microelectronic technologies now available for systems includes mature parts and some highly specialized processes. This accredited group of performers formed the **trusted suppliers group** as part of a **Trusted Supplier Program**.

Around 2014, IBM divested itself of its fabs to the company GlobalFoundries, with IBM paying GlobalFoundries in this contractual transaction to offload its then-unprofitable microelectronics fabrication business. GlobalFoundries had major ownership investments from the United Arab Emirates, so the "sale" required approval from the US Committee on Foreign Investment in the United States (CFIUS). CFIUS required that the contracts were novated and continued to be executed with appropriate security for "GlobalFoundries US" under a proxy Board of Directors consisting of approved US citizens.

In 2016, as the initial contracts were nearing their end, the IC turned over the management of the entire Trusted Foundry Program to DoD. DMEA assumed the IC's TAPO responsibilities and created a new TAPO entity within DMEA with the combined program consisting of the Trusted Supplier Program and the trusted foundry contracts. These combined efforts were still called the Trusted Foundry Program, despite including multiple activities beyond simple trusted foundry access. After a re-compete, GlobalFoundries US retained contracts to supply access to the latest microelectronics technology as part of the expanded Trusted Foundry Program.

In 2018, GlobalFoundries made a business decision to offer only prior node geometries and not to attempt to keep up with the latest smaller geometries (smaller than 12nm), which would require billions of dollars in new investments. As a result, the TAPO contracts managed by DMEA could no longer guarantee access to trusted SOTA microelectronics, although they could supply the DoD needs for trusted mature technologies at nodes and geometries greater than 12nm.

GlobalFoundries' business decision reflected worldwide market conditions for microelectronics, resulting in the concentration of SOTA fabrication (now at geometries smaller than 12nm) in Taiwan and South Korea. This challenged the Trusted Supplier Program because the approved trust accreditation model only allowed for companies fully owned

and operating in the "five-eyes" nations (US, UK, Canada, Australia, and New Zealand).

The Trusted Foundry Program and TAPO nonetheless continue to supply accredited SOTP trusted parts and services to the DoD, despite the global migration of SOTA fabs to Asia, making trusted SOTA parts by any program unfeasible.

CURRENT CAPABILITIES

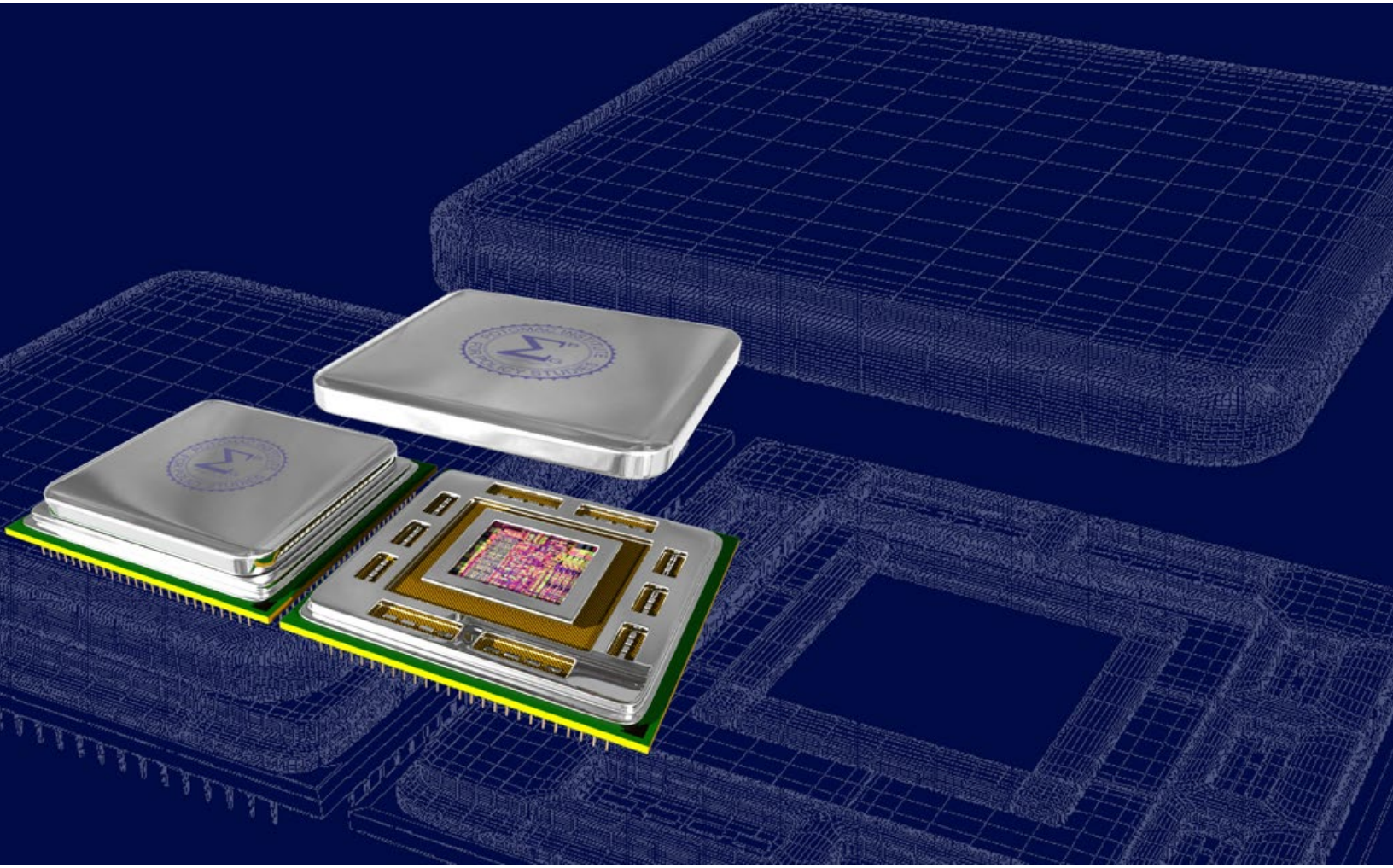
The Trusted Foundry Program continues to provide accredited secure services, including SOTP fabs (producing the most utilized parts within the DoD), albeit currently without the ability to provide accredited trusted parts at nodes below 12nm. The Trusted Supplier Program as part of the Trusted Foundry Program accredits all "trusted suppliers" in the microelectronics domain according to well-defined, auditable criteria. Trusted suppliers include not only foundries but also trust-accredited suppliers of design tools, ASIC design services, packaging and testing, assembly, prototyping services, or other stages in the development and manufacture flow of electronics for DoD systems. DoD programs use accredited suppliers, generally by direct interaction between the program's industry contractor(s) and their chosen accredited supplier. The requirement for the use of accredited suppliers flows from DoD policies as adjudicated by each program office and is often part of the customized "Program Protection Plan." Trust can also include protection of industry proprietary rights and security protection. The Office of the Secretary of Defense can issue waivers when necessary.

Still administered by the DMEA, the TAPO continues to provide DoD programs with access to microelectronics and electrical components that include a high degree of trust. GlobalFoundries US continues to have special contracts for access to their facilities giving TAPO priority access for runs involving multi-project wafers. These runs help solve the access issue for DoD by providing low-volume supplies for DoD programs and corporate research projects. A key to addressing the access issue caused by the economic preference for mass production runs is the aggregation of multiple requests from different projects onto a single wafer and executing the run through the trusted GlobalFoundries US fab. The TAPO contract for this trusted foundry includes pre-negotiated volume discounts for production at various breakpoints, paid for by the program offices requiring the parts. At this time, the technologies provided by GlobalFoundries allow for custom-designed devices necessary for US traditional and irregular warfare requirements. These technologies align with current DoD program needs but are already a few generations behind commercial SOTA. Nonetheless, highly qualified technologies can be integrated into critical national security programs, thus increasing the performance level of our systems.

TAPO processes can provide design tools to support DoD programs, providing proprietary intellectual property (IP) microelectronics components based on enterprise-wide licenses for current and legacy part designs. Security measures permit runs that support commercial proprietary, ITAR-restricted, Export Administration Regulations (EAR)-restricted, and trusted processing up to the Secret level.[5] TAPO can also provide microelectronics consultative support to DoD contractors using microelectronics experts and acquisition professionals cleared to the Top Secret/Sensitive Compartmented Information level.

In some cases, weapon systems must be sustained by producing small volumes of parts that replicate the form, fit, and functionality of obsolete COTS components. The Defense Logistics Agency has the Generalized Emulation of Microcircuits (GEM) program, and DMEA provides the Advanced Reconfigurable Manufacturing for Semiconductors (ARMS) program to address these needs.

Currently, 81 suppliers are accredited.[6] One of these is the GlobalFoundries "trusted foundry" and provides the highest level of trust. The remaining suppliers provide greater trust than buying commercial-off-the-shelf microelectronics. TAPO guides the use of accredited facilities,[7] but their use is the responsibility of the (defense) industry and the industry's program executive office. DoD programs can either encourage or require that their contractors use only accredited suppliers for their microelectronics needs, which can include design, multi-project wafer run aggregation, mask data preparation, mask manufacturing, wafer fabrication, dicing, packaging/assembly and testing, and customer support services. The use of accredited suppliers reduces vulnerabilities from supply disruptions or malfeasance. This proven methodology provides pre-approved and accredited suppliers which ensures a well-defined and audited trusted supply before manufacture starts, without time intensive, after-the-fact reviews of each part that could result in years' long delays of program development. It is important to note that to date (over 15 years), **no known malicious parts have come from the DMEA-accredited trusted suppliers.**



THE CHIPS AND SCIENCE ACT

During the peak of the COVID pandemic from 2020-21, microelectronics supplies for key industries, including automobile manufacturing, became limited. The auto companies canceled existing orders fearing a long downturn in demand. When production needed to ramp up due to unforeseen renewed demand, auto manufacturers had to delay production because of tight supplies. This circumstance was a wake-up call to policymakers who realized that commercial industry vulnerabilities due to foreign source dependencies and long supply chains will surely result in even more vulnerable defense industries. The defense industry relies on low volumes of specialized chips, which means that defense is particularly vulnerable to supply disruptions. Worse, foreign suppliers from adversary countries might be motivated to tamper with electronics intended for US weapon systems, especially for customized chips whose use is exclusive to defense applications.[8]

The Trusted Foundry Program, with its proven Trusted Supplier Program, ameliorates the vulnerabilities, but gaps remain. The CHIPS and Science Act of 2022 attempts to remedy these challenges by stimulating domestic production. The Act incentivizes firms to build fabs and other microelectronics production facilities in the US. The Act also provides funding, primarily through the Department of Commerce, for research so that future facilities can keep up with the fast rate of development in the microelectronics field. The Act further provides for a research program conducted by the DoD, the "DoD Microelectronics Commons," to stimulate development opportunities for researchers for specific DoD applications. The DoD Microelectronics Commons is intended to allow universities, small businesses, and industries to leverage fabs and design technologies to produce prototypes of microelectronics to serve DoD-specific needs.

The Act represents a bold attempt to strengthen a vital industry for US national security by using taxpayer funds

and tax incentives. But again, the fact that chips and electronic systems are built on US shores does not, by itself, guarantee trust. This is especially true for defense systems and US critical infrastructure. It also does not ensure that all future technologies will be produced domestically to serve all possible needs. Even if the goal of re-shoring microelectronics production was totally successful and domestic production served all needs, additional steps would be required to ensure trusted supplies to defense applications and critical infrastructure.

TECHNOLOGY DIRECTIONS

SOTA microelectronics fabrication has moved to 7nm and will soon progress to 3nm and 2nm designs. Other specialized technologies, such as Silicon-on-Carbon (SiC) and 3D packaging, provide non-scaling-based customized capabilities. Applications that require various technologies include communications and radio-frequency processing, optical applications, encryption applications, and microelectronics that will work on spacecraft subject to high radiation levels. While programmable microprocessors and other commodity microelectronic parts such as FPGAs can serve a large variety of needs, defense applications increasingly need customized microelectronics designed especially for their specific application. The DoD will need reliable access to trusted microelectronics that can serve these and other specialized applications.

TAPO 2.0

Today, TAPO is successful in accessing and supplying the trusted mature technologies that the DoD requires. In the future, defense systems will need the latest technologies to defeat adversary systems. Because SOTA fabs are currently concentrated in Asia, TAPO is constrained in supplying cutting-edge trusted microelectronics commodities. Defense systems will also need sustained supplies of legacy microelectronics that can be trusted.

The TAPO program run out of the DMEA has successfully addressed the issues of access, integrity, and confidentiality (i.e., trust) for the DoD for over 15 years without any known malicious parts coming from the TAPO's accredited trust program. This program can and should serve as a model and foundation to evolve into a TAPO 2.0 program. Such a program would combine CHIPS Act incentives to re-shore SOTA fabs to fill gaps in the trusted microelectronics supply chain with updated SOTA security protocols that take advantage of the current, more highly automated environment of a SOTA fab. In this way, TAPO 2.0 would only need a "light touch" and low-cost overhead to source secure parts within a commercial fab. These protocols have been developed such that they can provide the level of trust needed largely within the commercial fab's manufacturing process without the expense of a dedicated, trust-only fab. This effort would fill the current SOTA gap of the Trusted Foundry Program. The primary missing piece—access and trusted parts from SOTA facilities—would be a focus of this expanded portion of a trusted access program.

The existing and proven Trusted Access Program provides the necessary ingredients but will need to expand as new facilities and new technologies are introduced. New facilities will need to be accredited, audited, and advised on maintaining trust—for example, to avoid being compromised by nefarious hacking or malware. Expertise will need to be expanded for consulting services for defense contractors based on new technologies and customization needs. DMSMS management functions will require the procurement of sufficient supplies based on long-term needs assessments. Developers and program managers for defense systems and critical commercial systems will need to be aware of the offerings with greater trust. In some cases, for national security purposes, the use of trusted facilities will need to be mandated. Multiple "tiers of trust," properly defined, will need to be developed and managed according to the applications.[9]

The process and protocols for accrediting facilities for trust and maintaining trust accreditation will evolve with the technologies. For some applications, facilities at international allies and partners (beyond the "five-eyes" partners) may be accredited.

WAY FORWARD

The CHIPS and Science Act sets in motion the possibility of providing more domestic supplies of microelectronics to serve US needs. However, trusted supplies are necessary for national security applications, assured access in times of need, critical infrastructure applications, and other purposes. The Act did not explicitly address trust issues.

Accordingly, going forward, several steps are needed, requiring government actions:

1. Expand the current highly successful and proven Trusted Foundry Program at DMEA to coordinate with the CHIPS

Act that will encourage re-shoring of microelectronic sources. The TAPO office will need to give rise to a TAPO 2.0 expanded accreditation program, which develops criteria for "tiers of trust" at various levels, provides counsel to suppliers, and oversees an expansion of suppliers that can provide trusted microelectronics and electronics based on all levels of production. The office will need to expand the "intellectual property" building blocks of trusted design components offered to developers in designing customized secure microelectronics. New forms of shared capabilities are needed to enhance aggregation services, including design software and hardware production. TAPO 2.0 will need appropriate resources to accomplish these new goals.

2. Ensure that new manufacturers benefiting from CHIPS Act incentives comply with TAPO 2.0 trust accreditation processes and meet national security needs. Newly incentivized US-based fabs and facilities should be required to attain a level of trust accreditation to serve US needs.

3. Require providers using microelectronics in society-level critical infrastructure to use trusted microelectronics as accredited by TAPO 2.0. While such a requirement is useful to increase the market for trusted microelectronics, it is necessary for the security interests of the nation and provides a viable economic market for trusted parts.

4. Give new expanded authorities to TAPO 2.0 to develop accreditation agreements beyond "five-eyes" to include close partners and allies who are developing new manufacturing capabilities. TAPO 2.0 will also need to develop new accreditation levels and processes for accrediting new microelectronics processing steps, as added authorities may be required.

SUMMARY

Trust encompasses assured access when both state-of-the-art and legacy parts are needed, and assurance that the parts have high integrity so they can be trusted to perform precisely, as promised, and can satisfy the proprietary and security needs of withholding information from adversaries and competitors. These recommendations are common-sense approaches to completing the mission of the CHIPS and Science Act. With a properly resourced TAPO 2.0, the nation can be assured of an adequate supply of trusted microelectronics to fulfill needs in defense and commercial endeavors that require sufficient trust.

ACKNOWLEDGEMENTS

The author thanks reviewers and contributors Michael Fritze, Daniel Marrujo, Bob Hummel, Erica Kilgore and Sherry Loveless for their editorial and contextual support.

ENDNOTES

1 Potomac Institute for Policy Studies. (2021). *Re-Embrace American S&T: Reimagine, Reinvent, Restart.* Potomac Institute Press. https://www.potomacinstitute.org/steps/featured-articles/september-2021/re-embrace-american-science-and-technology-reimagine-reinvent-restart

2 Office of the Director of National Intelligence. (Feb 6, 2023). *Annual Threat Assessment of the U.S. Intelligence Community.* https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf

3 NDIA Electronics Division. (2021). *How to On-Shore Critical Semiconductor Production, Secure the Supply Chain, and Provide Access for the Industrial Base*. National Defense Industrial Association. https://www.ndia.org/-/media/sites/ndia/divisions/electronics/images---resources/ndia-on-shore-semiconductor-products-supply-chain-and-industrial-base-white-paper-final.pdf

4 Potomac Institute for Policy Studies. (2016). *An Analysis of the Impacts of the International Traffic in Arms Regulations (ITAR) on U.S. National Security and Economic Interests.* Potomac Institute Press. https://potomacinstitute.org/images/RSEC/ITAR.pdf

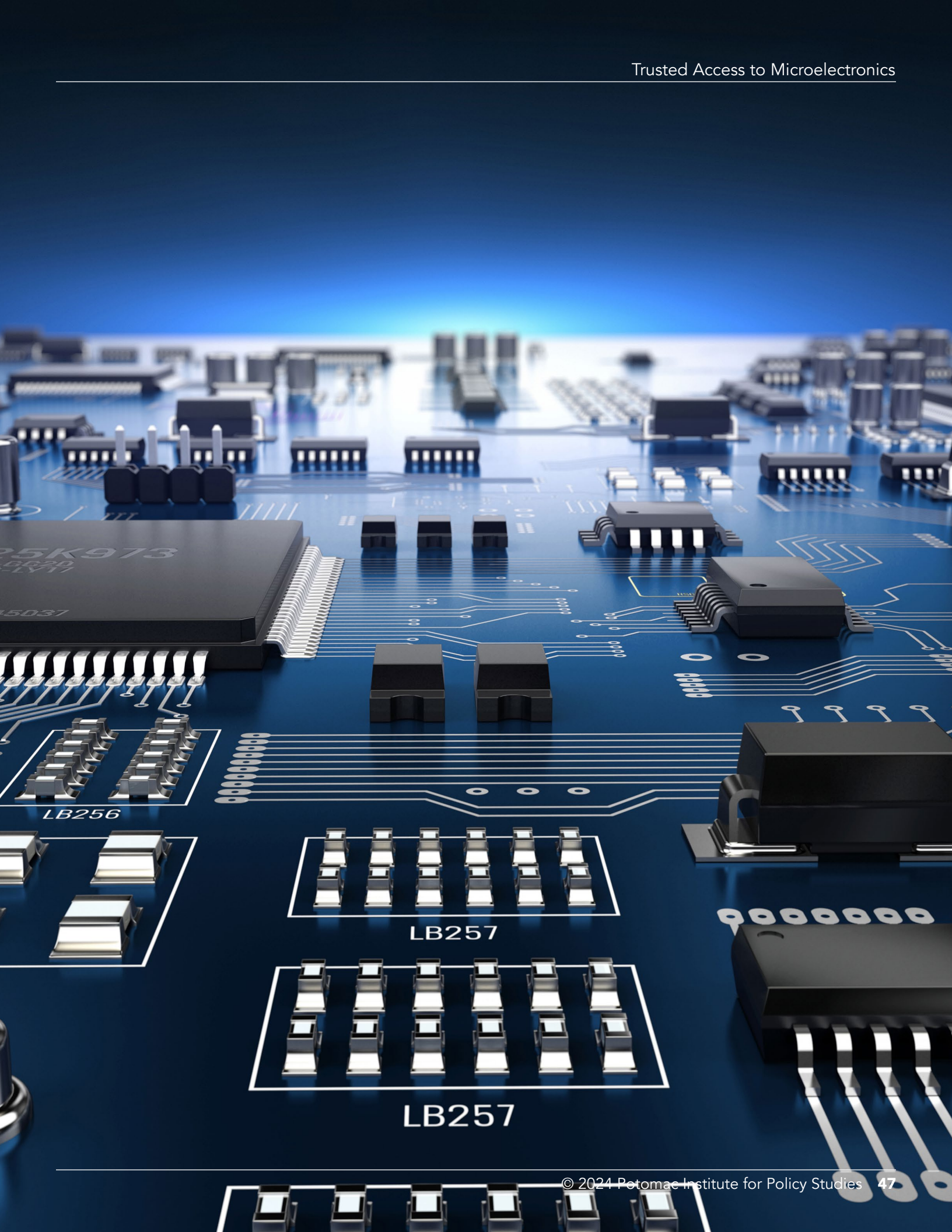
5 NDIA Electronics Division. (2021). *How to On-Shore Critical Semiconductor Production, Secure the Supply Chain, and Provide Access for the Industrial Base*. National Defense Industrial Association. https://www.ndia.org/-/media/sites/ndia/divisions/electronics/images---resources/ndia-on-shore-semiconductor-products-supply-chain-and-industrial-base-white-paper-final.pdf

6 Defense Microelectonics Activity, (2023). *Trusted Foundry Program. Accredited Suppliers*. https://www.dmea.osd.mil/otherdocs/accreditedsuppliers.pdf

7 US Department of Defense Instruction No. 5200.44. (Nov 5, 2012). *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)*. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520044p.pdf

8 Office of the Director of National Intelligence. (Feb 6, 2023). *Annual Threat Assessment of the U.S. Intelligence Community.* https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf

9 Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics. (July 2014). *Department of Defense Assured Microelectronics Policy. Senate Report 113-85*. DOPSR #14-C-0820. https://rt.cto.mil/wp-content/uploads/2019/06/DoD-Assured-Microelectronics-Policy-RTC-July2014.pdf


LB256
LB257
LB257