ETI EMERGING TECHNOLOGIES INSTITUTE | NDIA

Modernizing Defense Microelectronics

Challenges and Opportunities

White Paper • November 2023
NDIA Emerging Technologies Institute

Table of Contents

November 2023
First published in 2023 by NDIA's affiliate, the Emerging Technologies Institute. 2101 Wilson Blvd, Suite 700, Arlington, VA 22201, United States of America. (703) 522-1820

This report is made possible by general support to NDIA and the Emerging Technologies Institute. No direct sponsorship contributed to this report. This report is produced by NDIA, a non-partisan, non-profit, educational association that has been designated by the IRS as a 501(c)(3) nonprofit organization – not a lobby firm – and was founded to educate its constituencies on all aspects of national security. Its research is nonpartisan.

For more information please visit our website: EmergingTechnologiesInstitute.org

Written by Jacob Winn and Dr. Michael Fritze.
Typeset and produced by Hannah Meushaw, Alexander Feeser, and Eve Dorris.
Edited by Jacob Trask.

MEDIA QUERIES:
Habiba Hamid, Director of Public Affairs & Communications at hhamid@NDIA.org

Contributors

NDIA ETI

Writing Team

Jacob Winn
Associate Research Fellow, NDIA Emerging Technologies Institute

Dr. Michael Fritze
Consultant, NDIA Emerging Technologies Institute

Executive Director

Dr. Arun Seraphin

We also thank Dr. Mark Lewis and Dr. Anna Melker for their contributions, and the entirety of the NDIA ETI staff for their review.

External Reviewers*

Ted Glum
Member, Board of Directors,
Potomac Institute for Policy Studies
Former Director, Defense Microelectronics Activity (DMEA)

Stephanie Halcrow
NDIA Senior Fellow for Defense Industrial Base Health and Resiliency

Brett Hamilton
SVP of Microelectronics & Advanced Technology Strategy, Applied Research Institute (ARI)

Dr. Yadunath Zambre
Chief Microelectronics Technology Officer,
Air Force Research Laboratory

Selected Interviewees*

Dr. Victoria Coleman
Chief Scientist of the Air Force

Saverio Fazzari
Microelectronics Fellow, Booz Allen Hamilton

The Honorable James F. Geurts
Former Service Acquisition Executive for the US Navy, US Marine Corps, and US Special Operations Command

The Honorable Dr. Bruce D. Jette
Former Assistant Secretary of the Army for Acquisition, Logistics, and Technology
President and CEO, Innvistra LLC

Jay Lewis
Office of the CTO, Strategic Mission Technologies, Microsoft

Dr. Grant Meyer
Principal Program Manager
Lockheed Martin Corporation

Dr. Christine Michienzi
Owner, MMR Defense Solutions, LLC

The Honorable Al Shaffer
Distinguished Visiting Fellow, NDIA ETI

The Honorable Sean Stackley
Senior Vice President, Strategy, Growth, & Technology, L3Harris Technologies
Former Assistant Secretary of the Navy for Research, Development, and Acquisition

VADM Mat Winter, USN (Ret)
President, Winter Strategic Solutions, LLC

Dr. John C. Zolper
Principal Engineering Fellow & Microelectronics Lead, RTX Corporation

** This report is a product of NDIA ETI, developed through independent research and a series of interviews. The product was reviewed by a set of expert external reviewers. The contents of this report should not be construed as the opinions of any individual interviewee or external reviewer.*

Foreword

In an era of renewed great power competition, it is imperative that the military maintain its technical superiority across its suite of defense capabilities. Continued overmatch requires addressing the integral role microelectronics play in both legacy and emerging weapon systems. Fielded systems need to be upgraded to leverage more modern microelectronics in response to new threats, obsolescence, or the lack of fabrication facilities for purpose-built components requiring replacement. Scientists and engineers need to utilize commercial semiconductor technology to the greatest extent possible to meet unique war fighting demands as new systems are developed, tested, and operationalized.

The Department of Defense (DoD) has challenges with microelectronics. Similarly to software, the pace of microelectronics innovation is extremely fast and the majority of the technological expertise and the bulk of the demand is in the commercial sector and not within U.S. government organizations. Semiconductor research and development, engineering, fabrication, and integration with high- performance systems take place outside of government, while the number of career civilians skilled in the past, present, and future state within DoD continues to dwindle. The need to sustain current systems while modernizing the nation's military hardware and software depends on microelectronics, which are primarily fabricated offshore even though design and critical manufacturing equipment production occurs in the United States. Rapid development, production, and sustainment of microelectronics are constrained by unique appropriations for each of these lifecycle phases, requiring an artificial segmentation of activities leading to a fielded product.

We as a nation are challenged to use our collective capability to enable the DoD to maintain readiness and achieve meaningful modernization for our military departments by leveraging the best of American commercial microelectronics ingenuity for the unique performance, security, and resiliency that great power competition demands.

This paper is the result of critical thinking by a cross-section of individuals who provided history and perspective to identify the current state of DoD microelectronics as well as a focus on a future characterized by secure and resilient supply chains for critical defense capability. NDIA ETI consulted subject matter experts encompassing research and engineering, acquisition, and policy domains to ensure a balanced view of the microelectronics ecosystem. At the very least, this paper represents a comprehensive view of the defense microelectronics ecosystem today. More importantly, we can envision a path to a secure future guided by the information concisely presented.

I am hopeful that American technological and business model innovation will once again embrace the existential challenge we face to maintain our global leadership in the semiconductor industry. NDIA ETI is accelerating the realization of this hope by pointing towards pathways to redefine our microelectronics defense industrial base. Thank you to all who contributed!

The Honorable Ellen M. Lord
Former Under Secretary of Defense for Acquisition and Sustainment

Member, NDIA ETI Advisory Board

Executive Summary

The Department of Defense (DoD) is tasked with fielding military systems that meet America's national security needs. To do so, it constantly strives to strike a balance between fielding new capabilities while upgrading existing ones to provide the military with improved performance to keep pace with changing threats, or to integrate innovations generated by the private sector. However, the current state of defense microelectronics poses a significant challenge to modernizing defense systems efficiently in terms of cost, schedule, and distance from the microelectronics state of the practice on a variety of performance metrics.

Such modernization upgrades must enhance mission capabilities, which may involve leveraging advanced microelectronics to reduce size, weight, and power (SWAP) while simultaneously boosting computational performance and speed. Effectively managing national security risks, tackling supply chain complexities, and addressing manufacturing and workforce requirements are all essential components of this endeavor. Achieving success necessitates close collaboration among various stakeholders within the DoD, scientific, and technological communities (including universities and federal research organizations), the defense industrial base, and the global commercial microelectronics sector.

To address these issues, the National Defense Industrial Association's (NDIA) Emerging Technologies Institute (ETI) convened a workshop on microelectronics modernization and conducted a series of research activities in support of this report. ETI conducted interviews with a host of subject matter experts with backgrounds ranging from a lifetime of service at the DoD, to commercial microelectronics industry veterans, to defense industrial base engineers and business executives.

ETI hopes that this report's findings and recommendations foster a robust and constructive dialogue among stakeholders across the defense industrial base, the commercial microelectronics industry, academia, and the Department of Defense.

Selected Findings:

1. DoD lacks a centralized organization with sufficient authority, resources, and expertise to assist Program Offices with acquiring, sustaining, and modernizing their microelectronics.

2. Technical challenges include insufficient information on the cost and benefits of modernization and the need to adopt more advanced design, integration, qualification, and security practices.

3. Acquisition and requirements challenges encompass a lack of coordination in microelectronics investments, missed opportunities for government negotiation, and an absence of policies promoting continuous or regular microelectronics upgrades.

Top-Level Recommendations:

1. Encourage continuous microelectronics upgrades in defense systems.

2. Improve defense microelectronics security standards.

3. Use pilot programs to explore innovative practices for microelectronics acquisition.

4. Designate a centralized DoD microelectronics support activity.

5. Implement approaches to better integrate commercial state-of-the-practice microelectronics into defense systems.

Introduction

Microelectronic semiconductor chips are the core component underpinning computational power, supporting the simplest functions in "smart" refrigerators to the most complex performance in advanced weapon systems. Computer chips are the lifeblood of the modern American economy. The U.S. relies on increasingly sophisticated microelectronics to support the march of technological progress in sectors including electronics and machinery, communications, and the service economy. The speed of innovation has been staggering. As "Moore's Law" predicted, the number of transistors packed onto a chip has historically doubled approximately every 18 months for the past half century, while the costs of chips halve every 18 months.[1]

These technological breakthroughs and resulting economic gains were achieved through both manufacturing specialization and the widespread adoption of computers by businesses and consumers. Countries in East Asia – especially Taiwan and South Korea – specialize in advanced fabrication capabilities at their foundries and produce today's cutting-edge 3-nanometer nodes for chips designed by companies in other countries such as the United States.[2] Taiwan Semiconductor Manufacturing Company (TSMC) alone possesses 56% of the global foundry market share, and an even higher share of the state-of-the-art (SOTA) market.[3] While the Department of Defense (DoD) and the defense industrial base (DIB) were often the main parties offering a "demand signal" for innovative and increasingly powerful semiconductors, this has shifted over the past three decades as the commercial technology sector has grown to become the largest purchaser. Today, DoD and the DIB use microelectronics in the development of advanced weapon systems, sensors, and surveillance systems. While these systems are essential for maintaining the United States' strategic, tactical, and operational advantages and supporting the emerging technologies of the future, DoD and the DIB represent an increasingly small segment of the market.[4]

DoD has unique requirements for computer chips that are used in weapon systems. These requirements are driven by the need for high performance, reliability, power usage constraints, and security in the face of demanding environments that require significant levels of qualification against a variety of operational conditions, such as radiation or use in space.[5] Emerging technologies – especially those identified as critical technology areas by the Office of the Undersecretary of Defense for Research and Engineering (OUSD(R&E)), including artificial intelligence/autonomous systems, integrated network systems-of-systems, hypersonics, and integrated sensing – often require even more significant functionality due to the advanced datasets and calculation/communication speeds required for their operation.[6] Military requirements also demand exceptionally low failure rates. All of this can mean that technical requirements writers are incentivized to require very specialized microelectronics products that meet these needs. As a result, DoD and its contractors sometimes resort to using custom chips that are designed and manufactured specifically to meet these requirements, slowing down the acquisitions process and making it more difficult to upgrade a microelectronic later if every other subsystem was optimized for the original chip.

Because these chips are often designed for DoD-specific applications, they are not commercially viable and are often protected by export controls and other regulations that leave the U.S. military as the sole customer. A key challenge for DoD is the high cost associated with development, production, and sustainment of these specialized chips. Custom chips require significant investment in design and engineering, as well as specialized manufacturing processes and equipment and unique life-cycle support challenges. This can make them significantly more expensive than commercial off-the-shelf (COTS) chips, which are mass produced and can be cost-amortized over very large volumes. In addition to these challenges, the DoD also faces significant security concerns regarding its custom chip supply chain. Because these chips are used in critical weapon systems, they must be protected from tampering and other forms of security breaches. This requires careful management of the supply chain, including strict controls on who has access to the chips and how they are handled and transported.[7] These concerns further increase costs and have led DoD to prefer chips designed through the Trusted Foundry Program for critical custom needs, administered by the Defense Microelectronics Activity (DMEA).[8] In recent years – especially in the wake of the COVID-19 pandemic – national security experts and policymakers have become increasingly concerned that American supply chains for this technology, especially its foundry networks, should be on-shored or near-shored in response to growing access risks in the Asia-Pacific.

With these access, cost, and security concerns in mind across the defense, business, technology, and policy sectors, the passage of the CHIPS and Science Act of 2022 marks the onset of a new era of American microelectronics. However, how effective the

1 IEEE IRDS, "Future of Semiconductor Performance," https://irds.ieee.org/topics/future-of-semiconductor-performance

2 Nanometers are the unit of measurement for measuring the length of transistors. Because more transistors can be placed on a chip of the same size if they are smaller and closer together, computation time and energy are saved as transistors become smaller.

3 Counterpoint Research, "Global Semiconductor Foundry Market Share: By Quarter." September 12, 2023, https://www.counterpointresearch.com/insights/global-semiconductor-foundry-market-share/

4 NDIA Electronics Division, "How to On-Shore Critical Semiconductor Production, Secure the Supply Chain, and Provide Access for the Industrial Base," February 2021, https://www.ndia.org/-/media/sites/ndia/divisions/electronics/images---resources/ndia-on-shore-semiconductor-products-supply-chain-and-industrial-base-white-paper-final.ashx, p. 8.

5 U.S. Department of Defense, "Department of Defense Assured Microelectronics Policy for Senate Report 113-85," July 2014, https://rt.cto.mil/wp-content/uploads/2019/06/DoD-Assured-Microelectronics-Policy-RTC-July2014.pdf

6 Office of the Under Secretary for Research & Engineering, U.S. Department of Defense, "Critical Technology Areas." https://www.cto.mil/usdre-strat-vision-critical-tech-areas/

7 See NDIA's Microelectronics Division's 2021 white paper on semiconductor production supply chains, " How to On-Shore Critical Semiconductor Production, Secure the Supply Chain, and Provide Access for the Industrial Base," here: 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

8 Defense Microelectronics Agency, U.S. Department of Defense. https://www.dmea.osd.mil/TrustedIC.aspx

implementation of this policy is for strengthening American supply chains and addressing current vulnerabilities will only be made clear with time. The CHIPS and Science Act is an industrial policy that – through a mix of appropriations, authorizations, and tax credit incentives – seeks to invest $280 billion in the U.S. semiconductor industry. Its goals are:

1. to create state-of-the-art foundries in the United States,
2. to invest in regional semiconductor manufacturing capabilities throughout the United States, and
3. to bolster domestic microelectronics research and development. [9]

Amongst other provisions, the law appropriates $52.7 billion over five years for semiconductor manufacturing incentives, workforce development, and R&D. The rest of the $280 billion comes in the form of authorizations, such as $36 billion over five years to the National Science Foundation, which may or may not receive appropriations by future Congresses. This includes $20 billion for a new Tech Directorate.[10] Within the DoD, the Act also funds the Microelectronics Commons.[11] The Commons will be a network of regional innovation hubs and core facilities that provide state-of-the-art microelectronics to a variety of emerging technology areas.[12] This new network received over $2 billion in appropriations to enable rapid development from laboratory to fabrication of prototypes ("lab to fab"). These innovation hubs, and their grant awards, were announced on September 20, 2023.[13]

While the CHIPS and Science Act deserves praise for its timeliness, high funding level, and potential for success, challenges remain for proper implementation. These include the challenge of developing the U.S.-based workforce culture and technical knowledge, large capital investments required to construct American state-of-the-art foundries that will rest on corporations continuing to make their own substantial private investments, and the need for successful coordination across the federal interagency.[14] Moreover, the microelectronics industry is historically cyclical, raising the risk that current investments might not remain commercially viable as compared to global competitors.

As the broader American economy and government undertake these microelectronics-related reforms, defense policymakers are doing the same. Deputy Secretary of Defense Kathleen Hicks established the Defense Microelectronics Cross-Functional Team (DMCFT) in January 2021 to create a DoD microelectronics strategy.[15] The new strategy – partially released in May 2022 – seeks to provide a path forward on microelectronics modernization that accounts for the fact that most military systems utilize mature or legacy microelectronics and are sustained at high costs. Both modernization and acquisition timelines are highly dependent on the speed at which DoD and the DIB can push microelectronics through the lifecycle process of requirement identification, design, manufacturing, testing, and fielding.

Most recently, DoD and Congress have done the following in pursuit of these goals:

- Office of the Undersecretary of Defense for Acquisition and Sustainment (OUSD(A&S)) has sought to create incentives for DoD program offices to upgrade their microelectronic components using commercial state-of-the-practice (SOTP) components.
- OUSD(R&E) is investigating how to streamline the qualification process of new state-of-the-art microelectronics.
- The Senate Armed Services Committee's report on the FY2023 National Defense Authorization Act (NDAA) included language requiring the Under Secretary of Defense for Research & Engineering ("USD(R&E)") to further study the feasibility and cost-benefit calculus of upgrading legacy chips and reducing requirements for custom microelectronics.[16]

The National Defense Industrial Association's (NDIA) Emerging Technologies Institute (ETI) wrote this report with the questions and goals of these policymakers in mind. ETI also held a workshop in 2022 to convene representatives from the defense industrial base, commercial microelectronics sector, DoD, and Congress to discuss effective ways of transitioning modern microelectronics into defense systems. As part of the research process, ETI conducted interviews with a host of subject matter experts with backgrounds ranging from a lifetime of service at the DoD, to commercial microelectronics industry veterans, to defense industrial base engineers and business executives.

---

9 The White House, "Fact Sheet: CHIPS and Science Act Will Lower Costs, Create Jobs, Strengthen Supply Chains, and Counter China," February 3, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/09/fact-sheet-chips-and-science-act-will-lower-costs-create-jobs-strengthen-supply-chains-and-counter-china/

10 U.S. Congress, "CHIPS and Science Act of 2022", Public Law 117-167, https://www.congress.gov/bill/117th-congress/house-bill/4346.

11 Office of the Under Secretary for Research & Engineering, U.S. Department of Defense. "Microelectronics Commons." https://www.cto.mil/ct/microelectronics/commons/

12 Office of the Under Secretary for Research & Engineering, U.S. Department of Defense, "DoD Microelectronics Commons: A National Network for Defense Microelectronics Innovation" October 31, 2022, https://www.cto.mil/wp-content/uploads/2022/11/DoD_Microelectronics_Commons.pdf

13 C. Todd Lopez, U.S. Department of Defense, "DOD Names 8 Locations to Serve as New 'Microelectronics Commons' Hubs." September 20, 2023, https://www.defense.gov/News/News-Stories/Article/Article/3532338/dod-names-8-locations-to-serve-as-new-microelectronics-commons-hubs/

14 That coordination is being administered by the Department of Commerce.

15 U.S. Department of Defense, "Microelectronics Vision," May 2022, https://media.defense.gov/2022/Jun/15/2003018021/-1/-1/0/DEPARTMENT-OF-DEFENSE-MICROELECTRONICS-VISION.PDF.

16 https://www.congress.gov/117/crpt/srpt130/CRPT-117srpt130.pdf, p. 74.

OUSD(R&E) has been asked to ***"commission an independent assessment from experts in the field of commercial microelectronics and DOD requirements for microelectronics of the feasibility and the cost-benefit calculus of: (1) Upgrading the microelectronics in legacy systems with long projected service lives with modern semiconductors and new software via modeling, emulation, and testing rather than attempting lifetime buys of obsolete chips; and (2) Minimizing or even eliminating requirements for low volume custom-designed semiconductors and instead buying commodity commercial products and tailoring them to specific applications through heterogeneous packaging and software programming."***

Background

The State of Microelectronics

The modern microelectronics ecosystem is a complex network of industries, universities, and government agencies involved in the research, design, manufacture, and usage of microelectronic devices. A steady supply of research – especially university- and commercial-based research in fields such as metrology, materials science, electrical engineering, computer science, and physics – supports new techniques for designing and manufacturing computer chips that innovate on every component from semiconductors to wafer architecture. This research supports the development of increasingly intricate transistor designs, currently approaching a minimum feature length of 2-nanometers in the most cutting-edge designs, using a variety of digital modeling and simulation technologies.[17] These state-of-the-art designs are then manufactured through complex processes such as photolithography – the most advanced provided by the Dutch company ASML to the major foundries – and are produced in high volume at foundries such as TSMC and UMC (Taiwan), Samsung (Korea), GlobalFoundries (USA), and SMIC (China).[18, 19] Intel is in the process of scaling its own foundries.[20] Mature computer chips are manufactured by these larger too, though the United States possesses a larger share of the mature chip fabrication market, with China playing an increasing role.

Overall, United States commercial firms excel at chip design (including Electronic Design Automation (EDA) tools) and manufacturing semiconductor fabrication tools while Taiwanese and South Korean firms dominate the global advanced chip manufacturing market. There are several distinct types of business models across the commercial industry: integrated device manufacturers (IDMs), "fabless" companies that design but do not manufacture chips, and "pure-play" foundries that manufacture chips for other companies' designs.[21] IDMs, such as Intel,[22] are companies that design and manufacture their own semiconductors. These companies have their own fabrication facilities and control every aspect of the chip-making process, from design to fabrication to testing. On the other hand, fabless vendors (e.g., Nvidia, Apple, Qualcomm, etc.) design and market their computer chips, but outsource the manufacturing of their chips to third-party pure-play foundries such as TSMC, as well as packaging and testing. These industry players are highly concerned with the final "yield" at their foundry, referring to the percentage of computer chips manufactured at the quality desired at the design phase. Ideally, the cutting-edge commercial foundries aim for a yield rate well above 90% on state-of-the-practice semiconductors. Yield rates across hundreds of thousands, or even millions, of units must be assured to maintain costs and can be lower when manufacturing state-of-the-art chips, when using older production systems, or in facilities producing novel customized chips for military programs. This creates substantial risk to cost and schedule for DoD program offices. Further, higher yields have a positive correlation with reliability.[23] This can produce challenges for lower-yield, defense-specific technologies.

According to the Semiconductor Industry Association (SIA), semiconductors can be classified into three large categories: (1) Logic, (2) Memory, and (3) Discrete, Analog, and Other (DAO).[24] DoD's legacy and advanced weapon systems require all three:

- **Logic:** These general-purpose or highly customized reasoning microprocessors provide the bulk of the computational power for operational activities (e.g., complex targeting or autonomous systems).
- **Memory:** These components enable computation by storing complex information. Applications include large data storage and advanced radar processing.
- **Discrete, Analog, and Other (DAO):** These semiconductors "transmit, receive, and transform information dealing with continuous parameters such as temperature and voltage."[25] They are crucial for operating machinery in high-performance environments and for communications and sensor technology.

DoD requires microchips for virtually all of its weapon systems. These semiconductors vary from mature chips in older systems to state-of-the-art components. These chips are typically procured by prime contractors who are responsible for designing a weapon system, integrating all subsystems, and assuring that the final product meets all operational and technical requirements. However, the overspecification of performance requirements and failure tolerance in some defense system technical requirements can drive contractors to procure custom semiconductors rather than seek commercially-available products. In some cases, at the time of contract award, no existing commercial off-the-shelf product can fully satisfy the requirements.

Because microchips sit at the core of a system's functionality, once a custom chip has been designed, the weapon system's other components, electronics, and subsystems are optimized to function around the chip. In many cases, this means that the DoD program office plans for that custom chip to be used by the system for its

17 Major American computer chip designers include Qualcomm, IBM, Nvidia, Advanced Micro Devices (AMD), Micron, Broadcom, and Texas Instruments. https://www.investopedia.com/articles/markets/012216/worlds-top-10-semiconductor-companies-tsmintc.asp

18 In fact, ASML provides the entire global supply of extreme ultraviolet (EUV) lithography, a process used to print the smallest and most complex designs onto transistor wafers. https://www.cnbc.com/2022/03/23/inside-asml-the-company-advanced-chipmakers-use-for-euv-lithography.html

19 Prableen Bajpai, Nasdaq, "An Overview of the Top 5 Semiconductor Foundry Companies," October 1, 2021, https://www.nasdaq.com/articles/an-overview-of-the-top-5-semiconductor-foundry-companies-2021-10-01

20 Intel Corporation, "Intel Provides Update on Internal Foundry Model," June 21, 2023, https://www.intel.com/content/www/us/en/newsroom/news/intel-update-internal-foundry-model.html

21 Mordor Intelligence, "Semiconductor Foundry Companies - Market Share & Size," https://www.mordorintelligence.com/industry-reports/semiconductor-foundry-market

22 Intel is currently in the process of scaling an "open foundries" model that will produce more semiconductors on behalf of others.

23 Kuo, Way, and Taeho Kim. IEEE Xplore. "IEEE Xplore Full-Text PDF:" https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9043719

24 Antonio Varas, Raj Varadarajan, Jimmy Goodrich, and Falan Yinug, 2021, Semiconductor Industry Association, Boston Consulting Group, "Strengthening the Global Semiconductor Supply Chain in an Uncertain Era", April 2021, https://www.semiconductors.org/wp-content/uploads/2021/05/BCG-x-SIA-Strengthening-the-Global-Semiconductor-Value-Chain-April-2021_1.pdf, p. 9

25 Ibid.

entire lifecycle. As a result, sustainment contractors – often the original equipment manufacturer (OEM) – seek to buy the chip in bulk at the "end-of-life" when production is ending, or must re-engineer and re-qualify the system to work with other microelectronics.[26] Alternatively, the program office can seek to execute an Engineering Change Proposal to modify or upgrade the system with the latest microelectronic technology. The Defense Logistics Agency refers to this type of discontinuation as "Diminishing Manufacturing Sources and Material Shortages (DMSMS)."[27]

As the world changes, so must the military. Threats change over time, technology advances, and military strategy and doctrine adapt to address evolving strategic challenges. This has occurred at an unprecedented pace in the era of modern computing, leading defense and civilian policymakers to embark on a variety of modernization initiatives to overhaul and update systems' capabilities. This involves replacing not just the subsystems of legacy systems, but also the mature chips that are not optimized for modern capabilities and do not possess nearly enough computational power to support emerging operational capabilities and the joint force's growing communications and sensing needs.

Security is also a critical issue for defense microelectronics. Today, DoD often relies on its Trusted Foundry Program to procure microelectronics and designates approved microelectronics facilities whose products are assumed to be more secure because of more advanced security measures than those employed by typical commercial foundries.[28] While this system can produce a category of assured microelectronics, trusted foundry projects can put DoD further behind the commercial industry over time because DoD and the DIB can no longer make up a sufficient share of the market to make a compelling Trusted Foundry-based business case for SOTA technologies. Moreover, insider threats can still impact microelectronic systems despite existing security protocols. The Trusted Foundry Program may be modified to update its accreditation procedures to leverage modern SOTA fabrication automation as a result of the CHIPS and Science Act seeking to create new SOTA fabrication facilities within the United States.

All told, the government has indicated that some combination of "zero-trust" assurance, the trusted foundry network, and other modalities are likely to be used in combination. Currently, DoD is in the process of developing its zero-trust assurance approach for securing networks and both hardware and software systems.[29] A zero-trust system approach entails removing all implicit trust areas from the process, while requiring continuous re-validation of systems to ensure that they are not compromised. DoD released its Zero-Trust Strategy in November of 2022.[30] With respect to microelectronics, this includes a move towards procuring microelectronics that are closer to the commercial state-of-the-practice. These commercial SOTP microelectronics are assumed to be less secure as DoD releases control over the manufacturing process, with a plan for re-validation of these chips before they enter systems. With respect to procuring newer, custom microelectronics, DoD is experimenting with a new security method called "quantifiable assurance" ("MQA").[31] Some argue that more research and analysis are needed to implement these methodologies – and, even if they are implemented, the Trusted Foundry Program will still be necessary. For example, a July 2023 MQA Independent Assessment, convened by OUSD(R&E) to assess the technical viability of the MQA methodology under development by their Trusted and Assured Microelectronics (T&AM) team, finds that quantifiable assurance has made progress but is "not ready for deployment," and that "significant gaps exist.[32]

It is critical for DoD to be able to upgrade its existing and future systems to modern microelectronics in a manner that is rapid, cost-effective, and improves mission capabilities. Improving mission capabilities might include using advanced microelectronics to reduce size, weight, and power (SWAP) while also increasing computational power and speed. The Department will need to manage national security risks, supply chain challenges, and manufacturing and workforce needs. This requires deep collaboration among DoD organizations, science and technology ("S&T") stakeholders such as universities and federal intramural researchers, the defense industrial base, and the globalized commercial microelectronics industry. To-date, Congress, DoD, and other parts of the executive branch have begun establishing significant infrastructure in support of this goal. In alphabetical order, the government's ecosystem of agencies and major activities influencing microelectronics policy include, but are not limited to:

1. **CHIPS Implementation Steering Council:** Interagency group within the Executive Office of the President, responsible for consulting on the implementation of the CHIPS and Science Act. Established by Executive Order 14080.
2. **CHIPS Industrial Advisory Committee (IAC):** Advisory body made up of senior experts from industry, academia and non-profits created to support Department of Commerce (DoC) NIST CHIPS R&D implementation.
3. **DARPA Electronics Resurgence Initiative (ERI):** Initiated in 2017 with the Microsystems Technology Office to "forge forward-looking collaborations among the commercial electronics

26 Alan R. Shaffer, Chris Toffales, and Monique D. Attar, National Defense, "Microelectronics - A Critical National Resource," June 3, 2021, https://www.nationaldefensemagazine.org/articles/2021/6/3/microelectronics---a-critical-national-resource

27 Defense Standardization Program Office, Defense Logistics Agency (DLA), U.S. Department of Defense, "Diminishing Manufacturing Sources and Material Shortages," September 2009, https://www.dla.mil/Portals/104/Documents/LandAndMaritime/V/VA/PSMC/LM_SD22FINAL_151030.PDF, p. 4

28 See DoD Instruction 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)," for information on the Trusted Foundry Program's authority.

29 See NDIA's Microelectronics Division's 2021 white paper on zero-trust, "Zero-Trust for Hardware Supply Chains: Challenges in Application of Zero-Trust Principles to Hardware," here: https://www.ndia.org/-/media/sites/ndia/divisions/electronics/images---resources/zerotrustwhitepaper_20oct-revc.pdf

30 U.S. Department of Defense, " DoD Zero Trust Strategy," October 21, 2022, https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf

31 The National Security Agency's (NSA) JFAC Hardware Assurance Lab released key technical reports on protecting DoD microelectronics from adversary influence in December 2022. For detailed information on these technical reports, see https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3239938/nsa-releases-series-on-protecting-dod-microelectronics-from-adversary-influence/.

This follows the NSA's July 2022 technical report on microelectronics security, "Levels of Assurance Definitions and Applications". For more information, see https://media.defense.gov/2022/Jul/14/2003034921/-1/-1/0/CTR_DOD_MICROELECTRONICS_LEVELS_OF_ASSURANCE_DEFINITIONS_AND_APPLICATIONS_20220714.PDF

32 Shamik Das, MITRE Corporation, "Microelectronics Quantifiable Assurance (MQA) Independent Assessment," March 1, 2023, https://www.cto.mil/wp-content/uploads/2023/07/MQA-Assessment-Briefing-for-Release-Distro-A.pdf

community, defense industrial base, university researchers, and the DoD to address these challenges."[33] ERI also includes work on the Next-Generation Microelectronics Manufacturing (NGMM) program, working to develop the infrastructure for heterogeneous integration.[34]

4. **DARPA Microsystems Technology Office (MTO):** Focuses on developing advanced microelectronic technologies for military applications. MTO's work includes research and development, technical support, and standardization efforts in the field of microelectronics. Includes the ERI and the Next-Generation Manufacturing Program, for example.
5. **Defense Logistics Agency (DLA):** Through the Engineering and Technical Support Directorate (Land and Maritime-V), DLA maintains the microelectronics Qualified Manufacturers List (QML) and Qualified Product List (QPL). DLA also maintains and manages suppliers, supply chains, and stockpiling. The Sourcing and Qualifications Division manages microelectronics qualifications.
6. **Defense Microelectronics Activity (DMEA):** Designated as a Center for Industrial Technical Excellence (CITE) by Secretary of Defense Lloyd Austin in 2021, DMEA is an organization under the Assistant Secretary of Defense for Sustainment. It maintains a Trusted Access Program Office (TAPO) to facilitate access to Trusted Foundries and other key chip manufacturers. The Advanced Technology Support Program Office (ATSPO) is an "IDIQ" contract vehicle that allows DoD Programs to rapidly get access to proven advanced electronics needed for sustainment purposes.[35] DMEA also possesses its own capabilities to support needed obsolete technologies via their FlexFab in Sacramento and experiment with modern commercial technologies for legacy systems to mitigate DMSMS scenarios.
7. **Defense Microelectronics Cross-Functional Team (DMCFT):** Established by Deputy Secretary of Defense Kathleen Hicks in January of 2021 to "develop a DoD-wide [microelectronics] strategy that includes an implementation and transition plan for a sustainable U.S. ecosystem using the best commercial design, development, operation, sustainment, and modernization practices."[36]
8. **Defense Production Act (DPA) Title III Office:** Housed under the ASD for Industrial Base Policy, it has special authorities aimed at assuring and bolstering critically-needed domestic manufacturing capacity through direct procurements, loans, grants, or other commitments.
9. **Department of Commerce:** The chief cabinet agency responsible for awarding and implementing most of the $50 billion appropriated under the CHIPS and Science Act. Houses relevant organizations such as the National Institute of Standards and Technology and the CHIPS Industrial Advisory Committee.
10. **DoD(OUSD(A&S)):** In addition to leading the DMCFT, it addresses microelectronics through the Offices of the USDs for Acquisition and Sustainment, as well as through the office of the Assistant Secretary of Defense for Industrial Base Policy.
11. **DoD(OUSD(R&E)):** In addition to participation in the DMCFT, it operates microelectronics programs such as the Trusted and Assured Microelectronics portfolio of programs, the Rapid Assured Microelectronics Prototype (RAMP) program (and "RAMP-C" for facilitating commercial foundries' participation in the DoD ecosystem), and the State-of-the-Art Heterogeneous Integration Prototype (SHIP) Program.
12. **DoD Microelectronics Commons:** The DoD-specific component of CHIPS and Science Act funding, DoD(R&E) is managing this $2 billion effort focused on speeding up the "lab-to-fab" process for domestic chips of defense interest. It will seek to create public-private partnerships and bridge the microelectronics technological "Valley of Death."[37, 38]
13. **Joint Federated Assurance Center (JFAC)[39]:** JFAC is a federated organization under DoD(R&E) to assure security of DoD systems and components. It consists of multiple organizations carrying out hardware assurance (HwA) for systems like microelectronics as well as software assurance (SwA) and provides support to program offices such as DMEA.
14. **National Institute of Standards and Technology (NIST, DOC):** Semiconductors, alongside metrology, are a major focus area for NIST.[40] The agency sets standards, develops new metrology approaches, and collaborates with industry. See the fifth item in the next list – related to Sections 9902 and 9906 of the FY2021 National Defense Authorization Act – for more information about upcoming NIST-based agencies that were funded by the CHIPS and Science Act. Additionally, the Industrial Advisory Committee (IAC) reports to NIST. The recently formed IAC is an advisory committee consisting of leaders in industry, academia, and non-profits who collectively advise NIST on CHIPS-related research and development implementation.

33 Defense Advanced Research Projects Agency (DARPA), U.S. Department of Defense, "Electronics Resurgence Initiative 2.0," https://www.darpa.mil/work-with-us/electronics-resurgence-initiative

34 Defense Advanced Research Projects Agency (DARPA), U.S. Department of Defense, "Next-Generation Microelectronics Manufacturing Aims to Sustain R&D Ecosystem," July 20, 2023, https://www.darpa.mil/news-updates/2023-07-20

35 "IDIQ", also called a "Task Order," refers to a contract that provides the government with "Indefinite Delivery, Indefinite Quantity". It guarantees access to the product over a given period of time.

36 Department of Defense. "Microelectronics Vision," May 2022. https://media.defense.gov/2022/Jun/15/2003018021/-1/-1/0/DEPARTMENT-OF-DEFENSE-MICROELECTRONICS-VISION.PDF p. 3, 7

37 Ibid.

38 The "Valley of Death" problem in military acquisitions refers to the time gap between development of a new technology and the ability to provide it with full contract funding; this time gap can cause companies to either abandon a high-cost prototype, to modify it for commercial use rather than defense use, or to go out of business entirely.

39 For more information, see https://rt.cto.mil/stpp/syssec/jfac/.

40 For general information and reports, see https://www.nist.gov/semiconductors.

15. **Service Research Program Offices:** Agencies across the services such as the Army Development Command (DEVCOM, including the Army Research Lab (ARL)), the Office of Naval Research (ONR), and the Air Force Research Laboratory (AFRL) perform intramural and fund extramural research on microelectronics.[41]

Finally, both Congress and the executive branch have recently released several key high-level strategies and policies related to microelectronics research and industrial base issues. In reverse-chronological order, some of these include:

1. **Executive Order 14080[42]:** Promulgated in August of 2022, directs the implementation of the CHIPS and Science Act and establishes the CHIPS Implementation Steering Council.
2. **Draft National Strategy on Microelectronics Research (via Office of Science and Technology Policy, OSTP)[43]:** Released in September of 2022 for public comment, the strategy sets actionable goals for microelectronics R&D, workforce development and expansion, and transition of research to U.S. microelectronics industry growth.
3. **The CHIPS and Science Act of 2022[44]:** The law authorizes $280 billion over ten years, including over $50 billion in direct appropriations. The authorizations go towards R&D and commercialization, state-of-the-art and legacy semiconductor manufacturing, workforce development, and multiple technology centers.[45] Established the CHIPS for America Fund in the Department of Commerce, governed by the CHIPS for America Strategy released in September of 2022.[46]
4. **2022 DoD Microelectronics Vision[47, 48]:** The Microelectronics Vision – written by the DMCFT and released in May of 2022– directs DoD to:
   a. **Guarantee long-term microelectronics access:** (1) Onshore microelectronics capabilities and (2) eliminate sustainment issues.
   b. **Measurably secure microelectronics:** (3) Centralize DoD microelectronics knowledge and (4) Access secure and affordable microelectronics
   c. **Enable overmatch performance:** (5) Innovate and transition microelectronics ideas and (6) cultivate a right-sized workforce
5. **FY2021 National Defense Authorization Act, Title XCIX, "Creating Helpful Incentives to Produce Semiconductors (CHIPS) For America[49]:** These authorizations, passed in the FY2021 NDAA as the "CHIPS for America Act", were expanded and funded by the 2022 CHIPS and Science Act. Section 9902 authorizes DoD to create incentives to spur investment in facilities and equipment for chip fabrication and testing. Section 9906 authorizes the establishment of a National Semiconductor Technology Center (NSTC) to conduct R&D and prototyping activities, a National Advanced Packaging Manufacturing Program to focus on the packaging stage of manufacturing,[50] and three Manufacturing USA institutes.[51] All will be administered by NIST and received $11 billion in funding from the CHIPS and Science Act.
6. **Executive Order 14017:** Promulgated in February of 2021, directed all agencies to assess supply chains to "promote economic security [and] national security."[52] In-part, the initiative supported the work of the OSD DMCFT with respect to mitigating supply chain bottleneck and DMSMS scenarios.

ETI's 2022 Workshop: Topics and Findings

In 2022, ETI hosted an informal roundtable meeting to discuss ideas related to the transition of modern microelectronics into defense systems and to shape future ETI activities in this policy area. The workshop served as a motivation and foundation for this study. Participants included experts from ETI, defense industry, government research and acquisition personnel, Congress, and the commercial microelectronics industry. The group was convened to discuss and address several key microelectronics themes:

1. DoD has several programs aimed at improving – and assuring the Department's access to – state-of-the-art microelectronics, and its efforts are motivated by advances in the commercial sector. Despite meaningful enhancements for performance, cost-efficiency, security, and size/weight/power requirements, it is often easier for these SOTA devices to be adopted for commercial technologies than for defense systems.
2. Most of DoD's systems are reliant on legacy or state-of-the-practice microelectronics. While these are often sufficient at

41 For more information, see work done by: ONR's Electronics, Sensors, and Network Research Division, DEVCOM ARL's Army Research Office, and AFRL's Aerospace Components & Subsystems Technology Division.

42 U.S. Executive Office of the President, Executive Order 14080: Implementation of the CHIPS Act of 2022, August 25, 2022, https://www.federalregister.gov/documents/2022/08/30/2022-18840/implementation-of-the-chips-act-of-2022

43 The White House, "Draft National Strategy on Microelectronics Research," September 14, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/09/SML-DRAFT-Microlectronics-Strategy-For-Public-Comment.pdf

44 National Institute of Standards and Technology, U.S. Department of Commerce, "About CHIPS for America," October 5, 2023, https://www.chips.gov/

45 Justin Badlam, Stephen Clark, Suhrid Gajendragadkar, Adi Kumar, Sara Slayton O'Rourke, and Dale Swartz, "The Chips and Science Act: Here's What's in It," McKinsey & Company, October 4, 2022, https://www.mckinsey.com/industries/public-sector/our-insights/the-chips-and-science-act-heres-whats-in-it

46 National Institute of Standards and Technology, U.S. Department of Commerce. "A Strategy for the Chips for America Fund," September 28, 2022, https://www.nist.gov/chips/implementation-strategy

47 Department of Defense, "Microelectronics Vision," May 2022, https://media.defense.gov/2022/Jun/15/2003018021/-1/-1/0/DEPARTMENT-OF-DEFENSE-MICROELECTRONICS-VISION.PDF

48 Also see the 2018 DoD Digital Engineering Strategy, which will play a role in the DMCFT's work. https://ac.cto.mil/wp-content/uploads/2019/06/2018-Digital-Engineering-Strategy_Approved_PrintVersion.pdf

49 National Institute of Standards and Technology, U.S. Department of Commerce, "A Strategy for the CHIPS For America Fund," September 6, 2022 https://www.nist.gov/document/chips-america-strategy p.4

50 Ibid., p. 12.

51 Manufacturing USA, "About Us," https://www.manufacturingusa.com/about-us.

52 The White House, "Fact Sheet: Biden-Harris Administration Announces Supply Chain Disruptions Task Force to Address Short-Term Supply Chain Discontinuities," June 8, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/08/fact-sheet-biden-harris-administration-announces-supply-chain-disruptions-task-force-to-address-short-term-supply-chain-discontinuities/.

current threat levels, and we must secure access to mature microelectronics, they are not "future-proofed." Program offices have limited incentives to adopt modernized or SOTA microelectronics without clear top-down guidance, changes in requirements based on threat, or additional funding.

3. Operational capabilities could be improved, and program life cycle costs could be reduced, if DoD acquisition and sustainment policies and programs were tailored towards enabling the regular refresh of legacy systems with modernized systems.

Workshop participants discussed how the fast pace of technological change, combined with the actions of near-peer adversaries to develop, acquire, and adopt advanced technologies, indicates that the U.S. may lose some of its military technological superiority if innovative ways to incorporate and sustain advanced microelectronics in defense systems are not found. The participants reviewed ongoing efforts by the DoD, including the RAMP, RAMP-C, and SHIP programs. They identified that a key challenge for modernizing microelectronics is improving methods for securing commercial chips, including by quantifiable assurance, to support a sustainable business model that justifies the relatively low number of units manufactured for defense systems.

The participants discussed barriers to the adoption of advanced microelectronics into defense systems. These include (1) the lack of requirements defined for keeping pace with current technology and upgradability needs, (2) the lack of funding, (3) the perception that this type of technology insertion entails cost and technical and schedule risk, (4) difficulty in communicating the value of the use of modern microelectronics to relevant decision makers, (5) lengthy and costly testing and qualification processes, and (6) the lack of control of technical data and system interfaces along with the lack of open systems architecture approaches which make it more difficult to sustain and upgrade microelectronics.

The workshop also identified some best practices that have led to successful adoption of advanced technologies in defense systems and programs in the past. One of the strategies discussed was increasing the use of open systems architectures. Participants praised its use by the submarine community via the Advanced Rapid Commercial-Off-The-Shelf Insertion (ARCI) program. They noted that this approach works best when the community is small and technically competent and can closely partner with the associated operational community to control requirements effectively. Another successful policy mentioned was the use of advanced modeling and simulation techniques (e.g., digital twinning and advanced digital engineering) which can speed up the testing and qualification processes and address some of the risk aversion of programs and operators.[53] The group also discussed the value of special programs that identify and incorporate mature commercial technologies to reduce life cycle costs, such as the 1990s Commercial Operational Support & Savings Initiative (COSSI). This approach works when the commercial microelectronics industry responds to financial incentives and when programs and services are willing to invest funding upfront to reduce life cycle costs.

Finally, based on expressed interest from various stakeholders in the policy community, participants recommended that ETI conduct further research. This report collects best practices and recommendations on how policymakers can incentivize program offices to upgrade their microelectronics to SOTP components, streamline the qualification process of SOTA microelectronics, upgrade legacy systems to modern semiconductors to reduce reliance on "bulk buys" of legacy chips, and minimize the use of requirements that force a system to use customized, non-COTS chips. This report also incorporates some of the discussions and findings which came out of the workshop. The Workshop Summary can be found in Appendix A.

Findings

In addition to the 2022 workshop's findings and recommendations, ETI researched government agencies working on microelectronics, the commercial microelectronics industry, the defense industrial base, and their relationships with each other. ETI analyzed existing government microelectronics usage practices in the areas of defense acquisition, S&T, innovation, and industrial policy and compared them to the methods by which non-defense industries – such as automakers, aviation manufacturers, and critical infrastructure providers – interact with the commercial microelectronics industry.

Next, ETI conducted detailed background interviews. These 18 interviewees included technical microelectronics experts, defense acquisition professionals, former DoD and Service officials, Congressional staff, and companies across the defense industrial base. Alongside ETI's research and policy analysis, these interviewees' responses, experiences, and observations informed the bulk of the Findings and Recommendations sections of this report. ETI categorized its findings into four sets of challenges: Organizational, Technical, Acquisitions & Requirements, and Budgeting.

Organizational Challenges

- **The Department of Defense lacks an organization with sufficient authority, resources, and expertise to assist Program Offices with acquiring, sustaining, and modernizing their microelectronics.** Despite important work conducted across DoD – from DARPA to DLA to DMEA – there is no centralized organizational body assisting and facilitating a sustained push towards microelectronics modernization by analyzing threat information relative to microelectronics' capabilities, providing technical assistance on microelectronics capabilities and industrial base issues for programs, and funding to support program adoption of more modern microelectronics. There is no central repository of knowledge and staffing to assist programs with updating their technical microelectronics requirements

53 "Digital twins" are virtual representations of physical objects; these replicas can simulate the nature of a final product for manufacturing across the design, production, and maintenance of the object. Digital twinning allows engineers to optimize the design of these devices and to predict how they will function in different environments and under various conditions. They can also be used to simulate the manufacturing process for microelectronic devices, which can help manufacturers identify potential issues and optimize the production process. Additionally, digital twins can be used to monitor the performance of microelectronic devices in the field and to predict when maintenance or repairs may be needed.

or with the requalification process – while technical experts are dispersed across DoD, they are not regularly available to program offices to fund studies or provide detailed and enduring assistance. Moreover, DoD lacks a formal method devised and implemented by any organization to assess the microelectronics needs of the military as a whole.

Technical Challenges

- **In many cases, DoD lacks specific information on the cost, schedule, security, and performance benefits of microelectronics modernization on many of its systems.** In fact, both acquisition professionals and contractors lack visibility into the microelectronics that are being delivered at the subcontractor level. For existing systems, this is partially due to the government's lack of access to intellectual property and fully reworkable technical data packages. For new systems, this is because lifecycle cost, schedule, and performance needs are often not fully understood or considered during development and procurement, leaving problems later for sustainment. These problems are compounded by the dearth of program-specific studies with the level of technical detail required to make well-informed decisions on microelectronics acquisition topics such as modular systems architecture, subsystem design, and the qualification process.
- **Today, in many cases, military systems do not use state-of-the-art microelectronics, and in virtually all cases do not currently need to in order to meet their requirements.** These use cases are often limited to military data centers, machine learning, and artificial intelligence.[54] The small quantities of SOTA chips that the government uses also make them prohibitively expensive. Additionally, improvements in power efficiency and resiliency in rugged environments are rarely sufficient to justify their cost.
- **Going forward, custom chips may often be necessary to meet future programs' specific high-performance criteria, security requirements, and weight & power needs.** This is especially true when military performance needs outstrip what a commercial semiconductor can provide. Commercial systems are beginning to customize system architecture and software in order to economically optimize performance.[55, 56] DoD and the defense industrial base may eventually use these commercial processes, but have not yet. At the same time, defense programs lack access to the capability to securely obtain leading-edge custom chips (whether that be via Trusted Foundries, MQA processes, or other approaches).
- **There is no consistent policy for measuring and managing technical debt in microelectronics, and few incentives exist to encourage technical debt reduction.[57]** Technical debt tends to accrue during the development phase, driven by time and budget constraints, and by incomplete government access to intellectual property and technical data packages when these details are not negotiated for during acquisition. This technical debt can lead to time-consuming and expensive activities for sustainment and modernization teams further on in the program life cycle. Substantial software re-writes associated with upgrading older parts can also create higher costs and program delays.
- **Cutting-edge technical practices such as qualification-by-similarity,[58] virtual modeling,[59] and digital twins have not been fully evaluated for potential adoption as standards by DoD or the DIB.** This has prevented more rapid re-qualification processes and has prevented engineers from modeling how systems run with updated microelectronics. Meanwhile, advanced digital twinning approaches are used by the commercial world with increasing efficacy to rapidly qualify and insert new technologies into systems. Often, the government does not possess the appropriate technical data rights to operate digital twins.
- **In many cases, DIB companies are still working to incorporate new commercial modalities for designing and integrating chips that will change on a more rapid timetable.** This can lead to cost overruns. Additionally, prime contractors rarely have visibility into their microelectronics supply chains. The further down the supply chain a subsystem or part, the less likely the prime contractor is to have visibility into the design history, exact performance, and technical data used to produce it.
- **Advanced methods for enhancing and verifying security of microelectronics, such as zero-trust architectures (e.g., quantifiable assurance) and split manufacturing, have not been fully evaluated across the whole supply chain for efficacy and security, and therefore have yet to be implemented on DOD acquisition programs or procurement activities.** There are concerns regarding how these new modalities can be applied at all levels of the microelectronics fabrication process, such as evaluation both in the foundries and during final packaging.

54 In the case of AI, the military is much more likely to operationalize smaller neural networks than it is to create capabilities with high-computation capabilities. This is primarily because limited training data sets based on operational and battlefield conditions make it difficult to train larger AI models.

55 David Rotman, MIT Technology Review, "We're Not Prepared for the End of Moore's Law," April 21, 2021, https://www.technologyreview.com/2020/02/24/905789/were-not-prepared-for-the-end-of-moores-law/

56 For example, Apple's custom chip designs for its products help optimize performance and power needs for the iPhone and Mac. See: https://www.nytimes.com/2020/06/22/technology/apple-macs-intel-chips.html

57 Technical debt is commonly defined as the future costs of sustainment and modernization that result from initially prioritizing speed, cost, or convenience over careful consideration of lifecycle consequences. The term is commonly used in software development, but is also applicable for microelectronics.

58 "Qualification-by-similarity" refers to an approach for qualifying microelectronic parts for use in a larger system by relying on its similarity to an already-qualified part rather than by undertaking a time- and cost-intensive process to re-test the system against all of the qualification metrics. The practice attempts to qualify risk based on the predicted fail rate of an existing, similar system, rather than outright experimentation on the new part.

59 "Virtual modeling" refers to the simulation of some or all parts of a prototypical microelectronic part for the purposes of predicting functionality and understanding the resiliency of the part under certain environmental conditions.

- **While the Trusted Foundry program seeks to assure that access to microelectronics for critical systems are secure, there are few specific security standards for many other microelectronics components including commercial microelectronics used within defense systems.** Section 224 of the FY2020 NDAA was designed to address this problem.[60] It required DoD to establish trusted supply chain and operational security standards by January 1, 2021, and ensure that new parts in DoD systems followed these standards by January 1, 2023.[61] However, per a 2022 DoD Office of the Inspector General Report, the DoD was said to be behind schedule on implementing the policy changes required by Section 224 for the FY2020 NDAA.[62] At the time of writing, implementation of Section 224 has not occurred.
- **The scale of the security and reliability threats through the use of commercial microelectronics in defense systems has not been sufficiently studied to inform policies.** Program offices make use of commercial microelectronics or avoid their use based on more simplistic technical judgments, cost factors, or expediency.

Acquisition and Requirements Challenges

- **DoD's buying power is fractured across its programs. Additionally, agencies across the federal government do not sufficiently coordinate their microelectronics investments on defense and non-defense critical infrastructure.** This includes military systems, commercial satellites, the power grid, commercial aviation, and other elements of national infrastructure. This is the case even while many systems' equipment uses identical parts or the same suppliers. These entities negotiate separately and do not follow the same standards and regulations for microelectronics, and there is no national policy exactly defining microelectronics policies for critical infrastructure. This lack of coordinated buying activity often results in confusion for vendors and limits DoD's ability to reduce costs through bulk purchases.
- **DoD has not leveraged its overall negotiating power, and there is room for DoD to create more innovation and competition in the microelectronics ecosystem by negotiating with prime contractors for upgradability, modularity, technical data rights, and backwards compatibility of hardware and software during the competitive phase of contracting.** Reduced negotiating power also precludes DoD programs from offering larger, or more comprehensive incentives to companies. Additionally, program executive officers (PEOs) and program managers (PMs) – as well as the Services and Agencies – are siloed from each other, and even further separated from the rest of the federal government, resulting in very limited sharing of best practices related to microelectronics acquisition.
- **DoD does not have a standard policy that encourages program offices to identify a commercial solution that would fulfill all operational needs on a faster schedule.** Stringent technical requirements often implicitly push programs towards customized designs and parts as a standard practice. These currently take longer to develop and have lower yields, tending to lead to increased lifecycle costs and to the use of microelectronics that are not on-par with the state-of-the-practice.
- **Some commercial businesses struggle to remain viable in the defense sector**, deterring microelectronic innovation in the defense ecosystem. This is due to a variety of challenges, including complex acquisition and other regulatory rules as well as the pace of the government funding process. Adhering to some government regulations and practices can drive companies away from commercial best practices. Additionally, the small unit volumes of chips required by DoD customers, combined with acquisition practices, make DoD a less favorable market for non-traditional defense companies.
- **The current requirements process is not well-suited to allow programs to continuously upgrade system microelectronics.** Program offices often do not require upgradability or modularity, limiting the ability to incorporate upgrades at appropriate stages of the program lifecycle. Additionally, acquisition personnel have few incentives to build in more capability than necessary to meet the exact requirement, regardless of changing threat or technology. Program offices are often constrained to a specific design and technical requirement set before they publish their first request-for-information (RFI).
- **The costs associated with attempting to stockpile legacy microelectronics through "end-of-life" purchases to support legacy defense systems can be exorbitant when compared to a model of continuously upgrading embedded microelectronics.** This is because the government customer is still purchasing a small number of chips overall even when buying in bulk. On the other hand, programs and contractors can benefit from buying more up-to-date commercial microelectronics, which serve the wider economy and therefore rapidly become less expensive. In most cases, state-of-the-practice chips that are not quite the "state-of-the-art" still provide a significant increase in computational capability for defense systems over bulk-ordered legacy chips.

60 U.S. Code, 10 U.S.C. subtitle A, part V, subpart G, front matter: "Subpart G-Other Special Categories Of Contracting," https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title10-subtitleA-part5-subpartG-front&num=0&edition=prelim. Also found at: U.S. Congress, "Section 224 of the National Defense Authorization Act of FY2020," Public Law 116-92, div. A, title II, § 224.

61 Ibid.

62 Office of the Inspector General, U.S. Department of Defense, "Evaluation of the Department of Defense's Transition From a Trusted Foundry Model to a Quantifiable Assurance Method for Procuring Custom Microelectronics," Report DODIG-2022-084, May 2022, https://media.defense.gov/2022/May/04/2002989631/-1/-1/1/DODIG-2022-084_REDACTED.PDF, p. 27.

- **Future microelectronics sustainment and modernization needs are not properly considered during the acquisition processes at the beginning of the program life cycle, even though sustainment comprises approximately 70% of the program lifecycle.**[63] These decisions are made before Milestone B, and often do not include full technical data packages that would be crucial over the decades of sustainment to make changes as needed.[64]
- **Rules surrounding ITAR (International Traffic in Arms Regulations) and other export control regimes – foreign or domestic – are constraining the defense industry, the commercial sector, and the government's ability to promote innovation in microelectronics.** Companies investing resources in state-of-the-art microelectronics can risk losing the ability to export the product, limiting the ability to leverage global markets. For example, it is often not clearly delineated what attributes of a system would require the product to be either modified before export or restricted from export.
- **There are few consistent guidelines describing what technical data should be obtained from the DIB for an acquisition program.** These include criteria for what constitutes a complete technical data package from industry and a clear definition of a microelectronics digital twin.
- **DoD struggles to retain technical talent required to conduct technical oversight of its vendors such as prime contractors, federally funded research and development centers (FFRDCs), university-affiliated research centers (UARCs), and systems engineering & technical assistance (SETA) contractors. This is because DoD is in competition for workforce with the DIB and commercial sector in the domains of microelectronics, systems engineering, and acquisition.** Over time, there has been an increase in the use of contractors rather than government employees for some of these activities. The government technical workforce has an important role in developing system requirements which balance operational needs, technical realities, industrial capacity, cost, and schedule. A strong technical workforce will be better equipped to design and negotiate with vendors for continuously upgradable systems. In particular, DoD is sometimes unable to independently technically verify what it receives from its vendors. The lack of technical talent also reduces DoD's awareness and ability to track the global commercial microelectronics market and industrial trends. Additionally, some DIB companies also struggle to maintain and recruit microelectronics talent, which may lead to challenges in the design and integration of advanced microelectronics into complex defense systems.
- **Program offices lack training in using commercial business best practices for microelectronics procurement and sustainment.** While other cabinet agencies such as the Department of Commerce are creating new relationships with the commercial microelectronics sector, the Pentagon has undertaken more limited efforts along these lines.

Budgeting Challenges

- **The Pentagon requirements, programming, and resourcing processes, as well as the Congressional appropriations process, are too rigid to allow for procurement of mission-driven capabilities that stay closer to the state-of-the-practice.** Due to long planning and programming timelines, there are often few opportunities for upgrading subsystems. These systems can be so obsolete that there are no more stocks of the mature microelectronic parts in the system. This leads the program offices and subcontractors down an onerous path of designing and re-qualifying actively-manufactured chips for the dated system. The current resourcing process also struggles to give flexibility to decision makers in determining what programs to fund, for what purposes, and at what scale in a way that leads to optimal national security outcomes. For instance, microelectronic systems are similar to software as both have the opportunity and need for continuous upgrades.
- **The siloing of funds across various colors of money poses a barrier to modernization.**[65] Inconsistent guidance on the use of RDT&E, Procurement, and Operations & Maintenance (O&M) funding disrupts microelectronics modernization activities depending on the use case for upgrading; it is often unclear whether microelectronics upgrades qualify as sustainment, a new procurement, or a development activity. In some cases, DoD must seek reprogramming to achieve modernization goals, a process that is currently long and requires Congressional approval.
- **Microelectronics modernization is often difficult to fund through the services' sustainment budgets.** Microelectronics upgrades are not always considered maintenance, but as an addition of new capabilities. If a program office typically is operating with Operations & Maintenance funding, it is onerous to seek the RDT&E or procurement funding required for upgrades of microelectronics. The resulting delay in system upgrades can lead to higher lifecycle costs as well as degraded performance relative to emerging threats and commercial capabilities.

63 U.S. Government Accountability Office (GAO), "Weapon System Sustainment: The Army and Air Force Conducted Reviews and the Army Identified Operating and Support Cost Growth," GAO-23-106341, March 30, 2023, https://www.gao.gov/assets/gao-23-106341.pdf

64 Milestone B is the decision point in the acquisition process during which a program in a stage of technology development moves to the manufacturing process. The most convenient time to add requirements for characteristics like modularity would be during the technology design and development phases, though these needs are rarely communicated to the program office or contractor before this point; adding these characteristics later often proves to be a costly and time-consuming endeavor.

65 "Colors of money" refer to the various Appropriations categories used by Congress to group funding by the type of activities performed. These primary categories are: 1) Military Personnel, 2) Operations & Maintenance, 3) Procurement, 4) Research, Development, Test, and Evaluation; and 5) Military Construction.

Recommendations

This section provides a series of actionable recommendations to address the challenges facing the Defense Department in modernized microelectronic semiconductor chips for defense capabilities. These recommendations aim to ensure that the Department has access to the specialized, high-performance chips it needs to maintain its strategic, tactical, and operational advantages. The proposed recommendations address key issues such as DoD's challenges with custom chips, revising internal DoD processes, and improving microelectronics acquisition and sustainment procedures. Traditionally, DoD's efforts have focused on science, technology, and engineering techniques to develop microelectronics for defense systems. Acknowledging that the majority of costs occur during the sustainment phase, many of these recommendations focus on activities to upgrade microelectronics at the later end of the system lifecycle. By implementing these recommendations, the Defense Department can continue to maintain its technological edge in the face of increasingly sophisticated threats. Recommendations were generated throughout both the research and interview processes.

Top-Level Recommendations:

1. Encourage continuous microelectronics upgrades in defense systems.
2. Improve defense microelectronics security standards.
3. Use pilot programs to explore innovative practices for microelectronics acquisition.
4. Designate a centralized DoD microelectronics support activity.
5. Implement approaches to better integrate commercial state-of-the-practice microelectronics into defense systems.

1. The Congress, the Office of the Undersecretary of Defense for Acquisition and Sustainment ("OUSD(A&S)") and the military departments should make a series of changes to acquisition, requirements, and financial management policies and practices to encourage continuous microelectronics upgrades. In support of this:

- **DoD's acquisition strategies and instructions should specifically include Technology Refresh Events.** Program office strategies and timelines should include these events to provide a regular touch point for active market research and technical analysis. This may create opportunities to adopt available technologies into systems, consistent with DoD Instruction 5000.01 Section 1(f).[66] The activity described in Recommendation #4, below, should maintain a repository of microelectronics refresh activities across the Services and Defense Agencies for joint access to emerging best practices. DoD should phase this requirement into program timelines, depending on the maturity of the program and its microelectronics needs. For example, in DoDI 5000.85: Under 3C.3(a)(1)(b), Program Managers' acquisition strategies should go beyond identifying capability requirements that may evolve during the program lifecycle. Instead, Program Managers should be required to build regular reviews of all program capabilities' technology states into their program lifecycles to set aside time to proactively identify opportunities for microelectronics technology refresh. The reviews should examine current and programmed technologies for a system relative to: (1) commercial practice, (2) capabilities required to meet emerging threats, (3) capabilities required to meet stated requirements, (4) industrial base availability, (5) life cycle cost, and (6) potential to design for future upgrades when modernizing.
- **DOD should request, and Congress should appropriate, funding to the Services for Program Managers to conduct studies that re-assess threats, emerging technologies, and the state of commercial microelectronics relevant to the program's specific requirements.** These studies should be technical and independent and used to inform (a) the state of program-level microelectronics with respect to threat, and (b) quantify what improvements are necessary at the program level to keep reasonable pace with the state-of-the-practice. The new centralized microelectronics activity described in Recommendation #4, below, should communicate with program offices to support assessments of the cost and schedule impacts of adopting qualification-by-similarity protocols in conjunction with DLA.
- **Establish microelectronics upgradability as a Sustainment Key System Attribute (KSA).** This would create incentives for programs to develop technical requirements and provide financial incentives for system designs and architecture to support continuous upgrades of embedded microelectronics.
- **Budgeting and appropriation practices, and financial management regulations, should allow the use of Operations & Maintenance ("O&M") funds by programs, activities, Services, and agencies for the continuous upgrade of microelectronics.** Like software, microelectronics hardware is developed, deployed, and maintained on both an iterative and simultaneous basis. Using this type of funding ensures that programs can perform more seamless and iterative development, prototyping, maintenance, and upgrade activities during Technology Refresh Events. This can be based on lessons learned from the ongoing Research, Development, Testing, and Evaluation Budget Activity 8 software

66 U.S. Department of Defense, "The Defense Acquisition System," DoD Directive 5000.01, July 28, 2022, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/500001p.pdf

pilot.[67] Additionally, DoD programmers should make it a priority to provide sustainment funding in the out-years of the FYDP for microelectronics upgrades. This depends on anticipating costs arising from Technology Refresh Events over the program's lifetime based on analyses of costs and data from contractors.

- **To upgrade microelectronics in existing systems, DoD should request, and Congress should allocate, funds to the Services and/or the Defense Logistics Agency to procure a larger quantity of common sub-systems which use advanced microelectronics on behalf of multiple program offices** using Operations and Maintenance ("O&M") funds, Working Capital funds,[68] or RDT&E Budget Activity 7 funds. This enables greater buying power for program offices and can create a more consistent demand signal for industry while providing performance upgrades to a broad set of programs. When appropriate, this approach should be integrated into the Modular Open-Systems Approach (MOSA) acquisition strategy as mandated by Congress.

2. Policymakers should implement a number of changes to the microelectronics security and standards regimes. These actions will give DoD access to more secure microelectronics, supporting efforts to create strong and reliable supply chains. A number of these recommendations may require Congressional mandates and continuous collaboration with industry and appropriate international partners to increase effectiveness and compliance:

- **DoD should complete the implementation of Section 224 of the FY2020 NDAA.** Development of more common standards between commercial and defense systems will support DoD's ability to use commercial microelectronics when appropriate. The lack of DoD progress in implementing Section 224 has created challenges for industry and government has permitted systems to continue using less secure microelectronics.
- **DoD should develop policies and guidance, with Congressional direction if needed, that encourage contractors to proactively raise their microelectronics security standards, including by addressing counterfeiting and cloning threats.** Some possible incentives could be allowing companies that demonstrate an ability to deliver state-of-the-practice equivalent microelectronics in a cost-effective manner to:
  - Obtain preferential access (and potentially cost and source selection preferences) for participation in other defense modernization programs
  - Qualify for additional funding to further improve security
  - Be designated as approved secure microelectronics commercial strategic suppliers.
- **The Office of the Secretary of Defense (OSD) should stand up industry advisory groups that share microelectronics-related concerns with respect to ITAR and other controlled commodity lists with DoD and the Department of Commerce.** The government should use this forum to share its concerns about export controls and engage in a dialogue with industry to develop reform ideas and solutions. Streamlined ITAR policies should clearly describe the investment behaviors and information sharing processes that are permitted to allow for more confident business investment that follows all anticipated government regulations.
- **DoD and the Department of Commerce should conduct studies on best practices to improve microelectronics security across critical industries in a manner that is commercially viable.** These may include zero-trust and quantifiable assurance approaches, and the use of secure strategic suppliers. The studies should include an assessment of the relative lifecycle cost and performance benefits of security activities such as Trusted Foundries, MQA, split manufacturing, qualification-by-similarity, and digital twinning. These studies should be used to inform funding and rulemaking processes, and should be performed in close collaboration with industry, academia, and appropriate international partners.

3. DoD should request, and Congress should fund, pilots to operate through specific programs, selected in consultation with OUSD(R&E) and OUSD(A&S), which include:

- **A pilot to omit technical requirements for microelectronics, instead specifying a list of operational capabilities within a new acquisition program.** Within this pilot, Program Managers and performers should be given incentives to choose the most appropriate legacy or state-of-the-practice commercial part, if possible, that enables the desired system capability.
- **A pilot which authorizes the re-evaluation of requirements for selected older systems already in sustainment.** The evaluation should be informed by an understanding of current available technology and emerging threats. If the program office(s) assesses that the system or any subsystems would benefit from upgraded microelectronics, the Program Manager should be able to rapidly request and receive funds for these purposes.
- **A pooled funding pilot which allows several programs' contractors to jointly identify and purchase a shared legacy or commercial microelectronic component for multiple systems.** This could be executed via pooled purchases by DoD, which then issues the microelectronics as government-furnished equipment, with a goal of bolstering purchasing power by increasing the number of units ordered while reducing logistics burdens and creating a clearer market signal to industry.
- **An acquisition pilot which implements microelectronics upgradability as a well-defined new Sustainment Key Performance Parameter for a set of program offices developing new capabilities.** This recommendation is distinct from Recommendation #1c on a microelectronics upgradability KSA for all programs. The KPP pilot would measure and assess any appropriate operational and cost improvements derived from requiring contractors to be able to continuously upgrade the hardware, software, and firmware within a system's microelectronics architecture.

67 The RDT&E BA 8 pilot emerged from a 2019 Defense Innovation Board report on software acquisitions to recognize the continuous nature of software, as well as the fact that software cannot easily be distinguished between research, development, procurement, and sustainment.

68 Implementing this continuous procurement into Working Capital Funds would involve an authorization and requirements process.

- **A pilot that evaluates the reliability of commercial microelectronics components for operation in DoD environments.** This can include leveraging commercial automotive technologies and evaluating the feasibility of applying commercial safety standards for DoD programs. This should also include analysis of the ability to operate in required operational temperature ranges using both modeling and physical testing.
- **A pilot which authorizes a simulation of the performance benefits of a complete upgrade of a selected weapons system or platform with modern microelectronics.** This simulation exercise should be used to inform policies and practices relating to microelectronics upgrades for systems across DoD's inventory.

4. DoD should designate, and request funding for, a centralized microelectronics support activity, to provide expertise to program offices at all stages of the acquisition lifecycle – from research to sustainment. This activity can be established within an existing organization, or through the merger of multiple organizations. The activity can provide access to technical expertise, provide a repository for technical data and defense program usage of microelectronics, support market research and industry interactions, and provide contracting support. The activity could help provide networking and coordination between current Service and Defense Agency microelectronics activities and should have access to independent expertise – possibly through the use of UARCs or FFRDCs. Alternatively, the activity and the specific duties described below could be stood up as part of an expansion of an existing agency such as DMEA. The activity should be empowered to accomplish the following objectives:

- **Access private sector microelectronics experts** – Program Offices should use private sector experts to provide technical knowledge, re-evaluate technical microelectronics performance requirements with respect to evolving threat and capability needs, and evaluate trends in SOTP/SOTA innovation. These experts should also act as a repository of knowledge (and liaison with DLA, DMEA, and Service sustainment activities) for cleared parts and practices to program offices and military planners. This can be done using new or established personnel exchange programs and authorities.
- **Investigate incentives for the use of secure microelectronics** in both COTS and custom use cases. This would include incentives to contractors who integrate assured parts in the form of contract incentive fees, as well as tiered incentives to foundries and chip designers whose state-of-the-art commercial products can meet military-grade performance standards. To assist with this, the agency should work to streamline the re-qualification process for commercial chips that are already qualified for programs with similar technical requirements. This would include the establishment of a repository of information for qualified commercial devices.
- **Fund and support regular studies on best practices for microelectronics acquisition for DoD.** This might include studying the risks, challenges, benefits, costs, schedule, security, and performance associated with maintaining a system's legacy chips compared with a model of continuous upgrade.
- **Investigate innovative practices related to the use of digital engineering and other methodologies to streamline qualification processes, and re-qualification of parts for new use cases**, by prioritizing intramural and extramural investments in virtual modeling and simulation, digital twin programs, and other technologies. This should include active efforts in coordination with semiconductor foundries to encourage more virtual modeling of commercial products to predict the fail rates and security of commercial parts under DoD-requirements and typical use conditions (e.g., temperature, vibration, etc.).

5. OUSD(A&S) and OUSD(R&E) should implement a variety of new and revised policies and practices that support efforts to acquire and field more capable microelectronics. These policies may require Congressional mandates. Recommended policies include:

- **OUSD(A&S) and the Services should disseminate best practices used by program offices to modify their product support strategies, allowing for changes in sustainment strategies for programs during Technology Refresh Events.** These should be done in collaboration with threat assessments, assessment of available microelectronics capabilities, the organization described in Recommendation #1, and the involved contractor(s). For new programs, expectations of upgradability should be factored into contract negotiations with both developers and sustainers. These upgradability expectations, as part of upgradability's integration as a KSA, should be a part of the planning for Total Life Cycle Costs and Life Cycle Sustainment Plans. For existing programs, Service and OSD leadership should assess the costs and benefits of incurring the high price of early contract termination for the purposes of supporting microelectronics upgrades.
- **Update OUSD(A&S) policy guidance on the length of sustainment contracts to enable more recompetes** to encourage continuous comparative evaluation of technologies developed through industry-driven Independent Research & Development (IRAD) or government science and technology efforts, based on program-specific warfighting requirements. Re-competed contracts should improve capability performance and be driven, in part, by a technology refresh in microelectronics. OUSD(A&S) should develop a set of offsetting incentives to companies, such as increasing revenue at the initial procurement, to ensure that a business case remains for industry to participate in programs.
- **OUSD(A&S) and OUSD(R&E) should develop a policy process to assess microelectronics' end-of-life more accurately for a program and require program office justifications for system life extensions.** A comparative cost, schedule, and performance assessment of legacy versus potential replacement microelectronics for a defense system can be informed by market research, awareness of DoD technology development programs, and modeling & simulation of systems, amongst other methods.

- **OUSD(A&S) should expand protocols for acquiring, and negotiating for, microelectronics technical data packages during the competitive phase of contracting.** This includes defining the precise microelectronics data required in a technical data package that would be provided to the military customer. This effort can leverage DoD IP Cadre for support and expertise.[69]
- **To identify technical debt, OUSD(A&S) should review programs which have undergone extended periods of time without a microelectronics upgrade.** OUSD(A&S) should set policy requiring acquisition executives to support technical reviews of programs periodically. The results of these technical reviews should drive program restructuring or upgrades during technology refresh events. Additionally, program failure should be redefined to include capability stagnation relative to the state-of-the-practice to create incentives for upgrades, rather than endorsing compliance with out-of-date requirements that have not kept pace with threat or technological capabilities. The organization described in Recommendation #1 should study the impact of microelectronics-related technical debt on system performance and costs, especially relative to possible system performance using microelectronics at or near the state-of-the-practice. The additional costs of maintaining systems with significant microelectronics technical debt should also be understood.
- **Implement authorities with practices similar to the Foreign Comparative Testing (FCT) Program[70] and the Commercial Operations and Support Savings Initiative (COSSI).**[71] An authority similar to the FCT Program would allow DoD to re-source similar components and services during recompeted sustainment contracts based on the best-in-class capability for the warfighter on the basis of cost of performance. An activity similar to COSSI would establish the baseline operations and support costs of a military system with its current components and could enable a program office to apply to procure more modern microelectronics if they would reduce lifecycle costs compared to the baseline or improve performance at the same baseline cost.
- **Update the DoD Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs**[72] to endorse and mandate appropriate use of practices such as digital engineering and qualification-by-similarity. This would involve appropriate modifications to Chapter 2, Managing Risk by Acquisition Phase to integrate these practices as "Suggested Activities to Reduce Risk" across each phase of acquisition. Recurring digital engineering activities could also be implemented into Opportunity Management processes described in Chapter 4.73
- **OUSD(A&S) should re-state in policy, and implement training, to promote compliance with 10 U.S.C. 3453, the requirement to purchase commercial microelectronics when possible and appropriate.**[74] To reduce violations of this statutory requirement, DoD leadership and Congress should establish penalties for programs who do not follow the requirement. These commercial microelectronics should still meet security standards established under the requirements of Section 224 of the FY2020 NDAA and be procured along with appropriate technical data and IP rights to support cost-effective long-term sustainment of systems. When seeking a custom microelectronics part, Program Managers should be required to solicit commercial-off-the-shelf parts before seeking approval (from the PEO or Service Acquisition Executive (SAE) level) for development and acquisition of a custom part. With assistance from the organization described in Recommendation #4, Program Managers should assess cost, schedule, performance, reliability, and technical debt implications of choosing a custom versus commercial part.
- **OUSD(A&S) should add training and education for the acquisition workforce on microelectronics topics to increase technical fluency.** Acquisition training should include knowledge of the technical and strategic reasons for microelectronics modernization as well as the critical concerns for maintenance, assurance, sustainment, and modernization of microelectronics hardware and software. Program Managers should be exposed to interagency conversations that include industry and international perspectives on microelectronics technology and the global microelectronics market. Acquisition teams should include personnel with expertise at a variety of stages of program lifecycles to better understand the breadth of microelectronics-related acquisition challenges. The training should include information exchanges with the commercial and defense sectors. This can be done in conjunction with universities, think tanks, the Defense Acquisition University (DAU), and industry associations.

69 For more information on the DoD IP Cadre, visit their website: https://www.acq.osd.mil/asda/ae/ada/ip-cadre.html

70 The FCT program allows DoD to acquire foreign-developed technology with a high Technology Readiness Level (TRL) to rapidly satisfy defense requirements through side-by-side testing compared to the current capability, rather than undertaking a full development process.

71 The Commercial Operations and Support Savings Initiative (COSSI) was designed to place commercial products into existing military systems with a goal of reducing O&S costs. The COSSI program establishes baseline O&S costs for a system, then allows program offices to replace existing components with commercial parts if the purchase would reduce total lifecycle costs.

72 Office of the Deputy Assistant Secretary of Defense for Systems Engineering, U.S. Department of Defense, "Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs," January 2017, https://acqnotes.com/wp-content/uploads/2017/07/DoD-Risk-Issue-and-Opportunity-Management-Guide-Jan-2017.pdf

73 For more information on employing Digital Engineering to accelerate modernization, see NDIA ETI's report on the topic: James A. Faist, NDIA Emerging Technologies Institute, "Digital Engineering: Recommendations for the U.S. Department of Defense," November 2021, https://www.emergingtechnologiesinstitute.org/-/media/ndia-eti/event-documents/3r04---data-sharing/eti-de_report_2021-v2.pdf

74 10 U.S.C. 3453 requires a preference for commercial products wherever possible.

Conclusion

The Department of Defense depends on microelectronics for nearly all of its systems, whether they are used on the battlefield or in the back office. DoD struggles with the variety of microelectronics it needs to support its missions, which range from unique, highly specialized and cutting-edge devices down to globally and commercially available commodity circuits. It also struggles with challenges due to its own business practices, cultural obstacles, and policy and regulatory constraints which often serve to make it difficult to keep defense systems updated with appropriately modern microelectronics. Compounding these issues is the increasingly rapid pace of technological change in the microelectronics industry, the growing number of threats that can exploit security flaws in microelectronics systems, and the increasingly global nature of the entire microelectronics supply chain.

DoD and the government as a whole have put into place and are continuously refining a set of organizational structures, policy and regulatory activities, and funding initiatives to try to position themselves as better customers for microelectronics and regulators of the industry. This report – through its recommendations for Congress, DOD, and industry, based on interviews with government and industry experts and other research – seeks to meaningfully improve microelectronics modernization processes by enabling more continuous upgrades of semiconductors and increasing the options available to DoD program offices.

Many of these recommendations can also enable program offices to be better prepared to leverage both commercial and defense unique chips, and both state-of-the-art and state-of-the-practice chips, as appropriate for differing defense customers' needs. NDIA ETI hopes that this report serves to enhance dialogue between industry, government, and academia on the key technical and policy issues that need to be addressed to ensure that national security systems have the modern microelectronics they need.

Questions for Further Research:

Further research on a number of issues would contribute significantly to the understanding of the challenges of defense microelectronics modernization:

- Is the use of COTS or the use of ASICs more likely lead to end-of-life buys?
- Does the use of COTS or the use of ASICs represent a bigger security threat?
- Does the use of foreign COTS versus domestically-produced COTS represent a higher security threat?
- Are quantifiable assurance methodologies capable of providing information on both security and reliability of microelectronics? Can this information be implemented pragmatically when cost and schedule are factored in the evaluation?
- What business models could make trusted foundries commercially-viable? Can commercial lag and high costs be avoided?
- Can the performance, security, and reliability requirements of a system ever be met sufficiently by a COTS-based design versus an ASIC-based design?
- Do COTS-based designs provide real advantages for upgradability in the absence of a modular open systems approach (MOSA)?
- How can microelectronics technical debt be more precisely measured and assessed in defense systems? Would maintenance data from the Services help?

Appendix A

2022 NDIA ETI Workshop Summary

Summary

The NDIA Emerging Technologies Institute hosted an informal roundtable meeting in February 2022 to discuss ideas related to the transition of modern microelectronics into defense systems and to shape future ETI activities in this policy area. Participants included experts from NDIA, defense industry, government research and acquisition personnel, Congress, and commercial microelectronics. Key issues that were to be addressed included:

- DOD has a series of programs that are trying to advance the state-of-the-art (SOTA) in the microelectronics, including improving performance, enhancing security, reducing cost, and reducing size/weight/power requirements. These are paralleled by advances in the commercial sector. Traditionally, it is much easier for these devices to be used in commercial technologies and systems than defense systems, whether there are in development or in sustainment.
- Most of DOD's current systems are reliant on state-of-the-practice (SOTP) and legacy microelectronics, which are sufficient to meet their requirements, and so have limited incentives to adopt more modern microelectronics systems.
- The creation of policies and programs that enable refreshing of legacy systems or systems currently in development could benefit a wide range of defense sectors, including both the research enterprise to the acquisition and testing community. This would also potentially reduce program life cycle costs and improve operational capabilities.

Overview

The participants discussed the current landscape of microelectronics relevant to these transition issues. The accelerating pace of technological change combined with the activities of near peer adversaries to develop, acquire, and adopt advanced technologies suggests that the US will lose some of its military technological superiority if ways of incorporating advanced microelectronics in defense systems are not developed. The participants reviewed ongoing DOD efforts, including the RAMP (Rapid Assured Microelectronics Prototypes), RAMP-C (Rapid Assured Microelectronics Prototypes-Commercial), and SHIP (State-of-the-art Heterogeneous Integrated Packaging) programs. Key challenges to the transition of the products of these efforts relate to ensuring quantifiable assurance and rationalizing low defense production requirements to engage the commercial sector and support a sustainable business model.

The participants discussed typical barriers to the adoption of advanced microelectronics into defense systems. These included:

- The lack of specific requirements (and therefore funding) for most systems in development or sustainment to adopt more modern microelectronics, and the perception that this type of technology insertion entails cost and technical and schedule risk. This results in limited incentives for program offices or systems integrators to make efforts to incorporate these technologies.
- Difficulty in communicating the value of the use of modern microelectronics to relevant decision makers in the operational, requirements, and resourcing communities. There needs to be dialogue that better connects the technical and performance advantages to the resulting system performance, combat effectiveness, and life cycle cost.
- Lengthy and costly testing and qualification processes that must be navigated prior to insertion of new technologies into systems and operational use.
- The lack of control of technical data and system interfaces, along with the lack of use of open systems architecture approaches.

Best Practices

The participants discussed some best practices that have led to past success in the adoption of advanced technologies by defense systems and programs. There was some discussion about the value in deriving lessons learned from such success stories. The success models that were discussed included:

- The use of open systems architectures, such as employed by the submarine community in the Advanced Rapid Commercial-Off-The-Shelf Insertion (ARCI) program. These work best when the community is small and technical competent enough to control requirements well and closely partner with their associated operational community.
- The use of advanced modeling and simulation techniques, such as the digital twinning and advanced digital engineering efforts being used by multiple Services to speed the use of some modern electronics subsystems. This might speed testing and qualification processes and help address some of the risk aversion of programs and operators.
- The use of special programs to identify and incorporate mature commercial technologies, including to reduce life cycle costs, such as in the 1990s Commercial Operational Support & Savings Initiative (COSSI). This works when interest can be generated on the commercial side through appropriate financial incentives and if programs and Services are interested in investing funding upfront to reduce life cycle costs. This can also leverage demonstrated commercial successes, such as the security and reliability of commercial electronics being used in the financial sector or in critical medical applications.

Recommendations

The participants discussed some possible solutions to address some of the identified issues to technology adoption. These included:

- Better identifying the problems that will occur to DOD by not adopting more modern microelectronics. These can include life cycle cost growth and readiness and operational shortfalls.
- Identify a set of program offices who want to add new components to existing systems and have them opt in and budget it to support the diverse teams from industry and academia to perform the work.
- Develop a budget for a microelectronics modernization plan managed by a program office.

Next Steps

The participants recommended a series of next steps for NDIA to consider to promote the increased adoption of advanced microelectronics in defense systems, including:

- Collect best practices and recommendations on qualifying microelectronics for use in defense systems
- Collect stories of successful transitions of SOTA/SOTP microelectronics into systems and barriers to such transitions from NDIA members and government offices
- Identify costs and benefits for adoption of SOTA/SOTP microelectronics by defense systems in acquisition or sustainment to improve communicating the value to programs, operators, and resource sponsors

References

Badlam, Justin, Stephen Clark, Suhrid Gajendragadkar, Adi Kumar, Sara Slayton O'Rourke, and Dale Swartz. "The Chips and Science Act: Here's What's in It." McKinsey & Company. October 4, 2022. https://www.mckinsey.com/industries/public-sector/our-insights/the-chips-and-science-act-heres-whats-in-it

Bajpai, Prableen. Nasdaq. "An Overview of the Top 5 Semiconductor Foundry Companies." October 1, 2021. https://www.nasdaq.com/articles/an-overview-of-the-top-5-semiconductor-foundry-companies-2021-10-01

Counterpoint Research. "Global Semiconductor Foundry Market Share: By Quarter." September 12, 2023. https://www.counterpointresearch.com/insights/global-semiconductor-foundry-market-share/

Das, Shamik, MITRE Corporation. "Microelectronics Quantifiable Assurance (MQA) Independent Assessment." March 1, 2023. https://www.cto.mil/wp-content/uploads/2023/07/MQA-Assessment-Briefing-for-Release-Distro-A.pdf

Defense Advanced Research Projects Agency (DARPA), U.S. Department of Defense. "Electronics Resurgence Initiative 2.0." March 6, 2023. https://www.darpa.mil/work-with-us/electronics-resurgence-initiative

Defense Advanced Research Projects Agency (DARPA), U.S. Department of Defense. "Next-Generation Microelectronics Manufacturing Aims to Sustain R&D Ecosystem." July 20, 2023. https://www.darpa.mil/news-updates/2023-07-20

Defense Microelectronics Agency, U.S. Department of Defense. "Trusted IC." https://www.dmea.osd.mil/TrustedIC.aspx

Defense Standardization Program Office, Defense Logistics Agency (DLA), U.S. Department of Defense. "Diminishing Manufacturing Sources and Material Shortages," September 2009. https://www.dla.mil/Portals/104/Documents/LandAndMaritime/V/VA/PSMC/LM_SD22FINAL_151030.PDF p. 4

DoD Research & Engineering, OUSD(R&E). "DOD Research & Engineering, OUSD(R&E)." n.d. https://www.cto.mil/ct/microelectronics/commons/

Faist, James A. NDIA Emerging Technologies Institute. "Digital Engineering: Recommendations for the U.S. Department of Defense." November 2021. https://www.emergingtechnologiesinstitute.org/-/media/ndia-eti/event-documents/3r04---data-sharing/eti-de_report_2021-v2.pdf

IEEE IRDS. "Future of Semiconductor Performance." https://irds.ieee.org/topics/future-of-semiconductor-performance.

Intel Corporation. "Intel Provides Update on Internal Foundry Model." June 21, 2023. https://www.intel.com/content/www/us/en/newsroom/news/intel-update-internal-foundry-model.html

Intellectual Property Cadre, Office of the Under Secretary for Acquisition & Sustainment, U.S. Department of Defense. https://www.acq.osd.mil/asda/ae/ada/ip-cadre.html

Joint Federated Assurance Center (JFAC), DCTO, (S&T), OUSD(R&E), U.S. Department of Defense. https://rt.cto.mil/stpp/syssec/jfac/

Kuo, Way, and Taeho Kim. IEEE Xplore. "IEEE Xplore Full-Text PDF:" https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9043719

Lopez, C. Todd. U.S. Department of Defense. "DOD Names 8 Locations to Serve as New 'Microelectronics Commons' Hubs." September 20, 2023. https://www.defense.gov/News/News-Stories/Article/Article/3532338/dod-names-8-locations-to-serve-as-new-microelectronics-commons-hubs/

Manufacturing USA. "About Us." https://www.manufacturingusa.com/about-us

Mordor Intelligence. "Semiconductor Foundry Companies - Market Share & Size." https://www.mordorintelligence.com/industry-reports/semiconductor-foundry-market

National Institute of Standards and Technology, U.S. Department of Commerce. "Semiconductors." https://www.nist.gov/semiconductors

National Institute of Standards and Technology, U.S. Department of Commerce. "About CHIPS for America." October 5, 2023. https://www.chips.gov/

National Institute of Standards and Technology, U.S. Department of Commerce. "A Strategy for the Chips for America Fund." September 28, 2022. https://www.nist.gov/chips/implementation-strategy

NDIA Electronics Division, National Defense Industrial Association. "Zero Trust for Hardware Supply Chains: Challenges in Application Of Zero Trust Principles to Hardware." October 2021. https://www.ndia.org/-/media/sites/ndia/divisions/electronics/images---resources/zerotrustwhitepaper_20oct-revc.ashx

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

Nicas Jack, The New York Times. "Apple to Ditch Intel Chips in Macs as It Consolidates Its Power." June 22, 2020. https://www.nytimes.com/2020/06/22/technology/apple-macs-intel-chips.html

Office of the Deputy Assistant Secretary of Defense for Systems Engineering, U.S. Department of Defense. "Department of Defense Digital Engineering Strategy." June 2018. https://ac.cto.mil/wp-content/uploads/2019/06/2018-Digital-Engineering-Strategy_Approved_PrintVersion.pdf

Office of the Deputy Assistant Secretary of Defense for Systems Engineering, U.S. Department of Defense. "Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs." January 2017. https://acqnotes.com/wp-content/uploads/2017/07/DoD-Risk-Issue-and-Opportunity-Management-Guide-Jan-2017.pdf

Office of the Inspector General, U.S. Department of Defense. "Evaluation of the Department of Defense's Transition From a Trusted Foundry Model to a Quantifiable Assurance Method for Procuring Custom Microelectronics." Report DODIG-2022-084. May 2022. https://media.defense.gov/2022/May/04/2002989631/-1/-1/1/DODIG-2022-084_REDACTED.PDF

Office of the Under Secretary for Research & Engineering, U.S. Department of Defense. "Critical Technology Areas." https://www.cto.mil/usdre-strat-vision-critical-tech-areas

Office of the Under Secretary for Research & Engineering, U.S. Department of Defense. "DoD Microelectronics Commons: A National Network for Defense Microelectronics Innovation." October 31, 2022. https://www.cto.mil/wp-content/uploads/2022/11/DoD_Microelectronics_Commons.pdf

Reiff, Nathan. Investopedia. "10 Biggest Semiconductor Companies by Revenue." April 30, 2023. https://www.investopedia.com/articles/markets/012216/worlds-top-10-semiconductor-companies-tsmintc.asp

Rotman David, MIT Technology Review. "We're Not Prepared for the End of Moore's Law." April 21, 2021. https://www.technologyreview.com/2020/02/24/905789/were-not-prepared-for-the-end-of-moores-law/

Shaffer, Alan R., Chris Toffales, and Monique D. Attar. National Defense Magazine. "Microelectronics - A Critical National Resource." June 3, 2021. https://www.nationaldefensemagazine.org/articles/2021/6/3/microelectronics---a-critical-national-resource

Tarasov, Katie. CNBC. "ASML Is the Only Company Making the $200 Million Machines Needed to Print Every Advanced Microchip. Here's an inside Look." March 24, 2022. https://www.cnbc.com/2022/03/23/inside-asml-the-company-advanced-chipmakers-use-for-euv-lithography.html

The White House. "Draft National Strategy on Microelectronics Research." September 14, 2022. https://www.whitehouse.gov/wp-content/uploads/2022/09/SML-DRAFT-Microlectronics-Strategy-For-Public-Comment.pdf

The White House. "Fact Sheet: Biden-Harris Administration Announces Supply Chain Disruptions Task Force to Address Short-Term Supply Chain Discontinuities." June 8, 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/08/fact-sheet-biden-harris-administration-announces-supply-chain-disruptions-task-force-to-address-short-term-supply-chain-discontinuities/

The White House. "Fact Sheet: CHIPS and Science Act Will Lower Costs, Create Jobs, Strengthen Supply Chains, and Counter China." February 3, 2023. https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/09/fact-sheet-chips-and-science-act-will-lower-costs-create-jobs-strengthen-supply-chains-and-counter-china/

U.S. Code. 10 U.S.C. subtitle A, part V, subpart G, front matter: "Subpart G-Other Special Categories Of Contracting." https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title10-subtitleA-part5-subpartG-front&num=0&edition=prelim Also found at: U.S. Congress. "Section 224 of the National Defense Authorization Act of FY2020." Public Law 116-92, div. A, title II, § 224.

U.S. Congress. "CHIPS and Science Act of 2022." Public Law 117-167. https://www.congress.gov/bill/117th-congress/house-bill/4346

U.S. Congress. "Report on the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023." Senate Report 117-130. https://www.congress.gov/117/crpt/srpt130/CRPT-117srpt130.pdf, p. 74

U.S. Department of Defense. "DoD Zero Trust Strategy." October 21, 2022. https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf

U.S. Department of Defense. "Department of Defense Assured Microelectronics Policy for Senate Report 113-85." July 2014. https://rt.cto.mil/wp-content/uploads/2019/06/DoD-Assured-Microelectronics-Policy-RTC-July2014.pdf

U.S. Department of Defense. "Microelectronics Vision." May 2022. https://media.defense.gov/2022/Jun/15/2003018021/-1/-1/0/DEPARTMENT-OF-DEFENSE-MICROELECTRONICS-VISION.PDF

U.S. Department of Defense. "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)." DoD Instruction 5200.44.

U.S. Department of Defense. "The Defense Acquisition System." DoD Directive 5000.01. July 28, 2022. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/500001p.pdf

U.S. Executive Office of the President. Executive Order 14080: Implementation of the CHIPS Act of 2022. August 25, 2022. https://www.federalregister.gov/documents/2022/08/30/2022-18840/implementation-of-the-chips-act-of-2022

U.S. Government Accountability Office (GAO). "Weapon System Sustainment: The Army and Air Force Conducted Reviews and the Army Identified Operating and Support Cost Growth." GAO-23-106341. March 30, 2023. https://www.gao.gov/assets/gao-23-106341.pdf

U.S. National Security Agency. "DoD Microelectronics: Levels of Assurance Definitions and Applications." July 2022. https://media.defense.gov/2022/Jul/14/2003034921/-1/-1/0/CTR_DOD_MICROELECTRONICS_LEVELS_OF_ASSURANCE_DEFINITIONS_AND_APPLICATIONS_20220714.PDF

U.S. National Security Agency. "NSA Releases Series on Protecting DoD Microelectronics From Adversary Influence." Accessed December 8, 2022. https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3239938/nsa-releases-series-on-protecting-dod-microelectronics-from-adversary-influence/

Varas, Antonio, Varadarajan, Raj, Goodrich, Jimmy and Yinug, Falan, Semiconductor Industry Association, Boston Consulting Group, "Strengthening the Global Semiconductor Supply Chain in an Uncertain Era," April 2021. https://www.semiconductors.org/wp-content/uploads/2021/05/BCG-x-SIA-Strengthening-the-Global-Semiconductor-Value-Chain-April-2021_1.pdf

EMERGING TECHNOLOGIES INSTITUTE

SUPPORTING EMERGING TECHNOLOGIES TO SECURE U.S. NATIONAL DEFENSE AND ADVANCE U.S. ECONOMIC STRENGTH

The National Defense Industrial Association's Emerging Technologies Institute (ETI) performs research, hosts events, and bolsters public awareness through educational products and webinars focused on defense technology modernization and innovation. ETI also works to create a policy environment most conducive to the efficient development and delivery of new systems and technologies for the defense enterprise. ETI engages industry, academia, policymakers, and the public to explore emerging technologies' impact on national security and opportunities for industry-government partnerships to increase U.S. competitive advantage.

ETI reports, events, and workshops support NDIA's membership and the defense science & technology enterprise as part of its nonpartisan 501(c)(3) mission.

ETI was founded in 2021 and is staffed by researchers and subject matter experts and backed by a preeminent advisory board.

For more information, visit **EmergingTechnologiesInstitute.org**

EMERGING TECHNOLOGIES INSTITUTE

EmergingTechnologiesInstitute.org