February 2022

Perspective
EXPERT INSIGHTS ON A TIMELY POLICY ISSUE

JARED MONDSCHEIN, JONATHAN W. WELBURN, DANIEL GONZALES

Securing the Microelectronics Supply Chain

Four Policy Issues for the U.S. Department of Defense to Consider

The first solid state integrated circuits were invented in the United States at Fairchild Semiconductor and Texas Instruments in 1958 (Fegan, 2020). In the following decades, U.S. companies developed increasingly dense microelectronic components and manufacturing processes capable of production at large scales with high yields. Millions of computer chips flowed off production lines ready to be inserted into electronic calculators, mainframe computers, and later the first personal computers (PCs). IBM was an early developer of integrated circuits for its mainframe computers, but it was Intel that introduced the low-cost, efficient PC microprocessor ("Intel at 50," 2018). Intel and other U.S. companies, such as Fairchild Semiconductor, pioneered the production of memory components.

The microelectronics business has always been capital-intensive, which can discourage new entrants into the market and punish laggards who got their chips to market late and missed product cycles (Eden, 2000). If delays are encountered in either research and development (R&D) or in tuning manufacturing production lines to achieve high yields, companies can incur significant losses. Furthermore, as

RAND CORPORATION

new foundries have come online for commodity microelectronics, such as memory components, prices have declined and manufacturers have, at times, been unable to recoup investments in new facilities and equipment. As a result of these financial pressures and the risks involved in meeting production dates—and despite the initial dominance of U.S. firms such as Intel and IBM—U.S. investors significantly restricted investments in the semiconductor manufacturing sector.

Simultaneously, however, industry planners and foreign governments, notably Japan, China, Taiwan, and South Korea, have recognized that the microchip industry would play an important strategic role in both national and economic security by producing components essential to mass consumer products (e.g., PCs, televisions, and smartphones) and weapons systems. To facilitate the growth and the long-term viability of a domestic microelectronics ecosystem, these governments have provided substantial subsidies. For example, U.S. analysts have estimated that Chinese semiconductor companies receive government incentives of up to 30 to 40 percent of the cost of a new semiconductor foundry (which costs up to $20 billion), while the South Korean and Taiwanese governments provide incentives equivalent to about 25 to 30 percent of the total cost of a new foundry (White House, 2021). European incentive programs typically focus on targeted R&D funding that supports niche microelectronics sectors, such as photonics (Thompson et al., 2017). The U.S. federal government has not traditionally provided direct incentives to domestic semiconductor manufacturers, but state and local government incentives typically provide 10 to 15 percent of the cost of a new foundry (Varas et al., 2020).

The ever-tightening financial constraints of semiconductor manufacturing combined with different national policies have led to the business reality faced by U.S. consumers and leaders in 2021: The U.S. share of global semiconductor manufacturing capacity has fallen from about 38 percent in 1990 to 12 percent in 2020 and is expected to decline to less than 10 percent by 2030 (Platzer, Sargent, and Sutter, 2020).[1] The world's technology leaders are now based in Taiwan and South Korea (Taiwan Semiconductor Manufacturing Corporation [TSMC] and Samsung Electronics, respectively), and the manufacturing capacity of mainland Chinese semiconductor firms has grown from just a few percentage points of the total global market in 2000 to about 15 percent in 2020 (Varas et al., 2020). Intel and GlobalFoundries are U.S. manufacturers of state-of-

Abbreviations

CFIUS	Committee on Foreign Investment in the United States
CHIPS	Creating Helpful Incentives to Produce Semiconductors
COTS	commercial off-the-shelf
DARPA	Defense Advanced Research Projects Agency
DoD	U.S. Department of Defense
EAR	Export Administration Regulations
FASC	Federal Acquisition Security Council
ITAR	International Traffic in Arms Regulations
JFAC	Joint Federated Assurance Center
PC	personal computer
R&D	research and development
SCRM	supply chain risk management
TSMC	Taiwan Semiconductor Manufacturing Corporation

the-art logic circuits.[2] These companies do not have the manufacturing capabilities at the leading edge, and as a result, U.S.-based information technology companies, such as Apple, Nvidia, and Amazon—and the U.S. Department of Defense (DoD)—are increasingly reliant on TSMC and Samsung to manufacture advanced microelectronics.

The growing realization of these economic trends and their implications for U.S. national and economic security has resulted in a national conversation and a growing chorus of academic, industry, and government stakeholders arguing for varying policy solutions. Out of this dialogue have emerged critical knowledge gaps that will hamper decisionmakers' ability to make informed policy. We have identified four high-priority questions that should drive U.S. policymaking but that require additional data and insights:

1. Why are supply chain risk management (SCRM) strategies necessary to mitigate microelectronics supply chain disruptions?
2. Does DoD need access to the latest generation of microelectronics, or will a lag of several generations be acceptable to ensure trusted and reliable access to manufacturers and supply chains?
3. How can DoD create a coordinated effort to mitigate microelectronics supply chain risk?
4. What is the appropriate mix of policy levers to promote a microelectronics technology ecosystem that is aligned with U.S. strategic goals?

Although we recognize that this policy environment is rapidly evolving as new initiatives are announced and implemented and new data emerge, we believe that these four policy drivers will remain the foundation on which policy will be made over the long term. It is therefore vital to U.S. interests that the ongoing dialogue and policy conversations consider these four questions. This Perspective represents an initial attempt to explore these drivers and motivate future analyses.

Microelectronics Policy Drivers

Why are SCRM strategies necessary to mitigate microelectronics supply chain disruptions? An ongoing global semiconductor shortage has brought attention to a key problem: U.S. supply chains are dependent on fragile supply chains with a highly concentrated semiconductor industry at center stage. TSMC alone represents 71 percent of the total global foundry services market.[3] This indicates a staggering dependence on a single firm.[4] The coronavirus disease 2019 pandemic led to a series of supply chain disruptions that contributed to the chip shortage. Pandemic lockdowns led to increases in electronics demand to support teleworking (Liedtke and Krishner, 2021). Lockdowns also contributed to temporary halts in chip production (Hille, 2021). Companies such as auto manufacturers cut chip orders in expectation of low demand, leaving them unable to meet high demand under a faster-than-expected recovery ("Chip Shortage Shows the Pitfalls of 'Just in Time,'" 2021). U.S.-China trade tensions might have contributed to stockpiles of chips within China (Ting-Fang and Li, 2021). However, between natural disasters, cyber threats, and policy shifts, a rising specter of disruptions yields a core question: When, and for what applications, is there a need for the United States to bolster domestic manufacturing of microelectronics in support of both economic

and national security? And when might it be sufficient to rely on SCRM?

Because of the increasing concentration of production and supply chains, natural disasters present a clear and growing hazard for electronics supply chains. In 2011, the Tōhoku earthquake in Japan disrupted production at a Sony factory that was manufacturing complementary metal-oxide semiconductor image sensors (Yamazaki and Saoshiro, 2016). In addition to supplying a large share of the global market, the factory's sensors were a key input in the supply chain of Apple's iPhone. Later that year, large flooding in Thailand, home to 40 percent of global hard drive production, led to large shortages as Western Digital was forced to cut production (Romero, 2012). With its large concentration in Taiwan, the semiconductor industry is hardly safe from similar risks. A 2016 earthquake led to a near miss for TSMC (Webb, 2016). In addition, an ongoing Taiwanese drought threatens to hit the water-intensive fabrication process with water rations and reduced supply (Wu and Wang, 2021).

Cyber threats pose clear risks, too. A 2012 cyberattack against Saudi Aramco indirectly had a similar impact on global hard drive supplies as the 2011 Thai floods; malware wiped and destroyed tens of thousands of hard drives at the largest oil company, resulting in another temporary hard drive shortage as the company quickly purchased 50,000 new drives to respond and recover (Pagliery, 2015). However, when it comes to cyber risks, the concentration of the semiconductor industry also poses risks not only for disruption but also for exploitation (particularly via tampering). In 2018, a report from *Bloomberg Businessweek* detailed how Chinese spies had compromised motherboards produced by Supermicro—motherboards that made their way from Supermicro's subcontractors to their eventual customers at Apple and DoD (Robertson and Riley, 2018). The story was met with strong opposition from Apple and DoD, who argued against the story's veracity, but the story left ideas of what risks could exist beneath hardware supply chains (Lovejoy, 2021).

Securing the microelectronics supply chain will, therefore, require addressing several potential disruptions. This has led to calls for advancing beyond traditional just-in-time manufacturing (McLain, 2021). There have also been policy movements toward strengthening domestic supply chains and even decoupling from foreign suppliers (Biden, 2021). Strengthening domestic production—or shifting reliance to production from U.S. allies—might work to mitigate some risks, such as potential geopolitical shifts that cut off supply. For many other cases—from natural disasters to cyber threats—gains might come through increased use of SCRM strategies, better information-sharing, the integration of acquisition planning, and supply risk management (O'Connell et al., 2021). Specifically, individual organizations can implement SCRM (policies aimed at identifying sources' vulnerabilities across their supply gains, potential hazards, and mitigation strategies), and industrial policy can provide further gains through efforts to strengthen domestic manufacturing capacities, support competition, invest in human capital for key skillsets, and facilitate trade relationships with partner and ally nations. Furthermore, efforts to gather data on supply chain linkages, in combination with enhanced analytical capabilities, can be used to identify central nodes within supply chain networks that present systemic risks prior to large disruptions (Welburn et al., 2020). These practical approaches for making supply

chains more resilient to disruption might be more feasible than large efforts to reverse trade patterns and minimize participation in global semiconductor supply chains.

Does DoD need access to the latest generation of microelectronics, or will a lag of several generations be acceptable to ensure trusted and reliable access to manufacturers and supply chains? DoD has a complex demand for microelectronics that requires trusted and reliable access to commercial off-the-shelf (COTS) components and for components manufactured specifically for DoD applications.[5] Further complicating DoD's demand requirements is a typical service lifespan that can far exceed the lifespan of commercial sector products. DoD, therefore, must support and maintain older products even as the commercial sector rapidly adopts more-advanced microelectronics technologies (de la Serna et al., 2017). Simultaneously, DoD's objective to ensure continued warfighting advantage over adversaries via technological dominance often requires the integration of leading-edge components. There is also no single semiconductor manufacturing process that can meet the variety of DoD requirements, even across technology generations (i.e., nodes), because of divergent computational needs. Indeed, the microelectronics ecosystem is diverse and includes components for memory (e.g., flash, dynamic random access memory), photonics, and logic, each of which consists of a diverse variety of materials and architectures (U.S. Department of Energy, Office of Science, 2018). Furthermore, microelectronics can be carved into two categories: COTS components that are publicly available and tend to be for broad commercial applications and application-specific integrated circuits that are designed for distinct applications. The costs of accessing these technologies, both the financial costs and security costs, vary significantly, with important implications. Table 1 summarizes applications that are enabled across the range of node sizes available through commercial semiconductor manufacturers.

State-of-the-art microelectronics are characterized by node sizes of less than 14 nm (with the smallest nodes in production measuring about 5 nm) and enable applications that require significant computing power, such as artificial intelligence. Relying on advanced, state-of-the-art technologies significantly reduces costs associated with speed and energy consumption and therefore presents significant

TABLE 1
Applications That Are Enabled Across the Range of Node Sizes Available via Commercial Semiconductor Manufacturers

Application	Node Size
Artificial intelligence	<10 nm[a]
Edge computing	14 nm[b]
RF communications	22 nm[c]
Integrated silicon photonics	90 nm[d]
Space-based applications	90–180 nm[e]
Laser-based sensing	100 nm–1 mm[f]

NOTE: RF = radio frequency; nm = nanometer; mm = millimeter.
[a] Khan and Mann, 2020.
[b] GlobalFoundries, 2018.
[c] Thoma and Dupaix, 2020.
[d] GlobalFoundries, 2018.
[e] ON Semiconductor, 2021; SkyWater Technology, undated.
[f] MACOM, 2021.

advantages over older-generation microelectronics (Khan and Mann, 2020).

Historically, DoD has had access to state-of-the-art technologies through the Trusted Foundry program, which involved partnerships with IBM and then GlobalFoundries in 2014 following GlobalFoundries' purchase of IBM's semiconductor manufacturing unit (Ricknäs, 2014). However, significant R&D and infrastructure costs have led to the consolidation of the advanced semiconductor manufacturing market, and GlobalFoundries is not pursuing sub-12 nm manufacturing (King, 2018). As a result, only three firms produce nodes at or below 10 nm: Korea-based Samsung, Taiwan-based TSMC, and U.S.-based Intel (Khan and Mann, 2020). Of these, just Samsung and TSMC have successfully achieved sub-10 nm manufacturing (King and Wu, 2021).

State-of-the-practice microelectronics are characterized by node sizes between 14 nm and 100 nm and enable a wide variety of DoD-specific applications (e.g., communications at specific frequencies) and dual-use applications (e.g., phased arrays for communications; Zerbib, 2013). *Legacy microelectronics* are characterized by node sizes above 100 nm and enable DoD-specific use cases such as radiation-hardened microelectronics for space-based applications and III-V semiconductor-based lasers for sensor applications (ON Semiconductor, 2021; SkyWater Technology, undated). DoD access is provided by the Defense Microelectronics Activity's Trusted Foundry Program, which certifies U.S.-located suppliers to facilitate varying levels of secure access. Suppliers involved in this program include ON Semiconductor, SkyWater Technology Foundry, and Northrop Grumman, among others (Defense Microelectronics Activity, 2021). Obsolete legacy microelectronics (components that are no longer commercially available) can be manufactured by the Defense Microelectronics Activity's Advanced Reconfigurable Manufacturing for Semiconductors foundry (DoD, Office of Inspector General, 2020).

For DoD to maintain technological dominance over adversaries through the deployment of computationally intensive technologies, such as artificial intelligence, access to state-of-the-art semiconductors is critical. However,

A coordinated approach to delineating stakeholder authorities and responsibilities, synchronizing efforts across organizations, and addressing key capability gaps could be of significant value to ensuring trusted and reliable access to microelectronics.

DoD must not lose focus on maintaining access to older generations of microelectronics technologies to support DoD systems throughout their lifecycle.

How can DoD create a coordinated effort to mitigate microelectronics supply chain risk? There is a clear need for coordinated, well-defined SCRM practices at the strategic, tactical, and operational levels across DoD (Moore and Loredo, 2013). Indeed, even a thriving domestic manufacturing ecosystem and coordination among allies will not replace a need to have dedicated processes put in place to reduce risks of supply chain interruptions, particularly in the interim as domestic capabilities are being stood up. Within DoD (and the broader federal government), a coordinated approach to delineating stakeholder authorities and responsibilities, synchronizing efforts across organizations, and addressing key capability gaps (e.g., through trainings and information-sharing) could be of significant value to ensuring trusted and reliable access to microelectronics.

Authorities and responsibilities for relevant SCRM activities are scattered across the federal government, resulting in information siloes that make communicating and disseminating knowledge and best practices to community stakeholders challenging (O'Connell et al., 2021). Within DoD, the Chief Information Officer, the Under Secretary of Defense for Acquisition and Sustainment, the Under Secretary of Defense for Research and Engineering, DoD component leaders, and service secretaries have overlapping equities. Furthermore, separate policies govern DoD acquisition programs, the management of counterfeit parts, trusted security networks, and cybersecurity, resulting in significant coordination challenges. These policies can also be vague and might not provide necessary authorities for enforcement, further complicating efforts. We have found this to be a key barrier limiting forward progress.

Historically, DoD addresses challenges with strategy and implementation synchronization through the designation of an executive agent or an entity with coordinating authorities. This coordinating entity could enhance or facilitate interagency coordination and access to siloed capabilities. For example, DoD's Joint Federated Assurance Center (JFAC), which provides vulnerability analysis, testing, and protection tools for hardware and software assurance, might be able to support SCRM efforts across the federal government (DoD Research & Engineering Enterprise, undated). Additionally, this body could engage with industry partners and the Federal Acquisition Security Council (FASC), created by the Federal Acquisition Supply Chain Security Act of 2018 to facilitate information-sharing and mitigations across the federal government (Office of the Director of National Intelligence, 2019).

This coordinating function can designate DoD leads for improving capabilities that might be relatively weak across the SCRM enterprise, such as training and information management.[6] The availability of trainings to educate acquisition officials is fragmented and organization-dependent, although some entities (such as the U.S. Navy) offer training courses on counterfeit parts and supplier assessments. Such trainings could highlight the following:

- information to request for comprehensive assessments
- information sources (e.g., contractors; the Government–Industry Data Exchange Program; the Navy's Product Data Reporting and Evaluation Program; and Electronic Resellers Association International, a company that monitors, investi-

gates, and reports issues affecting global electronics supply chains)
- DoD capabilities for vulnerability testing (e.g., the JFAC)
- DoD-certified suppliers of microelectronics components (e.g., those that can be found via the Defense Microelectronics Activity's Trusted Foundry Program and Trusted Access Program Office or DARPA's Metal Oxide Silicon Implementation Service, which provides access to Intel's 22 nm process; Thoma and Dupaix, 2020)
- sources of obsolete parts (e.g., Defense Microelectronics Activity's Advanced Reconfigurable Manufacturing for Semiconductors foundry).

Program offices, which historically have struggled with limited visibility into supply chains and information about threats because of decentralization of data collection and classification barriers, would be primary customers of the developed trainings.

Policy options should be intimately connected to specific objectives across technology readiness levels and should consider trade-offs.

What is the appropriate mix of policy levers to promote a microelectronics technology ecosystem that is aligned with U.S. strategic goals? At the time of this writing, December 2021, a U.S. strategic plan for microelectronics has yet to be released. Indeed, the fiscal year 2021 National Defense Authorization Act requires the development of this strategy as part of the Creating Helpful Incentives to Produce Semiconductors (CHIPS) for America Act, but requisite funding has not yet been appropriated. These policy proposals in part have prompted a national conversation, but a microelectronics technology ecosystem that aligns with U.S. strategic goals has yet to be formally defined. It is not clear which part or parts of the semiconductor industry should be considered a critical national asset and maintained domestically. Because of the global nature of the semiconductor value chain, the role of foreign-based firms and researchers needs to be clarified, particularly given state and federal interests in incentivizing the construction of foreign-owned facilities domestically and a strategic need to rely on manufacturing facilities located abroad (Li and Ting-Fang, 2020; "Phoenix Approves TSMC Incentives," 2020). Coordinating policy and developing and tracking metrics to assess how well ongoing policy activities align with the national objective is murky at best without an identified strategic goal.

Policy options should be intimately connected to specific objectives across technology readiness levels and should consider trade-offs. Initiatives tend to fall within the following categories:

- **Promote**: State and local government incentives typically provide 10 to 15 percent of the cost of a new foundry (Varas et al., 2020). However, the U.S. federal government has not provided direct incen-

tives to domestic semiconductor manufacturers.[7] Instead, the U.S. government has invested in science and technology initiatives via the National Science Foundation, DoD, the Department of Commerce, and the Department of Energy. DoD-niche capabilities are typically pursued by DARPA, the Intelligence Advanced Research Projects Activity, and DoD service labs, and many of these technologies have transitioned into the commercial sector. Notably, some of this funding is directed toward foreign-based researchers and firms via their participation in U.S.-based public-private partnerships or DoD research grants.[8] Although the partnerships provide the United States with access to expertise, ideas, and facilities, off-shore development and subsequent commercialization could occur. Other nations offer a diverse set of incentives, including R&D tax credits, tax holidays and tax deferrals, talent subsidies, and capital expenditures (European Commission, 2013).

- **Protect**: Foreign access to U.S.-developed technologies across technology readiness levels is limited via a handful of policies. Regulations such as International Traffic in Arms Regulations (ITAR), Export Administration Regulations (EAR), and security classifications protect specific technologies and preclude access by specific firms. For example, adding Huawei, a Chinese firm, to the Entity List and amending the Foreign Direct Product Rule (as part of the EAR) imposed significant barriers that limited Huawei's access to software that facilitates the design of new integrated circuits and leading-edge manufacturers (Harold and Hodiak, 2020; Hodiak and Harold, 2020). The national security implications of specific transactions involving foreign investment in the United States are reviewed by the Committee on Foreign Investment in the United States (CFIUS) (U.S. Department of the Treasury, undated). CFIUS has blocked the acquisition of U.S. semiconductor firms Aixtron SE, Lattice Semiconductor, and Qualcomm by China-linked companies (McGaughey, 2021). Furthermore, the Department of Justice has led efforts to improve the security of the U.S. research community by countering adversarial acquisition and theft of intellectual property and illicit engagement with U.S. scientists (Stracqualursi and Jones, 2020; Wu, 2020). Within DoD, program offices have access to capabilities for vulnerability testing via the JFAC (DoD Research & Engineering Enterprise, undated); certified suppliers via the Trusted Foundry Program (Thoma and Dupaix, 2020); and supply chain risk information via the FASC (Office of the Director of National Intelligence, 2019). Additionally, security guidelines governing DoD acquisitions are outlined in the Federal Acquisition Regulation and Defense Federal Acquisition Regulation Supplement (O'Connell et al., 2021). Each of these protective policy measures have trade-offs; the Department of Justice–led efforts, for example, might isolate U.S. researchers from critical foreign talent. Other policies might add costs to defense programs, potentially straining budgets.

The measurable effectiveness of these policy options is complicated by the poor availability of supporting data, the

extended timescales over which impacts typically occur, and the complicated trajectories that technologies follow over their maturation paths. For example, transitioning nascent technologies developed via federal R&D funding into a commercialized product manufactured by a U.S.-based firm has been a long-running challenge, and so tangible domestic economic benefits are, at times, not realized or are instead gained by a foreign-based firm that transitions the technology (Sullivan, 2015). Moreover, although research indicates that R&D efforts targeting the development of DoD-niche technologies (e.g., radiation-hardened integrated circuits) is beneficial to DoD, DoD-funded research targeting more-generalizable technological advances often lags behind the capabilities of technologies developed via commercial R&D efforts (Slomovic, 1991).

Additionally, U.S. policymaking does not occur in a vacuum but rather in a globally distributed technology ecosystem with economically competitive countries and regions. Incentives developed in 2021 might not be sufficient to foster a domestic innovation base if European and Asian nations continue to offer a much more aggressive package of financial incentives that facilitate domestic commercial activity, as they historically have done (Varas et al., 2020). Furthermore, multinational R&D efforts, such as the European Union's Silicon Europe program, provide academic, government, and commercial-sector researchers with cross-border access to expertise, facilities, and ideas and sharply contrast with the U.S. government's typical U.S.-centric approach to public-private partnerships (Silicon Europe, 2012). DoD's relatively small share of the global demand for semiconductors (less than 1 percent) also constrains its ability to shape markets (Platzer, Sargent, and Sutter, 2020).

Conclusions

We have identified four high-priority questions that should drive U.S. policymaking but that require additional data and insights to fully answer. These four policy drivers should be revisited as new contexts present themselves and initiatives are designed and implemented. This Perspective represents an initial attempt to explore these drivers and motivate future analyses.

Why are SCRM strategies necessary to mitigate microelectronics supply chain disruptions? An ongoing global semiconductor shortage has brought attention to a key problem: U.S. supply chains are dependent on fragile supply chains with a highly concentrated semiconductor industry at center stage. Global events have highlighted the risks posed to global economies by threats to microelectronics supply chains, which have included natural disasters, such as the 2011 Tōhoku earthquake in Japan that disrupted production at a Sony facility, and software and hardware cyber threats. Although strengthening domestic production or shifting reliance to products from U.S. allies might mitigate some risks, additional gains might be achieved through increased use of SCRM strategies, better information-sharing, the integration of acquisition planning, and supply risk management. Industrial policy can produce further gains through efforts to strengthen domestic manufacturing capacities, support competition, invest in human capital for key skillsets, and facilitate trade relationships with partner and ally nations.

Does DoD need access to the latest generation of microelectronics, or will a lag of several generations be acceptable to ensure trusted and reliable access to manufacturers and supply chains? DoD has a complex demand for microelectronics. In certain use cases, access to the latest

generation, state-of-the-art microelectronics technologies confers tactical and operational advantage over competitors. Applications that require significant speed at minimal energy inputs, such as artificial intelligence, require integration with state-of-the-art microelectronics. However, DoD requires a diverse array of microelectronics technologies that includes node sizes that can be readily manufactured by less advanced facilities located within the United States and obsolete components that must be manufactured by DoD to ensure access. Regardless of manufacturing location or process, DoD aims to ensure secure access to domestic manufacturers via a supplier certification program managed by the Defense Microelectronics Activity.

How can DoD create a coordinated effort to mitigate microelectronics supply chain risk? Authorities and responsibilities for relevant SCRM activities are scattered across the federal government, resulting in often isolated pockets of excellence that struggle to communicate and disseminate information and best practices to community stakeholders. As a result, key individuals (e.g., acquisition officials) are often not aware of or do not have access to departmental or interagency resources, including trainings, information databases, and vulnerability analysis, testing, and protection tools for hardware and software assurance. There is a clear need for coordinated, well-defined SCRM practices at the strategic, tactical, and operational levels.

What is the appropriate mix of policy levers to promote a microelectronics technology ecosystem that is aligned with U.S. strategic goals? The federal government (and, to a certain extent, state and local governments) have been pursuing an uncoordinated, multipronged policy approach to promote and protect a domestic microelectronics innovation ecosystem. These efforts have included R&D investments, the funding of public-private partners and research consortia, financial and tax incentives to support commercial R&D and manufacturing, and federal regulations to limit undesired foreign access to U.S.-developed technologies via ITAR and EAR. Although these efforts have produced key successes while suffering setbacks, assessments are typically only conducted many years after the project's culmination, limiting the availability of lessons learned and best practices. Furthermore, evidence suggests that European and Asian nations typically offer a much more aggressive package of financial incentives that facilitate domestic commercial activity, so incentives developed in 2021 might not be sufficient to foster a domestic innovation base. DoD's relatively small share of the global demand for semiconductors also constrains its ability to shape markets. How policies fit into this broader ecosystem—and the intended and unintended effects on domestic innovation, the industrial base, foreign partners and allies, and foreign competitors—are important considerations for policymakers when weighing policy options to achieve strategic goals for microelectronics access across time horizons.

Global events have highlighted the risks posed to global economies by threats to microelectronics supply chains.

Notes

[1] These constraints include the capital-intensive nature of semiconductor manufacturing, significant R&D expenses required to maintain industry leadership, talent requirements, and the need to achieve massive economies of scale to recoup R&D and operating costs. See, for example, White House, 2021.

[2] Intel also has substantial manufacturing capacity abroad, with manufacturing facilities in Ireland, Israel, and China and assembly and test facilities in China, Costa Rica, Malaysia, and Vietnam.

[3] Foundry service firms, such as TSMC, provide manufacturing services to customers that don't have in-house manufacturing capacity (i.e., *fabless* companies). Of the six large semiconductor firms based in the United States, three are fabless. Seven of the ten largest fabless firms are located within the United States. For more information, see Platzer, Sargent, and Sutter, 2020.

[4] We used data from FactSet, undated, for our analysis.

[5] "Trusted and reliable access" occurs when the confidentiality, integrity, and availability of microelectronics have been ensured. For more information, see Defense Advanced Research Projects Agency (DARPA), undated.

[6] Industry partners might be a prime resource for SCRM practices that can be readily adopted by DoD. See, for example, a set of commercial best practices organized by the National Institute of Standards and Technology in Boyens et al., 2021.

[7] The CHIPS for America Act shifts this paradigm and provides federally funded incentives to domestic manufacturers.

[8] For U.S. mechanisms of funding foreign semiconductor R&D, see, for example, Office of Naval Research, 2016, and PowerAmerica, undated.

References

Biden, Joseph R., Jr., "Executive Order on America's Supply Chains," White House, February 24, 2021.

Boyens, Jon, Celia Paulsen, Nadya Bartol, Kris Winkler, and James Gimbi, *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry*, Gaithersburg, Md.: National Institute of Standards and Technology, U.S. Department of Commerce, NISTIR 8276, February 2021.

"Chip Shortage Shows the Pitfalls of 'Just in Time,'" *Financial Times*, June 9, 2021.

DARPA—*See* Defense Advanced Research Projects Agency.

Defense Advanced Research Projects Agency, *A DARPA Approach to Trusted Microelectronics*, Arlington, Va., undated.

Defense Microelectronics Activity, "Trusted Foundry Program: Accredited Suppliers," directory, last updated June 30, 2021. As of June 30, 2021:
https://www.dmea.osd.mil/otherdocs/AccreditedSuppliers.pdf

de la Serna, Antonio, Charles Adams, Craig Herndon, Dan Radack, Dean Brenner, Eric Dauler, Grant Meyer, Jeremy Muldavin, Jim Gobes, Kenneth H. Heffner, Kirk Reynolds, Manny Trejo, Michael Fritze, Ray Shanahan, Scott Anderson, Tim Lee, and Tyler Schmidt, Trusted Microelectronics Joint Working Group, *Team 1 White Paper: Future Needs & System Impact of Microelectronics Technologies*, New York: National Defense Industrial Association, July 2017.

DoD—*See* U.S. Department of Defense.

Eden, Scott, "Semiconductor Industry Group Sees End to Boom-and-Bust Cycle," *Wall Street Journal*, February 7, 2000.

European Commission, *Comparison of European and Non-European Regional Clusters in KETs: The Case of Semiconductors*, Brussels, 2013.

FactSet, homepage, financial data and analytics, undated. As of July 11, 2021:
https://www.factset.com/

Fegan, David, "Evolution of the Microchip," Royal Irish Academy, July 27, 2020.

GlobalFoundries, "GlobalFoundries Extends Silicon Photonics Roadmap to Meet Explosive Demand for Datacenter Connectivity," press release, Santa Clara, Calif., March 14, 2018.

Harold, Scott W., and Justin Hodiak, "China's Semiconductor Industry: Autonomy Through Design?" Institut Montaigne, September 25, 2020.

Hille, Kathrin, "Taiwan's Covid-19 Outbreak Spreads to Chip Companies," *Financial Times*, June 8, 2021.

Hodiak, Justin, and Scott W. Harold, "Can China Become the World Leader in Semiconductors?" *The Diplomat*, September 25, 2020.

"Intel at 50: The 8086 and Operation Crush," Intel Newsroom, May 31, 2018.

Khan, Saif M., and Alexander Mann, *AI Chips: What They Are and Why They Matter: An AI Chips Reference*, Washington, D.C.: Center for Security and Emerging Technology, April 2020.

King, Ian, "Globalfoundries Gives Up on Advanced Chip Production Technology," *Bloomberg*, August 27, 2018.

King, Ian, and Debby Wu, "Intel Talks with TSMC, Samsung to Outsource Some Chip Production," *Bloomberg*, January 8, 2021.

Li, Lauly, and Cheng Ting-Fang, "Exclusive: Washington Pressures TSMC to Make Chips in US," Nikkei Asia, January 15, 2020.

Liedtke, Michael, and Tom Krishner, "The Microchip Shortage Explained: How It's Impacting Car Prices and the Tech Industry," *USA Today*, April 2, 2021.

Lovejoy, Ben, "Bloomberg Resurrects Super Micro Spy Chip Story; NSA Still 'Befuddled' by the Claims," *9to5Mac*, February 12, 2021.

MACOM, "MACOM Introduces New Semiconductor Process for High Voltage Capacitors," press release, Lowell, Mass., April 27, 2021.

McGaughey, J. Tyler, "What Dealmakers Need to Know About CFIUS and Semiconductors," Winston & Strawn, July 21, 2021.

McLain, Sean, "Auto Makers Retreat from 50 Years of 'Just in Time' Manufacturing," *Wall Street Journal*, May 3, 2021.

Moore, Nancy Young, and Elvira N. Loredo, *Identifying and Managing Air Force Sustainment Supply Chain Risks*, Santa Monica, Calif.: RAND Corporation, DB-649-AF, 2013. As of June 30, 2021: https://www.rand.org/pubs/documented_briefings/DB649.html

O'Connell, Caolionn, Elizabeth Hastings Roer, Rick Eden, Spencer Pfeifer, Yuliya Shokh, Lauren A. Mayer, Jake McKeon, Jared Mondschein, Phillip Carter, Victoria A. Greenfield, and Mark Ashby, *Managing Risk in Globalized Supply Chains*, Santa Monica, Calif.: RAND Corporation, RR-A425-1, 2021. As of June 30, 2021: https://www.rand.org/pubs/research_reports/RRA425-1.html

Office of the Director of National Intelligence, "Supply Chain Risk Management: Federal Acquisition Supply Chain Security Act of 2018 Overview," fact sheet, 2019.

Office of Naval Research, "Enhanced Energy: ONR Global Seeks More Powerful Electronic Devices," press release, Arlington, Va., December 22, 2016.

ON Semiconductor, *Aerospace & Defense Solutions: Specialized Products, Processes, and Services from ON Semiconductor*, Aurora, Colo., BRD8079/D, Rev. 10, June 2021.

Pagliery, Jose, "The Inside Story of the Biggest Hack in History," CNN, August 5, 2015.

"Phoenix Approves TSMC Incentives," *Taipei Times*, November 20, 2020.

Platzer, Michaela D., John F. Sargent, Jr., and Karen M. Sutter, *Semiconductors: U.S. Industry, Global Competition, and Federal Policy*, Washington, D.C.: Congressional Research Service, R46581, October 26, 2020.

PowerAmerica, homepage, undated. As of June 30, 2021: https://poweramericainstitute.org/

Ricknäs, Mikael, "IBM Pays GlobalFoundries $1.5 Billion to Take Over IBM's Chip-Making Unit," *PCWorld*, October 20, 2014.

Robertson, Jordan, and Michael Riley, "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies," *Bloomberg Businessweek*, October 4, 2018.

Romero, Joshua J., "The Lessons of Thailand's Flood: The Hard Drive Industry Shows That Responding to Disasters Can Be More Important than Preventing Them," *IEEE Spectrum*, November 1, 2012.

Silicon Europe, "Silicon Europe: Cluster Alliance for European Micro- and Nanoelectronics Industry," press release, Dresden, Germany, October 8, 2012.

SkyWater Technology, "The Most Advanced U.S. Foundry for Rad-Hard by Process Technologies," webpage, undated. As of June 30, 2021: https://www.skywatertechnology.com/technology/rad-hard-microelectronics/

Slomovic, Anna, *An Analysis of Military and Commercial Microelectronics: Has DoD's R&D Funding Had the Desired Effect?* dissertation, Pardee RAND Graduate School, Santa Monica, Calif.: RAND Corporation, N-3318-RGSD, 1991. As of June 30, 2021: https://www.rand.org/pubs/notes/N3318.html

Stracqualursi, Veronica, and Sheena Jones, "Harvard Professor Among Three Charged with Lying About Chinese Government Ties," CNN, January 28, 2020.

Sullivan, Michael J., *Report to Congressional Committees, Defense Advanced Research Projects Agency: Key Factors Drive Transition of Technologies, but Better Training and Data Dissemination Can Increase Success*, Washington, D.C.: U.S. Government Accountability Office, GAO-16-5, November 2015.

Thoma, Morgan, and Brian Dupaix, "Security and Access—Access to State of the Art Microelectronics with Quantifiable Assurance," slides, presented virtually at the 2020 Electronics Resurgence Initiative 2020 Summit, Defense Advanced Research Projects Agency, August 19, 2020.

Thompson, Haydn, Emilio Lora-Tamayo, Werner Damm, Jean-Luc Dormoy, Leonard Hobbs, Margriet Jansz, Tomasz Kosmider, and Wolfgang Pribyl, *Final Evaluation of the ARTEMIS and ENIAC Joint Undertaking (2008-2013) Operating Under FP7*, Brussels: European Commission, June 2017.

Ting-Fang, Cheng, and Lauly Li, "US-China Tech War: Beijing's Secret Chipmaking Champions," *Financial Times*, May 12, 2021.

U.S. Department of Defense, Office of Inspector General, *Audit of DoD Hotline Allegations Concerning the Defense Microelectronics Activity*, Alexandria, Va., DODIG-2020-072, March 24, 2020.

U.S. Department of Defense Research & Engineering Enterprise, "Joint Federated Assurance Center (JFAC)," webpage, undated. As of June 30, 2021:
https://rt.cto.mil/stpe/rs/jfac/

U.S. Department of Energy, Office of Science, *Basic Research Needs for Microelectronics: Report of the Office of Science Workshop on Basic Research Needs for Microelectronics*, Washington, D.C., October 2018.

U.S. Department of the Treasury, "The Committee on Foreign Investment in the United States (CFIUS)," webpage, undated. As of August 31, 2021:
https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius

Varas, Antonio, Raj Varadarajan, Jimmy Goodrich, and Falan Yinug, *Government Incentives and US Competitiveness in Semiconductor Manufacturing*, Boston, Mass.: Boston Consulting Group and Semiconductor Industry Association, September 2020.

Webb, Jonathan, "The Taiwanese Earthquake That Nearly Flattened the Apple iPhone 7," *Forbes*, February 29, 2016.

Welburn, Jonathan William, Aaron Strong, Florentine Eloundou Nekoul, Justin Grana, Krystyna Marcinek, Osonde A. Osoba, Nirabh Koirala, and Claude Messan Setodji, *Systemic Risk in the Broad Economy: Interfirm Networks and Shocks in the U.S. Economy*, Santa Monica, Calif.: RAND Corporation, RR-4185-RC, 2020. As of June 30, 2021:
https://www.rand.org/pubs/research_reports/RR4185.html

White House, *Building Resilient Supply Chains, Revitalizing American Manufacturing, and Fostering Broad-Based Growth*, Washington, D.C., June 2021.

Wu, Debby, "Engineers Found Guilty of Stealing Micron Secrets for China," *Bloomberg*, June 12, 2020.

Wu, Debby, and Cindy Wang, "Taiwan Cuts Water Supply for Chipmakers as Drought Threatens to Dry Up Reserves," *Bloomberg*, March 24, 2021.

Yamazaki, Makiko, and Shinichi Saoshiro, "Japan Quakes Disrupt Sony Production of Image Sensors Used in Apple iPhones," Reuters, April 16, 2016.

Zerbib, G., "TowerJazz High Performance SiGe BiCMOS Processes," slides, presented at Common Technological Projects Between CERN and Israel, Weizmann Institute of Science, Rehovot, Israel, March 3, 2013.

About the Authors

Jared Mondschein is a physical scientist at the RAND Corporation. He focuses on a variety of national security and homeland security policy challenges, including supply chain risk management and defense modernization. Mondschein holds a Ph.D. in chemistry.

Jonathan W. Welburn is an operations researcher at RAND. He focuses on systemic risk in economic systems, supply chain risks, cyber security, and deterrence. Welburn holds a Ph.D. in decision science and operations research.

Daniel Gonzales is a senior scientist at RAND. His research focuses on command and control, communications, electronic warfare, cybersecurity, cloud computing, and cyber supply chain risk management. Gonzales holds a Ph.D. in theoretical physics.

Acknowledgments

We are sincerely thankful for the helpful feedback from Caolionn O'Connell, Meghan Biery, and Joel Predd and to Paul DeLuca, Christy Foran, Scott Harold, Chad Ohlandt, Edward Parker, Steven Popper, Richard Silberglitt, and Danielle Tarraf for the conversation that initiated this Perspective. We are also grateful for the helpful edits from Laurie Rennie.

About This Perspective

The ever-tightening financial constraints of semiconductor manufacturing have led to the business reality faced by U.S. consumers and leaders in 2021: The U.S. market share of global semiconductor manufacturing capacity has fallen from about 38 percent in 1990 to 12 percent in 2020 and is expected to decline to less than 10 percent by 2030. The growing realization of these economic trends and their implications for U.S. national and economic security has resulted in a national conversation and a growing chorus of academic, industry, and government stakeholders arguing for varying policy solutions. Out of this dialogue have emerged critical knowledge gaps that will hamper decisionmakers' ability to make informed policy. We have identified four high-priority questions that should drive U.S. policy but that require additional data and insights: Why are supply chain risk management strategies necessary to mitigate microelectronics supply chain disruptions? Does the U.S. Department of Defense (DoD) need access to the latest generation of microelectronics, or will a lag of several generations be acceptable to ensure trusted and reliable access to manufacturers and supply chains? How can DoD create a coordinated effort to mitigate microelectronics supply chain risk? What is the appropriate mix of policy levers to promote a microelectronics technology ecosystem that is aligned with U.S. strategic goals?

Although we recognize that this policy environment is rapidly evolving as new initiatives are announced and implemented and new data emerge, we believe that these four policy drivers will remain the foundation on which policy will be made over the long term. It is therefore vital to U.S. interests that the ongoing dialogue and policy conversations consider these four questions. This Perspective represents an initial attempt to explore these drivers and motivate future analyses.

The research reported here was completed in September 2021 and underwent security review with the sponsor and the Defense Office of Prepublication and Security Review before public release.

RAND National Security Research Division

This research was sponsored by the Office of the Secretary of Defense and conducted within the Acquisition and Technology Policy Center of the RAND National Security Research Division (NSRD), which operates the RAND National Defense Research Institute (NDRI), a federally funded research and development center (FFRDC) sponsored by the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the Navy, the Marine Corps, the defense agencies, and the defense intelligence enterprise.

For more information on the RAND Acquisition and Technology Policy Center, see www.rand.org/nsrd/atp or contact the director (contact information is provided on the webpage).

www.rand.org

PE-A1394-1