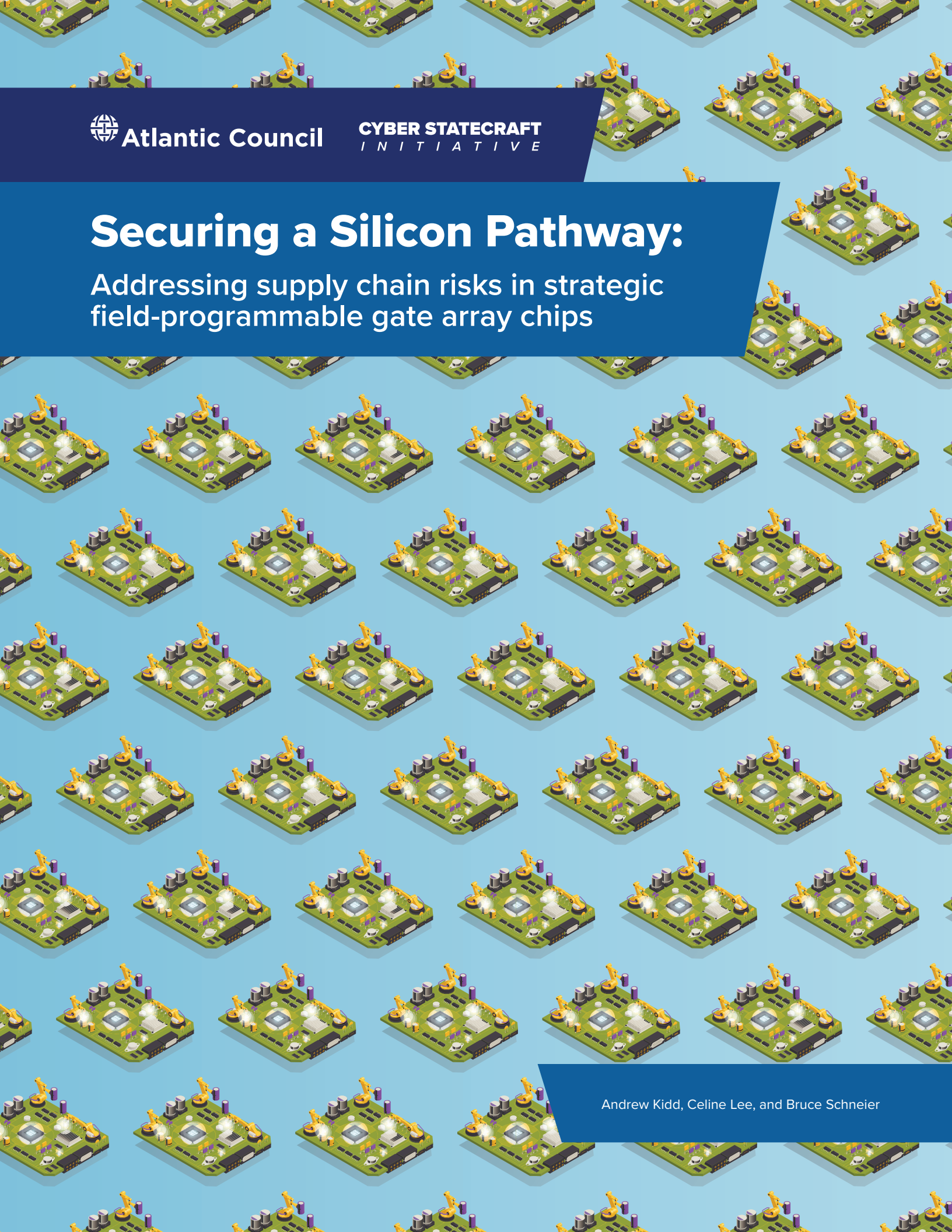


Atlantic Council

CYBER STATECRAFT INITIATIVE

Securing a Silicon Pathway:

Addressing supply chain risks in strategic field-programmable gate array chips

Andrew Kidd, Celine Lee, and Bruce Schneier

Atlantic Council

CYBER STATECRAFT INITIATIVE

The **Cyber Statecraft Initiative** works at the nexus of geopolitics, technology, and security to craft strategies to help shape the conduct of statecraft and to better inform and secure users. This work extends through the competition of state and non-state actors, the security of the internet and computing systems, the safety of operational technology and physical systems, and the communities of cyberspace. The Initiative convenes a diverse network of passionate and knowledgeable contributors, bridging the gap among technical, policy, and user communities.

Authors

Andrew Kidd
Celine Lee
Bruce Schneier

Cover: Adapted from graphic from Freepik.com

Please direct inquiries to:

Atlantic Council
1400 L Street NW, 11th Floor
Washington, DC 20005

2025

Table of contents

1. Executive summary

Field-programmable gate arrays (FPGAs) are specialized computer chips critical to the US economy and national security. FPGAs are vital components in American military systems like the Javelin anti-tank missile and F-35 fighter jet, American-built automobiles like Volvo's EX90, and cloud computing systems like Microsoft Azure. However, the supply chain for FPGA chips designed and used by US firms faces serious risks, particularly around cost, availability, and security, which have not been analyzed in depth from a policy perspective.

Contemporary analysis has largely focused on leading-edge logic chips, relying on assumptions about semiconductors that are not valid for FPGAs due to their unique flexibility and longevity.

This report analyzes the FPGA supply chain for US firms and the trade-offs these companies make among risks to cost, availability, and security; assesses how those trade-offs will change given a shifting global environment; and recommends policy interventions for the US government.

Overall, US firms tend to prioritize cost while significantly underinvesting in addressing substantial security and availability risks. Security risks are high given FPGAs' technical complexity. Availability risks are largely driven by geographic and supplier concentration. Over the medium term, the People's Republic of China's (PRC's) ongoing build-out of lagging-edge semiconductor manufacturing capacity will reduce FPGA costs, but this incremental boost in capacity will carry additional availability and security risks. In short, firms will continue prioritizing short-term costs and create negative externalities from availability and security risks.

US government intervention is required to build resilience against availability risks and develop technical measures that mitigate security risks, especially given increased PRC involvement in the FPGA supply chain. We recommend that the US government secure the US FPGA supply chain, protect critical national security capabilities and substantial economic industries, and continue to support American global technological leadership through four linked policy interventions:

1. Use existing government infrastructure as a **data-sharing and analytics hub** for FPGA supply chains to improve situational awareness and future policy interventions.
2. Invest in long-term efforts to **improve the technical security of FPGAs**.
3. Build **a stockpile of critical FPGAs** for military and commercial applications to provide bridge capacity in the event of supply disruptions.
4. Launch **cross-sector planning efforts for potential supply disruptions** to accelerate recovery.

These initiatives, coordinated by the Department of Commerce or Defense, should serve as a pilot for developing supply chain interventions for other critical technologies and industries.

2. Introduction

2.1 Problem statement

Semiconductors are critical to US national security and the economy. At the same time, the US semiconductor supply chain faces major economic and security vulnerabilities. These deficiencies have resulted in a flurry of (imperfect) legislation and policies in recent years, most notably the 2022 CHIPS and Science Act passed by Congress. However, specialized semiconductors like field-programmable gate arrays (FPGAs) have received much less policy attention despite their equality importance to US national interests.

Unfortunately, these recent US policies for semiconductors have ignored this market segment, assuming that the vulnerabilities and strengths in other semiconductor markets apply to specialized silicon. Export control discussions focus on leading-edge graphics processing units (GPUs) and the advanced manufacturing equipment needed to make them. Supply chain resiliency efforts often assume that all chips become obsolete as quickly as those leading-edge logic chips.

FPGAs are critical in many important applications. For example, the American military's advanced F-35 fighter jet and its FGM-148 Javelin anti-tank missile depend on FPGAs and other specialized semiconductors, particularly for guidance and control systems.[1] FPGAs are not only deployed in military equipment—they are also critical to most American automobiles and telecommunications networks. The electric EX90 SUVs Volvo assembles in North Carolina rely on FPGAs for their advanced driver assistance systems,[2] while AT&T relies on FPGAs in Nokia equipment to operate their 5G network.[3]

Unlike traditional leading-edge logic chips, FPGAs offer hardware-level flexibility, because the physical circuitry on an FPGA can be re-designed after they leave the factory. As a result, individual FPGAs often remain in production for over 20 years.[4] FPGAs offer a unique mix of customization and performance, meaning they cannot easily be replaced.

Today's policy debates lack the nuance to address specialized silicon and its unique characteristics. As a result, the FPGA supply chain has yet to be analyzed in depth, despite substantial differences from the overall semiconductor supply chain.

This report will address three key questions:

1. What are the **key risks** in the FPGA supply chain for US firms and **what trade-offs do firms make** between those risks?
2. **Are effective mitigations and adaptations in place** to address these risks?
3. Which **policy interventions** should the US government take to address these risks?

1 US Department of Defense, "Contracts for November 19, 2018," US Department of Defense, November 19, 2018, https://www.defense.gov/News/Contracts/Contract/Article/1694434/https%3A%2F%2Fwww.defense.gov%2FNews%2FContracts%2FContract%2FArticle%2F1694434%2F%2F; DePeng Kong, QingZhong Jia, and Hong Xu, "The Design of an Integrated Guidance and Control Computer System Based on Multi-Core DSP and FPGA," in *2015 8th International Congress on Image and Signal Processing (CISP)*, 2015, 1625–29, https://doi.org/10.1109/CISP.2015.7408145; Military Aerospace, "Navy Orders Diminishing Manufacturing Sources (DMS) FPGAs to Keep F-35s and Other Military Aircraft Flying," Military Aerospace, November 20, 2018, https://www.militaryaerospace.com/computers/article/16726578/navy-orders-diminishing-manufacturing-sources-dms-fpgas-to-keep-f-35s-and-other-military-aircraft-flying; *Why the Javelin Missile Guidance Computer Uses FPGAs*, 2023, https://www.youtube.com/watch?v=x-pNDYCTqbDY.

2 Joe Lorio, "2025 Volvo EX90 SUV Is an Emphatic Entry into the Electric Era," *Car and Driver*, May 11, 2023, https://www.caranddriver.com/news/a41897699/volvo-ex90-ev-revealed/; "Luminar Day: A New Era – Luminar Achieves Global Start of Production for Volvo Cars," Luminar Technologies, Inc., April 23, 2024, https://investors.luminartech.com/news-events/press-releases/detail/87/luminar-day-a-new-era-luminar-achieves-global-start-of; "Deep Dive Teardown of the Luminar Technologies Iris LiDAR 70-0034-00102203A15650 Automotive | TechInsights," TechInsights, accessed June 25, 2025, https://www.techinsights.com/products/ddt-2306-807?utm_source=direct&utm_medium=website.

3 Bevin Fletcher, "Nokia Highlights Turnaround with New 5G RAN Gear | Fierce Network," *Fierce Network*, June 24, 2021, https://www.fierce-network.com/5g/nokia-highlights-turnaround-new-5g-ran-portfolio; "Nokia Supports 5G for AT&T Customers with Five-Year C-Band Deal," GlobeNewswire, March 18, 2021, https://www.globenewswire.com/news-release/2021/03/18/2195265/0/en/Nokia-supports-5G-for-AT-T-customers-with-five-year-C-Band-deal.html; "AirScale Radio Access," Nokia, accessed June 25, 2025, https://www.nokia.com/mobile-networks/ran/macro/.

4 Semiconductor industry participant #1, interview with the authors, November 25, 2024.

The FPGA supply chain for US firms is the collection of such networks that involve US firms as suppliers, designers, manufacturers, or customers of FPGAs.[5] A *key risk* is a supply chain risk with sufficient likelihood or impact on the American economy or national security to merit policy intervention from the US government.

2.2 Policy significance

FPGAs differ from other logic chips in two fundamental ways. First, their hardware can effectively be reconfigured after they leave the factory. This capability creates flexibility and allows customers to redeploy FPGA chips between different applications with minimal difficulty. A single FPGA chip could be repurposed for many contexts over its lifetime. Second, this flexibility significantly extends FPGA product lifecycles, which often last 20 years or more.[6] In contrast, rapid product development cycles often quickly render other semiconductors obsolete.

Despite a relatively small market size of approximately $10 billion,[7] FPGAs play critical roles in the development and deployment of modern AI models, military equipment, telecommunications infrastructure, and automotive sectors. Any disruption to the cost, availability, or security of US FPGAs would have substantial negative impacts across these sectors.

These factors mean that the FPGA supply chain is fundamentally different than the broader semiconductor supply chain and requires distinct policies, particularly given China's growing capabilities in legacy-node semiconductors and FPGAs.[8]

Today, US policymakers hold largely untested assumptions regarding FPGA supply chain risks, mitigations, and adaptations. In particular, policymakers assume:

1. Semiconductor security vulnerabilities for non-military applications (i.e., commercial or consumer) are less critical than for military applications[9]
2. Onshoring leading-edge logic chip manufacturing ensures sufficient semiconductor supply chain availability (e.g., with the CHIPS and Science Act's $52 billion investment)[10]
3. The US government can exert sufficient influence and/or control over foreign firms to ensure the semiconductor supply chain meets:[11]
    a. US customers' economic needs for availability and cost-effectiveness[12]
    b. The US government's national security interest in secure and reliable semiconductors[13]

5 Mark L. Fagan, *Supply Chain Management: A Public Sector Perspective* (Northampton: Edward Elgar Publishing, 2024).

6 Semiconductor industry participant #2, interview with the authors, December 6, 2024.

7 "From Invention to AI Acceleration: Celebrating 40 Years of FPGA Innovation," AMD, February 6, 2025, https://www.amd.com/en/blogs/2025/from-invention-to-ai-acceleration--celebrating-40-years-of-fpga-.html.

8 Wen-Yee Lee, "Taiwan's Legacy Chip Industry Contemplates Future as China Eats into Share," *Reuters*, February 10, 2025, https://www.reuters.com/technology/taiwans-legacy-chip-industry-contemplates-future-china-eats-into-share-2025-02-10/; Celine Lee, Andrew Kidd, and Bruce Schneier, "Reprogramming the Future: The Specialized Semiconductors Reshaping the Global Supply Chain," Atlantic Council, June 11, 2025, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/reprogramming-the-future-the-specialized-semiconductors-reshaping-the-global-supply-chain/.

9 While the US government has developed non-binding security guidance such as the NIST Cybersecurity Framework for Semiconductor Manufacturing, official policies continue to de-emphasize non-military security vulnerabilities.

10 "CHIPS and Science Act, H.R. 4346, 117th Cong. (2022)," Pub. L. No. 117–167 (2022), https://www.congress.gov/bill/117th-congress/house-bill/4346/text.

11 "Critical and Emerging Technologies List Update," Office of Science and Technology Policy, February 2024; Bureau of Industry and Security, "Export Controls on Semiconductor Manufacturing Items," October 25, 2023, https://www.federalregister.gov/documents/2023/10/25/2023-23049/export-controls-on-semiconductor-manufacturing-items; "Implementation of Additional Due Diligence Measures for Advanced Computing Integrated Circuits; Amendments and Clarifications; and Extension of Comment Period," Bureau of Industry and Security, January 16, 2025, https://www.federalregister.gov/documents/2025/01/16/2025-00711/implementation-of-additional-due-diligence-measures-for-advanced-computing-integrated-circuits; "Implementation of Additional Export Controls: Certain Advanced Computing and Semiconductor Manufacturing Items; Supercomputer and Semiconductor End Use; Entity List Modification," Bureau of Industry and Security, October 13, 2022, https://www.federalregister.gov/documents/2022/10/13/2022-21658/implementation-of-additional-export-controls-certain-advanced-computing-and-semiconductor

12 Nicola Stoev, "CHIPS Act Wins the Battle, But Not the Semiconductor War," *Geopolitical Monitor*, June 3, 2024, https://www.geopoliticalmonitor.com/chips-act-wins-the-battle-but-not-the-semiconductor-war/; "CHIPS Act Update: Latest Insights on Innovation and Science," Center Forward Basics (Washington, DC, February 28, 2025), https://center-forward.org/basic/chips-act-update-latest-insights-on-innovation-and-science/.

13 Christine Mui, "What's Really inside a Secret Chips Project," *POLITICO*, May 8, 2024, https://www.politico.com/newsletters/digital-future-daily/2024/05/28/whats-really-inside-a-secret-chips-project-00160233.

These assumptions may not hold for FPGAs, whose unique characteristics and expanding strategic importance expose gaps in current US policy. Addressing these risks requires tailored approaches that account for the distinct role FPGAs play in both commercial and national security applications.

2.3 Supply chain risk framework

Supply chain risks are those that threaten the *cost*, *availability*, or *security* of FPGA chips designed and sold by US firms, used by US firms in other products or services, or used by American end-users. US firms face three primary categories of risk when sourcing FPGAs:

- **Cost risk** includes both certain and potential costs that may be incurred both today and in the future. For example, selecting a higher-priced vendor to avoid vendor lock-in creates certain immediate costs. In contrast, accepting vendor lock-in by designing equipment or chips to align with a specific vendor's products creates potential future costs if the vendor raises prices. Both of these risks are included as cost risks.[14] *Manufacturing quality* is also a part of cost risk.[15,16]
- **Availability risk** includes all risks that could limit the ability of US firms to acquire FPGAs. The two main availability risks are "*can't make*" and "*won't sell*" risks. "Can't make" risks include scenarios where suppliers or manufacturers no longer have the capacity to produce FPGA chips or required inputs. For example, a major earthquake in Taiwan could damage foundries and prevent manufacturers from producing FPGAs. "Won't sell" risks include scenarios where sufficient production capacity exists, but firms choose not to supply FPGAs to the US market. Those decisions could be caused by individual firms prioritizing higher-margin products or government regulation.
- **Security risk** includes all scenarios that reduce customers' confidence that the FPGAs will do only what customers expect.[17] Security risks include deliberate and unintentional failures to meet product specifications, particularly security specifications. For example, analysts recently identified undocumented communication devices in PRC-made power inverters, raising alarms over possible foreign access to US energy systems.[18] Similar security risks could be introduced to FPGAs through hardware, gateware (see more below), or related software.

Managing supply chain risks requires making trade-offs, typically along an "efficient frontier" where the only way to reduce one risk is to increase another.[19] These supply chain risks are deeply interrelated. For example, operating redundant distribution networks (e.g., warehouses, trucks) will reduce availability risk but increase cost risk.

In this model, government interventions to address FPGA supply chain risks can take two forms:

1. **Change the trade-offs:** Incentivize firms to make different trade-off decisions along the frontier (e.g., reducing security risk and increasing cost risk)

2. **Change the game:** Change the shape of the efficient frontier by implementing structural shifts (e.g., developing novel, low-cost solutions to security risks, imposing tariffs to increase cost of producing in some geographies)

14 Analytically, we construct our measure of cost risk as the net present value of all expected costs, where an expected cost is defined as the size of the financial cost multiplied by the estimated probability the cost will be incurred. This includes certain and potential costs in the present and in the future.

15 In modern manufacturing environments with intensive quality assurance and control programs, low-quality products are typically identified during the manufacturing process and not sold to customers, so manufacturing quality's primary impact is on cost efficiency.

16 Adriana Aragon et al., "Manufacturing Quality Today: Higher Quality Output, Lower Cost of Quality," McKinsey & Company, September 28, 2017, https://www.mckinsey.com/capabilities/operations/our-insights/manufacturing-quality-today-higher-quality-output-lower-cost-of-quality.

17 Paul Rosenzweig et al., "Creating a Framework for Supply Chain Trust in Hardware and Software," Lawfare, May 2022, https://www.lawfaremedia.org/article/how-can-one-know-when-trust-hardware-and-software.

18 Sarah Mcfarlane, "Rogue Communication Devices Found in Chinese Solar Power Inverters," *Reuters*, May 14, 2025, sec. Climate & Energy, https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/.

19 This model assumes that firms are already operating at the efficient frontier and have taken any actions that could improve one form of supply chain risk without affecting other risks.

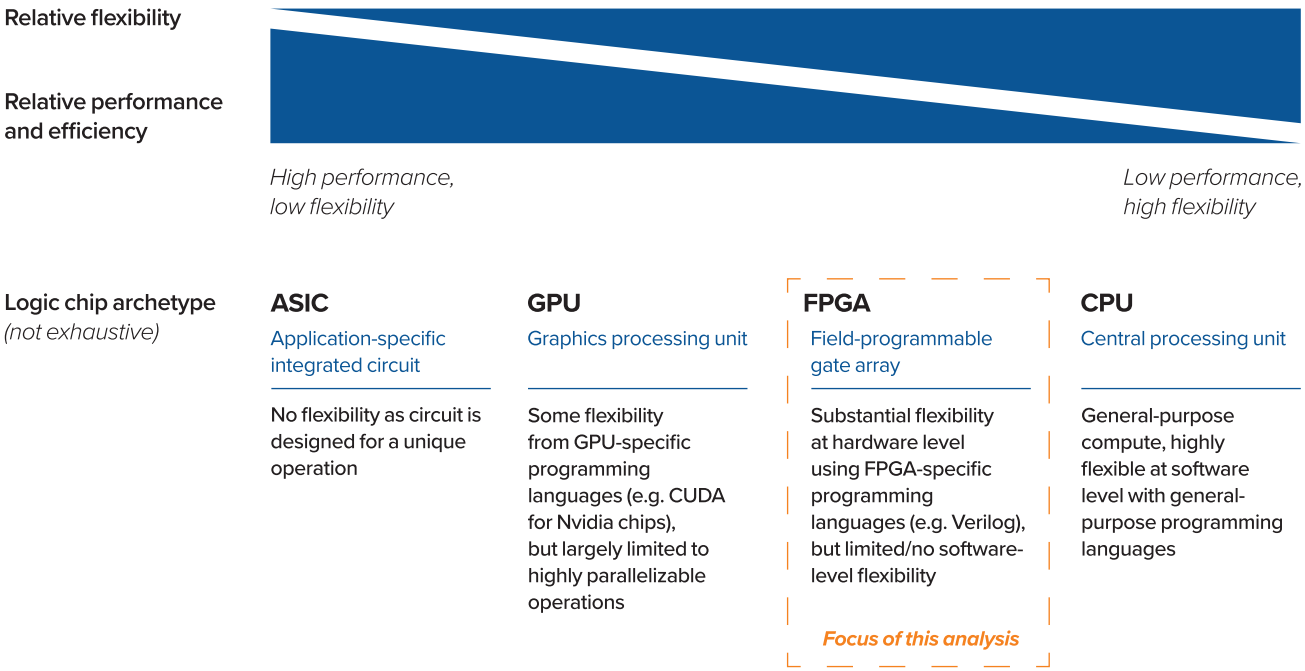
3. Field-programmable gate arrays (FPGAs)

3.1 FPGA overview

Field-programmable gate arrays (FPGAs) are used in diverse applications because they offer more flexibility and longevity than other logic chips.

FPGAs occupy a middle ground. They are somewhat flexible and can be reconfigured to execute different operations once manufactured, but with less performance or efficiency than ASICs.[20] FPGAs are reconfigured by loading specialized code onto the chip that describes the active physical connections and logic elements in the chip. This code, called gateware,[21] effectively transforms the FPGA into a new, custom-designed circuit, eliminating the need to manufacture new physical chips when responding to evolving requirements. As a result, FPGAs are typically used for workloads that require higher performance or efficiency than a general-purpose logic chip can provide, but that do not have the volume of demand to justify designing and manufacturing a custom ASIC chip. FPGAs are often used for research and development (R&D) as well as early versions of products. As production volume increases and unit economics shift, FPGAs

Figure 1: Chip archetypes mapped by performance and flexibility



As shown in Figure 1, there are four types of logic chips, which form a spectrum trading off performance and efficiency for flexibility. Central processing units (CPUs), like those in consumer laptops, represent one extreme as highly flexible semiconductors that perform a wide variety of tasks, but with relatively low performance or efficiency. On the other extreme are application-specific integrated circuits (ASICs), which can perform only the specific operations for which they were designed, but with relatively high performance or efficiency.

20 Timothy Prickett Morgan, "Intel To Broaden FPGA Lineup And Make Them At Home," *The Next Platform*, September 27, 2022, https://www.nextplatform.com/2022/09/27/intel-to-broaden-fpga-lineup-and-make-them-at-home/.

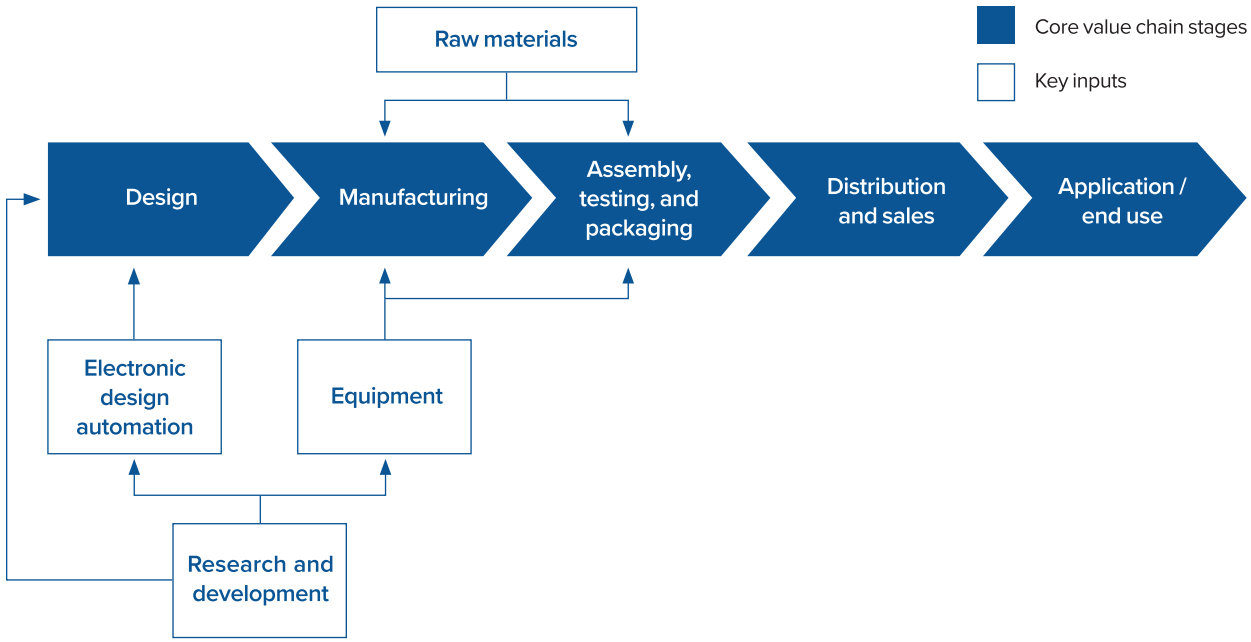
21 Practitioners use a variety of terms to refer to the hardware description language statements that define the configuration of an FPGA, including gateware, software, and firmware. For clarity, we use gateware throughout this report.

can be replaced by ASICs or CPUs in future product generations to optimize cost, performance, or power efficiency.[22]

FPGAs have a long working life and correspondingly long production lifecycles—often five to twenty-five years.[23] This longevity is due in part to FPGAs' flexibility, which allows for repurposing older FPGAs for novel tasks.[24] As such, the FPGA market is substantially less cyclical than other segments of the semiconductor market.[25] Most FPGAs on the market today are produced at legacy process nodes, typically between 16nm and 28nm.[26] In comparison, leading edge semiconductor production takes place at the 3nm process node, as of mid-2025.[27]

While alternative semiconductors exist, their adaptability and performance are insufficient compared to FPGAs. However, despite FPGAs' critical applications across sectors, they are only a small component of the broader semiconductor market. FPGAs have an estimated market size of roughly $10 billion,[28] which represents approximately 0.02 percent of the approximately $697.2 billion global semiconductor industry.[29]

Figure 2: An overview of the semiconductor value chain, from initial design through end use



22 FPGA engineer, interview with the authors, March 6, 2025.

23 Semiconductor industry participant #2, interview with the authors, December 6, 2024.

24 Ibid.Ibid.

25 Ibid.

26 Semiconductor industry experts, private FPGA policy roundtable, February 6, 2025.

27 Anton Shilov, "TSMC's 2nm N2 Process Node Enters Production This Year, A16 and N2P Arriving next Year," Tom's Hardware, April 24, 2025, https://www.tomshardware.com/tech-industry/tsmcs-2nm-n2-process-node-enters-production-this-year-a16-and-n2p-arriving-next-year.

28 AMD Adaptive Computing, "From Invention to AI Acceleration."

29 "2025 SIA Factbook," Semiconductor Industry Association, May 2025, 5, https://www.semiconductors.org/wp-content/uploads/2025/05/2025-SIA-Factbook-FINAL-1.pdf.

The semiconductor industry is highly globalized and concentrated, with clear leading countries and firms at most stages of the value chain.[30] We use the value chain model described in Figure 2 to analyze the FPGA industry,[31] focusing our analysis on four categories of participants:

Category	Definition	Examples
Suppliers	Providers of electronic design automation (EDA) software, semiconductor manufacturing equipment known as wafer fabrication equipment (WFE), and raw materials	ASML, Synopsys, Cadence
Chip designers	FPGA design firms, typically lacking their own manufacturing facilities	Altera, AMD (Xilinx)
Manufacturers	Firms that manufacture, package, test, and assemble FPGAs	TSMC, GlobalFoundries
End customers	Individuals or firms that use FPGAs or systems/ devices that include FPGAs	Ford, Microsoft

3.2 FPGA applications

AI, cloud, and data centers

FPGAs are often used as accelerators to supplement general-purpose logic chips for compute-intensive workloads in data center contexts, including AI model training and inference. FPGAs can provide parallel processing capabilities[32] for neural network inference, which can reduce latency and power consumption compared to traditional CPU or GPU solutions for some algorithms.[33] For other cloud-based workloads, cloud service providers often integrate FPGAs into their data center architectures. For example, Microsoft has installed FPGAs in most Azure data centers.[34] More broadly, FPGAs often underpin software-based networking approaches in data centers.[35] Given the integration of FPGAs and other semiconductors—particularly GPUs—in the AI context, FPGAs should be considered as a critical component of overall AI and semiconductor strategy.

Many FPGA customers in AI, cloud, and data centers are less price-sensitive, limiting the impact of cost risks.[36] However, availability risks could create economic harm, particularly as AI models

30 "Advanced Semiconductor Supply Chain Dataset (2022 Release)," Emerging Technology Observatory, 2022, https://eto.tech/dataset-docs/chipexplorer; Chris Miller, *Chip War: The Fight for the World's Most Critical Technology* (New York: Scribner, 2022);"2022 State of the U.S. Semiconductor Industry," Semiconductor Industry Association (SIA), November 2022,, https://www.semiconductors.org/wp-content/uploads/2022/11/SIA_State-of-Industry-Report_Nov-2022.pdf; Han-kii Yeo, Chris Miller, and Nick Montella, US Trade, Industrial, and Econ Security Policies & Semiconductor Supply ChainsCambridge, MA, November 12, 2024

31 Michael E. Porter, *Competitive Advantage: Creating and Sustaining Superior Performance* (New York : London: Free Press ; Collier Macmillan, 1985); "Porter's Value Chain," Institute for Manufacturing - University of Cambridge, accessed January 21, 2025, https://www.ifm.eng.cam.ac.uk/research/dstools/value-chain-/; Antonio Varas et al., "Strengthening the Global Semiconductor Supply Chain in an Uncertain Era," Semiconductor Industry Association (SIA) and Boston Consulting Group (BCG), April 1, 2021, https://www.semiconductors.org/strengthening-the-global-semiconductor-supply-chain-in-an-uncertain-era/; "Advanced Semiconductor Supply Chain Dataset (2022 Release)."

32 Parallel processing capabilities refer to the ability to perform multiple operations or tasks simultaneously.

33 "FPGAs for Artificial Intelligence (AI)," Intel, accessed January 23, 2025, https://www.intel.com/content/www/us/en/learn/fpga-for-ai.html; Amelia Smith, "Spotlight: The Latest FPGA Technology in 2024, Microchip USA, October 16, 2024, https://www.microchipusa.com/electrical-components/spotlight-the-latest-fpga-technology-in-2024/.

34 Jakub Szefer, "Cloud FPGA Infrastructures: Microsoft and IBM," https://caslab.csl.yale.edu/courses/EENG428/current/slides/eeng428-lecture-22-cloud-fpga-concepts-review.pdf.

35 Examples include Network Function Virtualization (NFV) and software-defined networking (SDN).

36 FPGA engineer, interview with the authors.

are deployed throughout the American economy. Security risks could also threaten economic harm and disrupt US technological leadership in AI development.

Military equipment and defense systems

FPGAs are extensively used in radar systems, electronic warfare equipment, and secure communications platforms, providing advanced signal processing and encryption capabilities.[37] The versatility and reprogrammable capabilities of FPGAs mitigate hardware obsolescence in defense systems by reducing the frequency and associated costs of hardware replacements,[38] making military customers relatively price-insensitive.[39] However, both availability and security risks in FPGAs could create major gaps in American security capabilities, particularly those involving missile guidance systems.

Telecommunications

FPGAs are often critical components in telecommunications infrastructure, where they excel in two principal areas. First, FPGAs deliver strong performance in signal processing tasks, allowing 5G networks to handle large volumes of data with minimal delays.[40] For example, 5G networks rely on FPGAs for multiple input/multiple output (MIMO) systems, which improve connection quality and speed by dynamically adjusting wireless signals.[41] Second, the reprogrammable nature of FPGAs allows telecommunications providers to reprogram the chips to adhere to evolving network standards, protocols, or applications.[42] Telecommunications infrastructure typically involves low margins and carries critical information, heightening the impact of cost and security risks respectively. [43] However, as telecommunications infrastructure is generally not replaced on an ongoing basis, the impact of availability risks is likely more limited.

Automobiles

FPGAs are fundamental to modern automobiles. In advanced driver assistance systems, FPGAs process data from multiple sensors (e.g., cameras, radar) to enable safety features like lane keeping and collision avoidance, while also integrating various sensor inputs for autonomous driving decisions.[44] FPGAs also power in-vehicle entertainment systems by managing video interfaces and multimedia features, performing tasks like video decoding, image rendering, and audio processing.[45] In electric vehicles, FPGAs often implement specialized control algorithms and execute complex computations to enhance power management by optimizing battery efficiency,[46] controlling power

37 "High-Performance FPGAs for Military, Aerospace, and Government," Intel, accessed January 23, 2025, https://www.intel.com/content/www/us/en/fpga-solutions/military-aerospace-government/overview.html.

38 Ibid.

39 Semiconductor industry participant #2, interview with the authors, December 6, 2024.

40 "FPGA Development Boards for Telecommunications," Conduant Corporation, May 23, 2024, https://conduant.com/articles/fpga-development-boards-for-telecommunications/; "Throughput vs Latency - Difference Between Computer Network Performances," Amazon Web Services, Inc., accessed January 22, 2025, https://aws.amazon.com/compare/the-difference-between-throughput-and-latency/.

41 Muthukumaran Vaithianathan et al., "FPGA-Based Adaptive Beamforming System for Improved Wireless Communication Performance, in *2024 Asian Conference on Intelligent Technologies (ACOIT)*, 2024, https://www.researchgate.net/publication/385281146_FPGA-Based_Adaptive_Beamforming_System_for_Improved_Wireless_Communication_Performance.

42 "Four Key Trends in the Networked Use of FPGAs," Arista, December 20, 2018), https://www.arista.com/assets/data/pdf/Whitepapers/Trends-in-FPGA-WP.pdf.

43 John Hendel, "Why Suspected Chinese Spy Gear Remains in America's Telecom Networks," *POLITICO*, July 21, 2022, https://www.politico.com/news/2022/07/21/us-telecom-companies-huawei-00047045; Ellen Nakashima, "U.S. Pushes Hard for a Ban on Huawei in Europe, but the Firm's 5G Prices Are Nearly Irresistible," *The Washington Post*, May 29, 2019, https://www.washingtonpost.com/world/national-security/for-huawei-the-5g-play-is-in-europe--and-the-us-is-pushing-hard-for-a-ban-there/2019/05/28/582a8ff6-78d4-11e9-b7ae-390de4259661_story.html.

44 Bob O'Donnell, "FPGAs Are Essential Building Blocks for Next-Gen Automotive Designs," Lattice Semiconductor, January 3, 2024, https://www.latticesemi.com/en/Blog/2024/02/29/19/41/FPGAs-Are-Essential-Building-Blocks-for-Next-Gen-Automotive-Designs; Monica Sachdev, "What Is Sensor Fusion for Autonomous Driving Systems? – Part 1," RGBSI, accessed January 22, 2025, https://blog.rgbsi.com/sensor-fusion-autonomous-driving-systems-part-1.

45 O'Donnell, "FPGAs Are Essential Building Blocks for Next-Gen Automotive Designs."

46 Sakthi Sundaram S et al., "Design and Development of DSP-FPGA Based Control Board for Electric Vehicle (EV) Applications," in *2022 Second International Conference on Power, Control and Computing Technologies (ICPC2T)*, 2022, 1–6, https://doi.org/10.1109/ICPC2T53885.2022.9777061."container-title":"2022 Second International Conference on Power, Control and Computing Technologies (ICPC2T

distribution,[47] and enabling sophisticated charging systems.[48] FPGA reconfigurability also allows automobile manufacturers to update and upgrade systems to increase efficiency, security, and safety throughout the vehicle lifecycle.[49] The automotive industry would face substantial economic impacts from cost and availability risks, as seen during the COVID-related automobile chipset shortage.[50] There are also emerging security concerns related to automobile software and hardware,[51] including risks from FPGAs.

47 Sundaram S et al."container-title":"2022 Second International Conference on Power, Control and Computing Technologies (ICPC2T

48 T Porselvi et al., "FPGA Based Power Quality Improvement of Grid Connected EV Battery System," in *2023 4th International Conference on Signal Processing and Communication (ICSPC)*, 2023, 400–405, https://doi.org/10.1109/ICSPC57692.2023.10125991.

49 Mark Hoopes, "Programmable Protection: How FPGAs Are Shaping the Future of Automotive Safety," Electronic Design, November 4, 2024, https://www.electronicdesign.com/technologies/embedded/digital-ics/fpga/article/55240420/lattice-semiconductor-automotive-and-functional-safety-fpgas-offer-programmable-protection.

50 Fagan, *Supply Chain Management*.

51 David Shepardson, "Biden Administration Finalizes US Crackdown on Chinese Vehicles," *Reuters*, January 14, 2025, https://www.reuters.com/business/autos-transportation/biden-administration-finalizes-us-crackdown-chinese-vehicles-2025-01-14/.

4. FPGA risk analysis

As described in Section 2.3, we focus our analysis on FPGA cost, availability, and security risks. We consider each type of risk across the FPGA value chain outlined in Section 3.2, then examine the trade-off decisions firms make between risks. Figure 3 shows which supply chain risks are most relevant for each stage of the FPGA value chain.

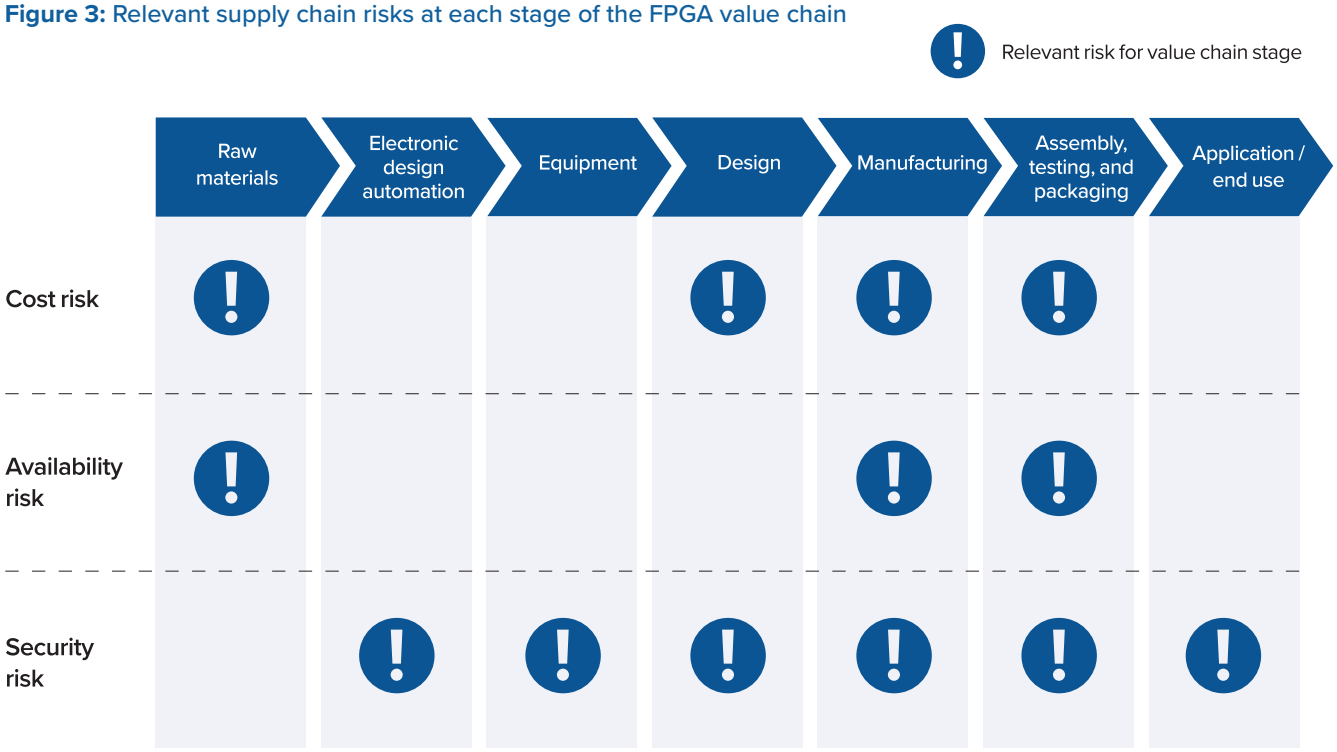
4.1 Cost

The FPGA supply chain faces four key drivers of cost risk:

1. Potential US government tariffs on semiconductor imports[52]
2. Short- and medium-term shortages in some key input materials
3. Medium- and long-term impacts of climate change
4. Medium-term increases in lagging-edge production capacity place downwards pressure on costs

First, recent proposals to impose tariffs on imported semiconductors have encountered widespread pushback from a broad spectrum of industries.[53] As the United States holds only an approximate 12 percent share of the overall semiconductor manufacturing market and less in assembly, testing, and packaging (ATP),[54] any tariffs would have broad impacts across the industry. Most manufacturing and assembly, testing, and packaging in the US FPGA supply chain also take place outside the country, meaning semiconductor import tariffs would substantially increase FPGA costs across the manufacturing and ATP stages of the value chain.

Figure 3: Relevant supply chain risks at each stage of the FPGA value chain



52 Ana Swanson and Tony Romm, "Trump Moves to Put New Tariffs on Computer Chips and Drugs," *The New York Times*, April 14, 2025, https://www.nytimes.com/2025/04/14/business/economy/trump-semiconductor-tariffs-china.html.

53 Michael Shepard, "Trump's Chip Tariff Threat Sparks Pushback From Auto Industry to Tech," *Bloomberg*, June 24, 2025, https://www.bloomberg.com/news/articles/2025-06-24/trump-s-chip-tariff-threat-sparks-pushback-from-us-auto-tech-companies.

54 Varas et al., "Strengthening the Global Semiconductor Supply Chain in an Uncertain Era," 5.

Second, increasing competition between the United States and the PRC raises the likelihood of further PRC restrictions on critical minerals, particularly given China's history of using its critical mineral supply as a geopolitical tool.[55] China dominates the market for several critical minerals that are essential inputs for FPGA manufacturing, particularly refined gallium, where it controls about 99 percent of the market.[56,57] Leveraging this dominance, China banned all exports of gallium to the United and imposed more stringent licensing requirements for other critical minerals in April 2025.[58] PRC restrictions have led to significant price increases, with the price of gallium alone rising 80 percent since December 2024.[59] While other countries could step in to provide additional gallium for the semiconductor industry, prices may remain elevated or increase further before production can scale.

Third, over the medium- and long-term, climate change creates mitigation and adaptation costs for suppliers, chip designers, and manufacturers. Semiconductor firms are likely to continue at least some investment in mitigation efforts and manufacturers will continue to face operational disruptions from the impacts of climate change, which will increase their cost structure to account for mitigation response and adaptation.

Fourth, our research indicates that the PRC is launching a major build-up of capacity at older, lagging-edge process nodes of semiconductor manufacturing, including substantial state investments in FPGA chipmakers.[60] Big Fund investments in PRC FPGA firms like Anlogic provide early indicators that FPGAs are a focus area for the PRC.[61] According to Jeremy Mark, Senior Fellow with the GeoEconomics Center of the Atlantic Council, there is "no evidence that there is a slacking of [Chinese] investments and commitment of resources toward semiconductors and SMEs [as] its technology growth strategy, particularly in AI, requires semiconductors."[62]

The PRC is also developing FPGA-specific design capabilities. PRC FPGA firms including Anlogic, Gowin Semiconductor, and Pango Microsystems have received substantial government support as they develop competitive portfolios, beginning at the low end of the segment.[63] These firms provide the PRC's semiconductor and AI ecosystems with critical FPGA capabilities—for example, Pango is now the largest FPGA supplier to Huawei.[64]

This growing FPGA manufacturing capacity will allow firms to produce FPGAs at lower costs than the current market, but this incremental capacity will likely come with higher availability and security risks than most of today's capacity. This will increase the effective cost of reducing availability and security risks in the FPGA supply chain.

Given the scale of PRC investments in lagging-edge manufacturing capacity overall and in FPGAs in particular, the resulting downward cost pressure will outweigh input-based and climate impacts on costs, driving FPGA costs down overall in the medium

55 Seaver Wang, Peter Cook, and Lauren Teixeira, "How Should We Interpret Chinese Critical Mineral Export Restrictions?," The Breakthrough Institute, accessed January 22, 2025, https://thebreakthrough.org/issues/energy/how-should-we-interpret-chinese-critical-mineral-export-restrictions.

56 While PRC export controls have often included both gallium and germanium, germanium is used much less extensively for FPGAs.

57 Amy Lv and Tony Munroe, "China Bans Export of Critical Minerals to US as Trade Tensions Escalate," *Reuters*, December 3, 2024, https://www.reuters.com/markets/commodities/china-bans-exports-gallium-germanium-antimony-us-2024-12-03/.

58 Gracelin Baskaran and Meredith Schwartz, "China Imposes Its Most Stringent Critical Minerals Export Restrictions Yet Amidst Escalating U.S.-China Tech War," December 4, 2024, https://www.csis.org/analysis/china-imposes-its-most-stringent-critical-minerals-export-restrictions-yet-amidst; "China Restricts Exports of Rare Earths and Other Minerals. How Does the System Work?," *Reuters*, April 24, 2025, https://www.reuters.com/world/china/china-is-restricting-mineral-exports-how-does-its-export-control-system-work-2025-04-24/; State Council of the People's Republic of China, "Regulations of the People's Republic of China on Export Control of Dual-Use Items," Pub. L. No. 792 (2024), https://www.gov.cn/zhengce/content/202410/content_6981399.htm"China Released the First Comprehensive Dual-Use Items Export Control Regulations," Squire Patton Boggs, November 2024, https://www.squirepattonboggs.com/-/media/files/insights/publications/2024/11/china-released-the-first-comprehensive-dual-use-items-export-control-regulations/china_released_dual-use_items_.pdf?rev=12f6bc0033914f37a9ee38f43c4ee0a6&sc_lang=en&hash=BBB7707AFC66F5010C8111266B99ABBA.

59 Archie Hunter and Mark Burton, "What Are Gallium and Germanium? The Niche Metals Hit by China's Export Ban," *Bloomberg*, December 3, 2024, https://www.bloomberg.com/news/articles/2024-12-03/china-gallium-and-germanium-us-export-ban-why-metals-are-key-in-trade-war.

60 Lee, Kidd, and Schneier, "Reprogramming the Future."

61 Wu XinZhu, "Where are the investment opportunities in the semiconductor industry chain?," June 11, 2024, https://finance.sina.com.cn/wm/2024-06-11/doc-inaykeac8310123.shtml.

62 Jeremy Mark, 2025.

63 Lee, Kidd, and Schneier, "Reprogramming the Future."

64 "The most popular domestic FPGA chip of the year, Sina, November 20, 2024, https://finance.sina.com.cn/jjxw/2024-11-20/doc-incwspwu2211604.shtml.

term. However, considering the uncertainty of US semiconductor tariffs and the timing of PRC capacity coming online, FPGA costs may increase temporarily in the short term as costs increase for the raw materials, manufacturing, and ATP stages.

Overall, the impact of increased cost risks for the US FPGA supply is moderate. Major defense firms and the US military are largely price-inelastic customers and would likely absorb any cost increases.[65] For commercial applications, our analysis suggests a substantial ability to absorb FPGA price increases. Using electric vehicles as an example of commercial use of FPGAs, we conducted a tear-down analysis of Tesla's financial statements.[66] Our findings suggest that Tesla could absorb approximately a five-fold price increase in FPGA components while breaking even on a gross margin basis.[67]

4.2 Availability

The FPGA supply chain faces two principal availability risks, "*can't make*" and "*won't sell,*" which affect the sourcing of raw materials, manufacturing, and ATP. "*Can't make*" risks include scenarios where suppliers or manufacturers no longer have the capacity needed to produce FPGA chips or required inputs. "*Won't sell*" risks include scenarios where the capacity exists, but firms choose not to supply FPGAs to the US market, either due to governments regulating firms' activities or individual firms prioritizing higher-profit opportunities elsewhere in the semiconductor market.

"Can't Make" risks

Industry concentration—including suppliers, manufacturers, and geographies more broadly—fosters several "can't make" risks. For example, ASML, the only supplier of the "extreme ultraviolet lithography" equipment needed to manufacture leading-edge chips and a leader in less-advanced lithography systems, relies largely on firmware that may be susceptible to bugs and security vulnerabilities, which could cause major downtime for manufacturing.[68]

Geographic concentration means an individual natural disaster (e.g., seismic activity in Taiwan)[69] or direct US-PRC conflict could eliminate substantial FPGA manufacturing capacity. The accelerating competition between the United States and the PRC creates the potential for kinetic conflict, likely in East Asia and possibly on or near Taiwan.[70] Any such conflict could substantially damage semiconductor industry facilities and limit manufacturing capacity. The likelihood of such a conflict is the subject of ongoing debate. The *Economist* Intelligence Unit assesses a low probability of such a conflict occurring in the short term,[71] while Harvard Kennedy School professor Graham Allison believes that conflict is possible, but far from certain.[72] In contrast, some US military leaders have assessed direct US-PRC conflict to be likely.[73] Overall, the probability of such conflict is low but not negligible.

"Won't Sell" risks

US-PRC competition also drives major "won't sell" risks. The United States has steadily increased export controls and commercial restrictions targeting the PRC. While the PRC response to date has largely focused on critical mineral exports,[74] growing PRC

65 Semiconductor industry experts, private FPGA policy roundtable, February 6, 2025.

66 We selected Tesla because it is the only at-scale, publicly traded, pure-play electric vehicle manufacturer.

67 This analysis assumes $950 of FPGA components are found in each vehicle, based on an overall automotive industry average of approximately $1,000 for total semiconductors in each vehicle, adjusted to account for the narrower scope of FPGAs and the increased use of both semiconductors and FPGAs in electric vehicles compared to industry averages.

68 Brooks Idlet, "ASML Holding N.V.," Stock Report (Charlottesville, VA: CFRA Equity Research, March 29, 2025); FPGA engineer, interview with the authors, March 6, 2025; Egbert Teeselink, "ASML Lithography Software," *YCombinator Hacker News*, May 30, 2020, https://news.ycombinator.com/item?id=23363938.

69 "AMD 2023 Annual Report on Form 10-K," AMD, January 31, 2024, https://ir.amd.com/sec-filings/filter/annual-filings/content/0001193125-24-076535/d648557dars.pdf?TB_iframe=true&height=auto&width=auto&preload=false; "Lattice Semiconductor Corporation Form 10-K," Lattice Semiconductor Corporation, February 14, 2024, https://ir.latticesemi.com/static-files/8669c218-1c1d-4477-ae3f-47fafa881586; "Strong Earthquake in Taiwan Injures 27 and Causes Scattered Damage," *Associated Press*, January 20, 2025, https://apnews.com/article/taiwan-earthquake-ec33fde6218f097c2aec6aac2a697761.

70 Graham T. Allison, *Destined for War: Can America and China Escape Thucydides's Trap?* (Boston: Houghton Mifflin Harcourt, 2017).

71 "World Growth and Inflation: Risk Scenarios | Country Forecast," *Economic Intelligence Unit Viewpoint*, September 1, 2024, https://viewpoint.eiu.com/analysis/article/474164030.

72 Allison, *Destined for War: Can America and China Escape Thucydides's Trap?*

73 Courtney Kube and Mosheh Gains, "U.S. General Predicts War with China in 2025, Tells Officers to Get Ready," *NBC News*, January 27, 2023, https://www.nbcnews.com/politics/national-security/us-air-force-general-predicts-war-china-2025-memo-rcna67967.

74 Lv and Munroe, "China Bans Export of Critical Minerals to US as Trade Tensions Escalate."

influence over semiconductor firms across Asia raises the possibility that the government could restrict semiconductor exports to the United States and its allies.[75] The FPGA industry is likely to face outsized risk from such restrictions or similar efforts. FPGA's small market size would limit the economic impact to the PRC and other East Asian actors, while its strategic importance to the United States increases its value as a target.[76]

"Won't sell" risks also include the possibility of firms independently re-prioritizing their production capacity towards larger and potentially higher-profit segments of the semiconductor industry. However, interviewed experts report that large segments of the FPGA market are relatively price-inelastic and could absorb price increases.[77] As such, these economically induced "won't sell" risks are assigned a low probability.

Overall, "can't make" risks have a low probability, and "won't sell" risks have a moderate probability of occurrence for the FPGA market. However, given their critical applications, any disruptions to FPGA availability could threaten US military readiness and economic prosperity.

4.3 Security

There are three categories of security vulnerabilities—hardware, gateware, and related software—in the FPGA value chain. Drawing on a framework and definitions developed by the Lawfare Institute's Trusted Hardware and Software Working Group, mitigating security risks is the process of building trust to ensure FPGAs do not contain security vulnerabilities.[78] The analysis considers mitigations in line with the three methods to build trust included in the Working Group's framework: trust in technical performance, trust in corporate governance, and trust in nation-state policy and law.[79]

First, hardware supply chain attacks on FPGAs involve physical tampering with the FPGA chip during manufacturing, assembly, testing, and packaging. This tampering could establish a foundation that enables nefarious actors to launch gateware and software attacks on FPGA end-users. Returning to the ASML example, their critical lithography machines could also pose a hardware supply chain risk, particularly if they use monolithic and poorly documented software systems.[80]

> The PRC may have successfully executed a hardware supply chain attack at Supermicro, a US-based server manufacturer, exposing US military network data to the PRC.[81] While this potential attack was focused on the assembly stage (not manufacturing) and experts disagree about the plausibility and success of this attack,[82] the fact that the incident cannot be deemed impossible, even in hindsight, demonstrates the feasibility of hardware supply chains as an attack vector across several stages of the value chain**. Today, there appear to be few barriers against hardware supply chain attacks on FPGAs, especially at the assembly, test, and packing (ATP) stage of the value chain.[83]**

Second, FPGA gateware (the reconfigurable code that defines the active physical connections and logic elements in the FPGA chip) could be compromised at the manufacturing, assembly, testing, and packaging, or application/end-use stages of the value chain. This risk includes insider attacks and improper security configurations, although it can be mitigated by vendor-provided proprietary security features like secure boot, which verifies

75 Ansgar Baums and Nicholas Butts, *Tech Cold War: The Geopolitics of Technology*, Studies in Technology and Security: Innovation, Impact, and Governance (Boulder, Colorado: Lynne Rienner Publishers, Inc., 2025).

76 Specialist in Asian politics and economics, interview with the authors, February 21, 2025.

77 Semiconductor industry experts, private FPGA policy roundtable, February 6, 2025.

78 Rosenzweig et al., "Creating a Framework for Supply Chain Trust in Hardware and Software."

79 Ibid.

80 FPGA engineer, interview with the authors, March 6, 2025

81 Jordan Robertson and Michael Riley, "The Long Hack: How China Exploited a U.S. Tech Supplier," *Bloomberg*, February 12, 2021, https://www.bloomberg.com/features/2021-supermicro/.

82 Bruce Schneier, "Chinese Supply-Chain Attack on Computer Systems," *Schneier on Security*, February 13, 2021, https://www.schneier.com/blog/archives/2021/02/chinese-supply-chain-attack-on-computer-systems.html.

83 Jordan Robertson and Michael Riley, "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies," *Bloomberg*, October 4, 2018, https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies; Jordan Robertson and Michael Riley, "New Evidence of Hacked Supermicro Hardware Found in U.S. Telecom," Bloomberg, October 9, 2018, https://www.bloomberg.com/news/articles/2018-10-09/new-evidence-of-hacked-supermicro-hardware-found-in-u-s-telecom; Schneier, "Chinese Supply-Chain Attack on Computer Systems."

gateware authenticity during startup.[84] Industry experts report that it is "easier to attack a chip by injecting code into the [gate] ware than by getting into TSMC."[85] Successful gateware attacks could compromise sensitive data or remotely introduce malicious configurations.[86]

Third, software supply chain attacks on FPGAs could emerge through the cloud stack used by chip designers at the design stage of the value chain.[87] Semiconductor designers usually do not have full control over the configuration their cloud-based design software, which is typically developed by an electronic design automation (EDA) firm such as Cadence or Synopsys.[88] Unsecured cloud layers may risk compromising FPGA chip designs and relevant intellectual property that provides the United States with technological advantage over other nations.[89] For example, in 2024, Microchip Technology, a US semiconductor company that specializes in FPGAs for defense, aerospace, and automotive applications, confirmed unauthorized access of the company's server, which led to manufacturing facilities operating at a reduced capacity and hindered the firm's ability to fulfill orders.[90]

The Spectre and Meltdown hardware vulnerabilities in Intel CPUs demonstrate the potential damage of supply chain attacks on FPGAs. While Spectre and Meltdown appear to have been caused by innocuous design errors, they represented massive security vulnerabilities in almost every processor in use at the time, including leaking data to potential attackers.[91] If a malicious actor were to insert similar vulnerabilities into FPGAs via the software used to design the chips, the full set of security and economic activities described in Section 3 would be at risk.

Turning to trust-building measures to mitigate these risks, we consider trust in *technical performance*, *corporate governance*, and *nation-state policy and law*. While these dimensions of trust are mutually interdependent, they provide a convenient categorization to assess trust-building.

Technical solutions to address the security concerns raised above (across hardware, gateware, and software attack vectors) are generally feasible and the US National Institute of Standards and Technology (NIST) has drafted best-practice security guidance, although these technical methods do incur incremental cost risk.[92]

Trust in a supplier's corporate governance generally requires extensive engagement and organizational audits—while also feasible, these would likely incur significant costs while providing less benefit than technical solutions.[93]

84 Nisha Jacob et al., "How to Break Secure Boot on FPGA SoCs through Malicious Hardware," 2017, Cryptology ePrint Archive, https://eprint.iacr.org/2017/625.

85 Semiconductor industry participant #2, interview with the authors, December 6, 2024.

86 Jacob et al., "How to Break Secure Boot on FPGA SoCs through Malicious Hardware."

87 We consider software-based attacks on heterogeneous systems which include FPGAs and other chips to be out of scope for this analysis.

88 Kaihui Tu et al., "Introduction," in *FPGA EDA: Design Principles and Implementation*, 1st ed. (Singapore: Springer, 2024), https://doi.org/10.1007/978-981-99-7755-0.

89 Semiconductor industry participant #3, interview with the authors, December 11, 2024.

90 "Microchip Technology Inc. - Form 8-K," US Securities and Exchange Commission, August 20, 2024), https://www.sec.gov/Archives/edgar/data/827054/000082705424000153/mchp-20240820.htm.

91 Bruce Schneier, "Spectre and Meltdown Attacks against Microprocessors," *Schneier on Security*, January 5, 2018, https://www.schneier.com/blog/archives/2018/01/spectre_and_mel_1.html.

92 FPGA engineer, interview with the authors, March 6, 2025; Semiconductor industry participant #3, interview with the authors, December 11, 2024; Jennifer Lynn et al., "Cybersecurity Framework Version 2.0 Semiconductor Manufacturing Profile," National Institute of Standards and Technology, February 27, 2025, https://doi.org/10.6028/NIST.IR.8546.ipd.

93 Semiconductor industry participant #3, interview with the authors, December 11, 2024.

Finally, appropriate levels of trust in nation-state policy and legal environments vary widely between countries involved in the FPGA supply chain. Figure 4 displays selected dimensions of the World Bank's Worldwide Governance Indicators for China, Taiwan, and the United States.[94] Across political stability and absence of violence/terrorism, regulatory quality, rule of law, and voice and accountability, the US and Taiwan receive generally high scores[95] whereas China receives generally lower scores. As such, we conclude that, in general, trust-building efforts focused on nation-state policy and law are less feasible for FPGA supply chain participants operating in China, but reasonably feasible elsewhere.

Most FPGA firms do not invest sufficiently in trust-building measures in any of the above dimensions.[96] This decision likely reflects the general market-based tendency to prioritize reactive security over preventative security measures, necessitating government intervention.[97]

Figure 4: World Bank governance indicators for China, Taiwan, and the United States (2025)

94 "Worldwide Governance Indicators," World Bank, October 30, 2024, https://www.worldbank.org/en/publication/worldwide-governance-indicators.

95 With the notable exception of the American score for political stability and absence of violence/terrorism.

96 Semiconductor industry participant #2, interview with the authors, December 6, 2024; Semiconductor industry experts, private FPGA policy roundtable, February 6, 2025.

97 "Market Incentives and the Future of Technology Security," National Cyber Security Center, accessed February 17, 2025, https://www.ncsc.gov.uk/collection/ncsc-annual-review-2024/chapter-03/market-incentives.2025, https://www.ncsc.gov.uk/collection/ncsc-annual-review-2024/chapter-03/market-incentives.

5. Overall assessment

The US FPGA supply chain faces substantial, unmitigated risks to availability and security, which will be exacerbated by a PRC build-up of FPGA manufacturing capacity, increasing the effective cost of ensuring availability and security.

Today, FPGA market participants overwhelmingly focus on reducing cost risk, often at the expense of increasing availability or security risks.[98] However, availability and security risks create broad externalities (see Sections 4.2 and 4.3), including substantial economic, national security, and geopolitical consequences. Individual FPGA firms cannot fully internalize the costs of these risks given information asymmetries and spillover effects.[99] As a result, firms underinvest in ensuring security and availability, leading to a market failure that requires US government intervention.

Appropriate interventions could include reducing the cost of production with low availability and security risks (e.g., through subsidies) or increasing the effective cost of production with high availability and security risks (e.g., through tariffs imposed on the sources of production). Both forms of intervention would incentivize firms to shift production towards a supply chain construct with lower availability and security risks, onshoring operations in the United States or in other, more trusted nations. Overall, the US government can exert sufficient influence over foreign firms to effectively manage security risks within today's FPGA supply chain structure but cannot rely on foreign components of the FPGA supply chain to manage availability risks.

The policymakers' assumptions described in Section 2.2 are mostly invalid, as described in the table below.

Policymakers' assumptions (described in more detail in Section 2.2)	Conclusion for the US FPGA supply chain
Semiconductor security vulnerabilities for non-military applications (i.e., commercial or consumer) are less critical than in military applications.	**Not valid**: The US FPGA supply chain faces serious security risks to hardware, gateware, and software, even outside of military/defense applications. **Technical solutions are needed to address these security risks.**
Sufficient supply chain availability is provided by onshoring manufacturing of leading-edge logic chips (e.g., TSMC facilities in Arizona).	**Not valid:** As FPGAs are largely produced at lagging-edge process nodes, US onshoring (focused on leading-edge nodes) provides insufficient availability protection given the large domestic demand for FPGAs. **Additional resiliency measures (e.g., stockpiling) are required to address these availability risks for FPGAs.**
The US government can exert sufficient influence and/or control over foreign firms to ensure the semiconductor supply chain meets: a. US customers' economic needs for availability and cost-effectiveness b. The US government's national security interest in secure and reliable semiconductors	**Partially valid:** The current supply chain meets US needs for cost-effective supply and can be adapted with technical solutions to meet security needs; however, it cannot address availability risks.

98 Semiconductor industry experts, private FPGA policy roundtable, February 6, 2025.

99 Joseph E. Stiglitz, "Markets, Market Failures, and Development," *The American Economic Review* 79, no. 2 (1989): 197–203.

6. Policy recommendations

Despite mounting security and availability vulnerabilities within the supply chain, FPGA firms continue to prioritize cost risk excessively. Availability and security risks will likely intensify as China expands its manufacturing capacity for lagging-edge semiconductors, particularly in the lower- and mid-tier FPGA segments. FPGAs remain relatively unaddressed by current US semiconductor policies, which implicitly assume that security risk is not significant for non-military applications, that sufficient availability is provided by onshore manufacturing of leading-edge logic, and that the existing supply chain construct can meet US economic and national security needs. Unfortunately, these assumptions are largely invalid, and policy interventions are needed to address the externalities of FPGA availability and security risks.

We recommend the US government focus on managing FPGA security risks within the existing supply chain structure, which includes a substantial foreign firm presence, and focus on domestic-oriented solutions to address FPGA availability risks.

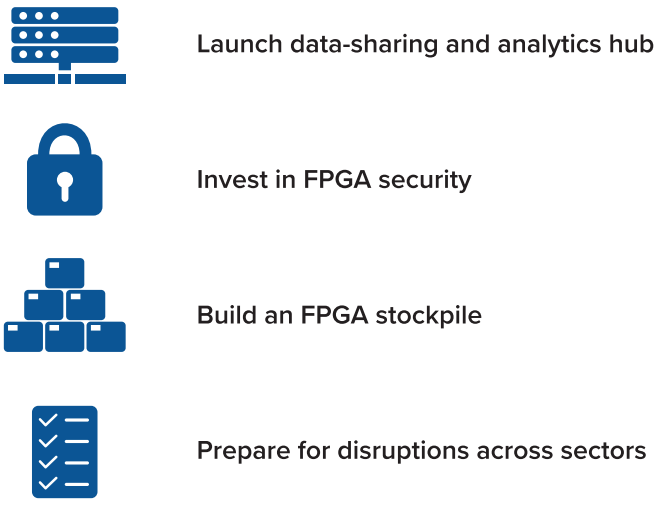
Addressing the significant, unmitigated risks facing the US FPGA supply chain will require the US government to implement four interrelated policy interventions. The first two address the security risks outside of military applications. The final two address availability vulnerabilities in the current FPGA supply chain as, contrary to typical policy assumptions, the United States' leading-edge onshoring efforts are inadequate to address domestic demand for FPGAs. These recommendations are summarized in Figure 5.

1. Launch a data-sharing and analytics hub

Designate the Department of Commerce's Supply Chain Center (SCC), administered by the International Trade Administration, as the national data-sharing and analytics hub for FPGA supply and sourcing. Direct the SCC to conduct their second planned 2025 tabletop exercise on FPGA chips.[100,101]

Strongly incentivize and, where appropriate, require public- and private-sector designers, manufacturers, distributors, and customers of FPGAs to provide the SCC with specific, SKU-level information on their FPGA supply chains, including quantities, prices, and suppliers. This information should include a detailed analysis of the origin countries of FPGAs and the origins of key inputs such as minerals or manufacturing equipment. These data-sharing agreements should become a requirement for CHIPS and Science Act funding agreements, government procurement of FPGAs (both military and commercial), and other federal government support for relevant firms.

Figure 5: Four policy interventions to address FPGA supply chain risks



100 US Department of Commerce, "Fact Sheet: Department of Commerce Announces New Actions on Supply Chain Resilience," Washington, DC: US Department of Commerce, September 10, 2024, https://www.commerce.gov/news/fact-sheets/2024/09/fact-sheet-department-commerce-announces-new-actions-supply-chain.

101 As of September 2024, the Department of Commerce announced only that the second exercise would "focus on an emerging technology where it is critical the United States maintain a strategic advantage".

The resulting SCC data will provide policymakers and the US FPGA supply chain participants a deeper understanding of the risk environment, enabling more effective design and delivery of policy interventions.

2. Invest in FPGA security

Direct federal research funders to prioritize academic and industrial R&D of enhanced FPGA security techniques, such as improving verification and validation. These funders include the Defense Advanced Research Projects Agency, the National Science Foundation, the Department of Energy, and the National Semiconductor Technology Center in the Department of Commerce.

Direct NIST to review existing FPGA product security standards and modernize them as needed, building upon its recent security report and guidance[102] on cybersecurity for the wider semiconductor manufacturing industry.

Direct NIST to develop security audit standards for FPGAs, supporting semiconductor firms' efforts to proactively investigate their supply chains to identify vulnerabilities and building on existing efforts to design assurance best practices for government use of FPGAs.[103]

Enhance existing engagement with semiconductor industry researchers, policymakers, manufacturers, and customers, including through existing consortia such as the SEMI Semiconductor Manufacturing Cybersecurity Consortium, to kickstart industry-wide efforts to develop FPGA-specific technical security solutions.

3. Build an FPGA stockpile

Using preliminary data and insights from the SCC's FPGA data-sharing and analytics hub, build a national stockpile of critical FPGA chips for both military and commercial applications. This stockpile would effectively address availability risks by allowing critical firms to source the FPGAs they need from the stockpile if their usual suppliers become unavailable.

Identify key SKUs with long expected lifecycles (5+ years) used for critical applications, in collaboration with public-sector (e.g., DoD, DoE, NSA) and private-sector end-customers of FPGAs, such as cloud service providers, defense prime contractors, telecommunications equipment manufacturers and adjacent firms, and automakers.

Develop and launch procurement, storage, and security strategies for these FPGAs as soon as possible, with an initial focus on specific SKUs with high availability and liquid markets to reduce market disruptions and distortions. Explore innovative procurement and contracting arrangements such as the fixed-price contracts recently deployed by the US government's Strategic Petroleum Reserve.[104]

4. Prepare for disruptions across sectors

Develop a government-wide playbook to address potential large-scale disruptions to the FPGA supply chain. The government response could include targeted subsidies to critical US firms, technical assistance in re-designing essential products to avoid unavailable FPGAs (e.g., replacing them with stockpiled SKUs or other types of chips), and measured, proportionate policies to respond if disruptions were caused by foreign competitors (e.g., increasing export controls).

Internally, use SCC FPGA data to develop plans for the prioritization of FPGA supplies in the event of supply chain disruptions, including a thorough assessment of legal and regulatory authorities to direct FPGA inventories to specific public- and private-sector actors.

Externally, encourage US FPGA firms and their end-customers to develop data-informed contingency plans for supply chain disruptions through tabletop exercises and computer-based simulations to identify vulnerabilities and develop mitigations. Similarly to the data-sharing agreements described above, the US government should consider a broad range of methods to encourage firms to participate, including CHIPS and Science Act funding and government procurement.

This overall set of measures would increase confidence in the technical performance of FPGAs, allowing FPGA firms to accept greater security risks as they seek lower-cost production, while also protecting the availability of critical FPGA chips through domestic stockpiling.

These policy interventions should be coordinated by a small project management team likely within the Departments of Commerce or Defense. This team should focus on managing the implementation of these recommendations with an agile

102 "Cybersecurity Framework Version 2.0 Semiconductor Manufacturing Profile," February 27, 2025."

103 Jeff Johnson, "Field Programmable Gate Array Levels of Assurance and Best Practices Overview," National Security Agency, 2023, https://cryptologicfoundation.org/file_download/inline/ae5f5efe-e47c-4d36-80c8-d6b2c96e8b08.

104 Daleep Singh and Arnab Datta, "Reimagining the SPR," *Financial Times*, February 24, 2024, https://www.ft.com/content/e948ae78-cfec-43c0-ad5e-2ff59d1555e9.

approach using existing government resources. In particular, the team should develop an integrated approach to performance measurement and management, including identifying specific objectives, metrics, and targets for each policy intervention. This performance measurement would enable a "test and learn" approach to iteratively improve the design and implementation of these interventions.

Given the critical role played by private firms in the US FPGA supply chain, the government should encourage engagement and cooperation from the private sector, particularly with security-related interventions. These measures should include procurement priority for federal government contracts and voluntary certifications.

Policies to reconsider

We also note three potential policies that we recommend the US government does not pursue:

1. **Subsidized onshore manufacturing, assembly, testing, and packaging of FPGAs**

   Several barriers prevent the onshore manufacturing of FPGAs.

   First, the scale of the lagging-edge market creates economic difficulties, as massive investments would be required to stand up the multiple fabs needed to enter the FPGA market at scale. According to an industry expert, "in order to have ATP nearshore, the United States would need more money and longer-term commitments than the CHIPS Act."[105]

   Second, operational feasibility is limited by the age of lagging-edge WFE, which in many cases is no longer in active production, and also by the PRC build-up of lagging-edge supply, which has limited WFE availability (see Section 4.1).

   Finally, following the implementation of the CHIPS and Science Act, semiconductors are often viewed politically as a "solved problem," limiting justification for massive investments in lagging-edge capacity.[106] Additionally, some experts, like the GeoEconomics Center's Jeremy Mark, view onshoring as "a bit of a fool's game to recreate what already exists in so many countries."[107]

   Instead, the US government should emphasize ongoing supply chain coordination with partner and allied nations. In many cases, these nations (e.g., Japan) can offer an appropriate balance of cost, availability, and security risks for many FPGA applications. In particular, their policy and legal environments can facilitate more trust in supply chain security than is generally feasible in China.

2. **Export controls on lagging-edge semiconductor manufacturing equipment**

   Most FPGA production takes place at lagging-edge nodes which have already achieved at-scale production across many countries,[108] limiting the impact of export controls in reducing access to lagging-edge chips. For example, ASML estimates that around 90 percent of all WFE it has ever sold is still in use,[109] representing significant manufacturing capacity at these legacy nodes.

   In particular, given China's extensive manufacturing capacity for lagging-edge logic chips, knowledge of these processes and relevant equipment is already widespread in the PRC, largely sourced from outside the United States (e.g., ASML in the Netherlands).[110] As such, export controls would likely be difficult to enforce and would produce limited impact.

   Export controls on lagging-edge manufacturing equipment would also impose three major costs on the United States: implementation costs, costs from potential retaliation, and geopolitical costs.

   Export controls would be implemented and administered by the Department of Commerce's Bureau of Industry and Security (BIS), which is already heavily resource-constrained.[111] Additional export controls on these highly technical products would require either incremental budget reallocations to BIS or redirecting existing capacity away from existing BIS priorities.

105 Semiconductor industry participant #2, interview with the authors, December 6, 2024.

106 Japanese semiconductor policymaker, interview with the authors, February 12, 2025.

107 Jeremy Mark, interview with the authors, February 21, 2025.

108 Semiconductor industry participant #4, interview with the authors, January 10, 2025.

109 H.-S. Philip Wong and Jim Plummer, "Implications of Technology Trends in the Semiconductor Industry," in *Silicon Triangle: The United States, Taiwan, China, and Global Semiconductor Security*, ed. Larry Diamond, James O. Ellis, and Orville Schell (Stanford, California: Hoover Institution Press, 2023).

110 Specialist in Asian politics and economics, interview with the authors, February 21, 2025.

111 Christopher Flavelle et al., "Mass Layoffs Begin at NOAA, With Hundreds Said to Be Fired in One Day," *The New York Times*, February 27, 2025, https://www.nytimes.com/2025/02/27/climate/noaa-layoffs-trump.html; Semiconductor industry participant #3, interview with the authors, December 11, 2024.

China is also likely to retaliate in kind to additional American export controls, particularly given the context of the current trade war.[112] Applying standard international relations frameworks, China is likely to misperceive these US export controls as being a deliberate and centrally-directed effort to hobble its economy.[113] This misperception would likely be exacerbated by the general tendency of nations to overestimate the degree to which they are being intentionally targeted by an adversary while overestimating their adversary's belief that they themselves are not a threat.[114]

Finally, from a geopolitical perspective, US allies, such as the Netherlands and Japan, have recently voiced hesitancy to continue mirroring US export control policies out of economic concerns and fear of PRC retaliation.[115] Should the United States pursue further implementation of semiconductor export controls via its allied nations, Mark also cautions that such "excessive control over exports would raise tensions significantly with other countries."[116]

3. Separating US FPGA supply chains from the PRC

We recommend that the US government does not in general prevent US FPGA firms from using PRC firms as part of their supply chain, either through direct regulation or through imposing substantial tariffs on PRC-produced FPGAs. Such a policy would be analogous to the Jones Act, which prevents domestic shipping from using vehicles built, owned, crewed, or flagged outside the United States.[117] While it has protected the resiliency of the American merchant marine, the Jones Act has imposed significant economic costs on the United States.[118]

In the case of FPGAs, we assess that PRC presence in the US FPGA supply chain poses risks to the security and availability of FPGAs. However, it also has undeniable cost benefits. While the global FPGA market remains small compared to the overall semiconductor market, FPGAs represent a major input cost for a broad set of products and FPGA unit economics affect product costs across the economy. We conclude that the resulting security risks can largely be mitigated with technical solutions and the availability risks with a US FPGA stockpile, as described in our policy recommendations.

Additionally, fully decoupling US FPGA supply chains from the PRC would substantially increase the cost structures of US FPGA firms, with negative impacts for on American economy and on wider US global technological influence. As many geopolitical analysts expected,[119] the technology ecosystem is beginning to fracture into US- and PRC-led components, with the PRC government actively encouraging domestic chip firms to use technical architectures not controlled by the United States.[120] Reducing the economic competitiveness of US FPGA firms would inhibit them from competing with PRC competitors globally, risking US leadership in the FPGA industry over the long run.[121] However, FPGAs used for highly sensitive and critical applications (e.g., military equipment and defense systems) should continue to prioritize security and availability risks. As a result, US and allied nations should lead the design, manufacturing, assembly, testing, and packaging of these chips.

If the US government does impose tariffs on semiconductor imports, we recommend that they should be narrowly targeted towards the PRC and any other nation that appears to be deliberately building large amounts of lagging-edge semiconductor manufacturing capacity and that poses substantial availability and security risks.

112 Lingling Wei, "China Wanted to Negotiate With Trump. Now It's Arming for Another Trade War.," *Wall Street Journal*, April 5, 2025, https://www.wsj.com/world/china/china-trump-tariff-foreign-policy-6934e493.

113 Robert Jervis, "Perceptions of Centralization," in *Perception and Misperception in International Politics*, 1st edition (Princeton, NJ: Princeton University Press, 1976).

114 Robert Jervis, "Overestimating One's Importance as Influence or Target," in *Perception and Misperception in International Politics*, 1st edition (Princeton, NJ: Princeton University Press, 1976).

115 Ana Swanson, "U.S. Vies With Allies and Industry to Tighten China Tech Controls," *The New York Times*, August 9, 2024, sec. Business, https://www.nytimes.com/2024/08/09/business/economy/china-us-chip-semiconductors.html.

116 Jeremy Mark, interview with the authors, February 21, 2025.

117 Thomas Grennes, "An Economic Analysis of the Jones Act," Mercatus Center, May 2, 2017, https://www.mercatus.org/research/research-papers/economic-analysis-jones-act.

118 Ibid.

119 Baums and Butts, *Tech Cold War*.

120 Jimmy Zhang, "Eight national departments jointly drafted guiding policies to encourage the use of open source RISC-V chips nationwide," *EE Times China*, March 5, 2025, https://scout.eto.tech/?id=4234.

121 Baums and Butts, *Tech Cold War*.

7. Conclusion

Overall, the US government faces a clear opportunity to secure the FPGA supply chain for US firms by leveraging existing government infrastructure to track and analyze supply chain data, launching an FPGA stockpile for critical chips, developing cross-sector plans for supply disruptions, and investing in technical solutions for FPGA security. More broadly, this integrated set of FPGA supply chain policy interventions should be treated as a lighthouse or pilot. This approach involves testing the interventions to harden the US supply chain for critical technologies with a small but important market, such as FPGAs, then adjusting policy design and implementation while rolling out the approach to other high-priority areas (like other types of specialized silicon), before scaling across industrial supply chains more broadly. These policy interventions will strengthen the American economy and ensure US national security.

About the Authors

Andrew Kidd holds a Master of Public Policy from the Harvard Kennedy School and was previously an engagement manager in the high-tech and public sector practices at McKinsey & Company.

Celine Lee holds a Master of Public Policy from the Harvard Kennedy School and previously held fellowships at the United States Senate Committee on Foreign Relations and the American Institute in Taiwan (AIT).

Bruce Schneier is a security technologist, and a fellow and lecturer at the Harvard Kennedy School.

Atlantic Council Board of Directors

Atlantic Council
1400 L Street NW, 11th Floor
Washington, DC 20005

(202) 463-7226

www.AtlanticCouncil.org