Federal Acquisition Regulatory Council
Office of Management and Budget
Office of Federal Procurement Policy
Department of Defense
General Services Administration
National Aeronautics and Space Administration

Federal Acquisition Regulation: Prohibition on Certain Semiconductor Products and Services

[48 CFR Parts 1, 2, 9, 12, 13, 39, 40, and 52
[FAR Case 2023-008; Docket No. FAR 2023-0008, Sequence No. 1]
RIN 9000-AO56

AUTHORS

Jack Burnham
Senior Research Analyst, FDD's China Program

RADM (Ret.) Mark Montgomery
Senior Director and Senior Fellow, FDD's Center on Cyber and Technology Innovation

Washington, DC
April 20, 2026

FDD
FOUNDATION FOR DEFENSE OF DEMOCRACIES

www.fdd.org

Introduction

China seeks to dominate the global market for foundational semiconductors, posing a threat to federal agencies that rely on them to run critical government services, store sensitive data, and power advanced military systems. In short, China's desire to control the market poses a threat to the entire federal government.

The FY2023 National Defense Authorization Act warned that several Chinese semiconductor foundries — Semiconductor Manufacturing International Corporation (SMIC), ChangXin Memory Technologies (CXMT), and Yangtze Memory Technologies Company (YMTC) — pose an unacceptable risk to U.S. national security.[1] While all Chinese-produced semiconductors may be vulnerable to tampering — a risk explicitly cited by the Federal Acquisition Regulatory (FAR) Council within its proposed restrictions — the firms making them represent the vanguard of Beijing's efforts to establish global market dominance of foundational chips and accelerate its military-industrial complex. Along with selling products and services to firms that supply federal agencies, these foundries are key suppliers to a broad range of sanctioned Chinese entities involved in military modernization and industrial espionage, including the National University of Defense Technology (NUDT), Huawei, Hikvision, and DJI.[2]

In response, the FAR Council should restrict federal agencies from purchasing electronic products and services that rely on semiconductors produced by these firms. These procurement regulations should also encourage private firms that bid on federal contracts or act as subcontractors to conduct greater due diligence into their own supply chains. This incentive should take the form of a structured liability shield that holds firms accountable for intentional due diligence failures while ensuring that firms that proactively report potential issues retain civil immunity.

China's Efforts To Dominate Global Semiconductor Market Pose National Security Threat

China's drive to dominate the semiconductor market has profound national security implications for federal supply chains, particularly those embedded within the Department of Defense (DOD) and other national security agencies. A single F-35, for example, contains tens of thousands of chips, while military-grade AI runs on hundreds of thousands of chips dispersed in data centers across the country.[3]

Beijing's semiconductor strategy is twofold: become self-reliant by indigenizing production while simultaneously seizing a commanding share of the global market as a means of imposing its ambitions on downstream customers. This strategy is underpinned internally by substantial

---

[1] James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. 117-263, 136 Stat. 2395 (2022).
[2] "Blue Heron: Semiconductor Manufacturing International Corporation," *SOS International*, August 2020. (https://cira.exovera.com/wp-content/uploads/2021/06/blue_heron_smic_footnoted.pdf); "Project 506: CXMT and China's Semiconductor Industrial Policy," *Horizon Advisory*, December 2022. (https://www.horizonadvisory.org/ttc/cxmt)
[3] Jack Burnham, Craig Singleton, and RADM (Ret.) Mark Montgomery, "Section 232 National Security Investigation of Imports of Polysilicon and Its Derivatives," *Foundation for Defense of Democracies*, August 6, 2025. (https://www.fdd.org/analysis/2025/08/06/section-232-national-security-investigation-of-imports-of-polysilicon-and-its-derivatives)

state subsidies and an influx of military-linked capital and externally by high-level industrial espionage and large-scale dumping efforts. Chinese firms receive significant funding across all layers of the supply chain, from refining polysilicon — a foundational input for semiconductor production — to silicon carbide (SiC) wafers, which form the backbone of most modern weapons systems.[4] This support is often paired with aggressive state-backed espionage against global competitors, including well-known cases of Chinese hacking groups targeting Taiwanese foundries, Dutch lithography manufacturer ASML, and Japanese chip design firms.[5]

While Chinese firms still struggle to manufacture the highest-end semiconductors — leading Chinese AI firms to engage in broad-based smuggling efforts — China has gained a decisive advantage in lower-end foundational chips.[6] The Rhodium Group, a research firm, estimates that within the next decade, Chinese firms will likely produce nearly 40 percent of all foundational chips and nearly half of all foundational chips within key niche markets.[7] Beijing has built this advantage using distortive trade practices to flood the U.S. market — Chinese firms routinely price key components below the cost of actual production, driving competitors out of the market and erasing the potential advantages offered by previous U.S. industrial policies such as the CHIPS and Science Act.[8]

America's reliance on Chinese-produced foundational chips creates several supply chain risks that extend deep into the defense industrial base. Beijing has shown its willingness to weaponize strategic supply chains, such as rare earth and critical minerals, to compel Washington to remove competitive actions and balance against other forms of asymmetric pressure. As with rare earths, China's control over foundational chips would allow Beijing to exercise leverage over supply chains supporting a range of DOD capabilities.[9]

---

[4] Ibid; RADM (Ret.) Mark Montgomery and Isaac Harris, "China's Acts, Policies, and Practices Related to Targeting of the Semiconductor Industry for Dominance," *Foundation for Defense of Democracies*, January 31, 2025. (https://www.fdd.org/analysis/2025/01/31/chinas-acts-policies-and-practices-related-to-targeting-of-the-semiconductor-industry-for-dominance)

[5] Anna Ribeiro, "China-aligned TA415 escalates cyberattacks on Taiwanese semiconductor manufacturing, supply chains," *Industrial Cyber*, September 17, 2025. (https://industrialcyber.co/ransomware/china-aligned-ta415-escalates-cyberattacks-on-taiwanese-semiconductor-manufacturing-supply-chains); Ian O'Connor, "Watch Out Europe: China is Stealing Your Chip Secrets," *Center for European Policy Analysis*, July 9, 2024. (https://cepa.org/article/watch-out-europe-china-is-stealing-your-chip-secrets)

[6] Jack Burnham, "Exposure of Major Chinese-Linked Chip Smuggling Operations Shows Limits of Industry Self-Policing," *Foundation for Defense of Democracies*, March 20, 2026. (https://www.fdd.org/analysis/2026/03/20/exposure-of-major-chinese-linked-chip-smuggling-operations-shows-limits-of-industry-self-policing)

[7] Reva Goujon, Jan-Peter Kleinhans, and Laura Gormley, "Thin Ice: US Pathways to Regulating China-Sourced Legacy Chips," *Rhodium Group*, May 7, 2024. (https://rhg.com/wp-content/uploads/2024/05/Thin-Ice-US-Pathways-to-Regulating-China-Sourced-Legacy-Chips.pdf)

[8] RADM (Ret.) Mark Montgomery and Isaac Harris, "China's Acts, Policies, and Practices Related to Targeting of the Semiconductor Industry for Dominance," *Foundation for Defense of Democracies*, January 31, 2025. (https://www.fdd.org/analysis/2025/01/31/chinas-acts-policies-and-practices-related-to-targeting-of-the-semiconductor-industry-for-dominance); CHIPS and Science Act, Pub. L. 117-167, 136 Stat. 1366 (2022).

[9] Jack Burnham, Craig Singleton, and RADM (Ret.) Mark Montgomery, "Section 232 National Security Investigation of Imports of Polysilicon and Its Derivatives," *Foundation for Defense of Democracies*, August 6, 2025. (https://www.fdd.org/analysis/2025/08/06/section-232-national-security-investigation-of-imports-of-polysilicon-and-its-derivatives)

Chinese chips may also contain another series of vulnerabilities beyond control over the supply chain, including backdoors buried in the silicon itself. As noted by the FAR Council in its filing, the U.S. National Counterintelligence and Security Center has warned that semiconductors produced by foreign adversaries may contain embedded vulnerabilities that allow firms and governments to gain access to critical systems. This risk is heightened by Beijing's willingness to compel firms under its jurisdiction to provide intelligence assistance, allowing these types of openings to function as backdoors for espionage efforts.[10]

Listed Firms Have Enduring Ties to the Chinese Military

Each of the firms listed in the FY2023 NDAA — SMIC, CXMT, and YMTC — encapsulates the risks posed by Chinese-produced foundational chips.[11] Collectively, these firms remain dedicated to furthering Beijing's technological ambitions, having received varying degrees of state support and serving as key suppliers of the People's Liberation Army (PLA).

China's SMIC is the country's largest semiconductor manufacturer and a cog in the PLA's defense industrial base. Supported by significant state funding, SMIC currently holds roughly 6 percent of global market share as the third-largest foundry in the world, just behind regional rivals TSMC and Samsung.[12] This growth may have been propelled by industrial espionage, with the Dutch firm ASML alleging that its China-based employees smuggled information related to its proprietary technology to the company's Chinese competitors.[13]

SMIC is also a key provider of chips to CETC Electronic Equipment Group, a state-owned firm whose explicit purpose is to leverage commercial innovation to modernize the PLA. CETC was critical to building China's first nuclear weapons and remains a key designer of laser weapons, radar arrays, and other emerging defense technologies.[14] SMIC also provides significant computing and manufacturing resources to other PLA-linked entities and programs, including defense universities, supercomputing clusters used in the design and testing of nuclear weapons, and the PLA's military space program.[15] The Department of Commerce has added many of these

---

[10] Jack Burnham, Mark Montgomery, Craig Singleton, and Johanna Yang, "Petition for Reconsideration of Action in Rulemaking Proceeding Application for Review of Action in Rulemaking Proceeding, *Foundation for Defense of Democracies*, March 17, 2026. (https://www.fdd.org/analysis/2026/03/17/petition-for-reconsideration-of-action-in-rulemaking-proceeding-application-for-review-of-action-in-rulemaking-proceeding)

[11] James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. 117-263, 136 Stat. 2395 (2022).

[12] Sheila Chiang, "China's largest chipmaker SMIC is now the No. 3 foundry in the world, Counterpoint says," *CNBC*, May 23, 2024. (https://www.cnbc.com/2024/05/23/chinas-smic-is-now-worlds-third-largest-chip-foundry-counterpoint.html)

[13] Jordan Robertson and Cagan Koc, "ASML Stolen Data Came From Technical Repository for Chip Machines," *Bloomberg*, February 15, 2023. (https://www.bloomberg.com/news/articles/2023-02-15/ex-employee-for-chip-machine-maker-asml-stole-data-from-technical-repositary)

[14] "Blue Heron: Semiconductor Manufacturing International Corporation," *SOS International*, September 5, 2020. (https://cira.exovera.com/wp-content/uploads/2021/06/blue_heron_smic_footnoted.pdf); Matthew Luce, "A Model Company: CETC Celebrates 10 Years of Civil-Military Integration," *Jamestown Foundation*, February 21, 2012. (https://jamestown.org/a-model-company-cetc-celebrates-10-years-of-civil-military-integration)

[15] Ibid.

institutions to its Entity List, including NUDT and the Wuxi Jiangnan Institute of Computing Technology, for assisting in PLA modernization by providing high-performance computing.[16]

CXMT is a state-backed semiconductor manufacturing firm specializing in the production of dynamic random-access memory (DRAM) chips — a component used in high-end AI servers, military platforms such as drones and satellite communications, and commercial electronics.[17] CXMT controls nearly 5 percent of the global DRAM market by revenue.[18] The company has received substantial funding from the provincial government of Hefei and additional support from Beijing's semiconductor investment programs and has also allegedly engaged in a pattern of industrial theft, including sponsoring talent recruitment schemes in Taiwan and stealing trade secrets from Samsung to improve its mass production capacity.[19] These issues prompted Congress — both the China Select Committee and the House Committee on Foreign Affairs — to request that CXMT be added to the Entity List in June 2023.[20]

CXMT also has ties to the PLA and other key elements of China's military-industrial base. CXMT publicly advertises its products as "military-grade" within China, and one of its wholly owned subsidiaries, Beijing Jiuxin Technology, conducts research with the Beijing Superstring Memory Research Institute, a core part of the Chinese Academy of Sciences Institute of Microelectronics (CASIM).[21] Commerce added CASIM to the Entity List in December 2024 due to its role in developing advanced semiconductor technology for the Chinese military.[22] CXMT, both independently and through its subsidiaries, also remains a key supplier to several other Chinese military-linked entities, including Hikvision, DJI, and Huawei, all of which are on both the Entity List and DOD's Chinese Military Companies list.[23] Given its position within the

---

[16] Addition of Certain Persons to the Entity List; and Removal of Person From the Entity List Based on a Removal Request, 80 Federal Register 8524, February 18, 2015.; Addition of Entities to the Entity List and Revision of an Entry on the Entity List, 84 Federal Register 29371, June 24, 2019.

[17] "Mission-Ready Memory: The Importance of Memory Components in Military Equipment," *SMARTsemi*, February 4, 2025. (https://smartsemi.com/mission-ready-memory-the-importance-of-memory-components-in-military-equipment)

[18] Yang Jie and Jiyoung Sohn, "The Chinese Company Taking On the World's Memory Chip Giants," *The Wall Street Journal*, January 11, 2026. (https://www.wsj.com/tech/the-chinese-company-taking-on-the-worlds-memory-chip-giants-78dfea55)

[19] Ibid.

[20] U.S. House Select Committee on Strategic Competition between the United States and the Chinese Communist Party, Press Release, "Letter to Secretary of Commerce to Take Action Following CCP Micron Ban," June 1, 2023. (https://chinaselectcommittee.house.gov/media/letters/letter-secretary-commerce-take-action-following-ccp-micron-ban)

[21] "Project 506: CXMT and China's Semiconductor Industrial Policy," *Horizon Advisory*, December 2022. (https://www.horizonadvisory.org/ttc/cxmt)

[22] Additions and Modifications to the Entity List; Removals From the Validated End-User (VEU) Program, 89 Federal Register 96830, December 5, 2024.

[23] "Project 506: CXMT and China's Semiconductor Industrial Policy," *Horizon Advisory*, December 2022. (https://www.horizonadvisory.org/ttc/cxmt); Addition of Entities to the Entity List, Revision of Entry on the Entity List, and Removal of Entities From the Entity List, 85 Federal Register 83416, December 22, 2020.; Addition of Certain Entities to the Entity List, 84 Federal Register 54002, October 9, 2019.; Addition of Entities to the Entity List, 84 Federal Register 22961, May 21, 2019.; "Entities Identified as Chinese Military Companies Operating in the United States in Accordance with Section 1260H of the William M. ('Mac') Thornberry National Defense Authorization Act for Fiscal Year 2021," *U.S. Department of Defense*, January 7, 2025. (https://media.defense.gov/2025/Jan/07/2003625471/-1/-1/1/ENTITIES-IDENTIFIED-AS-CHINESE-MILITARY-COMPANIES-OPERATING-IN-THE-UNITED-STATES.PDF)

Chinese market, CXMT is also slated to become a major supplier of high-bandwidth memory chips to Huawei, dramatically improving the latter's performance in powering frontier AI systems at scale.[24]

YMTC is also a state-owned semiconductor firm that receives significant support from Beijing and remains deeply embedded within the PLA's defense industrial base. YMTC has received millions in state subsidies to spur the production of NAND memory chips, often used both in commercial devices such as smartphones and in secure communications systems and precision guidance systems for missiles and drones.[25] YMTC has also likely supplied both Huawei, a designated Chinese military company, and the PLA directly via its ties to its former parent company, Tsinghua Unigroup.[26] These allegations led the Defense Department to list YMTC as a Chinese Military Company in 2024 and reaffirm its listing in 2025, an action that is currently being contested in federal court.[27]

Recommendations

The FAR Council should address the risks posed by listed Chinese foundries by banning federal agencies from procuring products and services that contain their semiconductors or rely on their services. This effort should be complemented with a structured liability shield that penalizes firms for failing to conduct due diligence and protects from civil prosecution those that report proactively.

- **The FAR Council should apply the restrictions outlined in the FY2023 NDAA to commercial products, commercial IT services, and commercial telecommunications services**. The firms listed in the NDAA pose a direct national security threat to the United States that can only be eliminated by their removal from federal supply chains. Along with containing potential vulnerabilities, the components federal agencies are currently purchasing create value for companies that fuel China's military-industrial complex. Purchasing these components helps their manufacturers to establish greater market share

[24] "Project 506: CXMT and China's Semiconductor Industrial Policy," *Horizon Advisory*, December 2022. (https://www.horizonadvisory.org/ttc/cxmt)

[25] Office of Senator Mark Warner, Press Release "Warner, Rubio Urge DNI to Review Risk Chinese Chipmaker YMTC Presents to National Security," September 22, 2022. (https://www.warner.senate.gov/public/index.cfm/2022/9/warner-rubio-urge-dni-to-review-risk-chinese-chipmaker-ymtc-presents-to-national-security); Bureau of Industry and Security, Press Release, "Commerce Implements New Export Controls on Advanced Computing and Semiconductor Manufacturing Items to the People's Republic of China (PRC)," October 7, 2022. (https://www.bis.gov/press-release/commerce-implements-new-export-controls-advanced-computing-semiconductor-manufacturing-items-peoples)

[26] Office of Senator Mark Warner, Press Release "Warner, Rubio Urge DNI to Review Risk Chinese Chipmaker YMTC Presents to National Security," September 22, 2022. (https://www.warner.senate.gov/public/index.cfm/2022/9/warner-rubio-urge-dni-to-review-risk-chinese-chipmaker-ymtc-presents-to-national-security)

[27] "Entities Identified as Chinese Military Companies Operating in the United States in Accordance with Section 1260H of the William M. ('Mac') Thornberry National Defense Authorization Act for Fiscal Year 2021," U.S. Department of Defense, January 7, 2025. (https://media.defense.gov/2025/Jan/07/2003625471/-1/-1/1/ENTITIES-IDENTIFIED-AS-CHINESE-MILITARY-COMPANIES-OPERATING-IN-THE-UNITED-STATES.PDF); Mike Scarcella, "Chinese flash memory maker YMTC sues US over military designation," *Reuters*, December 8, 2025. (https://www.reuters.com/legal/litigation/chinese-flash-memory-maker-ymtc-sues-us-over-military-designation-2025-12-08)

within the United States. To ease compliance costs as the FAR Council imposes its new restrictions, the restrictions should prioritize only the products and services most likely to be compromised.

- **The FAR Council should require entities that offer a response to a government solicitation to conduct a reasonable inquiry as to whether their electronic products or services contain covered semiconductors or require electronic products that include covered semiconductors**. Entities seeking to sell electronic goods and services to federal agencies should be required to document their efforts to identify the possible presence of covered semiconductors within their supply chains. While this effort may not fully eliminate all vulnerabilities, it will encourage firms to adopt stronger sourcing requirements and audit their own supply chains to remain eligible for federal contracts. Without being overly prescriptive, the FAR Council should encourage firms to use a broad range of sources, including the Department of Commerce website, supplier websites, manufacturer websites, supply chain illumination, and other due diligence tools.

- **The FAR Council should provide a liability shield to those companies that proactively disclose the presence of a covered semiconductor product in their supply chains.** An offeror or lower-tier supplier that provides a disclosure regarding covered semiconductor products or services in electronic products that are manufactured or assembled by an entity other than the offeror or lower-tier supplier should not be subject to civil liability nor determined to be presently responsible based on such notification. The purpose of the liability shield is not to ignore the cost of vulnerabilities but to encourage firms to accurately report the results of their supply chain assessment without jeopardizing future contracting opportunities. This liability shield should also extend to cases in which the offeror or lower-tier supplier conducted a reasonable inquiry into its own products and services but failed to identify covered semiconductors.

- **The FAR Council should further encourage firms to provide timely notification regarding the use of covered semiconductors in products or services that are manufactured or assembled by an entity other than the contractor or subcontractor by protecting those firms from civil liability**. After receiving a government award, firms should be encouraged to report on the presence of covered semiconductors within their products and services as soon as possible while still retaining responsibility for their own compliance failures. This structured liability shield also offers a self-enforcement mechanism by encouraging contractors and subcontractors to report on possible supply chain issues without risking a breach of their federal contracts.

Conclusion

By strengthening federal procurement regulations to protect against the risks posed by certain Chinese-produced semiconductors while encouraging private firms to conduct stronger due diligence reporting, the FAR Council can bolster U.S. national security and promote more secure supply chains for federal agencies.

Thank you for considering our comments. We look forward to seeing how our input is incorporated into the agency's ongoing policy work.