Department of Defense
Defense Acquisition Regulations System

Defense Federal Acquisition Regulation Supplement: Mitigating Risks Related to Foreign Ownership, Control, or Influence (DFARS Case 2021-D011)

48 CFR Parts 212, 217, 240, and 252
[Docket DARS-2026-0133]
RIN 0750-AL30

AUTHORS

Jack Burnham
Senior Research Analyst, FDD's China Program

Josh Birenbaum
Deputy Director, FDD's Center on Economic and Financial Power

Washington, DC
July 7, 2026

FDD
FOUNDATION FOR DEFENSE OF DEMOCRACIES

www.fdd.org

Introduction

As the United States prepares to surge spending into its defense industrial base, it should ensure that its financial controls can match its demand for firepower.

U.S. firms are not the only contractors and subcontractors seeking to fulfill Pentagon procurement contracts. As in past spending surges, both fraudulent firms and foreign adversaries use opaque corporate structures, particularly shell companies, to artificially inflate cost estimates, steal set-asides for small- and medium-sized firms, and illicitly access U.S. defense technologies. Along with misusing public funds, these structures hinder development of the U.S. defense industrial base. They divert necessary domestic investments; provide cover for stealing commercial secrets; create cover for the introduction of defective componentry; and provide potential supply chain chokepoints or leverage in the event of a conflict.

In response, the Department of Defense (DOD) should revise its Defense Federal Acquisition Regulation Supplement to fully implement the FY2020 and FY2021 National Defense Authorization Acts (NDAAs). The acts require the Pentagon to document beneficial ownership structures for contractors and subcontractors while recognizing the risk posed by suppliers further upstream within the supply chain. DOD should also consider developing new mechanisms to screen lower-level commercial contracts that may present novel risks due to a lack of preexisting financial controls.

Opaque Beneficial Ownership Structures Pose a National Security Risk

The U.S. defense industrial base is poised for a historic expansion following a combination of rapidly increasing defense spending and increased demand for precision munitions and advanced platforms.[1] This expansion also ensures that it becomes a growing target for both fraud and penetration by foreign adversaries.

Amid the Global War on Terror in 2012, the Commission on Wartime Contracting in Iraq and Afghanistan reported that between $30 billion and $60 billion had been lost due to contract fraud between 2001 and 2011, primarily due to poor oversight and inadequate accounting control measures.[2] While independent estimates have suggested that fraud measured as a percentage of

[1] Ryan Brobst, Cameron McMillan, and Bradley Bowman, "Trump Administration Requests Extraordinary $1.5 Trillion Defense Budget," *Foundation for Defense of Democracies*, April 23, 2026. (https://www.fdd.org/analysis/2026/04/23/trump-administration-requests-extraordinary-1-5-trillion-defense-budget)
[2] Commission on Wartime Contracting in Iraq and Afghanistan, "Transforming Wartime Contracting: Controlling Costs, Reducing Risks," August 2011. (https://cybercemetery.unt.edu/cwc/20110929213815mp_/http://www.wartimecontracting.gov/docs/CWC_FinalReport-lowres.pdf)

overall appropriations may be similar between war and peacetime, rising defense spending still ensures that unaccounted-for fraudulent spending continues to grow in absolute terms.[3]

Though the most notable fraud cases often involve major defense contractors, shell companies are a key vehicle for accessing the defense procurement process. Contractors may use shell companies to artificially inflate prices, engineer bidding wars to spur greater spending, and access specific set-asides under the Small Business Administration — all while using such entities to evade legal accountability.[4] This issue is particularly pressing at the subprime level, as procurement rules around registration are either insufficient or laxly enforced deep within the supply chain, opening gaps within preexisting financial control systems.[5] While contractors are required to register with the System for Award Management, the same standard has historically not applied to subcontractors. Moreover, contractors have historically only been required to disclose their "immediate" or "highest-level" owners, obscuring potential foreign ownership ties.[6]

While these shortfalls represent a loss to DOD, they also offer an opportunity for foreign adversaries, particularly China and Russia, to gain access to the U.S. defense industrial base to profit from government contracting, steal commercial secrets, and potentially degrade critical supply chains via espionage, defective goods, or outright sabotage. A 2019 Government Accountability Office study of just 32 defense contracting cases identified multiple instances in which foreign firms used shell companies to bid on contracts intended for domestic suppliers, costing the Pentagon millions of dollars and hindering the U.S. defense industrial base.[7]

China has previously used shell companies to target strategic American sectors while avoiding scrutiny. In 2015, Fosun Group, a Chinese entity, bought Wright USA, an insurance firm that handled claims for much of the U.S. intelligence community — the purchase allowed Fosun Group to access critical information before the deal was eventually canceled following an investigation by the Committee on Foreign Investment in the United States.[8] Chinese investors, often directly connected to Beijing, have also attempted to use beneficial ownership structures to penetrate the U.S. semiconductor market and gain access to potential intelligence posts to spy on

---

[3] James Carafano and Eric Sayers, "Defense Spending Fraud, Waste, and Abuse: Hype, Reality, and Real Solutions," *The Heritage Foundation*, November 20, 2008. (https://www.heritage.org/defense/report/defense-spending-fraud-waste-and-abuse-hype-reality-and-real-solutions)
[4] Rachael Hanna, "Shell Corporations Facilitate Contracting Fraud at the Department of Defense," *Lawfare*, April 21, 2020. (https://www.lawfaremedia.org/article/shell-corporations-facilitate-contracting-fraud-department-defense)
[5] Ibid.
[6] Ibid.
[7] U.S. Government Accountability Office, "Defense Procurement: Ongoing DOD Fraud Risk Assessment Efforts Should Include Contractor Ownership," November 25, 2019. (https://www.gao.gov/products/gao-20-106)
[8] Daniel Swift and Susan Soh, "Strengthening Transparency, Eligibility, and Jurisdictional Scope in Investment Reviews," *Foundation for Defense of Democracies*, March 19, 2026. (https://www.fdd.org/analysis/2026/03/19/strengthening-transparency-eligibility-and-jurisdictional-scope-in-investment-reviews); Josh Birenbaum, "The dangerous national security shell company game," *The Washington Examiner*, April 20, 2026. (https://www.fdd.org/analysis/2026/04/20/the-dangerous-national-security-shell-company-game)

U.S. military facilities, highlighting the danger posed by corporate opacity within national security contracting.[9]

This issue also compounds DOD's current Chinese exposure. An independent study by Govini, a defense procurement analysis firm, suggests that Chinese firms represent nearly 10 percent of all "Tier 1 suppliers" across a range of mission areas.[10] Moreover, DOD has previously suffered from alleged Chinese sabotage of mission-critical components. In 2021, *Bloomberg* reported that the Pentagon identified thousands of servers that had been infiltrated via hidden components inserted into products manufactured in China by U.S. firm Super Micro Computer, Inc.[11] In 2025, ProPublica revealed that for more than a decade, Microsoft allegedly failed to maintain proper oversight to protect government systems, while its engineers in China had access to DOD classified cloud-computing systems.[12] In each instance, improper oversight, combined with limited insight into its own supply chains, allowed Beijing to access departmental infrastructure before eventually being identified following contract delivery.

Russian firms have also increasingly penetrated the U.S. defense industrial base using beneficial ownership structures, both to engage in illicit contracting with the Department of Defense and to steal technical secrets and components to fuel Moscow's war machine. In 2018, the Department of the Air Force was forced to cancel a $420 million contract with A. Finkl & Sons Co. to produce components for next-generation "bunker-buster" munitions due to concerns over the firm's ties to Viktor Vekselberg, a sanctioned Russian oligarch.[13]

Russian firms have also established ties within the American defense industrial base to procure export-controlled components for the Russian military, particularly as the war in Ukraine has strained the country's production capacity. Even as the United States has targeted sanctions-evasion networks, the Royal United Services Institute, a British think tank, and Ukrainian intelligence estimate that more than 70 percent of foreign-produced components found in recovered Russian weapons were produced by American firms.[14] These networks also often involve American nationals, with the Department of Justice charging seven individuals, including two Americans, in 2022 for managing a network of shell companies to ship electronic

---

[9] Ibid.
[10] Sydney J. Freedberg Jr., "Nearly one in 10 'Tier 1' subcontractors to defense primes are Chinese firms: Report," *Breaking Defense*, June 27, 2025. (https://breakingdefense.com/2025/06/nearly-one-in-10-tier-1-subcontractors-to-defense-primes-are-chinese-firms-report)
[11] 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)
[12] Jack Burnham and Jiwon Ma, "Microsoft Omitted Key Details in DOD Security Filings on China-Related Program," *Foundation for Defense of Democracies*, August 25, 2025. (https://www.fdd.org/analysis/2025/08/25/microsoft-omitted-key-details-in-dod-security-filings-on-china-related-program)
[13] *A. Finkl & Sons Co. d/b/a Finkl Steel*, B-416582.4 (Comp. Gen. December 10, 2018). https://apps.dtic.mil/sti/pdfs/AD1157066.pdf
[14] The Wall Street Journal, "Inside the Lab Exposing U.S. Chips Powering Russia's Weapons," *YouTube*, June 3, 2024. (https://www.youtube.com/watch?v=LdWDgonI2yI)

components used in hypersonic weapons and thousands of rounds of tactical ammunition to Russia via transshipment points in Estonia.[15]

Recommendations

The Department of Defense should institute a new series of financial control mechanisms to ensure greater visibility in its contracting process, particularly by requiring contractors and subcontractors to disclose their beneficial ownership structure and potential ties to foreign owned, controlled, or influenced (FOCI) firms.

Though beyond the remit of the department, these measures would operate most effectively in combination with broader efforts to bolster corporate transparency across a range of strategic supply chains. The United States should fully enforce the Corporate Transparency Act, require full supply chain mapping of all suppliers at all tiers by covered suppliers, and expand screening measures to assess for a broader range of risks beyond ownership, control, and influence, including those entities that may have access to trade secrets, data, or other sensitive information.

- **The Department of Defense should revise the Defense Federal Acquisition Regulation Supplement (DFARS) to fully implement the relevant portions of Section 847 of the FY2020 NDAA and Section 819 of the FY2021 NDAA**. The relevant provisions will require contractors and subcontractors to disclose to the Defense Counterintelligence and Security Agency their beneficial ownership structure and whether they are under FOCI. These provisions will also require contractors and subcontractors designated as FOCI to provide additional information regarding their foreign ownership.

- **The Department of Defense should apply the revised DFARS to contracts for commercial products, including commercial off-the-shelf (COTS) items and services**. Beneficial ownership structures have proliferated across the defense industrial base and well into the commercial market due to enforcement gaps and differing state regulations of corporate governance. As such, DOD should ensure that its COTS purchases, along with other commercial contracts, are vetted for ties to foreign adversaries.

- **The Department of Defense should consider alternative regulatory models to screen contracts below the simplified acquisition threshold (SAT)**. While the relevant

[15] U.S. Department of Justice, Press Release, "Five Russian Nationals, Including Suspected FSB Officer, and Two U.S. Nationals Charged with Helping the Russian Military and Intelligence Agencies Evade Sanctions," December 13, 2022. (https://www.justice.gov/usao-edny/pr/five-russian-nationals-including-suspected-fsb-officer-and-two-us-nationals-charged)

portions of the FY2020 and FY2021 NDAAs are intended to apply to contracts valued above $5 million, DOD should consider whether alternative mechanisms for screening contractors' beneficial ownership structures may be appropriate given the risks posed by foreign adversaries seeking access to the U.S. defense industrial base. These mechanisms should also be capable of blocking contract awards to beneficial owners or entities under FOCI or that have been previously convicted of fraud or other related crimes.

Conclusion

As the United States seeks to rebuild its defense industrial base, the Department of Defense should ensure that foreign adversaries cannot use the department's procurement process as a position from which to perpetrate fraud, espionage, and sabotage. As such, the department must tighten its scrutiny of beneficial ownership structures for contractors and subcontractors.

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