Federal Communications Commission

Petition for Reconsideration of Action in Rulemaking Proceeding Application for Review of Action in Rulemaking Proceeding

47 CFR Part 2
[ET Docket Nos. 26-22, 26-23; Report No. 3232; FR ID 329036]

AUTHORS

Jack Burnham
Senior Research Analyst, FDD's China Program

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

Craig Singleton
Senior Director and Senior Fellow, FDD's China Program

Johanna Yang
Policy Analyst, FDD's Center on Cyber and Technology Innovation

Washington, DC
March 16, 2026

Introduction

DJI's petition to the Federal Communications Commission (FCC) for removal from the commission's Covered List should be dismissed on its merits. In its filing, DJI failed to acknowledge documented security vulnerabilities within its products, dismisses legitimate national security concerns held by numerous federal agencies and executive departments, and falsely alleges that the commission's actions were statutorily unlawful and relied on a flawed analysis of its products.

DJI's products contain several security vulnerabilities that directly endanger U.S. national security. DJI has flawed data storage and transfer practices, documented ties to the Chinese People's Liberation Army (PLA), and its products contain significant cybersecurity issues. These issues are heightened by irresolvable jurisdictional issues — as a Chinese firm, DJI is subject to the Chinese national security law that mandates that private entities provide collected information to Beijing upon request.

Federal agencies, including those with statutory authority to list DJI as a "national security risk," have long warned of these risks. Over the past six years, the Commerce Department, the Justice Department, the Department of Defense, and the Federal Bureau of Investigation (FBI) have all noted that DJI poses a risk to U.S. national security, whether due to its complicity in Chinese human rights abuses, its ties to the PLA, or its compromised cybersecurity practices.[1] These issues have also prompted Congress, repeatedly and on a bipartisan basis, to craft and pass multiple pieces of legislation to curtail DJI's access to the American market.

These risks and a congressional tasking prompted the FCC to use its statutory authority to add DJI to the Covered List due to the commission's national security concerns, which in turn were informed by a range of warnings, regulations, and legislation related to the firm. This process, which relied on publicly available information to determine specific risks related to DJI products entering the United States, was both appropriate and lawful.

DJI Poses a Clear and Pressing National Security Threat to the U.S.

Over the past decade, DJI's products have been routinely identified as a national security threat due to the firm's ties to Beijing and its numerous cybersecurity vulnerabilities. The integration of

[1] Bureau of Industry and Security, "Addition of Entities to the Entity List, Revision of Entry on the Entity List, and Removal of Entities From the Entity List," December 22, 2020. (https://www.federalregister.gov/documents/2020/12/22/2020-28031/addition-of-entities-to-the-entity-list-revision-of-entry-on-the-entity-list-and-removal-of-entities); National Defense Authorization Act for Fiscal Year 2025, Pub. L. No. 118-159, 138 Stat. 1515 (2024); Department of Defense, "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 (Public Law 116-283)," 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); Cybersecurity and Infrastructure Security Agency, Press Release, "Release Cybersecurity Guidance on Chinese-Manufactured UAS for Critical Infrastructure Owners and Operators," January 17, 2024. (https://www.cisa.gov/news-events/news/release-cybersecurity-guidance-chinese-manufactured-uas-critical-infrastructure-owners-and-operators)

DJI products into a range of U.S. critical infrastructure systems opened the possibility for these products to be used to conduct espionage and sabotage.

DJI Products Contain Significant Security Vulnerabilities

DJI's claim that federal government agencies have found no evidence of data transmission to the Chinese government or any other unexpected party is misleading and lacks significant context. Various federal agencies have documented significant cyber vulnerabilities associated with Chinese-produced unmanned aircraft systems (UAS) and acted accordingly, including noting that Chinese firms must comply with Beijing's request for private data under the auspices of the country's 2017 National Intelligence Law.[2] In 2017, the U.S. Army explicitly banned DJI drones due to "cyber vulnerabilities associated with DJI products."[3] Both the FBI and the Department of Homeland Security have also warned that Chinese-produced drones, including those that fit the criteria of UAS produced by DJI, pose a significant risk to U.S. critical infrastructure and may expose "sensitive information to PRC authorities."[4]

These findings have dramatically shifted federal guidance on the use of DJI products for government purposes, directly contradicting DJI's claims that the U.S. government has historically promoted its products. As part of the FY2024 National Defense Authorization Act (NDAA), Congress banned state, local, and tribal governments from using federal funds to purchase DJI UAS.[5] This effort complemented companion legislation passed in multiple states, including Florida and Nevada, to prevent local law enforcement offices from purchasing DJI UAS due to national security concerns.[6]

Moreover, the evidence that DJI cites to refute claims of data transmission is negated by publicly documented security flaws. While DJI has subjected some of its products to external auditing firms, most notably from Booz Allen Hamilton in 2021, other independent auditors have documented significant security vulnerabilities associated with DJI controllers and other products.[7] While all products have cybersecurity flaws, DJI's vulnerabilities are both more egregious — in one instance, a user was able to accidently reverse engineer a single DJI vacuum

---

[2] Jack Burnham, Craig Singleton, and Mark Montgomery, "Section 232 National Security Investigation of Imports of Unmanned Aircraft Systems (UAS) and Their Parts and Components," *Foundation for Defense of Democracies*, August 6, 2025. (https://www.fdd.org/analysis/2025/08/06/section-232-national-security-investigation-of-imports-of-unmanned-aircraft-systems-uas-and-their-parts-and-components); Cybersecurity and Infrastructure Security Agency, Press Release, "Release Cybersecurity Guidance on Chinese-Manufactured UAS for Critical Infrastructure Owners and Operators," January 17, 2024. (https://www.cisa.gov/news-events/news/release-cybersecurity-guidance-chinese-manufactured-uas-critical-infrastructure-owners-and-operators)

[3] Craig Singleton, "5 Things to Know About Chinese Drone Company DJI," *Foundation for Defense of Democracies*, June 12, 2024. (https://www.fdd.org/analysis/2024/06/12/5-things-to-know-about-chinese-drone-company-dji)

[4] Suzanne Smalley, "FBI and CISA warn of national security threat posed by Chinese drones," *The Record*, January 17, 2024. (https://therecord.media/fbi-cisa-warn-of-drone-threat-china)

[5] National Defense Authorization Act for Fiscal Year 2024, Pub. L. No. 118-31, 137 Stat. 136 (2023).

[6] Maurice Mugo, "DJI Ban in US 2026 Update, Timeline and Effects," *ABJ Drone Academy*, January 8, 2026. (https://abjacademy.global/drone-blog/dji-ban-in-us-update-timeline-and-effects)

[7] "Security Audits & Certifications," *DJI Trust Center*, accessed March 3, 2026. (https://www.dji.com/trust-center/resource/security-audits-certification); Mark Montgomery, "Extend the Pentagon's ban on China's consumer drones," *Defense One*, August 14, 2023. (https://www.defenseone.com/ideas/2023/08/extend-pentagons-ban-chinas-consumer-drones/389363)

to gain access to live audio and video feeds from 7,000 other vacuums — and are far riskier due to the firm's documented connections to Beijing.[8]

DJI Is Widely Recognized as a National Security Risk Across National Security Agencies

As discussed below, numerous executive agencies and Congress all share concerns about DJI, leading to a series of regulatory actions against the firm on national security grounds, a trend that DJI obfuscates throughout its filing.

Over the course of the past five years, a range of federal agencies, including those deemed by law as "appropriate national security agencies" for the purposes of determining FCC regulatory actions, have identified DJI as a security risk. The Bureau of Industry and Security (BIS) under the Department of Commerce added DJI to its Entity List in 2020 due to the firm's documented ties to human rights abuses conducted both within China and abroad — a finding that BIS declined to modify in a 2021 revision to DJI's standing.[9] The Department of Justice also restricted its grant recipients from using federal funds to purchase DJI products due to the department's concerns over DJI's potential compliance with China's National Intelligence Law and other Chinese laws that require the firm to transfer sensitive information to Chinese authorities.[10] These efforts complemented the Department of Defense's 2022 listing of DJI as a "Chinese military company" due to its affiliation with the PLA, a decision that survived a legal challenge by the firm in September.[11]

Congress has further identified DJI as a national security threat. Over the course of four consecutive sessions, Congress introduced several bills relating to DJI. Over the past four years, Congress enacted three of these laws. While each targeted different national security concerns through a range of regulatory mechanisms, they all consistently highlighted the firm's ties to Beijing, poor data storage and transfer practices, and the potential for DJI products to be used for espionage or sabotage.[12]

This trend directly contradicts DJI's argument that it should not be regulated as a threat to national security due to a lack of congressional interest. In its filing, the firm attempts to distinguish itself from TikTok by arguing that Congress does not have a similar track record of labeling its products as a threat. However, the legislative record clearly notes that DJI products pose an unacceptable risk to U.S. national security, having passed a series of bipartisan laws to target the firm's products. Most notably, Congress passed restrictions on DJI in both FY2024 and

[8] Mack DeGeurin, "Man accidentally gains control of 7,000 robot vacuums," *Popular Science*, February 21, 2026. (https://www.popsci.com/technology/robot-vacuum-army)
[9] Chaim Gartenberg and Russell Brandom, "US government adds DJI to Commerce blacklist over ties to Chinese government," *The Verge*, December 18, 2020. (https://www.theverge.com/2020/12/18/22188789/dji-ban-commerce-entity-list-drone-china-transaction-blocked)
[10] Maggie Miller, "DOJ bans use of grant funds for certain foreign-made drones," *The Hill*, October 8, 2020. (https://thehill.com/policy/cybersecurity/520269-justice-department-issues-policy-banning-use-of-grant-funds-for-certain)
[11] Mike Scarcella, "Drone maker DJI loses lawsuit to exit Pentagon's list of firms with Chinese military ties," *Reuters*, September 26, 2025. (https://www.reuters.com/legal/litigation/drone-maker-dji-loses-lawsuit-against-pentagon-claim-chinese-military-ties-2025-09-26)
[12] National Defense Authorization Act for Fiscal Year 2024, Pub. L. No. 118-31, 137 Stat. 136 (2023); National Defense Authorization Act for Fiscal Year 2025, Pub. L. No. 118-159, 138 Stat. 1515 (2024).

FY2025, showcasing the legislative branch's continued interest in pursuing restrictions on the use of Chinese UAS across a broad range of sectors.[13]

FCC Actions Maintained DJI's Right to Due Process

Contrary to DJI's claims, the FCC did not violate the firm's right to due process, and the FCC's decision-making process remains legally sound. Following nearly four years of regulatory actions across multiple administrations and subsequent congressional deliberation, the commission relied on its statutory authority to safeguard U.S. national security.

DJI's arguments that the FCC violated the firm's due process rights lack significant context, notably in the decision-making surrounding their addition to the Covered List. This difference is particularly notable given DJI's attempts to differentiate its claim from the precedent set by the Fifth Circuit in its 2021 decision in Huawei Techs. USA, Inc. v. FCC. While the FCC chose to identify Huawei for designation concurrent to its rule-making process on protecting the communications supply chain, the commission's basis for part of DJI's designation emerged from Section 1709 of the FY2024 NDAA.[14] The passage of this legislation involved significant public discussion over the merits of including DJI products on the Covered List. Section 1709 directly tasked the FCC with adding DJI to its Covered List.

This context suggests that DJI's claim of being denied due process is exaggerated — the affected party was informed of the basis of the action, was given access to unclassified evidence, and was afforded a series of platforms to rebut the presented evidence in public forums. While DJI may not have gained access to the deliberations of the interagency process that fed into the commission's actions, the firm should have been aware that such actions would occur following the passage of the NDAA. Rather, DJI's claims appear to rest on an effort to relitigate the outcome of a legitimate process, attempting to counter the FCC's implementation of a congressional directive.

Moreover, the penalties that DJI claims to have suffered due to the FCC's decision are not primarily a result of the commission's actions, but of congressional action. In its filing, DJI specifically contends that it will suffer $1.5 billion in losses from its inability to sell new "communications and video surveillance equipment and services" in the United States. The firm deems this loss illegitimate as it contends that the FCC cannot broadly ban components from specific countries.

However, the FCC used different statutory interpretations when regulating DJI UAS components as opposed to non-UAS components. While the commission does cite the text of the National Security Determination in its decision, which explicitly calls for a ban on foreign-produced UAS and UAS-critical components, the text of the Covered List that is relevant to non-UAS products

[13] National Defense Authorization Act for Fiscal Year 2024, Pub. L. No. 118-31, 137 Stat. 136 (2023); National Defense Authorization Act for Fiscal Year 2025, Pub. L. No. 118-159, 138 Stat. 1515 (2024).

[14] *Huawei Techs. USA, Inc. v. FCC*, 2 F.4th 421 (5th Cir. 2021). (https://www.ca5.uscourts.gov/opinions/pub/19/19-60896-CV0.pdf)

only cites the FY2025 NDAA.[15] This legislation notes only that the restrictions on communications or video surveillance equipment must apply to DJI and any affiliate, subsidiary, or partner, a clear indication of Congress's intent to regulate specific firms regardless of manufacturing footprint.

Conclusion

DJI's products pose a significant national security threat to the United States — a feature that has been repeatedly recognized by the U.S. military, national security agencies, the Department of Justice, and state governments over nearly a decade.[16] As such, DJI's petition to the FCC should be dismissed on its merits.

Thank you for considering our comments. We look forward to seeing how our input is incorporated into the FCC's consideration of this petition.

[15] Federal Communications Commission, Public Notice, "Public Safety and Homeland Security Bureau Announces Addition of Uncrewed Aircraft Systems (UAS) and UAS Critical Components Produced Abroad, and Equipment and Services Listed in Section 1709 of the FY2025 NDAA, to FCC Covered List," December 22, 2025. (https://docs.fcc.gov/public/attachments/DA-25-1086A1.pdf)

[16] Maurice Mugo, "DJI Ban in US 2026 Update, Timeline and Effects," *ABJ Drone Academy*, January 8, 2026. (https://abjacademy.global/drone-blog/dji-ban-in-us-update-timeline-and-effects)