



March 3, 2025

The Honorable Kristi Noem
Secretary
Department of Homeland Security
MS 0525 Department of Homeland Security
2707 Martin Luther King Jr. Ave SE
Washington, DC 20528-0525

The Honorable Pete Hegseth
Secretary
Department of Defense
1000 Defense Pentagon
Washington, DC 20301-1000

The Honorable Kash Patel
Director
Federal Bureau of Investigation
935 Pennsylvania Ave., NW
Washington, DC 20535-0001

The Honorable Gen. Timothy D. Haugh
Director
National Security Agency
9800 Savage Rd., Suite 6272
Fort George G. Meade, MD 20755-6000

The Honorable Tulsi Gabbard
Director
Office of the Director of National Intelligence
Office of Strategic Communications
Washington, DC 20511

Dear Secretary Noem, Secretary Hegseth, Director Patel, General Haugh, and Director Gabbard:

DJI was founded to develop drones that would make the world a better place and benefit society. From our beginnings in a single dorm room at the Hong Kong University of Science and Technology in 2006, DJI has grown to a global company with a global workforce. Today, DJI products are redefining industries. Professionals in law enforcement, agriculture, conservation, search and rescue, energy infrastructure, filmmaking and more trust DJI. Our products bring new perspectives to these professionals' work and help them accomplish feats more safely, faster, and with greater efficiency than ever before. They are also flown and enjoyed by hobbyists across America.

DJI has been credited with creating the small off-the-shelf drone category and holds (or has pending) more than 5,000 global patents. Thanks to this first-mover advantage and continued innovation, research, and development, global consumers choose DJI products overwhelmingly for commercial, scientific, public safety and recreational purposes.

Despite this success – or perhaps because of it – some policymakers have raised concerns that DJI's products may pose security or safety risks to the United States. And as you may know, Congress has tasked *any one of your agencies* with evaluating whether this is true.

We welcome this scrutiny.

Specifically, Section 1709 of the 2025 National Defense Authorization Act “mandates that within one year of enactment, a designated national security agency must evaluate whether communications and video surveillance equipment from these manufacturers pose ‘an unacceptable risk’ to U.S. national security or

the safety of American citizens.” If you determine that DJI’s drones pose an unacceptable risk, the Federal Communications Commission (FCC) must add them to its “covered list,” effectively restricting their use in the United States. If you do not evaluate DJI’s products in 2025, the FCC would also have to add the company’s equipment to its covered list, depriving DJI of its due process and depriving thousands of businesses, consumers, and public safety agencies of products that they want and need for no reason at all. **Accordingly, I write to request that *any or all* of your agencies begin this required evaluation of DJI’s products right away.**

DJI is confident that its products can withstand your strictest scrutiny. We are confident not only because we have nothing to hide, but because independent firms and other U.S. government agencies have repeatedly validated and confirmed that DJI’s products are secure. Through the years, companies including Booz Allen Hamilton,¹ FTI Consulting,² Kivu Consulting³ and TÜV SÜD,⁴ as well as the U.S. Department of Interior⁵ and the Idaho National Laboratory⁶, have purchased DJI products off-the-shelf, assessed DJI’s data security practices, and conducted thorough technical investigations. We have responded to their constructive feedback and shown a willingness to work with any agency as is requested; if necessary, we are also prepared to respond to and mitigate any specific vulnerabilities that anyone else may identify, as we regularly do through our “Bug Bounty” program as well.⁷

DJI data practices and products have previously received security certifications from international and U.S. government standard-setting bodies, including ISO 27001, ISO 27701, NIST FIPS 140-2 CMVP Level 1, and the American Institute of Certified Public Accountants SOC2 certification. Further, a 2022 audit confirmed that DJI products met NIST IR 8259 and ETSI EN 303645 standards in terms of network security and privacy protection. They are also GDPR-compliant and allow enterprise users to prevent unauthorized access to drone data by utilizing AES-256-XTS encryption – the longest encryption key length established by NIST when it developed its advanced encryption standard (AES).

Commercial, scientific, public safety and recreational users of DJI drones have a vested interest in the security of their data. As the world’s leading drone manufacturer, we stake our reputation on making sure our products and user data remain secure. We have implemented a number of features and protocols to ensure that our drones protect user data – while providing users with a way to fly their drones without any data transmission at all. For example:

- No flight logs, images, or videos are synced with DJI servers unless a user affirmatively chooses to sync with a DJI server.
- U.S. users cannot sync their flight records to DJI’s servers at all.
- Users can fly offline or in “Local Data Mode,” which severs the connection between the flight app and the internet to prevent data sharing, even inadvertently.

¹ Available at: [https://terra-1-g.djicdn.com/851d20f7b9f64838a34cd02351370894/trust-center/BOOZ%20ALLEN%20HAMILTON%20-%20UAS%20COE%20AUDIT%20\(2020\).pdf](https://terra-1-g.djicdn.com/851d20f7b9f64838a34cd02351370894/trust-center/BOOZ%20ALLEN%20HAMILTON%20-%20UAS%20COE%20AUDIT%20(2020).pdf)

² Two separate evaluations, conducted in 2022 and 2024, available at: https://security.dji.com/asset/files/2020_09--FTI%20Cybersecurity--Executive%20Summary%20of%20DJI%20Assessment.pdf and https://terra-1-g.djicdn.com/851d20f7b9f64838a34cd02351370894/trust-center/2024_09--FTI%20Cybersecurity--Executive%20Summary%20of%20DJI%20Assessment.pdf

³ See: <https://www.dji.com/newsroom/news/independent-study-validates-dji-data-security-practices>

⁴ See: <https://www.dji.com/newsroom/news/new-independent-audit-of-select-dji-products-successfully-tests-against-national-cybersecurity-and-privacy-protection-standards>

⁵ Available at: [https://terra-1-g.djicdn.com/851d20f7b9f64838a34cd02351370894/trust-center/U.S.%20DEPARTMENT%20OF%20INTERIOR%20AUDIT%20\(2019\).pdf](https://terra-1-g.djicdn.com/851d20f7b9f64838a34cd02351370894/trust-center/U.S.%20DEPARTMENT%20OF%20INTERIOR%20AUDIT%20(2019).pdf)

⁶ Available at: <https://terra-1-g.djicdn.com/851d20f7b9f64838a34cd02351370894/trust-center/INL-Drone-Report-Oct-2019.pdf>

⁷ Bug Bounty policy available at: https://security.dji.com/policy?lang=en_US

- Users can amend their data preferences at any time through the app's settings, easily delete information on the drone, or download third-party software solutions. They can even disable the DJI flight app altogether, if they prefer.⁸

DJI's drones are the most capable, best priced, and most reliable commercial drones currently in use today. Restricting DJI drone imports or use would have a ripple effect throughout the entire U.S. drone ecosystem. A recent economic impact analysis found that DJI enables more than \$116 billion in economic activity across the U.S. and supports more than 450,000 American jobs.

The people who have built livelihoods using DJI products deserve a fair and timely evaluation by your agencies to lift the cloud on our company and reassure DJI's customers and the American public that DJI's drones are safe and secure.

Our commitment to safety and security is steadfast, and we pledge our full cooperation during this process, including by providing you with any information or assistance that will help. We also believe it will be useful for you to meet with DJI as part of a fair evaluation process. Accordingly, we respectfully request a meeting with you or your staff at your earliest convenience to demonstrate the data security features on our drones, address any questions or concerns, and ensure your evaluation is carried out in a timely manner.

Sincerely,



Adam Welsh
Head of Global Policy
DJI

CC: Sen. Roger Wicker, Chair, Senate Armed Services Committee
Sen. Jack Reed, Ranking Member, Senate Armed Services Committee
Members of the Senate Armed Services Committee

Sen. Rand Paul, Chair, Senate Committee on Homeland Security & Governmental Affairs
Sen. Gary Peters, Ranking Member, Senate Committee on Homeland Security & Governmental Affairs
Members of the Senate Committee on Homeland Security & Governmental Affairs

Rep. Mike Rogers, Chair, House Armed Services Committee
Rep. Adam Smith, Ranking Member, House Armed Services Committee
Members of the House Armed Services Committee

Rep. Mark Green, Chair, House Homeland Security Committee
Rep. Bennie Thompson, Ranking Member, House Homeland Security Committee
Members of the House Homeland Security Committee

⁸ For more information about DJI's security and privacy features, visit <https://www.dji.com/trust-center>