



December 1, 2025

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

The Honorable Lt. Gen. William Hartman  
Acting 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

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

Dear Secretary Hegseth, Director Gabbard, Director Patel, and Acting Director Hartman:

We are writing to follow up on our letters to you dated March 3, 2025 and June 18, 2025, urging that one of your agencies initiate the security review of DJI Technology products as Congress has mandated under Section 1709 of the 2025 National Defense Authorization Act.<sup>1</sup> With less than one month left before the December 23, 2025 deadline, we urge you to take up this audit immediately to avoid any negative consequences to American drone users, including our public safety and law enforcement officers, and to provide them with answers about the security of DJI products.

Our position on this audit has never wavered: we stand ready to work with you, to be open and transparent, and provide you with the necessary information to complete a thorough review. To date, these offers have gone unanswered, and public reports suggest that this audit has not yet commenced. With time running out, we once again are calling for this audit to take place immediately to avoid the automatic addition of DJI products to the FCC's "Covered List" that would take place if the audit is not completed by December 23. Doing so would lead to widespread consumer confusion and deprive American drone users of due process – and of answers about the safety and security of the DJI products they use every day. Failing to undertake the review further goes against Congressional intent for a security review to be completed.

If a security review is carried out, we are confident that DJI products will withstand your scrutiny. In fact, DJI products have already undergone repeated validations by both independent firms and other U.S. government agencies, including those conducted by Booz Allen Hamilton,<sup>2</sup> FTI Consulting,<sup>3</sup> Kivu Consulting<sup>4</sup> and TÜV SÜD,<sup>5</sup> as well as the U.S. Department of Interior<sup>6</sup> and the Idaho National Laboratory (at the direction of DHS).<sup>7</sup> Each of these organizations purchased DJI products off-the-shelf, assessed DJI's data security practices, and conducted thorough technical investigations. We coordinated with these

---

<sup>1</sup> 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."

<sup>2</sup> 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)

<sup>3</sup> 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](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](https://terra-1-g.djicdn.com/851d20f7b9f64838a34cd02351370894/trust-center/2024_09--FTI%20Cybersecurity--Executive%20Summary%20of%20DJI%20Assessment.pdf)

<sup>4</sup> See: <https://www.dji.com/newsroom/news/independent-study-validates-dji-data-security-practices>

<sup>5</sup> See: <https://www.dji.com/newsroom/news/new-independent-audit-of-select-dji-products-successfully-tests-against-national-cybersecurity-and-privacy-protection-standards>

<sup>6</sup> 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)

<sup>7</sup> Available at: <https://terra-1-g.djicdn.com/851d20f7b9f64838a34cd02351370894/trust-center/INL-Drone-Report-Oct-2019.pdf>

agencies as needed and responded readily to any identified vulnerabilities. We are similarly prepared to cooperate with any or all of your agencies during this process, and are ready to respond to and mitigate any specific vulnerabilities that may be identified if given a fair right of reply.

In addition to undergoing and passing previous security reviews, DJI data practices and products have 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. Our drones 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).

The security of our users' data is the utmost priority, and we stake our reputation on the validity of these past audits and certifications. As countless commercial, public safety, and recreational users of DJI drones know, we offer features and protocols to ensure that they can remain in control of their data and what they choose to share. For example, U.S. users cannot sync flight logs to DJI servers at all, and no images or videos are synced with DJI servers unless a user proactively chooses to do so. Users can also fly offline or in "Local Data Mode," which severs the connection between the flight app and the internet to prevent data sharing, even inadvertently. If they prefer, they can even disable the DJI flight app altogether and instead use software from third-party providers, including several American companies.

We stand behind the security of our technology, and with time running out, we are keen to meet with you and ensure that this Congressionally-mandated security review takes place as soon as possible. My team and I are available at any time to provide information that may be helpful and ensure that a fair and thorough audit is indeed carried out before it is too late.

The American people, including those who use DJI drones for their jobs,<sup>8</sup> for their livelihoods, or for ensuring the safety and security of our communities, deserve no less.

Sincerely,

A handwritten signature in black ink that reads "Adam Welsh". The signature is fluid and cursive, with the first name "Adam" and last name "Welsh" clearly distinguishable.

Adam Welsh  
Head of Global Policy  
DJI

---

<sup>8</sup> 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.