March 3, 2025

SZ DJI Technology Co. Ltd. ("DJI") appreciates the opportunity to submit a comment on the Department of Commerce, Bureau of Industry and Security's ("BIS") advanced notice of proposed rulemaking ("ANPRM") entitled "Securing the Information and Communications Technology and Services Supply Chain: Unmanned Aircraft Systems."[1]

I. About DJI

DJI is the world's largest, privately-owned manufacturer of consumer and commercial unmanned aerial systems ("UAS"). The company is headquartered in Shenzhen, China, with offices throughout Asia, Europe, and the United States.

DJI has been a leader in consumer and commercial drone innovation, which has enabled it to offer the most capable drone products in the United States and more than 100 other countries. DJI's unique combination of range of products, reliability and product capability enable a large number of police departments, fire departments, other first responders, large and small companies, and hobbyists in the United States to use DJI drones to save lives and promote public safety, decrease the risk of worker injury, and accomplish other difficult tasks, improving the overall quality and value of the services they offer. DJI products have been consistently recognized for their quality and value. Last month, *PC Magazine* awarded DJI drones "Best Drone Overall," "Best Obstacle Avoidance System," "Best Drone for Pro Video and Cinema," "Best Selfie Drone," "Best Racing Drone," "Best Budget Drone," and "Best Entry-Level Cinema Drone."[2]

As one article noted: "No other company's offerings come close to DJI's cheap, powerful drones, experts say—potentially leaving government agencies, police and first responders in the lurch if DJI is shut out."[3] For example, a recent U.S. Government Accountability Office ("GAO") report found that the Department of the Interior's decision to not use Chinese-made drones (which primarily affects DJI drones), has left its component bureaus with an insufficient number of drones to mount an acceptable response in critical emergency situations.[4] Competitor drone companies simply do not

[1] Securing the Information and Communications Technology and Services Supply Chain: Unmanned Aircraft Systems, 90 Fed. Reg. 271 (Jan. 3, 2025).

[2] Jim Fisher, *The Best Drones for 2025*, PC MAG (Feb. 11, 2025), available here; *see also* Andrew Lanxon, Joshua Goldman, *Best Drones for 2025*, CNET (Jan. 22, 2025), available here (identifying DJI drones as its top 2025 picks for capturing high-quality photos or videos).

[3] Kaveh Waddell, *Searching for the next great American drone company*, AXIOS (Nov. 23, 2019), available here.

[4] GOVERNMENT ACCOUNTABILITY OFFICE, FEDERAL LANDS: EFFECTS OF INTERIOR'S POLICIES ON FOREIGN-MADE DRONES, 24-106924, 1-2 (Sept. 25, 2024).

provide products with the same functionality, meaning many government agencies and companies in the United States either use DJI drones or no drones at all.[5]

DJI contributes significantly to the U.S. economy. An economic impact report indicated that the use of DJI products generates more than $116 billion in economic benefits in the United States and supports 450,000 U.S. jobs.[6] U.S. software and hardware firms have built entire businesses around DJI products, while a number of U.S. companies and other organizations across sectors depend on them to perform important functions. DJI has been credited with creating the small UAS drone category as we were the first to put a complete drone out for sale in 2013 and moved to enterprise products rapidly after that in 2016. As such, 2/3 of drone service providers surveyed said they would go out of business without access to drones like DJI's.

As with many technology companies, DJI began as a start up in the dorm room of its founder. Today, DJI's founder and early-stage individual investors together hold more than 99% of the company's voting rights and approximately 90% of its shares, underlying the company's independence. No Chinese government entity or representative sits on DJI's board or has any role in its operations, and no shareholder maintains any special rights.

II. Discussion

To the extent BIS is contemplating proposing a blanket restriction on UAS manufactured in China, we respectfully submit that this approach is unnecessary, conceptually flawed, and would be extremely harmful to U.S. stakeholders.[7]

Any new UAS-specific ICTS regulation would be unnecessary given the existing ICTS rule that authorizes BIS, on a company-specific basis, to review and, if necessary, restrict certain transactions involving drones. In addition to being unnecessary, a blanket restriction on UAS manufactured in China would be based on the inaccurate assumption that all UAS manufactured by companies organized in China pose unreasonable security risks. However, differences in UAS security features (regardless of a manufacturer's location) determine the level of potential security risks posed by UAS. There are more targeted means to achieving BIS's security goals without wholesale cutting off products that numerous U.S. first responders and companies use every day to save lives, protect workers from injury, promote innovation, and provide other valuable services.

[5] *See id.* at 6.

[6] *See The Secret to DJI's Market Leadership*, VIEWPOINTS (June 28, 2024), available here.

[7] This comment focuses on several substantive flaws in the contemplated rulemaking, but does not address other substantive and legal issues.

Therefore, any regulatory action should focus on the security features of UAS, and not on the country in which the UAS manufacturers[8] are located.

Below, we (1) explain why a new rule targeting ICTS transactions involving UAS is unnecessary because the existing ICTS rule already covers UAS; (2) provide important clarification regarding the ANPRM's discussion of potential risks related to Remote ID and No-Fly Zones; and (3) describe the security features used by DJI drones, which mitigate the security concerns described in the ANPRM.[9]

1. BIS Should Not Initiate the Proposed Rulemaking Because Drones Are Already Covered by the Existing ICTS Regulation

The contemplated rulemaking would be the quintessential example of the unnecessary regulation that President Trump promised to cut.[10] BIS has made clear its position that it already has authority to review and restrict certain transactions involving drones under the existing ICTS regulation.[11] In fact, BIS recently updated that regulation with the intention of covering a broader range of ICTS transactions involving UAS.[12] The ANPRM does not explain why that existing ICTS rule is inadequate to address the identified risks or justify the overbroad regulatory burdens the contemplated rulemaking would impose on UAS manufacturers and U.S. stakeholders that buy and use drones.

2. The ANPRM's Discussion of Risks Related to Remote ID and No-Fly Zones Ignores the Role of Federal Aviation Administration Regulations

The ANPRM inaccurately portrays the nature of the risks related to Remote ID and geofencing. DJI complies with Federal Aviation Administration ("FAA")

---

[8] DJI here uses "manufacturers" as an umbrella term that includes, as defined in the ANPRM, UAS companies, UAS Original Equipment Manufacturers, and UAS service providers. *See* 90 Fed. Reg. 271, 276.

[9] This comment therefore responds to BIS's request for "comment on processes and mechanisms that BIS could implement in a potential rule to authorize otherwise prohibited ICTS transactions if the parties to such transactions adopt certain mitigation measures or otherwise mitigate the undue and unacceptable risks to U.S. national security, including U.S. ICTS supply chains and critical infrastructure, or to the safety and security of U.S. persons." *Id.* at 279.

[10] *See* Exec. Order No. 14,192, 90 Fed. Reg. 9065 (Jan. 31, 2025) ("It is the policy of the executive branch to . . . alleviate unnecessary regulatory burdens placed on the American people."); *Fact Sheet: President Donald J. Trump Launches Massive 10-1 Deregulatory Initiative*, Whitehouse.gov (Jan. 31, 2025), available here ("Overregulation stops American entrepreneurship, crushes small business, reduces consumer choice, discourages innovation, and infringes on the liberties of American citizens.").

[11] *See* 15 C.F.R. § 791.3 (authorizing BIS to review of "Any ICTS Transaction that . . . (4) involves ICTS and software, hardware, or any other product or service integral to one of the following . . .(i) information and communications hardware and software, including . . . (E) internet-enabled sensors, cameras, and any other end-point surveillance or monitoring device, or any device that includes these components such as drones").

[12] *See* Securing the Information and Communications Technology and Services Supply Chain, 89 Fed. Reg. 96872 (Dec. 6, 2024) (removing the one million unit or person threshold for ICTS transactions involving drones or software applications, among other ICTS items).

regulations and best practices. BIS should not penalize DJI (or any other UAS manufacturer) for complying with lawfully-promulgated regulations and guidance by characterizing such compliance as a security "risk."

a. Remote ID

As required by FAA regulations, DJI drones emit Remote ID radio signals.[13] These signals function as a type of "license plate" for UAS, allowing authorities to identify the UAS and pinpoint its location and altitude, as well as its control station's location.[14] Importantly, Remote ID data is *not* collected or stored by DJI. BIS, citing articles that warn of risks related to Remote ID,[15] notes that "researchers studying this issue have been successful in reverse engineering the radio frequency that controls a UAS and have been able to pinpoint the position of the UAS, the UAS home point, and the remote pilot's location."[16] Their access, BIS states, "could lead to the exfiltration of sensitive data, including real-time video feeds and geolocation information, which can be used to gather intelligence and conduct surveillance to threaten U.S. national security, including U.S. ICTS supply chains and critical infrastructure, or the security and safety of U.S. persons."[17]

The ANPRM's discussion of these potential risks completely ignores that the FAA *requires* all UAS to provide Remote ID. In fact, the ANPRM fails to mention that the FAA, in its 2021 rule on "Remote Identification of Unmanned Aircraft," explicitly considered and then rejected permitting drone operators to encrypt their Remote ID because, as FAA explains, encryption would frustrate "receiving wireless devices[' ability] to decode the messages and make the contents of the remote identification messages usable to the public."[18] Thus, to the extent that the FAA's required Remote ID creates risks of threat actor intrusion, it is a risk that DJI—and any other UAS manufacturer—legally cannot mitigate.[19] Any risks posed by the unencrypted nature of Remote ID are present for all UAS, regardless of where they are manufactured.

---

[13] *See Remote Identification of Drones*, Fed. Aviation Admin., available here (accessed Feb. 14, 2025).

[14] *FAQs about FAA Remote ID Compliance*, available here (accessed Feb. 15, 2025).

[15] Among these articles, BIS cites a U.S. Army determination that DJI pose "operational risks," however, the Army's memo does not explain what those risks are, nor does BIS explain how those un-identified risks might apply to the civilian context. 90 Fed. Reg. at 277 (citing Gary Mortimer, *US Army calls for units to discontinue use of DJI equipment*, sUAS (Aug. 2018), available here). It therefore does not provide additional support for BIS's above conclusions.

[16] *Id.* at 277-78.

[17] *Id.* at 278.

[18] *Remote Identification of Drones*, Fed. Aviation Admin., available here (accessed Feb. 14, 2025); *Remote Identification of Unmanned Aircraft*, 86 Fed. Reg. 4390, 4428 (Jan. 15, 2021).

[19] Note that this comment also responds directly to BIS's request for comment on "[w]hat, if any, industry standard policies or procedures govern how UAS communicate, [and] what kinds of information UAS can communicate . . . ?" 90 Fed. Reg. at 278.

Moreover, the ANPRM conflates the ability to access Remote ID data with a potential risk of remote access. The ANPRM posits that "malicious actors could gain illicit access to cloud platforms used by UAS to store data or authorize remote control access." Such a theoretical hacking risk exists for any electronic system. DJI has implemented a comprehensive security program, described in more detail below, which mitigates such risk by limiting the information that DJI collects, designing DJI drones to be able to be used with no internet connection at all, and additional measures to secure DJI drones and user data, including settings that allow users to avoid sending data to cloud platforms at all or to utilize private server deployments.

b. No-Fly Zones

DJI is the industry leader in drone safety and was the first major civilian UAS manufacturer to implement geofencing, a mechanism that prevents UAS from entering into or taking off from restricted zones. Geofencing was not required by law or regulation, but DJI added it as an additional safety feature, determining restricted zones, including airports, power plants, and prisons, based on aviation and public safety requirements, and has worked with local authorities to implement additional geofencing requests. Since DJI first implemented geofencing in 2013, global regulations and user awareness of flight restrictions have increased significantly, and so in January 2025, DJI announced that it was updating its geofencing system to display FAA "No Drone Zone" data to align with U.S. regulations. [20]

Notwithstanding the public safety rationale for introducing geofencing and the FAA's prohibitions on users flying in restricted zones, the ANPRM portrays geofencing as a security *risk*. It states that "pushing forced [geofencing] updates that disable UAS in predefined zones" is a "vector" "through which a foreign adversary could abuse its access and influence over a company intentionally to target UAS products owned by U.S. persons or operated in the United States, disrupt their operation, and in turn severely impact U.S. national security[.]"[21]

DJI is not aware of any allegations that it or any other UAS manufacturer has abused geofencing technology, such as to improperly "disrupt" the use of drones by users. In any event, as a result of the January 2025 updates noted above, DJI will notify users about FAA restrictions and will no longer disable DJI's drones from operating in restricted areas pursuant to FAA regulations, rendering moot the risk that a foreign adversary could force DJI to disable UAS from operating in certain areas. Further, the notion that DJI or any UAS manufacturer would misuse geofencing technology to improperly disrupt users' operation of the drones is unrealistic, entirely speculative and patently untrue, particularly given the liability risk that manufacturers could incur for such actions.

[20] *DJI Updates GEO System in U.S. Consumer & Enterprise Drones*, VIEWPOINTS (Jan. 13, 2025), available here.

[21] 90 Fed. Reg. at 276.

3. DJI's Security Features Mitigate Security Risks

As the discussion above regarding Remote ID and geofencing illustrates, many of the potential risks associated with UAS are ubiquitous and not limited to UAS manufactured in China. Any regulatory approach to address perceived risks to U.S. users, such as those associated with potential data exfiltration and remote access control, should ensure that all UAS manufacturers take appropriate steps to mitigate these risks. As BIS considers potential mitigation measures, DJI believes that many of its practices can serve as a model for all UAS manufacturers. Below, DJI provides a high-level overview of its approach to security that mitigates potential risks related to data exfiltration and remote access control. More detailed information can be found in DJI's Drone Security White Paper, which outlines key systems in DJI drones and the security measures that DJI has implemented to bolster security, enhance privacy controls, and protect the integrity of user data.[22]

First, DJI drones sold in the United States do not incorporate telecommunication capabilities. Specifically, DJI drones sold here do not have any internet connection capability, nor do they need to connect to the internet to operate. Following initial activation, DJI drones can be used entirely offline, including with a drone control app on a device in "airplane mode." Additionally, consumer and enterprise drone users can enable Local Data Mode, which prevents any data from being transmitted to or from DJI's flight apps and servers while allowing users to access the internet for particular purposes like map services. As a result of these practices, DJI is able to "secure data that is transmitted, received, or stored during the normal operation of a UAS without connecting it to the internet."[23]

Second, by default, customer data such as flight records, device logs, video, and geolocation data is not shared with DJI. Thus, unless they affirmatively choose to share their data with others, DJI UAS users are the only parties with "authorized access to, or control of, data collected by the[ir] UAS."[24] Even if users chose to share their UAS data through the DJI drone control app (e.g., when a user proactively chooses to upload photos or videos to DJI sharing services, or shares device logs in connection with a request for service or repairs), they retain the ability to decide when to stop sharing. In other words, users maintain control over the sharing of their data. DJI encourages users to review the app's privacy features before UAS operation and provides users with guidelines on drone data privacy controls.[25]

Third, for the user data and other data that DJI drones do receive, DJI has adopted industry and government standard data encryption measures for securing user data in the

---

[22] Drone Security White Paper Version 3.0, DJI, available here (accessed Feb. 26, 2025).

[23] 90 Fed. Reg. at 277.

[24] *Id.*

[25] *User Guide: Consumer Drone Privacy Controls*, DJI, available here (accessed Feb. 17, 2025); *User Guide: Enterprise Drone Privacy Controls*, DJI, available here (accessed Feb. 17, 2025).

course of data transmission and data storage. As a result, user data, signature, authentication, digest, and data transmission are all encrypted. This set of "cybersecurity measures, authentication, or controls" that DJI utilizes to "mitigate risks surrounding data collection, access, storage, processing, and exfiltration,"[26] mitigates concerns about the potential interception of data associated with the normal operation of DJI UAS.

Fourth, DJI UAS do not contain any features or functionality that would allow DJI to remotely access, control, or monitor those products. DJI can only access users' UAS if a user provides DJI with *physical* access to the drone, such as for repair services.

Fifth, with respect to DJI enterprise UAS customers, DJI incorporates a range of security and privacy features. These features include a number of network security modes including Local Data Mode, integration of DJI software on private clouds, offline maps and offline firmware updates, media data encryption, and cache management, and drone log one-click deletion.[27] These are further examples of "cybersecurity measures, authentication, or controls [that] UAS service providers . . . use to mitigate risks surrounding data collection, access, storage, processing, and exfiltration."[28]

Sixth, for over a decade, DJI has consistently invested in improving and testing its security features and protocols. In 2017, DJI launched its Bug Bounty program, incentivizing third-parties to search for and flag possible "bugs" in DJI software so that DJI can locate and address possible security risks.[29] DJI also regularly engages independent consulting firms to conduct third-party audits to validate its data practices.[30] Third-party consulting firms such as Booz Allen Hamilton, FTI Consulting, and Kivu Consulting have analyzed various DJI products and validated their security.[31] So too have the U.S. Department of the Interior, the U.S. National Oceanic and Atmospheric Administration, the U.S. Department of Homeland Security, and the U.S. Department of Defense.[32] These audits review DJI's data security practices including, but not limited to,

---

[26] 90 Fed. Reg. at 277.

[27] *See* Drone Security White Paper Version 3.0*, supra*.

[28] 90 Fed. Reg. at 277.

[29] *See DJI Bug Bounty Program Policy*, DJI (updated Mar. 27, 2024), available here.

[30] *See, e.g. New Independent Audit Confirms Robust Privacy Controls Available To DJI Drone Operators*, VIEWPOINTS (Sept. 25, 2024), available here.

[31] *New Independent Audit Confirms Robust Privacy Controls Available To DJI Drone Operators*, VIEWPOINTS (Sept. 25, 2024), available here; *New Independent Audit Finds No Evidence of Data Transmission to DJI, China, or Any Unexpected Party*, VIEWPOINTS (Dec. 9, 2021), available here (detailing the scope of these security evaluations and their findings).

[32] More information about the scope of these security evaluations and their findings can be found at *New Independent Audit Finds No Evidence of Data Transmission to DJJI, China, or Any Unexpected Party,* VIEWPOINTS (Dec. 9, 2021), available here; *see also* Chris Mills Rodrigo & Maggie Miller, *Pentagon report clears use of drones made by top Chinese manufacturer*, The Hill (June 1, 2021), available here ("An analysis of the two Da Jiang Innovations [DJI] drones built for government use found 'no malicious code or intent' and are 'recommended for use by government entities and forces working with US

practices related to "any data generated by, owned by, or otherwise associated with U.S. persons."[33]

III. Conclusion

The ANPRM takes a flawed approach in its apparent treatment of all UAS manufactured in China as posing unreasonable security risks. Any risk varies from manufacturer to manufacturer depending on the security features of their UAS and data collection practices. A more sensible regulatory approach—to the extent any new rulemaking is necessary to address risks that cannot be addressed under provisions in the existing ICTS regulation that explicitly cover UAS—would be to impose minimum security requirements across all UAS manufacturers, regardless of their country of incorporation. By contrast, an approach that wholesale prohibits UAS manufactured in China would significantly harm a number of U.S. stakeholders, including numerous public safety agencies, small businesses, software companies, and many other private sector and governmental organizations throughout the United States that depend on DJI drones to save lives, decrease the risk of worker injuries, earn their living, and accomplish other critical tasks.

services.'"). The report was later disavowed without explanation in a subsequent press release. *See* Department Statement on DJI Systems, U.S. Dep't of Defense (July 23, 2021), available here.

[33] 90 Fed. Reg. at 277.