RAND PAUL, KENTUCKY, CHAIRMAN

RON JOHNSON, WISCONSIN
JAMES LANKFORD, OKLAHOMA
RICK SCOTT, FLORIDA
JOSH HAWLEY, MISSOURI
BERNIE MORENO, OHIO
JONI ERNST, IOWA
ASHLEY MOODY, FLORIDA

GARY C. PETERS, MICHIGAN
MARGARET WOOD HASSAN, NEW HAMPSHIRE
RICHARD BLUMENTHAL, CONNECTICUT
JOHN FETTERMAN, PENNSYLVANIA
ANDY KIM, NEW JERSEY
RUBEN GALLEGO, ARIZONA
ELISSA SLOTKIN, MICHIGAN

United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
WASHINGTON, DC 20510–6250

December 18, 2025

Robert Blalock
Chief Executive Officer
Brasfield & Gorrie, LLC
3021 7th Avenue South
Birmingham, AL 35233

Dear Mr. Blalock:

I am writing to request information about your company's relationship with the Chinese drone manufacturer Da-Jiang Innovations (DJI) and compliance with federal rules regarding the use of DJI drones, as well as the potential exposure of sensitive information about defense, nuclear, and border security facilities. The U.S. government considers the use of Chinese-made drones generally — and DJI drones specifically — a threat to national security and prohibits their use by federal agencies or contractors. Recent reporting, however, has raised questions about the extent to which key contractors have complied with these prohibitions and the nature of their relationships with DJI.

Construction companies use drones for a variety of purposes, including, but not limited to, surveying and mapping, tracking construction progress, and inspecting potential safety issues.[1] Such drones can be equipped with a variety of cameras and sensors, including systems that use lasers to map the exact shape of buildings, terrain, and vegetation.[2] These drone-supported cameras can capture large amounts of information about the locations they are employed at, including strategically important locations and secure facilities. Importantly, detailed information about the design of secure facilities is often sensitive and can be classified if it shows undisclosed security features or potential vulnerabilities.[3]

---

[1] DJI Enterprise, *Drones in construction: Aerial assistance on the job site* (July 6, 2022) (enterprise-insights.dji.com/blog/construction-drones).

[2] *Id.*

[3] *Sensitive Documents, Including White House Floor Plans, Improperly Shared with Thousands*, The Washington Post (Apr. 20, 2025) (www.washingtonpost.com/politics/2025/04/20/trump-biden-sensitive-documents-shared/); *See also*, 10 CFR § 73.22.

Large construction companies were early adopters of drone technology, a market DJI has dominated.[4] Companies that use DJI construction drones include the builders of some of the most sensitive defense and border security sites in the United States. This includes the Bechtel Corporation (Bechtel), which has constructed nuclear weapons labs and missile bases[5] and was one of the first engineering and construction companies to establish a drone program.[6] As early as 2017, Bechtel cohosted a webinar with DJI entitled, "Getting Started with Drones in Construction."[7] Likewise, Hensel Phelps, a contractor for nuclear weapons facilities as well as ports of entry along the Southwest Border,[8] was the first construction company to obtain government approval to fly construction drones over populated areas.[9] A profile of the company and an interview with a Hensel Phelps executive from 2020 remains available on DJI's website.[10] Brasfield & Gorrie, another construction contractor at ports of entry and U.S. military bases,[11] was the subject of a DJI case study in 2017 that highlighted drones' data collection capabilities.[12]

According to a January 2024 joint bulletin from the Cybersecurity & Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI), Chinese-manufactured

---

[4] *The Secret to DJI's Drone Market Dominance: Revealed*, Drone DJ (Aug. 13, 2024) (dronedj.com/2024/08/13/dji-china-drone-success-secret/).

[5] Bechtel, *National Defense & Security Projects* (www.bechtel.com/markets/national-defense/).

[6] Bechtel: *Bechtel Among First Companies to Use Unmanned Aircraft System Technology in Construction* (Apr. 6, 2015) (www.bechtel.com/press-releases/bechtel-among-first-companies-to-use-unmanned-aircraft-system-technology-in-construction/).

[7] Skycatch, *Getting Started with Drones in Construction,* YOUTUBE (Aug. 31, 2017) (www.youtube.com/watch?v=WLnouZ8szo4).

[8] *E.g.*, Hensel Pehlps, *Calexico West Land Port of Entry Phase 2A* (www.henselphelps.com/project/calexico-west-land-port-of-entry-phase-2a-modernization/); Hensel Phelps, *Meeting America's Deterrence Needs Through Energizing Partnerships* (Mar. 26, 2025) (www.henselphelps.com/americas-deterrence-needs-through-partnerships/).

[9] Hensel Phelps: *FAA Grants Hensel Phelps Approval for Drone Operations Over People* (June 6, 2019) (www.henselphelps.com/faa-grants-hensel-phelps-approval-drone-operations-people/).

[10] DJI Enterprise, *General Contractor Hensel Phelps Is Pushing the Boundaries Of Drones In Construction* (May 20, 2020) (enterprise-insights.dji.com/user-stories/drones-in-construction-hensel-phelps).

[11] Brasfield & Gorrie, *Government* (www.brasfieldgorrie.com/markets/government/).

[12] DJI Enterprise, *DJI and DroneDeploy Bring New Turnkey Mapping Solution to the Construction Industry* (May 15, 2017) (enterprise.dji.com/news/detail/dji-and-dronedeploy-bring-new-turnkey-mapping-solution-to-the-construction-industry).

drones present three key security vulnerabilities.[13] First, they provide a means of data transfer and collection.[14] The bulletin states that "[drones] controlled by smartphones and other internet-connected devices provide a path for [drone] data egress and storage, allowing for intelligence gathering on U.S. critical infrastructure."[15] Second, patching and firmware updates to drones could "introduce unknown data collection and transmission capabilities without the user's awareness."[16] Third, drones connected to a network create "the potential for data collection and transmission of a broader type — *for example, sensitive imagery, surveying data, facility layouts* [emphasis added]."[17] As CISA and the FBI note, these risks are present with all drone technology but are especially concerning with Chinese-made drones, as Chinese law compels cooperation between private companies and state intelligence services.[18] In short, it appears that the use of these types of drones at sensitive and secure facilities creates the potential to provide a pathway for the transfer of important national security-related information to the Chinese government. For its part, DJI disputes claims that it poses a national security risk to the United States and has commissioned several third-party audits appearing to show that its drones are secure.[19]

The U.S. government, however, has reported on potential security risks associated with DJI since at least 2017.[20] In recent years, Congress and the Executive Branch have sought to address these possible risks, including through a 2019 Congressional prohibition on the Department of Defense (DOD) using or purchasing Chinese-made drones;[21] the 2020 addition of DJI to the Department of Commerce Entity List, designating the company as a national security concern;[22] a 2021 executive order advising all federal agencies against purchasing and using

---

[13] Cybersecurity & Infrastructure Security Administration and the Federal Bureau of Investigation, *Cybersecurity Guidance: Chinese-Manufactured UAS* (Jan. 17, 2024).

[14] *Id.*

[15] *Id.*

[16] *Id.*

[17] *Id.*

[18] *Id.*

[19] *New Independent Audit Confirms Robust Privacy Controls Available To DJI Drone Operators*, DJI Viewpoints (blog) (Sept. 25, 2024) (viewpoints.dji.com/blog/new-independent-audit-confirms-robust-privacy-controls-available-to-dji-drone-operators).

[20] Homeland Security Investigations, *Da Jiang Innovations (DJI) Likely Providing U.S. Critical Infrastructure and Law Enforcement Data to Chinese Government* (ICE-IL-17-0019) (Aug. 9, 2017).

[21] National Defense Authorization Act of 2020, Pub. L. 116-92, Sec. 848 (2019).

[22] Department of Commerce, 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,* 85 Fed. Reg. 83416 (Dec. 12, 2020) (final rule).

drones manufactured by foreign adversaries;[23] and the October 2022 addition of DJI to the DOD list of Chinese military companies, which triggered a statutory ban on government contracts using DJI drones.[24] In November 2024, the General Services Administration (GSA) issued acquisition regulations that further codified and clarified prohibitions on the use of Chinese drones by federal agencies and in government contracts.[25]

Despite these restrictions, recent reports have raised questions about the extent to which construction contractors may be using prohibited drones on government contracts, as well as the extent to which data gathered by approved drones may be stored on vulnerable computer networks. The GSA Office of the Inspector General (OIG), for example, has found multiple cases of construction contractors using prohibited DJI drones. These include a major contractor that "frequently used a [DJI] drone to take aerial photographs to document construction progress" at the San Luis, Arizona, Port of Entry as recently as January 2025.[26] Another GSA OIG report describes the use of DJI drones at six Northern Border ports of entry as recently as August 2022.[27] Corporate social media posts also suggest ongoing relationships between federal contractors and DJI. For example, in July 2025, a Bechtel post on LinkedIn about the 10-year anniversary of the company's drone program featured a DJI drone and celebrated more than 1.5 million images collected by drones over the past decade.[28] DJI drones are also featured in a

[23] Exec. Order 13981, 86 Fed. Reg. 6821 (Jan. 22, 2021).

[24] John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. 115-232, Sec. 889(f)(3)(d) (2018); 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)* (Oct. 5. 2022).

[25] Defense Department, General Services Administration, and National Aeronautics and Space Administration, *Federal Acquisition Regulation: Prohibition on Unmanned Aircraft Systems From Covered Foreign Entities,* 89 Fed. Reg. 89464 (Nov. 12, 2024) (interim rule).

[26] General Services Administration, Office of Inspector General, Office of Audits, *Alert Memorandum: PBS Allowed the Use of a Drone from a Prohibited Source to Photograph Construction at a Land Port of Entry in San Luis, Arizona* (A220036-5) (Mar. 13, 2025).

[27] General Services Administration, Office of Inspector General, Office of Audits *Oversight of PBS's Projects Funded by the Infrastructure Investment and Jobs Act: Audit of Paving Project at New York State's Northern Border* (A220036/P/2/R24008) (Sept. 24, 2024).

[28] Bechtel, LinkedIn post (July 2025) (www.linkedin.com/posts/bechtel-corporation_did-you-know-bechtel-was-the-first-engineering-activity-7349148539324678146-Agr4).

September 2024 promotional YouTube video from Hensel Phelps[29] and a May 2024 article about how Brasfield & Gorrie combines data from drones with other sources, among other examples.[30]

To aid Congress in understanding security issues associated with the potential use of DJI or other Chinese-made drones at sensitive government facilities, please provide responses to the following document and information requests for Fiscal Years 2020 through 2025, unless otherwise noted:

1) A description of the relationship between Brasfield & Gorrie and DJI;

2) A list of all drones owned, operated, or leased by Brasfield & Gorrie, including the make, model, and initial date of operation;

3) A list of all Chinese-made drone critical components currently owned, operated, or leased by Brasfield & Gorrie, including the make, model, and initial date of operation;

4) A list of all DOD, Intelligence Community, National Nuclear Security Administration, or Department of Homeland Security contracts where Brasfield & Gorrie provided architectural, engineering, or construction services, and where Brasfield & Gorrie operated drones, regardless of whether drones were a contract deliverable, including the dates and locations of drone operation;

5) A list of all DOD, Intelligence Community, National Nuclear Security Administration, or Department of Homeland Security contracts in which Brasfield & Gorrie subcontractors operated drones in the performance of their subcontracts, regardless of whether drones were a contract or subcontract deliverable, including the names of such subcontractors, and the dates and locations of drone operation;

6) Documents sufficient to show all waivers sought by Brasfield & Gorrie for the use of drones or drone components as part of DOD, Intelligence Community, National Nuclear Security Administration, or Department of Homeland Security contracts, regardless of whether drones were a contract or subcontract deliverable, including the location of services to be performed, the date of the request, and whether a waiver was granted;

---

[29] Hensel Phelps, *Landmark: Discover the Game-Changing Tech Used by a Top Construction Company,* YOUTUBE (Sept. 11, 2024) (www.youtube.com/watch?v=mbaTPpJsHq0).

[30] *Efficiency, Safety, and Accuracy: How Brasfield & Gorrie Use Drones for Construction Projects*, Commercial UAV News (Aug. 29, 2024) (www.commercialuavnews.com/efficiency-safety-and-accuracy-how-brassfield-gorrie-use-drones-for-construction-projects).

7) All Brasfield & Gorrie policies and procedures related to drones and/or drone components covered by Section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019, Section 817 of the National Defense Authorization Act of 2023, and/or the American Security Drone Act of 2023, including versions of Brasfield & Gorrie policies that have been superseded, and including policies and procedures related to:

   a. Cybersecurity, including network connectivity and data storage;
   b. Use of mobile devices associated with such drones and/or drone components;
   c. Compliance with federal acquisition regulations and policies;
   d. The retention, storage, and/or destruction of data obtained from the use of such drones/and or drone components; and
   e. Reporting of anomalous incidents involving such drones/and or drone components;

8) A description of any testing, auditing, or related work Brasfield & Gorrie undertook internally or engaged externally to evaluate and/or mitigate potential national security risks posed by DJI drones or Chinese-made drone components, including the date of any such work, and any reports or other documents generated in connection with this work; and

9) A description of Brasfield & Gorrie network connectivity or data storage, including dedicated device requirements, for drone data located in or administered by an entity domiciled in a covered foreign country under the American Security Drone Act of 2023.

Please respond no later than January 15, 2026. If you have any questions related to this request, please contact [redacted] at [redacted] or [redacted]. Please send any official correspondence relating to this request to [redacted].

Sincerely,

Margaret Wood Hassan
United States Senator

Gary C. Peters
Ranking Member
Committee on Homeland Security
and Governmental Affairs