



**TIM GRIFFIN**  
ATTORNEY GENERAL

April 9, 2024

*Sent via First Class Mail*

The Honorable Mike Johnson  
Speaker of the House  
United States House of Representatives  
H-232, U.S. Capitol  
Washington, D.C. 20515

The Honorable Charles Schumer  
Majority Leader  
United States Senate  
S-221, U.S. Capitol  
Washington, D.C. 20510

The Honorable Mitch McConnell  
Republican Leader  
United States Senate  
S-230, U.S. Capitol  
Washington, D.C. 20510

The Honorable Hakeem Jeffries  
Minority Leader  
United States House of Representatives  
H-204, U.S. Capitol  
Washington, D.C. 20515

Re: Letter from the State of Arkansas and 10 other States in support of the Drone Infrastructure Inspection Grant Act, included in the Federal Aviation Administration Reauthorization

Dear Speaker Johnson, Majority Leader Schumer, Republican Leader McConnell, and Minority Leader Jeffries:

The States of Arkansas, Florida, Georgia, Kentucky, Louisiana, Mississippi, Missouri, South Carolina, South Dakota, Utah, and West Virginia urge Congress to promptly pass the Drone Infrastructure Inspection Grant (DIIG) Act. The DIIG Act responds to the clear and present industrial and national-security threats posed by the proliferation of Chinese-made drones in the United States. Such drones—often used by State and local law-enforcement and in connection with critical-infrastructure projects—present a clear security threat. And the People’s Republic of China’s practice of illegally “dumping” cheap, state-subsidized drones into the U.S. marketplace to drive out American competitors has only made this problem worse. By making the purchase of American-made drones more financially feasible, the DIIG Act encourages development of the American industrial base for unmanned-aircraft systems while safeguarding national security.

This bipartisan legislation was introduced in the Senate (S. 1817) by Senators John Boozman (R-AR), Jacky Rosen (D-NV), and Richard Blumenthal (D-CT), and in the House (H.R. 3593) by Representatives Greg Stanton (D-AZ), Garret Graves (R-LA), and Dina Titus (D-NV). The DIIG Act has been incorporated into legislation reauthorizing appropriations for the Federal Aviation Administration in the Senate (S. 1939, sec. 818) and in legislation that recently passed

the House (H.R. 3935, sec. 620). We urge both chambers to quickly adopt this bipartisan, national security legislation.

### **Background**

FBI Director Christopher Wray recently warned Congress that “[t]here has been far too little public focus” on the Chinese Communist Party’s efforts to “target[] our critical infrastructure—our water treatment plants, our electrical grid, our oil and natural gas pipelines, our transportation systems—and the risk that poses to every American requires our attention now.” Christopher A. Wray, *Director Wray’s Opening Statement to the House Select Comm. on the Strategic Competition Between the United States and the Chinese Communist Party*, Fed. Bureau of Investigation (Jan. 31, 2024), <https://perma.cc/58VE-QPJL>.

Fortunately, some are beginning to wake up to the unprecedented threat. For example, the federal government has now committed more than \$20 billion to replace the remotely-controlled cargo cranes at American ports made by Chinese state-owned companies after determining that they represent an urgent “espionage and disruption risk.” Dustin Volz, *U.S. to Invest Billions to Replace China-Made Cranes at Nation’s Ports*, Wall St. J. (Feb. 21, 2024), <https://perma.cc/P9B4-PN6S>. More recently, prompted by TikTok’s mass collection of Americans’ sensitive personal data and concerns that the Chinese social-media platform’s powerful algorithms influence Americans’ preferences, biases, and beliefs, the House overwhelmingly passed a bill that would require the Chinese company ByteDance, Ltd. to divest itself of TikTok’s U.S. assets. *See Protecting Americans from Foreign Adversary Controlled Applications Act (H.R. 7521)*, <https://www.congress.gov/bill/118th-congress/house-bill/7521>.

Despite the People’s Republic of China’s efforts to portray these actions as unjustified paranoia, the threats are real and grounded in China’s military-civil fusion reflected in, among other things, its National Intelligence Law of 2017, which “compels all PRC firms and entities to support, assist, and cooperate with the PRC intelligence services, creating a legal obligation for those entities to turn over data collected abroad and domestically to the PRC,” and which “may compel PRC firms to create backdoors and other security vulnerabilities in equipment and software sold abroad so that the PRC government can easily access data not controlled by PRC firms.” U.S. Dep’t of Homeland Security, Off. of Strategy, Pol’y & Plans, *Data Security Bus. Advisory: Risks and Considerations for Bus. Using Data Services and Equip. from Firms Linked to the People’s Republic of China*, at 6 (December 22, 2020), <https://perma.cc/WZ8R-CYAJ>.

### **Threats Posed by China’s Illegal Drone Dumping**

Similar urgent threats are posed by Americans’ use of inexpensive Chinese-made unmanned-aircraft systems. Beginning in 2015, the Chinese Communist Party “took aggressive measures to dominate the global [drone] manufacturing and technology market.” Association for Uncrewed Vehicle Systems International, *Whitepaper: AUVSI P’ship for Drone Competitiveness*, at 1 (Sep. 14, 2023) (hereinafter “AUVSI Whitepaper”), <https://perma.cc/XWQ4-2BUZ>. The Chinese Communist Party has worked “to project [its] influence abroad and use [its] monopolistic

position to put U.S. manufacturers at a disadvantage by flooding the global market with subsidized drones,” *id.*, an illegal trade practice the U.S. Department of Homeland Security Immigration and Customs Enforcement has characterized as “dumping.” U.S. Immigr. and Customs Enf’t, *Da Jiang Innovations (DJI) Likely Providing U.S. Critical Infrastructure and Law Enf’t Data to Chinese Gov’t*, Nat’l Sec. Archive (Aug. 9, 2017), <https://perma.cc/5ESQ-WUMU> (“dumping” is “[t]he illegal practice of exporting a product at a price lower than the cost to manufacture the product or lower than the price the manufacturer would charge in its own home market”). As a result, Chinese drones now “account for more than 90% of the consumer market, 70% of the enterprise market (drones used as industrial tools), and 92% of the first responder market.” AUVSI Whitepaper at 2 (footnotes omitted).

The Chinese company Da Jiang Innovations (DJI) is “the world’s largest drone manufacturer and has a dominant share of the U.S. and global drone market,” accounting for “77% of the U.S. hobby drone market and 90% of the commercial drone service provider market.” *Id.* at 3 (footnote omitted). DJI, while a “leading supplier of drones to U.S. law enforcement,” has “obscured its Chinese government funding while claiming that Beijing had not invested in the firm.” Cate Cadell, *Drone Company DJI Obscured Ties to Chinese State Funding, Documents Show*, The Washington Post (Feb. 1, 2022), <https://perma.cc/GFU8-BW9G>.

In 2019, the Department of Homeland Security issued an alert that “Chinese-made drones may be sending sensitive flight data to their manufacturers in China, where it can be accessed by the government there.” David Shortell, *DHS Warns of “Strong Concerns” that Chinese-Made Drones are Stealing Data*, CNN (May 20, 2019), <https://perma.cc/DUY3-DKHC>. The following year, the Department of Commerce added DJI to its Entity List for “activities that are contrary to the national security or foreign policy interests of the United States.” U.S. Dep’t 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. 22, 2020), <https://perma.cc/H5Q5-DS86>. And the Department of Defense issued a special statement that “systems produced by Da Jiang Innovations (DJI) pose potential threats to national security.” Dep’t of Defense, *Dep’t Statement on DJI Systems* (July 23, 2021), <https://perma.cc/9HR5-JZS4>. The Department of the Treasury has prohibited investment in DJI due to its role as part of “the Chinese military-industrial complex.” U.S. Dep’t of Treasury Off. of Foreign Assets Control, *Treasury Identifies Eight Chinese Tech Firms as Part of The Chinese Military-Industrial Complex* (Dec. 16, 2021), <https://perma.cc/QP83-4F4F>.

With DJI’s bad press, another Chinese drone manufacturer, Autel Robotics, has gained market share. AUVSI Whitepaper at 3. The U.S. Capitol Police stopped using Autel drones after Sen. Marco Rubio (R-FL) highlighted the national-security risks associated with their use. Rebecca Shabad, *U.S. Capitol Police Have Stopped Using Chinese-Made Drones*, NBC News (June 2, 2023), <https://perma.cc/VK47-54WG>. Nevertheless, like DJI, Autel has made inroads with American law-enforcement agencies such as the Huntsville, Alabama Police Department, which describes its 16 Autel drones as a “game changer” for their “ease of use, long mission time,

and durability,” as well as for their ability to livestream information. Autel Robotics, *Critical to Mission Success: How Huntsville PD Started an Exemplary Drone Program* (March 9, 2022), <https://perma.cc/Q488-PJPU>.

The Huntsville Police Department’s example well illustrates the potential national-security risks of State and local use of Chinese drones: Huntsville, besides containing a significant amount of critical infrastructure, borders Redstone Arsenal, which hosts 75 different federal agencies, including the U.S. Army’s Space and Missile Defense Command and the U.S. Army’s Aviation and Missile Center, among numerous other sensitive governmental programs. U.S. Dep’t of Defense, *Redstone Arsenal*, Military OneSource (March 6, 2024), <https://perma.cc/2QY2-57AT>; U.S. Army Space and Missile Defense Command, *Contacting USASMDC*, <https://www.smdc.army.mil/RESOURCES/ContactUs/>; U.S. Army DEVCOM Aviation and Missile Center, *Who We Are*, <https://perma.cc/CK45-MUNW>.

Federal, state, and local entities have acquired Chinese drones due to their low cost, with the U.S. Navy, for example, being “unable to find a product” made in the United States “that matches the[ir] utility and price point.” Kelsey D. Atherton, Official Navy Memo on DJI Drones Noted Cheap Cost, Risk (Dec, 16, 2019), <https://perma.cc/Z6KW-3KLL>; see U.S. Dep’t of the Navy, *Operational Risks with Regards to DJI Family of Products*, Nat’l Sec. Archive (May 24, 2017), <https://perma.cc/Z93Z-C3V7>. The United States “do[es]n’t have much of a small UAS [unmanned-aircraft system] industrial base because DJI dumped so many low-price quadcopters on the market, and we then became dependent on them.” Lara Seligman, *Pentagon Seeks to Counter China’s Drone Edge*, Foreign Policy (Aug. 27, 2019) (quoting Pentagon official Ellen Lord), <https://perma.cc/G2YV-5FAH>.

Late last year, Congress passed the American Security Drone Act of 2023, which prohibits federal departments and agencies from operating or procuring drones manufactured or assembled by particular foreign entities, including those based in China. National Defense Authorization Act for Fiscal Year 2024, Pub. L. No. 118-31, Div. A, Title XVIII, subtitle B, sec. 1821 et seq, 137 Stat. 136, 691-99 (Dec. 22, 2023). States are similarly beginning to prohibit the public purchase or use of foreign drones. See Ark. Code Ann. 25-1-129; Fla. Admin. Code Ann. r. 60GG-2.0075; Miss. Code Ann. 31-7-67; Tenn. Code Ann. 4-56-112, 12-4-120. Indeed, preserving the security of our States “requires a whole-of-government approach, as the Department of Defense has neither the mission nor the necessary authorities to defend civilian critical infrastructure.” Madelyn R. Creedon, et al., *America’s Strategic Posture: The Final Report of the Congressional Commission on the Strategic Posture of the United States*, at 105 (Oct. 2023), <https://perma.cc/M2Q8-HE79>.

Congressional action remains necessary to make it more feasible for States and local governments to purchase American-made drones for law-enforcement and critical-infrastructure projects. The DIIG Act is designed to help fill that gap.

### The Drone Infrastructure Inspection Grant Act

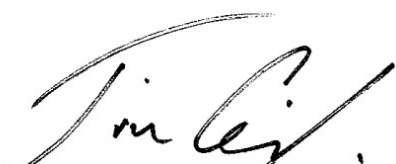
As originally introduced, the DIIG Act would establish a \$100 million grant program to facilitate the use of drones by States and local governments and to promote college- and university-level workforce training in the use of drone technology. The current language incorporated into the Senate and House versions of the FAA reauthorization bill reduces that amount to \$2 million for 2024 and \$12 million for each of 2025, 2026, 2027, and 2028. *See* FAA Reauthorization Bill (S. 1939, sec. 818; H.R. 3935, sec. 620). Grants awarded under the program may be used to purchase or lease drones weighing up to 55 pounds, to contract for services with those having expertise in the use of small unmanned-aircraft systems, or to support the operational or program-management capabilities of the States or local governments using those systems.

Crucially, to receive a grant, an entity must use drones that are manufactured or assembled by a company from the United States. The DIIG Act expressly prohibits the use of drones manufactured or assembled by companies that are, among other things, on the Department of Commerce's Entity List or that are domiciled in, or subject to the influence or control of, the People's Republic of China or the Russian Federation, including any subsidiary or affiliate. The Act prioritizes projects that support the operation, inspection, or maintenance of critical infrastructure, including public bridges, tunnels, roads, highways, dams, electrical grids, water infrastructure, communication systems, pipelines, and other assets.


The DIIG Act will encourage the development of the American industrial base by making it more financially feasible for State and local governments to purchase American-made unmanned-aircraft systems while safeguarding our national-security interests.

### Conclusion

Therefore, we urge you to support passage of the DIIG Act and to restore the original funding level for the DIIG program so that our States and local governments can take advantage of secure, American-made products suitable for use in the operation, inspection, and maintenance of our Nation's critical infrastructure.




TIM GRIFFIN  
Arkansas Attorney General




CHRIS CARR  
Georgia Attorney General

Sincerely,



ASHLEY MOODY  
Florida Attorney General



RUSSELL COLEMAN  
Kentucky Attorney General

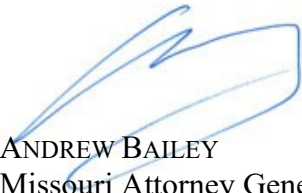




LIZ MURRILL  
Louisiana Attorney General



LYNN FITCH  
Mississippi Attorney General



ANDREW BAILEY  
Missouri Attorney General



ALAN WILSON  
South Carolina Attorney General



MARTY J. JACKLEY  
South Dakota Attorney General



SEAN REYES  
Utah Attorney General



PATRICK MORRISEY  
West Virginia Attorney General