Date of Hearing: March 21, 2023

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Jesse Gabriel, Chair
AB 740 (Gabriel and Petrie-Norris) – As Amended March 9, 2023

SUBJECT: Department of General Services: drone cybersecurity

SYNOPSIS

This bill would establish much-needed cybersecurity and privacy standards for data collected by drones that are operated by California state and local government entities.

It would require the California Department of Technology (CDT) to issue regulations meant to ensure the confidentiality, integrity, and availability of data collected, transmitted, and stored by government drones. The regulations, at minimum, would have to ban the use of drones made by certain entities identified by the federal government; forbid government entities from selling drone data; and require that these entities collect, process, and use drone data in a manner that is reasonably necessary and proportionate to the lawful purposes for which it is collected.

The bill would also require CDT to specify requirements for governmental entities to adopt comprehensive plans to discontinue use of non-compliant drones no later than January 1, 2026.

If a government entity requires a non-compliant drone in order to perform an important task, it may apply to CDT for an exception by showing the drone's use is necessary or essential, and that no other drone can fulfill this purpose.

This bill is sponsored by Skydio and is supported by the Association for Uncrewed Vehicle Systems International (AUVSI) and by Oakland Privacy.

If passed by this Committee, this bill will next be heard by the Assembly Accountability and Administrative Review Committee.

SUMMARY: Directs the California Department of Technology to issue regulations establishing cybersecurity and privacy requirements for data collected by drones operated by state and local government entities. Specifically, **this bill**:

1) Defines "government entity" to include all of the following:

    a) Any department, division, independent establishment, or agency of the executive branch of the state government.

    b) The California State University.

    c) Any city, city and county, county, district, or other local governmental agency or public agency authorized by law.

2) Requires the California Department of Technology (CDT), in consultation with the Chief of the Office of Information Security, to adopt regulations to ensure that each unmanned aircraft

and unmanned aircraft system used by a government entity for any purpose meets appropriate safeguards to ensure the confidentiality, integrity, and availability of any data collected, transmitted, or stored by that unmanned aircraft or unmanned aircraft system.

3) Provides that the regulations under 2) must, at minimum, do all of the following:

   a) Prohibit the use of unmanned aircraft or unmanned aircraft systems manufactured by an entity, or a subsidiary of an entity, identified pursuant to any of the following:

      i) Section 889 of the National Defense Authorization Act for Fiscal Year 2019.

      ii) The United States Department of Defense pursuant to Section 1260H of the National Defense Authorization Act for Fiscal Year 2021.

      iii) Section 817 of the National Defense Authorization Act for Fiscal Year 2023.

      iv) The Entity List designated by the United States Secretary of Commerce.

   b) Prohibit any government entity from selling, renting, leasing, or engaging in any other commercial transaction pursuant to which the entity receives monetary or other valuable consideration for the data.

   c) Require collection, transmission, storage, processing, and use of the data to be conducted in a manner reasonably necessary and proportionate to the lawful purposes for which the data is collected, transmitted, stored, processed, or used.

4) Further requires CDT, in consultation with the Chief of the Office of Information Security, to adopt rules and regulations specifying requirements for a comprehensive plan to be adopted by government entities to discontinue the use of unmanned aircraft and unmanned aircraft systems not in compliance with the regulations under 2).

5) Specifies that the requirements for the comprehensive plan under 4) shall, at minimum, include ensuring the confidentiality, integrity, and availability of data collected, transmitted, or stored by discontinued unmanned aircraft or unmanned aircraft systems.

6) Permits CDT to consult with state and federal agencies and departments, as well as any relevant federal guidance, in developing the regulations under 2) and 4).

7) Specifies that the regulations under 2) and 4) must be adopted by January 1, 2025.

8) Restricts a government entity, once the regulations under 2) are adopted, from using an unmanned aircraft or unmanned aircraft system it did not previously use—unless the aircraft or aircraft system complies with all of the requirements set by the regulations under 2).

9) Requires, by July 1, 2025, each government entity that uses an unmanned aircraft or unmanned aircraft system that does not comply with the regulations under 2) to submit to CDT a comprehensive plan that complies with the regulations under 4). Further requires each government entity to execute this plan upon CDT approval.

10) Requires, by January 1, 2026, each government entity to cease the use of any unmanned aircraft or unmanned aircraft system that does not comply with the regulations under 2).

11) Clarifies that this bill applies to unmanned aircraft and unmanned aircraft systems (i) that a government entity purchases or otherwise acquires, as well as (ii) to those it uses through contract or other agreement with a third party. The bill also applies regardless of whether the government entity or the third party operates the drone.

12) Permits a government entity to use an unmanned aircraft or unmanned aircraft system that would otherwise be prohibited under this bill under either of the following circumstances:

    a) If the government entity applies to CDT for an exception and CDT finds (i) that the proposed use is necessary or essential for the government entity and (ii) that no nonprohibited unmanned aircraft can fulfill the proposed use.

    b) For cybersecurity research.

13) Includes a severability clause.

EXISTING LAW:

1) Defines the following terms:

    a) "Unmanned aircraft" means an aircraft that is operated without the possibility of direct human intervention from within or on the aircraft. (Gov. Code § 853.5(a).)

    b) "Unmanned aircraft system" means an unmanned aircraft and associated elements, including but not limited to, communication links and the components that control the uncrewed aircraft, which are required for the pilot in command to operate safely and efficiently in the national airspace system. (Gov. Code § 853.5(b).)

2) Establishes CDT in the Government Operations Agency (GovOps). (Gov. Code § 11545.)

3) Establishes the Office of Information Security within CDT to ensure the confidentiality, integrity, and availability of state systems and applications, and to promote and protect privacy as part of the development and operations of state systems and applications to ensure the trust of the residents of this state. (Gov. Code § 11549.)

FISCAL EFFECT: As currently in print this bill is keyed fiscal.

COMMENTS:

1) **Background.** Drones—termed "unmanned aircraft" and "unmanned aircraft systems" in the Government Code—are increasingly used by all levels of California government. For example:

- CalFire uses drones to help firefighters determine where to create containment lines when fighting wildfires. (Bouchot, *How Cal Fire uses drones to fight wildfires* KESQ News Channel 3 (June 15, 2022), *available at* https://kesq.com/news/2022/06/15/how-cal-fire-uses-drones-to-fight-wildfires/.)

- Caltrans uses dozens of drones for infrastructure inspection, and is looking into using drones and video imaging to assess "bridge damage and deploying emergency resources following a major quake." (Cal. Dept. of Transportation, *Bridge, Other Inspections*

Taking to the Skies, *available at* https://dot.ca.gov/programs/public-affairs/mile-marker/spring-2020/bridge-inspections-taking-to-the-skies.)

- The Chula Vista Police Department utilizes more than two dozen drones as part of a drone-as-first-responder program. (Sisson, *Welcome to Chula Vista, where police drones respond to 911 calls*, MIT Technology Review (Feb 27, 2023), *available at* https://www.technologyreview.com/2023/02/27/1069141/welcome-to-chula-vista-where-police-drones-respond-to-911-calls/.)

Yet, surprisingly, there are virtually no cybersecurity or privacy standards in place to govern the data obtained by government drones. In response, this bill would authorize the California Department of Technology (CDT) to issue regulations governing drones used by government entities in California. The regulations are meant to establish appropriate safeguards to ensure the confidentiality, integrity, and availability of data that is collected, transmitted, and stored by government-operated drones.

2) **Author's statement.** According to the author:

> The development of drone technology over the past decade has been extraordinary. Drones are now regularly used at all levels of state and local government, including for lifesaving functions like inspecting critical infrastructure and surveilling hostage situations.
>
> While in operation, drones collect vast amounts of data—including audio, visual, and geospatial information—in the locations where they are operated. Yet the state lacks legal standards to govern the collection, transmission, storage, and usage of this data. If data regarding critical infrastructure, a law enforcement operation, or other sensitive information were to fall into the wrong hands, the consequences could be disastrous.
>
> AB 740 will address the current lack of cybersecurity and privacy standards for government-operated drones.

3) **What this bill would do.** This bill would work as follows:

1. By January 1, 2025, CDT will issue regulations meant to ensure the confidentiality, integrity, and availability of data collected, transmitted, and stored by government drones. The regulations, at a minimum, must ban the use of drones made by certain entities identified by the federal government; forbid government entities from selling drone data; and require that these entities collect, process, and use drone data in a manner that is reasonably necessary and proportionate to the lawful purposes for which it is collected. These regulations would apply to both state and local governmental entities.

2. By January 1, 2025, CDT will issue regulations specifying requirements for governmental entities to adopt comprehensive plans to discontinue their use of non-compliant drones. Again, these regulations would be meant to ensure the confidentiality, integrity, and availability of data collected, transmitted, or stored by any discontinued drones.

3. Once the regulations under #1 are adopted, a governmental entity that wants to use a drone it did not previously use may only use a drone that complies with these regulations.

If a governmental entity wishes to use a non-compliant drone, it may apply to CDT for an exception by showing the drone's use is necessary or essential, and that no other drone can fulfill this purpose.

4. By July 1, 2025, a governmenatal entity that uses a drone which does not comply with the regulations under #1 must submit a comprehensive plan to CDT (a plan that complies with the regulations under #2) for how it will discontinue use of the drone.

5. By January 1, 2026, each governmental entity must discontinue use of non-compliant drones, and once its plan is approved by CDT, implement that plan.

4) **Summary of federal prohibitions.** Under this bill, CDT's regulations would ban state and local governments from using drones manufactured by entities that are identified via the following federal legislation and/or agencies:

1. Section 889 of the National Defense Authorization Act for Fiscal Year 2019 (2019 NDAA).

Section 889, which can be reviewed at https://www.congress.gov/bill/115th-congress/house-bill/5515, prohibits federal agencies and their contractors from acquiring telecommunications and/or video surveillance equipment and services produced or provided by five named Chinese companies and their subsidiaries or affiliates. It also prohibits such acquisitions from companies that the Secretary of Defense reasonably believes to be owned or controlled by, or otherwise connected to, the government of a "covered foreign country," defined under the 2019 NDAA as China. (To date, the Secretary of Defense has not identified any companies meeting this criteria.)

2. Section 1260H of the 2021 NDAA, as identified by the U.S. Department of Defense.

Section 1260H, which can be reviewed at https://www.congress.gov/bill/116th-congress/house-bill/6395, requires the Secretary of Defense to "identify each entity the Secretary determines, based on the most recent information available, is operating directly or indirectly in the United States or any of its territories and possessions, that is a Chinese military company," as defined. The most recent list is available at https://media.defense.gov/2022/Oct/05/2003091659/-1/-1/0/1260H%20COMPANIES.PDF.

3. Section 817 of the 2023 NDAA.

Section 817, which can be reviewed at https://www.congress.gov/bill/117th-congress/house-bill/7776, expands on Section 848 of the 2020 NDAA (not explicitly referenced in this bill, but which can be found at https://www.congress.gov/bill/116th-congress/senate-bill/1790). Section 848 prohibited the Department of Defense from procuring drones manufactured by entities in a "covered foreign country," initially defined as China. Section 817 of the 2023 NDAA expands on this prohibition by adding certain drone manufacturers, including Da-Jiang Innovations (DJI) and its affiliates and subsidiaries, and entities on the U.S. Department of Commerce's Consolidated Screening List, to the list of prohibited companies. Section 817 also adds Iran, Russia, and North Korea to the definition of "covered foreign country."

4. The U.S. Secretary of Commerce's Entity List.

The Entity List "identifies entities for which there is reasonable cause to believe, based on specific and articulable facts, that the entities have been involved, are involved, or pose a significant risk of being or becoming involved in activities contrary to the national security or foreign policy interests of the United States." (*Additions and Revisions of Entities to the Entity List* (Mar. 6, 2023) 88 FR 13673.)

5) **Analysis of federal prohibitions.** The main issue for this Committee is whether this bill strikes an appropriate balance between providing state and local governments the flexibility to utilize drones with needed capabilities, while simultaneously safeguarding vital information from being obtained by potential malefactors.

The basic problem lies with the People's Republic of China (PRC) National Intelligence Law of 2017. As summarized by the United States Department of Homeland Security:

> This law forms the baseline of the modern data collection regime, and 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. Article 7 of this law states "any organization or citizen shall support, assist and cooperate with the state intelligence work in accordance with the [National Intelligence] Law, and keep the secrets of the national intelligence work from becoming known to the public." **A PRC intelligence agency may request that any PRC firm or entity secretly share access to a U.S. business or individual's data, or otherwise face penalties. In addition, the National Intelligence Law 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.** The law further establishes a system of incentives for compliance and penalties for non-compliance, stating that the PRC "commends and rewards individuals and organizations that have made significant contributions to national intelligence work" and that, "whoever… obstructs the state intelligence work organization and its staff from carrying out intelligence work according to law" shall be dismissed, investigated, and/or detained. (U.S. Dept. of Homeland Security, *Data Security Business Advisory: Risks and Considerations for Businesses Using Data Services and Equipment from Firms Linked to the People's Republic of China* (Dec. 20, 2020), *available at* https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf [internal citations omitted] [emphasis added].)

In other words, the Chinese government has the legal ability to demand data from Chinese companies without any of the due process protections required under American law, and to require these companies to build in security vulnerabilities to facilitate data extraction.

The United States Cybersecurity & Infrastructure Security Agency (CISA) has published a series of reports on Chinese cyber attacks against the United States. Its findings are summarized as follows:

> Malicious cyber activities attributed to the Chinese government targeted, and continue to target, a variety of industries and organizations in the United States, including healthcare, financial services, defense industrial base, energy, government facilities, chemical, critical manufacturing (including automotive and aerospace), communications, IT (including managed service providers), international trade, education, video gaming, faith-based organizations, and law firms. (CISA, *China Cyber Threat Overview and Advisories*, *available at* https://www.cisa.gov/china.)

The sources quoted above were published by federal agencies during both the Trump and Biden Administrations.

Da-Jiang Innovations (DJI), whose drones would be banned by this bill, is the world's largest-selling manufacturer of consumer and commercial drones. (Asia Perspective, *China's Thriving Drone Industry* (Jun. 9, 2021), *available at* https://www.asiaperspective.com/china-thriving-drone-industry/.) Just this week, a bipartisan group of sixteen U.S. Senators sent a letter to CISA's Director which provided:

> We write today regarding the cybersecurity risks posed by the widespread use of drones manufactured by Shenzhen DJI Innovation Technology Co., Ltd. ("DJI") to operators of critical infrastructure and state and local law enforcement in the United States. In short, we believe that given the company's identified connections to the Chinese Communist Party ("CCP"), the use of its drones in such sensitive contexts may present an unacceptable security vulnerability. We ask that the [CISA] evaluate this concern and make the results of its evaluation available to the public through the National Cyber Awareness System. (https://www.warner.senate.gov/public/_cache/files/c/8/c8dbcd57-7d3c-4842-85f2-466dc2b70f66/B56DAFD9C216FD3E54239A3E14E281EF.final-2023.03.15-letter-to-cisa-re-dji.pdf)

German researchers recently found 16 security vulnerabilities in four DJI drone models; these included "bugs allow[ing] an attacker to gain extended access rights" and a finding that "transmitted data is not encrypted, and that practically anyone can read the location of the pilot and the drone with relatively simple methods." (Weiler, *Security vulnerabilities detected in drones made by DJI* (Mar. 2, 2023), *available at* https://news.rub.de/english/press-releases/2023-03-02-it-security-security-vulnerabilities-detected-drones-made-dji.)

There are conflicting reports on whether DJI drones have been used to turn information over to the Chinese government. According to a recent article, "[C]laims [are] thus far unsubstantiated…that the firm's [unmanned aerial vehicle] operating systems allow private, potentially sensitive user data to be transmitted to authorities in China's government for exploitation." (Crumley, *German research finds security flaws in four leading DJI drones* (Mar. 5, 2023) Drone DJ, *available at* https://dronedj.com/2023/03/05/german-research-finds-security-flaws-in-four-leading-dji-drones/.) That said, the Senate letter quoted above cites a 2017 U.S. Immigration and Customs Enforcement (ICE) report which claims:

> [T]he Chinese government is likely using information acquired from DJI systems as a way to target assets they are planning to purchase. For instance, a large family-owned wine producer in California purchased DJI UAS to survey its vineyards and monitor grape production. Soon afterwards, Chinese companies began purchasing vineyards in the same area. According to the [source of information], it appeared the companies were able to use DJI data to their own benefit and profit. (ICE, *Da Jiang Innovations (DJI) Likely Providing U.S. Critical Infrastructure and Law Enforcement Data to Chinese Government* (Aug. 9, 2017), *available at* https://info.publicintelligence.net/ICE-DJI-China.pdf.)

Given these conflicting reports, this bill should be viewed as prudential: given the legal obligation of Chinese companies to transfer data to their government on request, and well-documented exploitation of cybersecurity vulnerabilities by Chinese state-sponsored actors, the fact that drones are increasingly being used in sensitive operations in California strongly suggests that it would be prudent to ban government use of drones made by companies subject to

the PRC National Intelligence Law. The reason to do this now, rather than waiting till security vulnerabilities are proven, is that there is no way to claw back information exploited through such vulnerabilities once it is exposed. Or, as Will Rogers said, "Lettin' the cat outta the bag is a whole easier 'n puttin' it back in."

Crucially, this bill does not impose a blanket ban on prohibited drones. Situations may arise in which a Chinese-made drone is superior to any non-Chinese-made drone for a specific purpose. In such a situation, a government entity that wishes to use the drone can apply to CDT for an exception to the ban.

Finally, while perhaps not dispositive of the issue, there are arguably moral considerations in using certain Chinese-made drones as well. The United States Treasury Department has identified DJI as "actively support[ing] the biometric surveillance and tracking of ethnic and religious minorities in China, particularly the predominantly Muslim Uyghur minority in Xinjiang." (U.S. Dept. of Treasury, *Treasury Identifies Eight Chinese Tech Firms as Part of The Chinese Military-Industrial Complex* (Dec. 16, 2021), *available at* https://home.treasury.gov/news/press-releases/jy0538.)

Given the foregoing, these provisions appear to strike a measured, appropriate balance in ensuring the cybersecurity and privacy of data collected by government-operated drones in California.

6) **Related legislation.** AB 955 (Petrie-Norris, 2023) as referred to this Committee, would have prohibited any state or local agency from acquiring or using a drone made by a manufacturer covered by Section 889 of the 2019 NDAA. The bill has since been amended to impose criminal penalties for selling fentanyl on social media platforms, and re-referred to the Assembly Public Safety Committee.

AB 1129 (Chau, Chap. 749, Stats. 2019), among other things, added "unmanned aircraft systems" to the list of devices that could be used to commit the crime of invading an individual's privacy.

AB 527 (Caballero, Chap. 404, Stats. 2017) allowed commercial drone operations for the purpose of pesticide application for mosquito and vector control, provided that the drone operator complies with Federal Aviation Administration (FAA) rules governing drone flight and the drone operator has approval from the California Department of Pesticide Regulation (DPR). This bill also creates a new pest control aircraft pilot certificate for drone operators, to be provided upon passage of an exam.

SB 807 (Gaines, Chap. 834, Stats. 2016) provided local public entities and their employees with immunity from civil liability for any damage to a drone, if the damage was caused while a local public entity and its employees were providing, and the drone was interfering with, the operation, support, or enabling of specified emergency services.

ARGUMENTS IN SUPPORT: Oakland Privacy recognizes the imperative for this bill:

> There is no doubt that Californians' concerns about commercial uses of unmanned aircraft videos and the safety, security and protection of drone-captured images can potentially be better addressed than they have been to date. We appreciate the proposal for a comprehensive review of data security and data integrity in the context of unmanned aircraft use. It would

not be hard for the state to enhance existing protections and strengthen regulations over the status quo.

REGISTERED SUPPORT / OPPOSITION:

Support

Skydio (sponsor)
Association for Uncrewed Vehicle Systems International (AUVSI)
Oakland Privacy

Opposition

None on file

Analysis Prepared by: Jith Meganathan / P. & C.P. / (916) 319-2200