Date of Hearing: April 16, 2026
Fiscal: Yes

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
AB 2043 (Calderon) – As Amended April 6, 2026

SUBJECT: Countering Unmanned Aircraft Systems Task Force

SYNOPSIS

Unmanned aircraft systems (UAS), or drones, have become increasingly popular due to their various applications and mass availability. However, concerns about the potential for drones to harm critical infrastructure and the public has led local and federal law enforcement to invest in drone detection and mitigation. Under the 2025 SAFER SKIES Act, local and tribal law enforcement are authorized to actively mitigate malicious drones if the drone poses a safety or security risk. Additionally, 2025 Presidential Executive Order 14305 establishes a federal task force to develop protocols to respond to drone threats and enables local and tribal law enforcement agencies to apply for federal grants for drone detection and identification equipment.

This bill mirrors federal law by establishing a statewide drone task force, housed under the Office of Emergency Services, to enhance the state's capabilities to detect, identify, track, and monitor drones and to support local and tribal law enforcement in combatting drones that pose safety and security risks. This bill requires the Director of Emergency Services to include representatives of specific public and private entities on the task force, including local law enforcement, California sports teams, and organizations concerned with privacy protections, with the goal of developing response plans specific to unauthorized drones.

This bill is supported by the Peace Officers Research Association of California (PORAC). It has no registered opposition.

This bill was previously heard by the Assembly Emergency Management Committee, where it passed with a 6-0 vote.

This bill contains an urgency clause.

EXISTING LAW:

1) Establishes that the United States Government has exclusive sovereignty of airspace of the United States, but that a citizen of the United States has a public right of transit through navigable airspace. (49 U.S.C, § 40103.)

2) Establishes definitions related to unmanned aircraft systems (UAS), or drones, as well as various requirements and restrictions on the operation of drones, including integration of civil drones into national airspace, safety standards, carriage of property by small unmanned aircraft, certain exceptions for limited recreations operations, and other provisions. (49 U.S.C. Ch. 448.)

3) Defines, through the Critical Infrastructures Protection Act of 2001, "critical infrastructure" as the systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters, and states that it is the policy of the United States that that any physical or virtual disruption of the operation of the critical infrastructures the United States be rare, brief, geographically limited in effect, manageable, and minimally detrimental to the economy, human and government services, and national security of the United States. (42 U.S.C, § 5195c.)

4) Authorizes the Secretary of Transportation and Attorney General of the United States, through the Preventing Emerging Threats Act of 2018, to authorize certain personnel to take such actions as are necessary to mitigate a credible threat that a drone or unmanned aircraft poses to the safety or security of a covered facility or asset, including disrupting control of the drone by the operator, seizing the drone and using reasonable force, as necessary, to disable, damage, or destroy the drone or unmanned aircraft. (6 U.S.C, § 124n.)

5) Authorizes the Administrator of the Federal Aviation Administration (FAA) to issue special security instructions in the interest of national security, with which any person operating an aircraft, including a drone, in a national security sensitive area must comply. (14 CFR, § 99.7 and 14 CFR Part 107.)

6) Authorizes state, local, Tribal, and territorial law enforcement officers, after completing detailed training, to take necessary action to mitigate a credible threat than an unmanned aircraft or drone poses to the safety or security of people, facilities, and assets, a venue or set of venues used for large-scale public gatherings or events, critical infrastructure, or correctional facilities. (6 U.S.C, § 124n(a)(2).)

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

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

9) Makes it a misdemeanor for a person to use a drone to look through a hole or opening into the interior of an area in which the occupant has a reasonable expectation of privacy, with the intent to invade the privacy of a person or persons inside. (Pen. Code § 647(j)(1).)

10) Establishes that a person is liable for physical invasion of privacy when the person knowingly enters onto the land or into the airspace above the land of another person without permission or otherwise commits a trespass in order to capture any type of visual image, sound recording, or other physical impression of the plaintiff engaging in a private, personal, or familial activity and the invasion occurs in a manner that is offensive to a reasonable person. (Civ. Code § 1708.8(a).)

11) Makes it unlawful for any person to operate a drone in pest control unless the pilot operating the drone holds a valid manned pest control aircraft pilot's certificate or a valid unmanned pest control aircraft pilot's certificate issued by the director and is certified or otherwise

authorized by the FAA to operate a drone approved by the FAA to conduct pest control. (Food & Agr. Code § 11901(b).)

12) Establishes a misdemeanor for a person who goes to the scene of an emergency, or stops at the scene of an emergency, and uses a drone for the purpose of viewing the scene or the activities of police officers, firefighters, emergency medical, or other emergency personnel, unless it is part of the duties of that person's employment to view that scene, and impedes emergency personnel in the performance of their duties. (Pen. Code, § 402.)

THIS BILL:

1) Creates the Countering Unmanned Aircraft Systems Task Force, housed under the Office of Emergency Services, to develop a statewide strategy to protect mass gatherings, critical infrastructure, and other soft targets from attacks by unmanned aircraft systems.

2) Authorizes the Director of Emergency Services to compose a membership of the task force with one or more representatives of the following:

    a. State Threat Assessment Center.

    b. Department of the California Highway Patrol.

    c. Military Department.

    d. Department of Forestry and Fire Protection.

    e. Utilities Emergency Association.

    f. California State Sheriffs' Association.

    g. California Police Chiefs Association.

    h. California Fire Chiefs Association.

    i. Organizing Committee of the 2028 Olympic and Paralympic Games.

    j. A National Football League team based in California.

    k. A Major League Baseball team based in California.

    l. Rank and file police officers.

    m. Firefighters employed by a public agency.

    n. An organization devoted to the protection of personal privacy.

3) Authorizes the Director of Emergency Services to appoint additional members to the task force, at their discretion.

4) States that the purpose of the task force is to organize and enhance the state's ability to detect, identify, track, and monitor drones and local law enforcement in combatting the

unlawful use of drones that poses a threat to the safety and security of individuals, communities, or critical infrastructure.

5) States that the task force's primary objective is to develop and implement a statewide strategy to deter and counter attacks by drones.

6) Establishes the goals of the task force including, but not be limited to, the following:

    a. Protect critical infrastructure, mass gatherings, and other soft targets from threats.

    b. Support the deployment of fixed or portable systems for the detection, tracking, identification, and mitigation of unmanned aircraft.

    c. Ensure statewide readiness, in coordination with federal officials, to respond to emergencies or public safety threats associated with malicious use of drones.

7) Authorizes the task force to:

    a. Develop or update response plans specific for drones as necessary.

    b. Conduct risk assessments to identify high-priority areas for the detection of drones, including critical infrastructure, public events, or disaster-prone areas.

    c. Create standard operating procedures for responding to unauthorized or malicious activity by drones.

    d. Coordinate with federal agencies to ensure compliance with and provide feedback on federal laws and regulations governing drones.

    e. Plan for the integration of detection systems for drones within existing public safety technologies.

    f. Ensure first responders receive appropriate training in the operation of specific detection systems for drones.

    g. Develop other necessary training including but not limited to training for trainers, scenario-based response training, table-top exercises.

COMMENTS:

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

The purpose of the Countering Unmanned Aircraft Systems Task Force is to enhance California's capabilities to detect, identify, track, or monitor unmanned aircraft systems and to support local and tribal governments in combatting the unlawful use of unmanned aircraft systems that pose a threat to the safety and security of individuals, communities, and critical infrastructure. In recent years, criminals, terrorists, and hostile foreign actors with malicious intentions have intensified their use of drones. We need to have a statewide strategy to counter this evolving threat and to keep the World Cup and Olympic Games safe.

2) **Background**. Unmanned aircraft systems (UAS), commonly known as drones, have become increasingly popular in the United States due to their widespread availability. Originally intended for military and commercial applications, drones are commonplace in a variety of fields, including delivery, agriculture, infrastructure development, search and rescue, security, and have become a popular recreational hobby. The FAA projects that the popularity of drones will only increase in coming years, forecasting commercial drone fleet (drones used in connection with a business) will reach 955,000, and that recreational fleet (drones operated for personal enjoyment) will number around 1.82 million by 2027.[1]

In 2026, the FAA reported registering over 855,000 drones. Of these registered drone operators, nearly two-thirds (63 percent) are hobbyist flyers.[2] Although the vast majority of drone operators are recreational flyers, concerns about how drones can interfere with public safety, including through invasive surveillance, weaponization and terrorism, airspace interference, and potential property damage, have percolated in law enforcement spheres. In December 2023, several drones swarmed a military base in Virginia for 17 days, confounding government officials and law enforcement.[3] In November 2024, the Federal Bureau of Investigation (FBI) thwarted a man who attempted to use a drone rigged with explosives to destroy an energy facility in Nashville.[4] These cases highlight potential vulnerabilities in American infrastructure, as explained by an article in the *Journal of Domestic Preparedness:*

> In the U.S., most critical infrastructure was designed and built in a relatively low-threat environment, designed to survive weather events, minimize accidents, and prevent theft, rather than built to protect against attack or sabotage. The idea that people would intentionally destroy infrastructure was generally not considered. For instance, in the energy sector, most substations were simply protected by chain link fences and signage indicating the dangers of high voltage. The reason for fencing was to deter theft and protect the public.
>
> […]
>
> Wars in Ukraine and Israel have shown how drones can be used to destroy civilian infrastructure. In a similar fashion, transnational crime organizations embrace weaponized drones to combat rivals and police, as the use of weaponized drones is spreading beyond war zones. In 2020, a drone was used in an attempt to disrupt the U.S. power grid by attacking a substation in Pennsylvania by dropping a metal cable across high-voltage lines. Fortunately, the attack was unsuccessful. However, it is only a matter of time before a drone attack disables or destroys critical infrastructure.[5]

---

[1] U.S. Government Accountability Office, "Drone Operations," https://www.gao.gov/drone-operations.
[2] "What Are the Statistics for Drones? The Ultimate 2026 Data Dive," *Drone Brands,* (Jan. 26, 2026), https://www.dronebrands.org/what-are-the-statistics-for-drones/#data-methodology-how-we-gathered-and-analyzed-drone-statistics.
[3] Gordon Lubold, L. Seligman, & A. Viswanatha, "Mystery Drones Swarmed a U.S. Military Base for 17 Days. The Pentagon Is Stumped." *Wall Street Journal,* (Oct. 12, 2024), https://www.congress.gov/119/meeting/house/118165/documents/HHRG-119-GO06-20250429-SD004.pdf.
[4] Jonathan Mattise, "Man pleads guilty to charges that he meant to blow up a Nashville power site with a bomb-laden drone," *Associated Press,* (Sept. 9, 2025), https://apnews.com/article/nashville-weapons-power-grid-f186115d41fb97e59615adbb2ee97afc.
[5] David Winks et al., "Protecting Critical Infrastructure From Weaponized Drones," *Journal of Domestic Preparedness,* (Dec. 4, 2024), https://domesticpreparedness.com/articles/protecting-critical-infrastructure-from-weaponized-drones/.

Drones also have the potential to act as tools for public safety and support. Drones are beginning to be deployed in remote regions to deliver lifesaving medicine and supplies to patients who would otherwise be left waiting hours for conventional transit systems like delivery vans.[6] In Canada, drones are being used to assist in avalanche control. Rather than throwing explosives from helicopters or firing artillery weapons to stimulate small, manageable avalanches (much like controlled fire burning), drones can drop an explosive remotely, saving the government time, money, and potentially lives.[7] Like any emerging technology, the potential benefits of expansive drone use must be weighed alongside potential harms to determine how best to protect public interest and safety.

3) **Artificial intelligence and drones.** Unlike remotely piloted drones that rely on constant human input to navigate, autonomous drones rely on artificial intelligence (AI) to adapt to their surroundings and operate without human oversight.[8] This is the "unmanned" part of unmanned aircraft systems. These drones rely on AI for things like object perception and recognition, terrain mapping, target identification, obstacle avoidance, and multi-drone coordination – a technique known as drone swarming. Drone swarms refer to when a group of drones operate as a natural swarm, like bees, to coordinate complex tasks through decentralized decision-making and synchronized behaviors.[9] By acting as a natural swarm feeding off one another's actions, drones can quickly and effectively coordinate across a range of complex behaviors to assist in agricultural operations and potentially even mining without the need for human intervention. However, AI use exposes these drones to bias and security risks, as AI systems are vulnerable to signal jamming and GPS spoofing – software that can send incorrect coordinates to drones to change a drone's position in the sky.[10] These tools can be used to mitigate malicious drones by disrupting the drone's link with its controller and thus sending it off course (as with signal jamming) or by encouraging the drone to redirect or avoid a private area by sending it inaccurate GPS coordinates (as with GPS spoofing).[11]

3) **Federal laws regarding drone mitigation.** Historically, federal law generally prohibited non-federal law enforcement officers from disrupting drone links, seizing control, or disabling drones. Non-federal law enforcement was allowed to identify and track drones, although active mitigation of drones was restricted to certain federal agencies. However, in December 2025, Congress passed the SAFER SKIES Act, which authorized non-federal law enforcement, after training and certification, to "take actions necessary to mitigate a credible threat" that a drone poses to people, facilities, assets, large-venue events, critical infrastructure, or correctional facilities.[12] Credible threat refers to a statement or action that a reasonable person would interpret

---

[6] Meshari Aljohani, R. Mukkamala, & S. Olariu. "Delivery of Medical Supplies to Remote Locations via Unmanned Aerial Vehicles: Approaches, Challenges, and Solutions," *Transportation Research Procedia,* vol. 84 (2025), https://www.sciencedirect.com/science/article/pii/S235214652500095X.
[7] "Drones could change avalanche control in Canada. Here's how," *CBC,* (Apr. 11, 2026), https://www.msn.com/en-ca/public-safety-and-emergencies/health-and-safety-alerts/drones-could-change-avalanche-control-in-canada-here-s-how/ar-AA20EabL?ocid=BingNewsVerp.
[8] For the purposes of this analysis, "drones" has the same meaning as "autonomous drones or "UAS."
[9] Vladimir Spinko, "Drone swarms: How they actually work and what industries should care," *The Robot Report,* (Aug. 3, 2025), https://www.therobotreport.com/drone-swarms-how-they-actually-work-and-what-industries-should-care/.
[10] "How Anti-Drone Jammers and GPS Spoofers Disrupt Unauthorized Drones," *Laffaz,* (Oct. 18, 2025), https://laffaz.com/anti-drone-jammers-gps-spoofers-disrupt-unauthorized-drones/.
[11] *Id.*
[12] (6 U.S.C, § 124n(a)(2).).

as a genuine intent to inflict harm, coupled with the likelihood that the actor could carry out that harm.[13]

In June 2025, the President signed Executive Order (EO) 14305 establishing the Federal Task Force to Restore American Airspace Sovereignty that was tasked with reviewing operational, technical, and regulatory frameworks and developing and proposing solutions to drone threats.[14] In addition to creating a task force, the order enabled non-federal law enforcement agencies to access grant programs for the intention of purchasing drones or equipment for the detection, tracking, or identification of drones and drone signals. The same day, EO 14307, "Unleashing American Drone Dominance," was signed, which seeks to enhance U.S. productivity in drone development, commercialization, and export.[15]

4) **The potential impact of drone usage on California Infrastructure.** California hosts some of the largest events in the world. The 2028 Los Angeles Olympics, for example, are projected to draw record numbers of sports enthusiasts from around the globe. Conservative estimates suggest a minimum of 1-1.5 million visitors to Los Angeles for the Olympics, making the event one of the largest attractions hosted in the state. [16]

Large events like the Olympics can increase the demand for public safety protocols and procedures to identify and circumvent potential threats. Indeed, concerns regarding drone strikes were raised during the Paris Olympics in 2024, with security authorities noting that:

> While authorities planned for the possibility of drones being used to deliver harmful devices, the more common incidents involved spectators trying to capture [unauthorized] footage or conduct activity that could resemble surveillance.[17]

Law enforcement should consider previous mass gatherings as case studies for understanding the threats that drones may pose to public safety. Although there have been no reports of malicious drone use at prior Olympics or sporting games, drone usage has been employed widely for unauthorized surveillance across a range of live events. A recently introduced bill, AB 2113 (McKinnor), aims to curb this practice by prohibiting drones within 400 feet of an outdoor ticketed entertainment event.

5) **Drones as a tool for mass surveillance.** Equipped on nearly every commercially available drone is a camera capable of capturing hours of footage high above unsuspecting eyes. Footage captured by drones, be it a concert that does not allow filming or of a private property without an owner's consent, can violate privacy and impede autonomy, especially when these tools are in the hands of the government. Despite the fundamental right to privacy enshrined in the California constitution, state and local governments continue to purchase and implement

---

[13] "What Legally Constitutes a Credible Threat in the United States," *Legal Guide Team,* (Nov. 7, 2025), https://thelegalguide.org/what-legally-constitutes-credible-threat-united-states/.
[14] Trump, Donald, "Restoring American Airspace Sovereignty," *The White House,* June 6, 2025, https://www.whitehouse.gov/presidential-actions/2025/06/restoring-american-airspace-sovereignty/.
[15] Trump, Donald, "Unleashing American Drone Dominance," *U.S. Government Information,* June 6, 2025, https://www.govinfo.gov/content/pkg/DCPD-202500670/pdf/DCPD-202500670.pdf.
[16] Grant Morningstar, "How Many People Will Actually Attend the LA 2028 Olympics – and What That Means for Brands," *Eleven8 blog,* (Mar. 15, 2026), https://elev8.la/blog/how-many-people-will-attend-la-2028-olympics.
[17] Rory Carroll, "US security team flags drone threat at Milano Cortina Games," *Reuters,* (Jan. 26, 2026), https://www.reuters.com/world/us-security-team-flags-drone-threat-milano-cortina-games-2026-01-26/.

surveillance tools under the guise of protecting public safety. In April 2026, Oakland County approved a Flock drone pilot program that aims to deploy drones in response to 911 calls.[18] Flock, an automated license plate reader camera company, is well-known for their contracts with the Department of Homeland Security's Immigration and Customs Enforcement (ICE) agency, which relies on the hours of footage from Flock cameras to identity and track suspected undocumented immigrants.[19] The idea of Flock technology now becoming airborne and mobile understandably concerns some community members, with one constituent arguing at the Oakland County board meeting:

> [Flock drones] could cost our privacy, our rights, and our personal data. Drone surveillance introduces a public eye in the sky, recording movement, faces, and private property, often without clear oversight or consent.[20]

The task force should carefully consider how to implement policies and procedures that effectively monitor for malicious drones whilst ensuring that these practices do not encourage mass surveillance. Common methods of drone detection such as radar and radio frequency analyzers do not require increased surveillance or monitoring of the public and should be encouraged over cameras and other surveillance tools that may impact the most vulnerable populations. Care should be taken in establishing a balanced task force that incorporates both law enforcement experts, as well as privacy experts and government watchdogs to ensure that the strategies developed for countering drones are holistic and focused on public safety and security, rather than providing tools that would allow law enforcement unfettered access to our personal lives.

Additionally, the task force may wish to consider what, if there are any federal grants, now accessible to local law enforcement under EO 14305, they may wish to pursue. Notably, EO 14305 allows for the purchasing of both drones and the equipment used to track and identify them. The goals of this task force, which are to ensure that the state is prepared in the event of a malicious drone attack, are not aligned with investing government resources in purchasing drones for law enforcement's use. The Legislature may wish to establish clear limits regarding the investment in these drones to ensure that government resources are not spent on tools that can be used to surveil its constituents. Rather, the task force should invest in resources and in equipment to identify and protect them from malicious drones whilst maintaining privacy protections for all Californians.

ARGUMENTS IN SUPPORT: PORAC writes in support:

> The rapid expansion of unmanned aircraft systems (UAS) brings growing risks to public safety, including interference with emergency operations, threats to mass gatherings, critical infrastructure, and community spaces. With major events like the 2028 Olympics approaching, a coordinated statewide approach is essential.

---

[18] Amber Eikenberry, "Oakland County approves Flock drone pilot program despite strong opposition from some residents," *Fox2 Detroit,* (Apr. 9, 2026), https://www.fox2detroit.com/news/oakland-county-approves-flock-drone-pilot-program-despite-strong-opposition-from-some-residents.
[19] Jack Lemnus, "Florida police use Flock license plate cameras for ICE surveillance," *Saints Wire,* (Apr. 7, 2026), https://saintswire.usatoday.com/story/news/local/florida/2026/04/06/florida-police-use-flock-license-plate-cameras-for-ice-surveillance/89243062007/.
[20] Eikenberry, "Oakland County approves Flock drone", *Fox2 Detroit.*

AB 2043 takes an important step forward by bringing together public and private stakeholders to assess these risks and develop comprehensive response strategies. The integration of UAS detection systems into existing emergency operations plans and incident command structures will help ensure that first responders are better equipped to prevent, identify, and respond to emerging threats.

REGISTERED SUPPORT / OPPOSITION:

Support

Peace Officers Research Association of California (PORAC)

Opposition

None on file.

Analysis Prepared by: Kate Davis / P. & C.P. / (916) 319-2200