USICA and the "American Security Drone Act" – Frequently Asked Questions

What is the "American Security Drone Act," and what does it do?

The "American Security Drone Act" is a provision (Sec. 4401) of the U.S. Innovation and Competition Act, the U.S. Senate bill designed to address technology and national security concerns emanating from China. Under the "American Security Drone Act," certain federal agencies would not be allowed to procure, operate, or provide grant money for drones from covered countries (including DJI drones) unless they obtain a waiver on a case-by-case basis.

Does the "American Security Drone Act" apply to all federal agencies procuring or using drones?

No, there are some exceptions. The "American Security Drone Act" contains several exemptions for specific agencies and use cases, including:

- The Department of Homeland Security, Department of Defense, and Department of Justice, if the drone procurement or operations are "required in the national interest in the United States" and only used for certain purposes. These purposes include research, evaluation, training, testing, or analysis for electronic warfare, information warfare operations, development of UAS or counter-UAS technology, counterterrorism or counterintelligence activities, and federal criminal, or national security investigations.
- The Department of Transportation, if the drone operations are used for the sole purpose of research, evaluation, training, testing or analysis for the Federal Aviation Administration's ASSURE Center of Excellence for Unmanned Aircraft Systems.
- The National Transportation Safety Board (NTSB), if necessary for the sole purpose of conducting safety investigations.
- The National Oceanic Atmospheric Administration (NOAA), if necessary for the sole purpose of marine or atmospheric science or management.

In addition, the provision allows the head of any federal agency to waive the prohibition on DJI drones on a case-by-case basis, as long as they notify Congress and obtain approval from either the Secretary of Homeland Security or Secretary of Defense.

Does the "American Security Drone Act" apply to <u>all</u> federal funds for contracts or grants for DJI drones?

No, there are also certain exceptions for federal funding for contracts or grants "required in the national interest in the United States." First, all federal agencies are exempt from the "American Security Drone Act" if the contract or grant was awarded prior to the law going into effect – which means that it will not apply to any contracts or grants that have already been awarded to date.

The provision also contains an exemption for all federal agencies if the grants or contracts are only used for certain purposes, as determined by the Secretary of Homeland Security, the Secretary of Defense, or the Attorney General. These purposes include research, evaluation, training, testing, or analysis for electronic warfare, information warfare operations, development of UAS or counter-UAS technology, counterterrorism or counterintelligence activities, the safe integration of drones into the national airspace, and federal criminal or national security investigations.

In addition, the provision allows the head of any federal agency to waive the prohibition on providing grants for the purchase or use of DJI drones on a case-by-case basis, as long as they notify Congress and obtain approval from either the Secretary of Homeland Security or Secretary of Defense.

What would the "American Security Drone Act" mean for federal agencies that use DJI drones and do not have an exemption?

The "American Security Drone Act" would have an immediate impact on how these federal agencies use their DJI drone if they do not have exemptions. Their current drone fleets would be grounded, and agencies would no longer be able to purchase DJI drones in the future either. Although an agency can request a waiver to continue its drone use on a case-by-case basis, this one-off approval system stands to disrupt ongoing drone operations at the impacted agencies and delay critical work, including wildfire mitigation efforts, routine wildlife surveys, environmental monitoring, scientific research, and much more. In fact, a similar policy prevented the Department of the Interior from carrying out more than 70% of planned, controlled burns in 2020 alone, making fighting wildfires more difficult.

Would the "American Security Drone Act" impact others in the drone industry ecosystem as well?

Yes. As detailed above, the "American Security Drone Act" would prevent certain federal agencies from providing federal grant money or contracting for the purchase or use of DJI drones. This means that public safety agencies could be cut off from grants to purchase DJI drones or support drone programs that include DJI drones in their fleet, and universities would not be able to carry out government-funded research projects if they use DJI drones to collect data. Contractors and small businesses that supply the federal government and these organizations with DJI drones would also be hurt under these provisions, all through no fault of their own and for no security benefit.

What data security safeguards does DJI have in place?

DJI gives its drone operators control over the data they collect and generate. The company cannot proactively access any flight logs, photos, or videos generated during drone flights – and neither can anyone else. The only way that data gets shared is if the operator decides to share it by opting in. Operators can also take additional steps to ensure the security of the data collected by their drones. For example, if Internet access is not required for a mission, DJI drones can be used entirely offline via "airplane mode" on the phone or tablet attached to the remote controller. If a user does need the Internet for other reasons, such as to access map services, DJI also offers a "Local Data Mode" that prevents any data from being transmitted to or from DJI's flight apps and the Internet – essentially an "airplane mode" that applies only to the drone's software. This eliminates any possibility that the drone operator could inadvertently share flight information from the app, including the location of flights, photos, or videos.

DJI drones can also be used without DJI software – if users prefer the features and security configurations of drone software developed by other companies around the world, they can choose from dozens of options.

Has DJI's data security been confirmed by outside organizations?

Yes. Several government agencies and independent private sector firms have analyzed DJI products and issued reports attesting to their security. For example:

- In 2018, San Francisco cybersecurity firm Kivu Consulting conducted a first-of-its-kind detailed examination of DJI drones, mobile apps, and servers, as well as the data streams they transmit and receive. Kivu purchased DJI drones off the shelf, downloaded DJI software from the Internet, then scrutinized every bit of data they exchanged over the Internet to determine whether customer data was in fact protected. The ensuing report concluded that DJI did not access photos, videos, or flight logs generated by the drones unless drone operators voluntarily chose to share them.
- A March 2020 risk assessment conducted by Booz Allen Hamilton tested the data security of certain DJI drones and found no evidence that the data, or information collected by these drones was transmitted to DJI, China, or any other unauthorized party.
- FTI Consulting found when Local Data Mode is enabled, "no data that was generated by the application was sent externally to infrastructure operated by any third party, including DJI." In its cybersecurity assessment last year, it also noted "a number of instances where DJI employed security best practices."
- The U.S. Department of the Interior, which has used drones for monitoring wildfires, conducting geological surveys, and inspecting volcanic activity, conducted a flight test and technical evaluation of its DJI drones. After a careful evaluation, DOI concluded that DJI drones were the best suited for accomplishing their missions while at the same time protecting the data they generate.
- The Idaho National Laboratory conducted its own cybersecurity test and evaluation of two DJI drones on behalf of the Department of Homeland Security's Cybersecurity and Infrastructure Agency, finding that "there are no major areas of concern related to data leakage."

How do you know DJI doesn't collect data?

Here's just one example. In 2017, DJI received a subpoena from the National Transportation Safety Board for information after a U.S. Army Black Hawk helicopter collided with a DJI drone over New York harbor. This data provided an obvious safety benefit, and DJI wanted to provide it – it was legally required, and it was the right thing to do. But because the drone pilot had never shared that data with DJI, the company simply didn't have any data to provide. Ultimately, the NTSB was able to access flight logs and other detailed information directly from the pilot, but it showed how DJI's commitment to data privacy works in practice.