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 bill that would prohibit most federal agencies from procuring, operating, or providing grant money for drones from covered countries, including drones manufactured in China, 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, the "American Security Drone Act" contains several exemptions for specific agencies and use cases, including:

- The Department of Homeland Security, Department of Defense, Office of the Director of National Intelligence, and Department of Justice, if the drone procurement is "required in the national interest in the United States," and is only used for certain purposes. The bill requires the exemption to be for the sole purposes of "research, evaluation, training, testing, or analysis for electronic warfare, information warfare operations, cybersecurity, or development of unmanned aircraft system or counter-unmanned aircraft system technology," or "conducting counterterrorism or counterintelligence activities, protective missions, or Federal criminal or national security investigations, including forensic examinations, or for electronic warfare, information warfare operations, cybersecurity, or development of an unmanned aircraft system or counter-unmanned aircraft system technology," or can no longer connect to a "covered foreign entity" and otherwise poses no national security cybersecurity risks.
- The Department of Transportation and the Federal Aviation Administration, if the drone operations or procurement are used for maintaining public safety or are deemed to support "the safe, secure, or efficient operation of the National Airspace System," including activities carried out at the FAA's Alliance for System Safety of UAS through Research Excellence (ASSURE) Center of Excellence (COE).
- The National Transportation Safety Board (NTSB), if the operation or procurement is necessary for the sole purpose of conducting safety investigations.
- The National Oceanic Atmospheric Administration (NOAA), if the operation or procurement is necessary for the sole purpose of meeting NOAA's science or management objectives or operational mission.
- Any appropriate federal agency, in consultation with the Secretary of Homeland Security, if the procurement or operation "is necessary for the purpose of supporting the full range of wildfire management operations or search and rescue operations."
- Elements of the intelligence community, in consultation with the Director of National Intelligence, if the procurement or operation "is necessary for the purpose of supporting intelligence activities."
- Tribal law enforcement or tribal emergency service agencies, if the procurement or operation "is necessary for the purpose of supporting the full range of law enforcement operations or search and rescue operations on Indian lands."

In addition, the provision allows the head of any federal agency to waive the prohibition on covered drones on a case-by-case basis, as long as they notify Congress and obtain approval from the Director of the Office of Management and Budget, in consultation with the Federal Acquisition Security Council.

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

There are certain, limited exceptions for federal funding for contracts or grants. NOAA, the Department of Transportation, and the Federal Aviation Administration, among other agencies, also can be exempt for certain purposes, similar to as described above.

In addition, the provision allows the head of any federal agency to waive the prohibition on providing grants for the purchase or use of covered drones on a case-by-case basis, as long as they notify Congress and obtain approval from the Director of the Office of Management and Budget, in consultation with the Federal Acquisition Security Council.

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

The "American Security Drone Act" would have an immediate impact on how these federal agencies use their covered drones, including drones manufactured in China, if they do not have exemptions. Their current drone fleets would be grounded, and agencies would no longer be able to purchase similar drones in the future. 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 wildlife surveys, environmental monitoring, scientific research, and much more.

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 certain drones – including those from the world's largest drone manufacturer. While it purports to provide exemptions for state, local, or territorial law enforcement or emergency service agencies, they are subject to the same complex case-by-case waiver process that will make it extremely challenging for them to maintain their critical safety operations. This means that public safety agencies could be cut off from grants to purchase certain drones or support drone programs that include drones manufactured in China in their fleet, and universities would not be able to carry out government-funded research projects if they use drones manufactured in China or other covered drones to collect data. Contractors and small businesses that supply the federal government and these organizations with covered drones would also be hurt under these provisions, all through no fault of their own and for no security benefit.

What data security safeguards do drones manufactured in China have in place?

As an example, the worlds' leading manufacturer, 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.

Have drones manufactured in China been subject to security audits by outside organizations??

Yes. This information is not available for all manufacturers based in China, but several government agencies and independent private sector firms have audited the leading drone manufacturer, DJI 's products and issued reports attesting to their security. For example:

- San Francisco cybersecurity firm **Kivu Consulting** conducted a detailed examination of DJI drones, mobile apps and servers, as well as data streams they transmit and receive. Kivu purchased DJI drones off the shelf, downloaded DJI software from the Internet, and scrutinized every bit of data they exchanged over the Internet to determine whether customer data was in fact protected. The ensuing report confirmed that "users have control over the types of data DJI drones collect, store, and transmit" and that DJI did not access photos, videos, or flight logs generated by the drones unless drone operators voluntarily chose to share them.

- A risk assessment conducted by **Booz Allen Hamilton**, which tested the data security of DJI drones, found no evidence that the data or information collected by the analyzed drones was transmitted to DJI, China, or any other unauthorized party.

- **FTI Consulting** found that 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, it also noted "a number of instances where DJI employed security best practices." The report also noted that when users opted to share their data with DJI, there was no data transmission to Chinese servers. All data went to servers in the U.S., or western Europe.

- The **U.S. Department of the Interior** (DOI), 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**, which conducted a cybersecurity test and evaluation of two DJI drones on behalf of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, found that "there are no major areas of concern related to data leakage."
- The **U.S. Department of Commerce** validated DJI's Core Crypto Engine, confirming it meets NIST standard FIPS 140-2, for cybersecurity relating to government procurement.

How do you know drones manufactured in China do not collect data?

Here's just one example from the world leading drone manufacturer. 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.