Manufacturer: Drones should transmit identifier for security

March 27 2017, by Joan Lowy

In this Jan. 5, 2017 file photo, a drone flies in Las Vegas. The world's largest manufacturer of civilian drones is proposing that drones be required to continually transmit identification information to help government security agencies and law enforcement figure out which might belong to rogue operators. (AP Photo/John Locher, File)

The world's largest manufacturer of civilian drones is proposing that the craft continually transmit identification information to help government

security agencies and law enforcement figure out which might belong to rogue operators.

DJI, a Chinese company, said in a paper released Monday that radio transmissions of an identification code, possibly the operator's Federal Aviation Administration's registration number, could help allay security concerns while also protecting the operator's privacy. The paper suggests steps that can be taken to use existing technologies to develop an identification system, and that operators could include more identification information in addition to a number if they wish.

Anyone with the proper radio receiver could obtain those transmissions from the drone, but only law enforcement officials or aviation regulators would be able to use that registration number to identify the registered owner.

Law enforcement agencies and the U.S. military raised security concerns last year after FAA officials proposed permitting more civilian drone flights over crowds and densely populated areas.

In response, the FAA announced in January that it was delaying a public notice of the proposal while the agency works to address the concerns. On Monday, FAA Administrator Michael Huerta kicked off a three-day drone symposium in suburban Washington by announcing that the agency is forming an advisory committee to make recommendations on how to remotely track drones, as well as trying to facilitate a dialogue between government agencies and the drone industry on how best to address security concerns.

State and local authorities, as well as some industries, want to ban drone flights near certain sensitive sites, such as nuclear power and chemical plants.

"How can we make sure unmanned aircraft don't gain access to sensitive sites? And after seeing how drones can be used for ill-intent overseas, how can we ensure similar incidents don't happen here?" Huerta told the symposium. "These aren't questions the FAA can or should answer alone."

A key concern is that there are no means for security agencies to differentiate between drones that may pose security risks from those that don't.

Brendan Schulman, an attorney for DJI, compared the identification transmissions to a car license plate. The lack of a license plate is a reason for police to stop a car for a further look while letting cars with proper plates continue to travel by, he said.

Last year, Congress directed the FAA to develop approaches to remotely identifying drone operators and owners, and set deadlines for doing so over the next two years.

Security concerns about civilian drones extend beyond the United States. Regulations have been proposed in Europe regarding technology to enable authorities to remotely identify drones, including by the European Aviation Safety Agency, the FAA's counterpart. France and Germany have also called for remote identification technology. Italy and Denmark already include identification technologies in regulations that seem not to be enforced because a means of compliance doesn't yet exist, the DJI paper said.

FAA and drone industry officials have been discussing the possible creation of an online network that could be accessed by a mobile phone so that drone operators can submit flight plans before taking off. Those plans would be available to law enforcement and other government agencies and possibly to the public.

Airlines and other manned aircraft operators already submit flight plans to the FAA in order to receive air traffic control services. In 2011, Congress gave operators the ability to block public access to their plans if they wish.

A remote transmission system is preferable to a network that attempts to track or record the location of all drones in real time, which would be far more complex to develop and would expose the confidential information of drone users, the DJI paper said.

That approach "would result in the collection and access to flight information by people who do not need it, such as far-away business competitors," Schulman said.