



## Securing the Drone Supply Chain

**New proposed rulemaking aims to safeguard the U.S. drone supply chain from foreign threats.**

**W**hen mysterious drones began flying over New Jersey in December it fueled speculation and concern over where the unmanned aircrafts originated from, who was operating them and why they were even there in the first place. In response, the FAA temporarily banned drone flights in many New Jersey and New York areas. On a deeper level, however, this was yet one more highly publicized issue signaling the need for better drone security and oversight.

“The FBI, the Homeland Security Department and state agencies have been investigating, but officials say there has been nothing so far to suggest any drones have posed a national security or public safety threat,” *AP* reported. “Authorities say many of the drone sightings have actually been legal drones, manned aircraft, helicopters and even stars.”

In December, the FAA said the FBI had received tips of more than 5,000 reported drone sightings during the prior few weeks with approximately 100 leads generated. “Consistent with each of our unique missions and authorities, we are quickly working to prioritize and follow these leads,” the FAA said [in a statement](#). “We have sent advanced detection technology to the region. And we have sent trained visual observers.”

As of early January, authorities had yet to publicly identify the drone operators or their motives.

### Enlisting Help

Uncle Sam is taking a keen interest in securing the drone supply chain. “With the rapid development of advanced technology, commercial drones are now commonplace across the United States,” the Bureau of Industry and Security states in an agency [press release](#). In January, the agency announced new rules to secure the drone supply chain in the form of [advance notice of proposed rulemaking \(ANPRM\)](#) regarding unmanned aircraft systems (UAS).

“As we did with connected vehicles, we are beginning our inquiry by asking a series of questions to better understand the ICTS integral to UAS, the risks associated with UAS, and the involvement of foreign adversaries in the supply chain,” Elizabeth Cannon, executive director, OICTS, said in a [press release](#).

*ExecutiveGov* says the notice outlines several areas for comment, such as assessments of ICTS transaction risks arising from foreign adversaries like China and Russia. The BIS notice

also seeks public feedback on potential approval processes for requests to engage in regulated commercial transactions, possible economic impact of prohibiting certain ICTS deals and steps to mitigate potential adverse effects of the supply chain rules.

U.S. Secretary of Commerce Gina Raimondo called the BIS rulemaking on the drone ICTS supply chain an essential step to protect U.S. vulnerabilities from foreign entities. “Securing the unmanned aircraft systems technology supply chain is critical to safeguarding our national security,” she says. “This ANPRM is an essential step in protecting the United States from vulnerabilities posed by foreign entities.”

### Not for Espionage

In “[US seeks public input on drone supply chain rules](#),” DroneDJ’s Ishveena Singh says the Department of Commerce’s initiative highlights concerns over foreign adversaries, including China and Russia, exploiting vulnerabilities in the drone supply chain to access sensitive U.S. data. The agency is seeking feedback on several critical areas: definitions of drones and their components, assessments of risks posed by different foreign adversaries, potential economic impacts of regulations and viable mitigation strategies.

As drones continue to play a vital role in industries ranging from agriculture to public safety, Singh says ensuring the integrity of their supply chains is more critical than ever. For example, Chinese tech giant DJI, a leading player in the U.S. commercial drone market, finds itself at the center of the ongoing debate.

“Lawmakers have raised concerns that foreign adversaries could exploit DJI’s devices to access sensitive information,” she writes. “DJI has pushed back against these claims, asserting that its drones are designed for consumer and commercial use, not for espionage.”