

Articles + Publications | February 4, 2021

## Locke Lord QuickStudy: USA for Your UAS?

Locke Lord LLP

### WRITTEN BY

[T. Patrick Byrnes](#) | [Matthew J. Kalas](#) | [Berne C. Kluber](#)

### RELATED OFFICES

Houston

---

In a shot from beyond his presidency via Executive Order 13981 (signed on January 18, 2021, but published in the Federal Register after President Biden's inauguration), Former President Trump wants government agencies and their contractors to scrutinize their UAS aircraft, controllers, and systems for software or critical electronic components manufactured by foreign adversaries, and either strip them out or replace their UAS.

EO 13981:

1. Calls for the use of no taxpayer dollars for tainted aircraft or controllers, i.e., those that fall within the definition of "covered UAS" as discussed below, or the storage of data collected by a UAS outside the U.S.?
2. Requires executive departments and agencies to review their UAS assets to determine if they are tainted, cease using such tainted equipment or contractors that use them, and provide a report to the Office of Management and Budget identifying any legal authority to take the actions outlined above.
3. Within 60 days the departments and agencies are to provide "a report to the Director of National Intelligence and the Director of the Office of Science and Technology Policy describing the manufacturer, model, and any relevant security protocols for all UAS" used by the departments and agencies that are manufactured by foreign adversaries or otherwise contain tainted parts.
4. The Director of National Intelligence has 180 days from the Order to issue a report to the President covering the security risks associated with the current UAS fleet, complete with mitigation plans, which could include removal of covered UAS from the fleet.
5. Within 270 days, the FAA is to propose regulations pursuant to Section 2209 of the FAA Extension, Safety, and Security Act of 2016 (Public Law 114–190). Section 2209 calls on the FAA to establish a process for applicants to request that the FAA prohibit or restrict UAS operations near fixed site facilities, such as energy production, transmission, distribution facilities and equipment, oil and chemical refineries and facilities, amusement parks, and similar types of locations.
6. The departments and agencies are to work with the Budget office to find funding to replace covered UAS.

"Adversary countries" are the usual suspects: China, Iran, North Korea, Russia, and any other country the

Secretary of Commerce identifies. Of course, China is the biggest issue since many of the “critical electronic components” (defined as any electronic device that stores, manipulates, or transfers digital data) installed in UAS flight controllers, ground control system processors, radios, digital transmission devices, cameras, or gimbals are manufactured there. Fortunately, critical electronic components excludes “passive electronics such as resistors, and non-data transmitting motors, batteries, and wiring.”

The definition of “covered UAS” is very broad. It includes any UAS or critical electronic component made in an adversarial country. It does, however, exclude separate communication devices, such as cell phone or tablet apps designed to perform independently of a UAS system, which may be incorporated into the operation of the UAS. On the broader side, it covers UAS that use network connectivity or data storage located outside the U.S. or administered by any entity in an adversarial country. Finally, it includes any UAS with hardware or software components manufactured in an adversary country used for transmitting data from the UAS (photographs, videos, location information, flight paths, etc.).

So, if you fly or maintain UAS on federal jobs, clear off the work bench and get those screwdrivers busy. And if you are a U.S. component manufacturer, or looking to enter the sector, this EO helps level the playing field a bit, and provides a potential opening in a very challenging market.

## **RELATED INDUSTRIES + PRACTICES**

- [Privacy + Cyber](#)