CLIENT ALERT

Legislation to Stop Threatening Drones in Their Tracks

Jul.31.2018

New unmanned aircraft regulations may be on their way – and not from the FAA. A new bill introduced in the Senate in May of this year just received the administration's endorsement on July 17, 2018. The new bill, S.2836 – Preventing Emerging Threats Act of 2018, seeks to expand the regulatory powers of the Department of Homeland Security and the Department of Justice to unmanned aircraft systems (UAS) in an effort to enhance the United States' ability to respond to potential threats to national security – specifically threats to the safety and security of certain government facilities or assets.

The administration's statement this month expressed "strong" support for the bill, which is described as providing the United States the ability "to mitigate threats posed by careless, threatening, or malicious drone operations, while enabling the further development of the commercial drone industry, protecting privacy and civil liberties, and ensuring the safety of the National Airspace System." Now in committee, the new bill would provide DHS and DOJ the following expanded powers to use at their discretion:

1. Detect, identify, monitor, and track UASs without prior consent (including by communications intercept).
2. Use passive or active physical, electronic, radio, or electromagnetic means to warn a UAS operator.
3. Disrupt UAS control without prior consent.
4. Seize or assume control of UAS without prior consent.
5. Seize or confiscate a UAS.
6. Disable, damage, or destroy a UAS without prior consent.

The bill allows the Secretary of Homeland Security and the Attorney General, in consultation with the Secretary of Transportation, to determine the existence of a threat to a covered facility or asset. It further commissions a DHS study to evaluate the potential threats posed by UAS, which would be presented to Congress for consideration. The administration's statement adds color to the threats posed by UAS, advocating for the "development of a legal framework that protects the public from nefarious uses of this technology, such as facilitating terrorist attacks, conducting espionage, or facilitating other criminal activities such as illicit surveillance, interfering with the safe operation of aircraft, interfering with law enforcement operations, delivering contraband inside prisons, or smuggling drugs or other harmful materials across our Nation's borders." The bill is much more tailored and does not address all of the threats outlined in the administration's statement, many of which are criminal acts covered by other law enforcement powers.

The bill also includes privacy protections such as limiting collection "to the extent necessary," disclosure restrictions, and limits on how long captured data can be stored. And DHS and DOJ powers would be limited to their particular protection missions associated with, for example, U.S. Customs and Border Protection security operations, U.S. Secret Service operations, and the Federal Bureau of Prisons operations. The powers could also be used, upon request, to support state and local law enforcement for significant gatherings. But these limitations have not assuaged many opponents, who argue that the bill's exceptions to the Wiretap Act and Stored Communications Act are too broad.

The bill as written appears to cover all types of drones regardless of size, weight, or other features so commercial users and consumers are left without guidance from the bill on whether their drones would be subject to the new DHS and DOJ regulations should the bill become law. In the meantime, however, there are some issues that commercial developers and users may begin considering and potential consequences that consumers can anticipate:

New Flight Restrictions

- There will likely be new flight restrictions for UASs near government facilities and assets.
- These restrictions may not always be pre-determined, as the bill does not concretely define what constitutes a "threat" meriting such restrictions.

New Operational Challenges

- Drone operators need to ensure their use patterns do not trigger threat concerns.
- Both commercial users and consumers should be aware that they may incur more than a mere fine for even inadvertent regulatory violations, including the disabling or destruction of their drone.

Information Security/Privacy Risk

- A drone's encryption and other information security features may become more attractive options to some users.
- Drone developers may find themselves responding to government inquiries to bypass their products' security.

The bill's bipartisan support, as well as its national security nexus, increases the likelihood that some version of expanded counter-drone powers will become law.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Cheryl A. Falvey
Partner – Washington, D.C.
Phone: +1 202.624.2675
Email: cfalvey@crowell.com

Adelicia R. Cliffe
Partner – Washington, D.C.
Phone: +1 202.624.2816
Email: acliffe@crowell.com

Maria Alejandra (Jana) del-Cerro
Partner – Washington, D.C.
Phone: +1 202.624.2843
Email: mdel-cerro@crowell.com

Kate M. Growley, CIPP/G, CIPP/US
Partner – Washington, D.C.
Phone: +1 202.624.2698

Email: kgrowley@crowell.com

Stephanie L. Crawford
Associate – Washington, D.C.
Phone: +1 202.624.2811
Email: scrawford@crowell.com