Hacker No Fly Zone: FAA and TSA Propose Cybersecurity Rules for Drone Ecosystem

Client Alert | 6 min read | 10.08.25

Marking a significant milestone toward the broad deployment of commercial drones over American skies, the Federal Aviation Administration ("FAA") and Transportation Security Administration issued a proposed rule in August that would streamline how drones can operate when they fly beyond the visual line of sight of their operators.

Aspects of this landmark proposed rule, **Normalizing Unmanned Aircraft Systems Beyond Visual Line of Sight Operations** (the "NPRM" or "Proposed Rule"), have been the subject of several recent Crowell & Moring **client alerts**. This installment focuses on the cybersecurity obligations that the NPRM would impose on the Unmanned Aircraft Systems (UAS) industry.

Three categories of entities would be subject to the Proposed Rule's cybersecurity requirements: Commercial Drone Operators, Automated Data Service Providers, and UAS Manufacturers. The Proposed Rule would require familiar, yet far reaching, cybersecurity requirements on all stakeholders in the UAS ecosystem.

Commercial Drone Operators (§§108.435 and 108.535)

The NPRM divides Commercial Drone Operators into two groups. First, Operators that conduct *lower risk, limited-scale operations*, such as package delivery, agriculture work, civil interest deployments, training, and recreation could operate under a permit issued by the FAA. Second, Operators that conduct *higher risk, larger-scale, and more complex operations* would need to operate under a certificate that would require thorough FAA review and oversight.

The NPRM anticipates that both groups of Operators would rely on complex technologies that would likely be susceptible to many of the same security risks faced by other connected technologies. Given these common threats, the NPRM would require both categories of Operators to develop cybersecurity policies and procedures. *See* §§ 108.150(c), 108.435, 108.535.

A required cybersecurity policy would "at a minimum" outline processes for:

1. Protecting software, hardware, and network computing infrastructure necessary to protect operations from unauthorized access;
2. Ensuring that employee network access privileges are limited to those necessary to fulfill normal job duties, and are revoked for former employees; and
3. Preparing for, responding to, and mitigating the impact of cyber attacks.

In addition to implementing these processes, Operators would also be required to review their cybersecurity policies at least annually and revise as necessary to reflect changing circumstances.

The NPRM's cybersecurity policy requirements intentionally forego prescriptive controls (i.e., specific, step-by-step rules that dictate how to achieve a security outcome) in favor of performance-based goals, which focus on the desired result without mandating a specific method. As many U.S. government contractors attempting to implement requirements that are similarly performance-based have witnessed, this flexibility leaves risky room for interpretation in an untested regulatory requirement.

In addition to requiring organizations to implement cybersecurity policies and procedures, the proposed rule would explicitly require Operators to notify the FAA in the event of a cybersecurity incident. *See* §§ 146.325, 108.45. Specifically, Operators would be required to report any incident that:

1. Results in loss of control of the unmanned aircraft;
2. Results in unauthorized access to the Operator's facilities, aircraft, loading areas, hazardous materials, or goods to be transported; or
3. Results in unauthorized access to the Operator's networks, devices, or data irrespective of whether it affects the integrity, accuracy, or reliability of unmanned aircraft operations.

Such a report would need to be made to the FAA no later than "96 hours after the occurrence" (not discovery) and would need to include:

1. The date and time of the incident;
2. The nature and scope of the incident;
3. Identification of any vulnerabilities that led to loss of control or unauthorized access;
4. The corrective actions taken; and
5. Additional information as it becomes available.

Automated Data Service Providers (§146.305)

The second category of entities that would be subject to the proposed rule are Automated Data Service Providers, which include the digital services and infrastructure that manage drone operations at low altitudes. These services, often referred to as UAS Traffic Management providers, include flight planning, real-time tracking, and conflict management to promote safety in shared airspace.

Specifically, the Proposed Rule would require Service Providers to develop and implement cybersecurity policies and processes to protect networks, devices, and data from unauthorized access.

Similar but not identical to the policy required for Operators, the Service Providers' cybersecurity policy would need to include processes for:

1. Protecting software, hardware, and network computing infrastructure from unauthorized access;
2. Ensuring that employee access privileges are limited to those necessary to fulfill normal job duties;
3. Preparing for, responding to, and mitigating the impact of cyber attacks;
4. Collecting and analyzing data to measure the effectiveness of the cybersecurity policy and processes; and
5. Revising the cybersecurity policy.

Here too, the NPRM notes that Service Providers may be able to demonstrate compliance with their requirements by relying on industry standards. The Proposed Rule suggests that the FAA would consider the

certificate-based information security standard ISO 27001 to be "one way, but not the only way, to demonstrate compliance" with this section. *See* §146.305.

Regarding incident response requirements, Service Providers would be required to notify the FAA of any incident that:

1. Results in an unscheduled service outage;
2. Results in unauthorized access to the certificated service provider's networks, devices, or data irrespective of whether it affects the integrity, accuracy, or reliability of the services provided to the service recipient; or
3. Any other occurrence specifically identified in a certificate or authorization issued under the rule.

However, unlike the enumerated notification requirements proposed for Operator incidents, the NPRM does not suggest specific elements to be included in the Service Provider notification. Rather, the proposed rule states that the Service Provider notice would need to be provided "in a form and manner acceptable to" the FAA administrator. *See* §146.325.

UAS Manufacturers (§108.875)

Finally, the NPRM proposes cybersecurity requirements for those that are involved in the manufacturing and design process of UAS. Those involved in the design and testing process would need to satisfy "Requirements for Airworthiness Acceptance."

The rule would require manufacturers to ensure that UAS equipment, systems, and networks are protected from "Intentional Unauthorized Electronic Interactions." *See* §108.875. Intentional Unauthorized Electronic Interaction ("IUEI")—a term of art—refers to cyber attacks or security breaches involving the unauthorized access or disruption of aircraft, including UAS. IUEIs include malware and the effects of external systems on UAS, such as software supply chain attacks. IUEIs do not include physical attacks or electromagnetic jamming.

Notably, the Proposed Rule does not stipulate a particular cybersecurity standard to which UAS manufacturers must adhere. Instead, the Proposed Rule references the National Institute of Standards and Technology's ("NIST") Cybersecurity Framework as a potentially acceptable approach, noting that the FAA "expects that a standard with similar requirements in the NIST Cybersecurity Framework would be found acceptable as a [means of compliance] for cybersecurity." The FAA invited comments on appropriate cybersecurity standards for UAS manufacturers, which remained open until October 6, 2025. *See* § 108.875.

Finally, while the NPRM appears to contemplate similar reporting obligations for Manufacturers, it does not do so explicitly. *See* NPRM V(D). Instead, the rule would require Manufacturers of a UAS that has received airworthiness acceptance to notify the FAA Administrator of any "identified hazard involving its [UAS] models" within 10 calendar days. Because the term "hazard" is not defined, we believe it is reasonable for the FAA to consider cybersecurity incidents as reportable hazards.

Conclusion

The NPRM is both unique and familiar. If finalized, it would impose cybersecurity regulations on UAS Operators, Service Providers, and Manufacturers for operations beyond visual line of sight for the first time. Yet, it proposes a mix of cybersecurity requirements that are themselves commonplace. As outlined above,

they are largely modeled after existing frameworks, including NIST's Cybersecurity Framework and ISO 27001, with which many private sector companies already have significant experience.

Contacts

Matthew F. Ferraro
Partner
Washington, D.C. D | +1.202.624.2610
mferraro@crowell.com

Kate M. Growley
Partner, Crowell Global Advisors Senior Director
Washington, D.C. D | +1.202.624.2698
Washington, D.C. (CGA) D | +1 202.624.2500
kgrowley@crowell.com

Sarah Rippy
Associate
She/Her/Hers
Denver D | +1.303.524.8634
srippy@crowell.com