Department of Transportation
Federal Aviation Administration

14 CFR Parts 1, 74, 91, and 107
[Docket No. FAA-2026-4558; Notice No. 26-03]
RIN 2120-AL33

AUTHORS

Jack Burnham
Senior Research Analyst, FDD's China Program

Emmerson Overell
Project Coordinator, FDD's Center on Cyber and Technology Innovation

Annie Fixler
Director and Senior Fellow, FDD's Center on Cyber and Technology Innovation

Washington, DC
August 5, 2026

FDD
FOUNDATION FOR DEFENSE OF DEMOCRACIES

www.fdd.org

Introduction

Unmanned aircraft have become an increasingly serious threat to U.S. critical infrastructure. Small, commercially available drones can bypass traditional perimeter defenses to conduct surveillance, collect sensitive facility data, or deliver conductive materials, incendiary devices, and explosives. Recent incidents involving electrical substations, military installations, and other sensitive facilities demonstrate that this threat is no longer abstract, while advances in autonomy and payload capacity will only make these systems more difficult to detect and defeat.

The Federal Aviation Administration's (FAA's) proposed process for establishing unmanned aircraft flight restrictions could help address this threat by reducing unauthorized overflights and distinguishing legitimate operators from potentially malicious actors. However, the current proposal places an unnecessarily high and poorly defined burden of proof on critical infrastructure owners and operators seeking protection to demonstrate vulnerabilities that are already broadly recognized by Congress, the administration, and federal security agencies. It also risks limiting the national security value of Section 2209 by requiring applicants to disclose existing security measures.

The FAA should revise its proposed framework to provide critical infrastructure with more proactive and predictable protection. Specifically, the agency should ease and clarify the application requirements for standard flight restrictions, strengthen consequences for deliberate violations involving national security risks, and reserve special restrictions for defense-specific critical infrastructure.

Unmanned Aircraft Pose a Critical National Security Risk

Unmanned aircraft pose a distinct threat to fixed U.S. critical infrastructure sites because they combine surveillance, access, and payload delivery in a small and relatively inexpensive platform that can bypass fences, gates, and other ground-based defenses. The Cybersecurity and Infrastructure Security Agency (CISA) recognizes unmanned aircraft as both a cyber and physical threat to critical infrastructure and warns that drones can be converted into or used to carry improvised explosive devices capable of harming people and infrastructure.[1] A commercially available drone can rapidly map a generation facility or a transmission substation, identify transformers, control buildings, security posts, and operating patterns, providing the drone operator with information that would be difficult to collect from the ground.[2] Malicious actors can also modify the same platform to carry conductive materials, incendiary devices, or explosives, introducing greater sabotage risks from both criminals and nation-state actors.

Recent cases demonstrate how easily drones can be used to collect information about sensitive facilities. In November 2024, federal authorities arrested a man for allegedly flying an

[1] U.S. Cybersecurity and Infrastructure Security Agency, Office for Bombing Prevention, "Suspicious UAS Identification Poster and Postcard," accessed July 24, 2026. (https://www.cisa.gov/resources-tools/resources/suspicious-uas-identification-poster-and-postcard)

[2] Jack Burnham, Craig Singleton, and RADM (Ret.) Mark Montgomery, "Section 232 National Security Investigation of Imports of Unmanned Aircraft Systems (UAS) and Their Parts and Components," *Foundation for Defense of Democracies*, August 6, 2025. (https://www.fdd.org/analysis/2025/08/06/section-232-national-security-investigation-of-imports-of-unmanned-aircraft-systems-uas-and-their-parts-and-components)

unregistered drone over Vandenberg Space Force Base and photographing the installation.[3] Systems at the base detected the drone approximately one mile above the base on the same day that SpaceX launched rockets carrying payloads for the National Reconnaissance Office.[4] In a separate case, federal prosecutors charged a Canadian citizen with using a drone on three occasions in January 2025 to photograph launch complexes, a payload-processing facility, a submarine wharf, and munitions bunkers at Cape Canaveral Space Force Base.[5] Although these incidents involved defense installations, they illustrate a surveillance capability that is equally relevant to energy infrastructure: drones can provide users with detailed information about facilities, critical assets, security perimeters, and operating patterns. The Nuclear Regulatory Commission has also received numerous reports of drones operating over nuclear power plants and, in 2024, began requiring operators to report such sightings to federal authorities and local law enforcement.[6]

More concerningly, other domestic incidents highlight the risk of another dangerous yet increasingly plausible scenario: a strike which destroys equipment whose loss would cause cascading effects across the U.S. economy.

In July 2020, authorities recovered a modified drone near a Pennsylvania electrical substation. Luckily the drone had crashed prior to reaching its target because authorities discovered a copper wire suspended beneath the drone, likely to create a short circuit.[7] Four years later, federal authorities disrupted a plot to attack a Nashville electrical substation. Before his arrest, the defendant researched attacks on substations, conducted reconnaissance of the intended target, and prepared to attach an armed explosive device to a drone.[8]

While these strikes would have likely caused similar outages to those caused by major weather events, a more deliberate assault could isolate and destroy targets or components that are difficult to replace or transport and remain essential to generating and transmitting large amounts of electricity. The Department of Energy (DOE) estimates that more than 90 percent of electricity consumed in the United States passes through high-voltage or large power transformers at some

---

[3] U.S. Attorney's Office, Central District of California, Press Release, "Northern California Man Arrested for Allegedly Flying Drone Over and Photographing Vandenberg Space Force Base," December 11, 2024. (https://www.justice.gov/usao-cdca/pr/brentwood-man-arrested-allegedly-flying-drone-over-and-photographing-vandenberg-space)

[4] Mike Wall, "SpaceX launches next-gen US spy satellites, 20 Starlink spacecraft from California," *Space.com*, November 30, 2024. (https://www.space.com/space-exploration/launches-spacecraft/spacex-to-launch-next-gen-us-spy-satellites-20-starlink-spacecraft-from-california-early-nov-30)

[5] U.S. Attorney's Office, Middle District of Florida, Press Release, "Canadian Citizen Charged With Aerial Photography of Defense Installation," February 13, 2025. (https://www.justice.gov/usao-mdfl/pr/canadian-citizen-charged-aerial-photography-defense-installation)

[6] U.S. Nuclear Regulatory Commission, "Drones and Nuclear Power Plant Security," January 2025. (https://www.nrc.gov/reading-rm/doc-collections/fact-sheets/fs-drone-pwr-plant-security)

[7] U.S. House of Representatives, Committee on Homeland Security, Subcommittee on Transportation and Maritime Security, "Surveillance, Sabotage, and Strikes: Industry Perspectives on How Drone Warfare Abroad Is Transforming Threats at Home," July 15, 2025. (https://www.congress.gov/event/119th-congress/house-event/LC75001/text)

[8] U.S. Department of Justice, U.S. Attorney's Office, Middle District of Tennessee, Press Release, "Man Arrested and Charged with Attempting to Use a Weapon of Mass Destruction and to Destroy an Energy Facility in Nashville," November 4, 2024. (https://www.justice.gov/usao-mdtn/pr/man-arrested-and-charged-attempting-use-weapon-mass-destruction-and-destroy-energy)

point.[9] Large power transformers are expensive, difficult to transport, typically custom-made, and often not interchangeable.[10] The destruction of even a limited number of carefully selected components could therefore create restoration challenges far more severe than utilities ordinarily face after storm damage. DOE has historically estimated procurement periods of at least one year, although the department stated in 2026 that lead times for large transformers had increased to between three and four years.[11]

Recent attacks in Ukraine illustrate how drones can target the electrical grid's most consequential components. Russian forces have used small drones controlled through fiber-optic cables, which make them impossible to jam, to penetrate barriers around high-voltage substations and strike autotransformers. These large pieces of equipment change voltage so that electricity can move between different parts of the transmission grid. Destroying an autotransformer can disable an entire transformer unit, eliminating a major pathway for moving electricity into or through a region and isolating a region from a national grid.[12] Although the United States does not face the same wartime conditions as Ukraine, these attacks demonstrate the threat vector available to a knowledgeable adversary: inexpensive drones can bypass perimeter security, exploit gaps in fixed defenses, and destroy individual components to create widespread geographic impact.

American utilities attempt to manage the risk of equipment failure by maintaining strategically located spares, participating in mutual-assistance arrangements, and designing systems to reroute electricity when individual components fail. Yet these measures do not eliminate the danger posed by a coordinated attack on scarce or non-interchangeable equipment. Industry representatives identified a compound event — such as severe weather occurring alongside a physical, cyber, or drone-enabled attack — as particularly concerning because repair crews, replacement equipment, communications systems, and alternative transmission routes could already be under strain. These risks will likely only grow more pressing as advances in autonomy render commercial drones capable of independently evading defensive systems.[13]

Surveillance and sabotage risks intersect with another critical dimension: the ubiquity of Chinese-produced unmanned aircraft in the United States. While the Federal Communications Commission and Congress have banned new drones and related equipment produced by Chinese firms such as DJI and Autel Robotics, many of their older systems remain present within the domestic market.[14] These systems pose a range of national security threats, with the CISA, the

---

[9] U.S. Department of Energy, Office of Electricity, "Addressing Security and Reliability Concerns of Large Power Transformers," June 8, 2016. (https://www.energy.gov/oe/addressing-security-and-reliability-concerns-large-power-transformers)

[10] U.S. Department of Energy, Press Release, "Department of Energy Invests $7.5 Million to Strengthen the Resilience of the Nation's Power Grid," November 14, 2018. (https://www.energy.gov/articles/department-energy-invests-75-million-strengthen-resilience-nations-power-grid)

[11] U.S. Department of Energy, Office of Electricity, "Distribution Transformer Webinar Text Alternative," March 5, 2026. (https://www.energy.gov/oe/distribution-transformer-webinar-text-alternative)

[12] Max Hunder, "Russia evades Ukraine electrical substation defences with small, unjammable drones," *Reuters*, July 10, 2026. (https://www.reuters.com/business/aerospace-defense/russia-evades-ukraine-electrical-substation-defences-with-small-unjammable-2026-07-10)

[13] Bart Elias, "Protecting Against Rogue Drones," *Congressional Research Service*, September 3, 2020. (https://www.congress.gov/crs-product/IF11550)

[14] Jack Burnham, RADM (Ret.) Mark Montgomery, Craig Singleton, and Johanna Yang, "Petition for Reconsideration of Action in Rulemaking Proceeding Application for Review of Action in Rulemaking Proceeding,"

FBI, Commerce Department, and Department of Defense (DOD) all warning of DJI's ties to the Chinese military and its insufficient cybersecurity practices.[15]

The presence of Chinese-produced drones presents a new set of dangers to U.S. critical infrastructure. Rather than assist a radicalized "lone wolf" actor or criminal element to conduct an operation against U.S. critical infrastructure, Chinese-produced drones may pass information directly back to Beijing, complementing its current efforts to conduct operational preparation of the battlefield by targeting critical infrastructure in cyberspace. Both the FBI and Department of Homeland Security (DHS) have warned explicitly that Chinese-produced drones pose a threat to critical infrastructure and may expose collected information — such as detailed imagery, geolocation information, facility layouts, and operational data — to Chinese authorities.[16] Such information may allow China to map privately-owned and -operated nodes across the American economy essential for maintaining military mobility — providing targeting information for Beijing's ongoing cyber and potential future kinetic operation against U.S. critical infrastructure.[17]

The FAA Should Enhance Its Role in Safeguarding Critical Infrastructure

In response to this threat, the FAA should use flight restrictions to give critical infrastructure owners and operators clearer airspaces, allowing them to readily identify possible threats from malicious actors. The agency can enhance national security by preventing legitimate actors from incidentally conducting dangerous overflights.

However, the proposed rule extends an unclear and potentially onerous burden of proof for owner-operators seeking protection and its requirements exceed the FAA's statutory authority under relevant Congressional legislation and run counter to the Trump administration's executive order.

The agency's proposal attempts to balance public access with protecting critical infrastructure by requiring owner operators to extensively document their risk profile rather than assuming that such assets are inherently vulnerable and require protection. To file for an Unmanned Aircraft Flight Restriction (UAFR), an applicant must also already have protective security measures commensurate with its "criticality" and file a report on the amount of drone traffic currently within the vicinity of their facility. These rules are even more stringent for "high-risk" sites, as the FAA would require this subset of applicants to have preexisting layered defenses against drones and other possible threats.

However, the FAA has declined to outline a clear standard of proof that would be sufficient for a successful application — specific security measures such as the presence of Remote ID sensing, the consistency of overflights that would trigger protective measures, or how these overflights

---

Foundation for Defense of Democracies, March 17, 2026. (https://www.fdd.org/analysis/2026/03/17/petition-for-reconsideration-of-action-in-rulemaking-proceeding-application-for-review-of-action-in-rulemaking-proceeding)

[15] Ibid.

[16] Ibid.

[17] Ibid; Mike Minihan and RADM (Ret.) Mark Montgomery, "America's Military Plans Depend on Infrastructure It Doesn't Secure," *Foundation for Defense of Democracies*, July 13, 2026. (https://www.fdd.org/analysis/2026/07/13/americas-military-plans-depend-on-infrastructure-it-doesnt-secure)

must be documented across different sites and operators. Along with inherently placing the burden of proof on owner-operators, these gaps add regulatory uncertainty that may deter certain operators from initially applying for protection regardless of the severity of the threat.

Moreover, there is limited evidence to suggest that these requirements are supported by congressional statute or administrative intent. While the FAA's proposal operationalizes Section 2209 of the FAA Extension, Safety, and Security Act (FESSA) of 2016, its structure implies safeguards not named in the statute, overly limiting its national security impacts. Under Section 2209, Congress required the FAA to consider aviation safety, protection of property and individuals, and national security in determining restrictions on drones flying over fixed facilities.[18] Pointedly, this section was intended as a specific carveout from the FAA's statutory focus on protecting the public's right-of-transit under 49 U.S.C. § 40103.[19] While the agency's default authority from Congress is to protect Americans' right to access airspace, Section 2209 mandates that the FAA focus specifically on critical infrastructure protection, even if may intercede on the public's right to transit or access certain locations. To that end, the relevant statute requires the FAA to solely focus on each specific criterion, either together or separately, in reaching a determination to grant a UAFR, not to develop multi-part tests that fall outside of its bounds. Moreover, since FESSA's passage, Congress has largely sought to heighten drone security measures by dispensing authorization to intercept unmanned aircraft towards state, local, and tribal governments under the Safer Skies Act, which was passed as part of the FY2026 National Defense Authorization Act.[20]

The Trump administration has also clearly outlined the necessity of securing the airspace over critical infrastructure in Executive Order 14305. While the FAA cites this order as its impetus for its proposal, the order explicitly prioritizes safeguarding critical infrastructure, stating that such installations are "subject to frequent — and often unidentified — UAS incursions" and that "immediate action is needed to ensure […] that its airspace remains safe and secure."[21] The executive order requires DOD, DHS, Department of Justice (DOJ), and Department of Transportation (DOT) to recommend whether the White House should designate critical infrastructure as "covered facilities" or "covered assets" under 6 U.S.C. 124n and 10 U.S.C. 130i — statutes which authorize the destruction of unmanned aircraft that approach such facilities.[22] Moreover, the order also requires DHS, FAA, and sector risk management agencies to publish guidance that aids critical infrastructure owners and operators in better deploying security technologies to counter intrusions by unmanned aircraft — a process disrupted by the FAA's insistence that applicants highlight their current security protocols to receive a restriction order.[23]

The FAA's approach to managing flight restriction orders cuts against recent interagency and state actions to counter drones, particularly those produced by foreign adversaries. Along with

[18] FAA Extension, Safety, and Security Act of 2016, Pub. L. No. 114-190, § 2209, 130 Stat. 615, 634 (2016), codified at 49 U.S.C. § 40101 note.
[19] Sovereignty and use of airspace, 49 U.S.C. §40103. (https://www.law.cornell.edu/uscode/text/49/40103)
[20] National Defense Authorization Act for Fiscal Year 2026, Pub. L. No. 119-60, div. H, tit. LXXXVI, §§ 8601-8607, 139 Stat. 718, 1938-45 (2025).
[21] Executive Order 14305, 90 Fed. Reg. 24719, "Restoring American Airspace Sovereignty," June 11, 2025.
[22] Ibid.
[23] Ibid.

the FBI and DHS warning that Chinese-produced drones pose a direct threat to critical infrastructure, Congress and DOJ have banned federal funds from being used to purchase DJI products, particularly by law enforcement, recognizing their risk to security operations. States such as Arizona, Arkansas, and Louisiana have also passed laws that preemptively restrict unauthorized flights over critical infrastructure sites, such as power plants, without the need for owners and operators to petition for protection.

Recommendations

Both the Trump administration and Congress have rightly noted the national security risks posed by the unsafe operation of drones around sensitive sites. The FAA can contribute to its national security mission by preventing lawful operators from conducting overflights of critical infrastructure. Drones that continue to operate in restricted areas will, by definition, be violating the law.

To clarify the operating picture so that law enforcement can prosecute criminal or nation-state actors, the FAA should focus on easing the burden of proof on owners and operators, enhancing penalties for unlawful access of restricted airspace, and adding additional safeguards for defense-specific critical infrastructure.

- **The FAA should ease the burden of proof for applicants seeking a UAFR and proactively provide greater protection to critical infrastructure.** The risk posed by small drones to U.S. critical infrastructure is well documented by multiple national security agencies, the Trump administration, Congress, and a range of state, local, and tribal governments. As such, the FAA should not require standard UAFR applicants to provide overflight statistics or detail how drones pose a risk to their facilities. Instead, the FAA should explicitly place the burden on other airspace users to demonstrate why a given restriction will unduly hinder their public-access rights. The agency should also allow a standard UAFR to apply for a longer period of time, with renewal periods tied to either major changes in site design or five-year increments.

- **The FAA should consider applying criminal penalties for violations of standard UAFRs in certain national security-related circumstances.** While drone operators should likely receive civil penalties in the case of accidental violations, the United States has already experienced a pattern of UAS intrusions that suggest ties to either criminal organizations, terrorism, or an adversarial nation-state actor. As such, the FAA should consider applying criminal penalties under 49 U.S.C. 40103(b)(3) and 46307 for violations of standard UAFRs when those violations relate to national security.

- **The FAA should limit the application of a Special UAFR to defense-specific critical infrastructure.** The agency's proposed delineation between "critical infrastructure" and facilities that support "defense production, intelligence operations, continuity of government functions, or other activities where disruption could create significant national security risks" is unnecessarily broad and generates regulatory uncertainty due to overlapping statutory definitions. Rather, the FAA should limit the application for a special UAFR to defense-specific critical infrastructure owner-operators, such as those

outlined in 16 U.S.C. § 824o-1 and DoDD 3020.45, along with the recommendation of a designated national security agency (DHS, DOD, DOE, and DOJ).

Conclusion

The FAA cannot eliminate the threat posed by malicious drones, but it can make it easier to identify potentially dangerous activity by reducing legitimate and accidental overflights of sensitive facilities. The agency should revise its proposal to place fewer burdens on critical infrastructure owners and operators while providing stronger, more predictable safeguards for facilities essential to U.S. national security, economic resilience, and public health and safety.

Thank you for considering our comments. We look forward to seeing how our input is incorporated into the FAA's final rule.