October 6, 2025

Federal Aviation Administration
U.S. Department of Transportation (DOT)
1200 New Jersey Avenue SE
Room W12-140, West Building Ground Floor
Washington, DC 20590-0001

Attention: Docket ID No. FAA-2025-1908
Submitted to the Federal eRulemaking Portal (www.regulations.gov)

Re: ***Normalizing Unmanned Aircraft Systems Beyond Visual Line of Sight Operations (FAA-2025-1908)***

To Whom It Concerns:

The Alliance for Chemical Distribution ("ACD"), the American Chemistry Council ("ACC"), American Fuel & Petrochemical Manufacturers ("AFPM"), the American Gas Association ("AGA"), the American Public Gas Association ("APGA"), the American Petroleum Institute ("API"), the GPA Midstream Association ("GPA Midstream"), and the Interstate Natural Gas Association of America ("INGAA") (collectively, "the Associations") appreciate the opportunity to submit comments on the proposed rule entitled "Normalizing Unmanned Aircraft Systems Beyond Visual Line of Sight Operations" [1]("Proposed Rule" or "Proposal"). We applaud the U.S. Federal Aviation Administration ("FAA") for swiftly publishing this comprehensive regulatory framework in advancing commercial beyond visual-line-of-sight ("BVLOS") operations under the newly proposed Parts 108 and 146 of Title 14 of the Code of Federal Regulations ("CFR"). In the comments below, the Associations will offer suggestions and recommendations to improve critical infrastructure security and operations.

The Associations represent diverse segments of the energy and chemical industries[2] and, within the scope of the BVLOS Aviation Rulemaking Committee ("ARC"), we are recognized as

---

[1] 90 Fed. Reg. 54732 (Aug. 7, 2025)
[2] For additional information on the listed trades, please visit their respective websites below:
ACD - www.acd-chem.com
ACC - www.americanchemistry.com
AFPM - www.afpm.org
AGA - www.aga.org
APGA – www.apga.org

critical infrastructure as defined in 42 U.S.C. § 5195c[3]. As critical infrastructure, our members utilized unmanned aircraft systems ("UAS") since they were commercially available. UAS provide our facilities and infrastructure with countless safety and inspection uses that limit human exposure to potentially hazardous environments and grant operators substantial cost savings. Additionally, our facilities enhance fenceline security through the use of UAS surveillance, identifying threats like vandalism, theft, and trespassing, and to secure access points by ensuring only authorized personnel are on site.

FAA's BVLOS regulatory framework would not only enhance these existing operations but also expand the possibilities for the safe deployment of advanced UAS operations at our sites. To that end, the Associations are well positioned to comment on this proposed rulemaking and support an expeditious finalization of the rule.

BACKGROUND

1. Executive Summary

Our members represent industries with facilities and infrastructure that are essential to U.S. national and economic security, and which stand to benefit significantly from safe, predictable, and scalable BVLOS operations. The Associations appreciate the FAA's efforts to establish a comprehensive regulatory framework and movement away from ad hoc waivers and exemptions toward a consistent, performance-based framework that recognizes permits as flexible pathways, formalizes Automated Data Service Providers ("ADSPs"), and requires cybersecurity programs and security threat assessments for operators. These elements will allow for wider adoption of UAS while maintaining high standards of safety and security.

At the same time, the proposed rule must go further to account for the unique risks and needs of critical infrastructure. Specifically, the Associations urge the FAA to:

- **Protect critical facilities explicitly:** The FAA should expand "shielded areas" and establish a clear, partitionable Part 74 flight restriction process so that chemical plants, refineries, pipelines, and other high-risk fixed-site facilities receive the protections envisioned by Congress. The FAA should publish the long-awaited Section 2209 proposed rule to implement an application process for critical infrastructure to receive restricted airspace designation against unauthorized UAS.

API - www.api.org
GPA Midstream - www.gpamidstream.org
INGAA – www.ingaa.org

[3] In 42 U.S.C. § 5195c, critical Infrastructure is defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

- **Ensure operational security:** Refine data reporting requirements so that they preserve situational awareness for airspace users without exposing sensitive site locations.
- **Clarify accountability:** Define liability and governance frameworks for ADSPs, and ensure robust standards for cybersecurity, data integrity, and coordination with operators and law enforcement.
- **Avoid duplicative and excessive reporting burdens:** Recognize existing the Department of Homeland Security ("DHS") vetting programs (*e.g.,* Transportation Worker Identification Card ("TWIC"), HazMat Endorsement) and calibrate reporting and recordkeeping requirements to protect confidential business information and ensure proportionality for operators.
- **Ensure the final rule allows for flexibility:** Any new rule should allow for the breadth of operations that are currently allowed under the waivers and exemptions that have been granted and not be overly prescriptive to limit what operators are already proving in practice.

In short, the Associations welcome the FAA's commitment to enabling safe BVLOS operations, but emphasize that security, infrastructure protection, and operational clarity must advance in parallel. This is especially critical as our industries operate facilities that are vital to U.S. energy, manufacturing, and supply chains—and that must be safeguarded as BVLOS operations scale.

By incorporating these refinements, the FAA can achieve its goal of expanding BVLOS operations while ensuring that the regulatory framework enhances—not undermines—the resilience and security of the nation's critical infrastructure.

2. Overview of BVLOS History and Our Coalition's Involvement

BVLOS operations have been under consideration by the FAA for more than a decade. Initially, BVLOS flights were generally allowed only through restrictive waivers under 14 CFR §107.31 as well as exemptions under Part 91 and Section 44807 for more advanced or legacy UAS operations. Recognizing the need to expand safe and routine BVLOS operations, the FAA launched the UAS Integration Pilot Program ("IPP") in 2017, which ran through 2020, and tested complex operations like BVLOS with state, local, and industry partners.

Building on the IPP, the FAA created the BEYOND program on October 26, 2020, to focus on developing performance-based standards and scalable use cases for BVLOS. In 2021, the FAA's BVLOS ARC was convened, delivering its final report on March 10, 2022, which recommended establishing an acceptable level of risk and regulatory pathways for routine BVLOS operations.

The FAA issued the BVLOS NPRM ("Normalizing UAS BVLOS Operations") on August 7, 2025 (Docket FAA-2025-1908). The NPRM outlines new Part 108 permitting, detect-and-avoid and separation requirements, and critical infrastructure protections.

The Associations have been actively engaged throughout this process. We have collaborated to:

- Participate in the BVLOS ARC to ensure critical infrastructure operations were represented in the considerations of a forthcoming rulemaking.
- Provide feedback on the FAA BVLOS proposals and ARC recommendations, highlighting the importance of ensuring airspace protections for hazardous materials sites and critical energy infrastructure.
- Engage with the FAA, DHS, and CISA to ensure BVLOS policy reflects operational realities and risk management needs for facilities that are both high-value targets and vital to national resilience.
- Submit joint letters to Congress and the Administration emphasizing the urgent need for Section 2209[4] implementation, which would affect flight paths in regards to BVLOS operations.

COMMENTS

1. **Support for BVLOS objectives**
    a. **Scalability & Performance-Based Framework**

    Reference §108.120 General Operating Rules, §108.170 Preflight Requirements; pp. 38233, 38235

The current exemption and waiver process available to operators is burdensome, but it allows greater flexibility than proposed in this rulemaking. Our main concerns with the proposed rule are the overly prescriptive requirements for flight plans. As proposed, the proposal limits control of the UA ("Unmanned Aircraft") to only the pre-designed flight plan. That means operators do not have the ability to use circle back to more closely inspect an asset by using a joystick to control the UA. Under this proposal, that type of maneuver would require an entirely new flight plan.

The FAA should amend the framework to provide more flexibility to the operator during the flight. "UAS-based collection and analytics can inspect more energy production, transmission, and

[4] Section 2209 of the FAA Extension, Safety, and Security Act of 2016 (Pub. L. 114–190) directs the FAA to establish a process for federal, state, or private entities to petition for airspace restrictions over fixed-site critical infrastructure. This includes facilities such as oil refineries, chemical plants, energy production sites and others labeled 'critical infrastructure'. Once approved, these areas are designated as flight restricted areas, prohibiting unauthorized UAS operations.

storage infrastructure per day compared to a manual, ground-based inspection, which significantly increases the opportunity to detect and remedy leaks and other issues."[5] The detection portion will often require closer inspection, which could be accomplished in real time, if the FAA allows some amount of manual control during an approved flight. The need to resubmit flight plans for approval every time an operator needs to make a change or slightly change a flight path may constrain the scalability of this rulemaking. The Associations are concerned that an overly prescriptive approach may hinder the broad adoption of BVLOS operations, undermining the intent of the rule itself. We recommend that the final rule require a filed flight plan to identify any critical infrastructure locations within that flight plan that will be contacted prior to the flight to inform them of the UA use.

Furthermore, the proposed rule specifies two paths for FAA granting Part 108 operations: permits and operating certificates. Under both paths, FAA proposes that "civic interest" may be deemed an appropriate use for BLVOS operations. While the Associations appreciate this protection for civil liberties, the term "civic interest" is vague and could be used as a justification for adversarial drone use that could result in significant harm to critical infrastructure. FAA should narrow the civic interest category to explicitly disapprove of BLVOS uses that may endanger the public, national or economic security, and that interfere with critical infrastructure operations.

b. **Focus on Critical Infrastructure Objectives**

Reference §108.205 Operations in Shielded Areas; p. 38247

America's energy and chemical infrastructure is the backbone of the economy and crucial to the national security. It is the responsibility of every operator to protect their assets, the environment, their workers, and the communities in which they operate. UA operations are one tool in the toolbox that operators can utilize to ensure safety and reliability and expanded BVLOS operations that support that mission. The Associations applaud the FAA for acknowledging that UA can support critical infrastructure across the country. The Associations also appreciate the restrictions proposed for operating over certain critical infrastructure. As noted, the infrastructure buffer supports numerous operations, including pipelines, railways, and other potential infrastructure inspection. It is crucial to strike a balance between allowing an adequate distance away from infrastructure for the safety of the UA and general camera and imaging equipment capabilities, with an appropriate safety margin from manned aircraft operations. The FAA should engage with stakeholders to ensure the final rule reflects the operational realities of critical infrastructure sectors.

2. Operational Suggestions

a. **Shielded Areas**

[5] *Normalizing Unmanned Aircraft Systems Beyond Visual Line of Sight Operations*, 90 Fed. Reg. 38212, 38222 (Aug. 7, 2025) (to be codified at 14 C.F.R. pts. 91, 107, 135).

Reference §108.205 Operation in Shielded Areas, §108.175 Operating Restrictions; pp. 38237, 38247

Proposed § 108.205 grants UA the right-of-way while conducting operations within 50 feet of certain infrastructure labeled "shielded areas". Shielded areas are defined as "power lines and substations, railroads, bridges, and pipelines, when permission from the facility or infrastructure owner is obtained."

The Associations support this provision as it allows our inspection flights to be conducted with the precision and ease required when monitoring sensitive infrastructure. Additionally, we support the requirement to obtain approval from critical infrastructure owners/operators before labeling an airspace "shielded." Critical infrastructure owners/operators are best position to understand the airspace operation requirements for their equipment. If there are locations that require use of manned aircraft (*e.g.*, close-up fixed-wing or helicopter inspection) then those pilots already have specialized procedures and knowledge to deconflict those areas from UA. The FAA should formalize the procedure for requesting a "shielded area" designation, clarify who may grant permission on behalf of critical infrastructure owners the duration of the designation, and the process of renewal.

While we support maintaining a right-of-way ("ROW") buffer around critical midstream infrastructure, the rule lacks clarity on how that radius is measured. Given the variability in pipeline configurations, such as lateral lines, valve sites, and compressor stations, it's unclear where the right-of-way begins and ends along different segments of the asset. The rule also does not explicitly clarify whether this includes buried pipelines or only above-ground, visible pipelines. It is assumed that the proposed 50 feet reflects the horizonal distance from the pipeline centerline or from any surface marker. The final rule should specify whether underground linear infrastructure is included and from where and how the 50 feet is taken so they can be integrated into aviation operations.

The FAA's proposal for a 100-foot lateral shielded corridor does not align with current 30-meter requirements on either side of the pipeline for pipeline ROW inspections. The final rule should extend the lateral shielded corridor to at least 100 feet on either side of the infrastructure, to align with the BVLOS ARC recommendation, or provide a waiver or deviation mechanism for pipeline operators who can demonstrate that wider shielded corridors are necessary to meet pipeline inspection requirements. Consultations from pipeline experts would be beneficial here with examples of shielded areas around such critical infrastructure.

Another uncertainty around these operations is the vertical dimensions and altitude limit of this specialized airspace in combination with the above ground level ("AGL") requirement. Under § 108.175(a)(2), the FAA proposes that operators may fly above 400 feet AGL if the UA remains within a 400-foot horizontal radius of a structure and does not exceed 400 feet above the structure's highest point. However, this is not specified in the shielded area permissions under

§ 108.205. We request the FAA clarify where flights under shielded areas fit into the 400 feet AGL requirement.

Lastly, the FAA notes on page 38237 that while they identified specific infrastructure types, such as power lines, substations, railroads, bridges, and pipelines, as qualifying for shielded area operations under § 108.205, the Agency acknowledges that additional structures may warrant inclusion and is soliciting public comment on expanding the list. We request that shielded areas are expanded to not only linear infrastructure, but fixed-site facilities as well (*e.g.,* refineries, chemical plants, and similar energy facilities). This would be consistent with ARC's final report, which defines shielded areas (which would include fixed-site facilities within the same industry) as critical infrastructure under 42 U.S.C. § 5195c. This change is necessary because UAS teams conduct inspections not only over pipelines, but around fixed-site facility equipment and fencelines. Limiting the precision and ease of piloting in shielded areas to only linear equipment severely reduces the applicability of this provision for our UAS operations. For example, there are situations where we utilize "drone-in-a-box" technology to remotely inspect or survey our facilities, and the FAA's narrow definition does not consider the vast UAS BVLOS benefits here. Therefore, the FAA include such infrastructure in their definition of shielded areas and increase the shielded area to 200 feet for fixed site facilities, as is standard for part 107 waivers.

b. **Broader Benefits, Not Just Below 400 ft. AGL**

Reference § 108.195 Operations Near Aircraft: Low Altitude Right-of-Way Rules; pp. 38244

While the NPRM primarily addresses mixed operations at ≤400 ft AGL, portable Electronic Conspicuity ("EC") materially benefits other airspace users across the national airspace system ("NAS"). EC that is tuned for air-to-air visibility (not Air Traffic Control ("ATC") surveillance) gives all crewed and uncrewed participants a common, low-friction way to be seen by modern Automatic Dependent Surveillance-Broadcast ("ADS-B") IN displays and UAS DAA receivers without imposing electrical, weight, or certification burdens on legacy fleets. These include Part 103 ultralight vehicles, lighter than air balloons, gliders, and vintage aircraft without electrical systems exempted from the ADS-B mandate.

Enabling and encouraging voluntary, portable EC beyond the sub-400 ft context builds a broader "cooperative bubble" around vulnerable, lightly equipped aircraft, improves UAS-to-manned mutual awareness, and does so with minimal cost, weight, or installation complexity. These benefits accrue across seasons, events, and altitudes wherever mixed operations occur without converting EC into an ATC separation service or imposing equipage requirements[6] on users for whom those burdens are impractical.

c. **License Requirements**

[6] 14 CFR § 91.225/§91.227.

Reference §108.315 Personnel Knowledge & Training; Subpart C; pp. 38256

The Associations appreciate that Part 107 and Part 108 are complementary, yet separate regulatory pathways for different types of drone operations. As Part 108 is designed for more advanced, higher-risk drone operations, it is understandable that FAA is requiring specific training requirements to cover the advanced areas beyond Part 107's scope. As the skills developed under the Part 107 licensing requirements, including flight planning, airspace awareness, and aeronautical decision-making, remain valuable for Part 108 licensing requirements, it is unclear in the proposal whether FAA intends to require Part 107 certification as a prerequisite for Part 108 roles. The Associations request that FAA clarify this requirement and address whether a Part 107 certificate fulfills any "general aeronautical knowledge" component of Part 108 training requirements.

d. **Take-Off Operations Near Facilities and Populations**

Reference §108.165 Areas of Operations, §108.910 Noise; pp. 38311

The Associations agree that operators must address physical security and prevent unauthorized access to the operation's pre-designated facilities, including controlled access areas. This is intended to be performance-based for flexibility due to the size, scope, and complexities of different operations. However, clarification is needed on stand-off distances for the safety and security of all operation personnel. The current proposed rule does not specify a standard minimum separation distance between personnel and UAS take-off and landing areas, likely due to the broad range of aircraft type and concept of operations. The Associations support these performance-based standards, but request that safety information (*i.e.,* suggested stand-off distances) be made available through an original equipment manufacturer ("OEM") recommendation that can then be documented in the OEM manual as part of the Means of Compliance process.

Next, the Associations recognize and agree with the FAA that noise and environmental considerations are important. However, these need to be flexible as BVLOS operation locations will greatly vary, and each location should be given site-specific considerations. For example, pipeline inspections occur mainly in remote or rural areas with few people or noise-sensitive sites; we believe most operations will inherently have minimal noise impact. The FAA should consider flexibility for remote-area operations. Heavier UAS that might produce more noise could still be acceptable in rural locations where they pose little disturbance.

e. **ADSP Accountability**

Reference Part 146 (esp. Subparts D & E), §108.190 Strategic Deconfliction, § 108.195 Operations Near Aircraft: Low Altitude Right-of-Way Rules, §108.725 Data Reporting, ; pp. 38242, 38244, 38299

The Associations strongly support the FAA's proposal to establish a certification framework for Automated Data Service Providers ("ADSPs") under new Part 146. Formalizing ADSP roles is a critical step in ensuring that core functions—such as strategic deconfliction, conformance monitoring, and flight coordination—are delivered in a consistent, reliable, and auditable manner across the BVLOS ecosystem. Recognizing ADSPs as certificated entities will build trust in their services, encourage investment in advanced capabilities, and enable scalability of BVLOS operations beyond today's waiver-based system.

At the same time, the framework must provide clarity on accountability and risk allocation. If an operator relies on an ADSP for conflict management or conformance monitoring, failures in those services could have direct safety and security consequences. The rule should therefore:

- Define a shared-risk model that delineates responsibility between operators and ADSPs, ensuring operators are not left with sole liability for failures beyond their control.
- Require minimum reliability and performance metrics, with audit trails and data retention requirements that allow the FAA and law enforcement to investigate incidents.
- Establish clear expectations for incident reporting by ADSPs, including timely notification to affected operators and appropriate coordination with FAA, TSA, and local law enforcement.
- Mandate baseline cybersecurity and data privacy safeguards, given that ADSPs will handle sensitive operational data, including flight paths near critical infrastructure.
- Clarify how confidential business information will be protected, especially where ADSP services involve aggregation of data across multiple operators or facilities.

By strengthening accountability and governance around ADSP operations, the FAA can ensure these services become reliable enablers of BVLOS, while protecting operators, communities, and critical infrastructure from unintended risk. The Associations stand ready to work with FAA and industry partners to help shape standards that balance innovation, safety, and security in this critical domain.

The Associations support a broader requirement of ADSB-IN integration. Requiring ADS-B IN on all Part 108 UAS creates a common cooperative baseline that enables timely detection of crewed aircraft that already broadcast through installed avionics and the proposed EC devices and clarifies yielding behavior under §108.195. ADS-B IN for drones is readily available via multiple pathways: integrated receivers or modular add-ons for the UA, standalone AE receivers, and managed network reception. This diversity allows operators to meet the rule without redesigning aircraft or incurring prohibitive costs. Unlike the retroactive equipage mandate for crewed aircraft for ADS-B Out systems. The FAA can require forward fit of this core technology for these new entrants. Through this requirement, the FAA indirectly encourages broader ADS-B Out adoption among crewed aircraft improving overall NAS safety.

The Associations strongly support the FAA's proposal for the usage of EC devices to enable low altitude right of way and tactical deconfliction. It is critical for the FAA, industry, and pilots recognize that EC in this context is for air-to-air conspicuity and tactical deconfliction, not ATC separation services—and it allows general aviation operators to participate immediately in the low altitude right-of-way construct, accelerating safety gains without new mandates.

f. **Recordkeeping & Reporting**

Reference §108.40 Recordkeeping, §108.45 Reporting; pp. 38227, 38229

The FAA proposes a comprehensive set of recordkeeping and reporting requirements under sections 14 CFR § 108.40 and § 108.45 for Part 108 operators. The Associations recognize the importance of FAA maintaining detailed data to ensure the safe and secure oversight of BVLOS operations; however, the extensive recordkeeping and reporting requirements may impose a significant burden on UAS teams already managing substantial operational responsibilities. Any sort of streamlined or standardized formats that reduce the labor hours for submission to the FAA would greatly improve the efficiency and utility of this section, for both commercial stakeholders and the FAA compliance professionals. The Associations request the FAA to recognize this recordkeeping and reporting burden and preemptively minimize that effect. The FAA should clarify that all reporting pertains only to systems involved in UAS operations.

Furthermore, there are concerns about the confidentiality of the required information to be reported to the FAA. The security of the sensitive information that is submitted to FAA through BVLOS operations is of the utmost importance to our members' operations. The examples below highlight key reporting concerns:

- Loss of control due to unauthorized access (careless or malicious)
- Unauthorized access to operator facilities (*e.g.*, UAS loading areas, hazardous material storage, goods prep zones)
- Unauthorized access to networks, devices, or data regardless of operational impact
- Date and time of the incident
- Nature and scope of the breach
- Identified vulnerabilities
- Corrective actions taken

The Associations understand the importance of the information the FAA is looking to receive, but such information must be considered confidential business information ("CBI"). CBI already falls under established procedures to protect sensitive and proprietary business information submitted by regulated entities in the FAA's 14 CFR § 413.9, where entities may request that trade secrets or proprietary commercial or financial data be treated as confidential. The Associations strongly encourage the FAA to treat the above information as confidential.

3. Security Suggestions

a. **General Security and Cyber**

Reference §108.150(c), §108.435, §108.535, §108.875, §108.45(c), 49 CFR 1544.101(g); NPRM TSA sections; pp. 38229, 38234, 38270, 38280, 38309,

The Associations have been involved in security policy and regulatory development on a variety of issues, including cybersecurity, physical security, and regulatory implementation to physical security of sites through TSA, CISA, and USCG. The Associations have a long history of collaborating with DHS, TSA, and USCG, and we look forward to working with the FAA on drone security issues. There are three main security issues concerning the use of drones beyond the visual line of sight: unauthorized access, security assessments of operators, and cybersecurity.

The Associations agree with TSA that unauthorized access to operations (§ 108.150(c)) must be prevented. Our operators support a performance-based approach to allow for flexibility in the application of preventing unauthorized access, as each operating facility and controlled access area may be different, from a taped off perimeter to high fences. Currently, our members use a variety of methods to create controlled access areas depending on where a UA may be operating in or around a site or critical assets. However, we encourage the FAA to allow flexibility in applying this section to emergency landing areas.

The Associations recognize and agree that the FAA is concerned that BVLOS operations are at risk for cybersecurity attacks by malicious actors to gain access to various systems and services, and interfere with remote control, communication, and other functions. To address this concern, the FAA is requiring operators to develop and implement cybersecurity policies to protect from unauthorized access, similar to CISA's "secure by design" principles from § 108.435, 108.535, and 108.875. However, the Associations recommend that the FAA explicitly clarify that the required cybersecurity protections be applied only to systems relevant to UAS operations.

Under § 108.45(e) operators must report to the FAA any security breach where an operator loses control of UAS, and/or where there is unauthorized access to an operator's BVLOS facilities, any unauthorized access to networks, data, or devices, regardless of the impact on UAS operations, within 96 hours. The Associations agree with the reporting of security-related incidents and support a 96-hour reporting timeframe of a security breach.

Nonetheless, this reporting obligation should be limited to the scope of systems used for UAS operations rather than a blanket requirement for all network systems, devices, and data within a company. The preamble states "an operator would need to report unauthorized access to the operator's networks, devices, or data, *regardless of its impact on UAS operations' integrity, accuracy, or reliability."* The inclusion would trigger burdensome company-wide policies for reporting all cyber breaches to the FAA, regardless of whether the systems are connected to BVLOS operations. This broad scope risks conflating enterprise IT incidents, such as breaches of unrelated HR or finance systems, with those that genuinely impact aviation safety or UAS

command and control. Such overreporting could dilute the FAA's focus on critical security threats, overwhelm operators with compliance obligations, and divert resources from actual risk mitigation. The proposal does not mention of multinational companies either, which maintain networks that span internationally and open the possibility of mandating reporting non-U.S. based events. The FAA should clarify this reporting obligation is limited to those sights within the U.S.

Additionally, non-UAS reporting is duplicative of existing cyber reporting requirements such as TSA's Security Directives, USCG's Maritime Transportation Security Act, and the upcoming Cyber Incident Reporting for Critical Infrastructure Act of 2022 rule. This duplication results in overreporting, and potential contradictory reporting, leading to significant burdens and creating little to no value for the FAA overall.

The FAA is proposing that operators contact TSA and obtain a limited security program equivalent to 49 CFR 1544.101(g) before package delivery operations. Also, the FAA is proposing expanding the security program to: control cargo, prevent unauthorized access, designate a security coordinator at the corporate level, conduct security inspections of each aircraft before operation, and train individuals on security duties. The FAA recognizes that security programs should be based on risk profiles of the UAS operations (many of which may be at industrial sites, crowded areas, or remote pipeline locations), size, use, capabilities, payloads, and ranges of the UAS. The Associations consider these security program categories legitimate for consideration, as use cases truly need to be based on risk profile, and the FAA recognizes that the risk is different over a critical infrastructure site compared to delivering food to a residence.

b. **TSA Security Threat Assessment ("STA") Background Checks**

Reference §108.335; pp. 38262

The Associations have a long history of complying with security agency background checks, including TSA's TWIC, the prior CISA Chemical Facilities Antiterrorism Standard ("CFATS") Personnel Surety Program, ("PSP"), and the Department of Transportation ("DOT") HazMat background checks. However, all of these are tied to facilities that transport hazardous materials, which can be very different scenarios for BVLOS operations. Operators could be delivering pizza, spare parts, or medical supplies in a wide variety of locations.

Background security checks for drone operators should be risk-based, considering the location of operations and the type of material being delivered. The risk profile of a delivery site must be a consideration as well, for example, a critical refinery versus a remote pipeline station. The Associations urge the FAA to work with the security agencies and develop a flexible risk-based security background check program.

The Associations also recommend that the FAA recognize the use of other agency background checks by drone operators, such as the TSA TWIC, TSA Pre✓, Global Clearance, Part

107 sUAS, or other existing frameworks. These security background checks should be sufficient for drone operators, both commercially and among drone teams the Associations' membership.

c. **BVLOS Flights and Part 74 locations (Section 2209)**

Reference §108.205, §108.220, Executive Summary / TSA Authority; pp. 38247, 38250

BVLOS flights should only be allowed over 14 CFR §108.220 flight restricted and Section 2209 implementation locations with the express allowance of these owner/operators. The Associations urge the FAA to maintain BVLOS flight restrictions over 2209-qualified areas without the consent of the facility owners. Allowing BVLOS flights to essentially trespass across 14 CFR §108.220 flight restricted facilities will only cause confusion, increase risks to both sites and the UAS, and create opposition to the BVLOS program. The Associations urge the FAA not to allow these overflights at this stage of the BVLOS program.

While the potential benefits of BVLOS operations are well known, the widespread use of UAS introduces significant risks. With diffuse assets essential to national security, the economy, and public safety, critical infrastructure owners and operators are especially vulnerable to malicious UAS use. Critical infrastructure is frequently cited as potential targets for domestic violent extremists. For example, on September 9, a Nashville man plead guilty to attempting to bomb an electrical substation using a UA.[7] Without a process for restricting UAS flights above critical facilities, bad actors have free rein in the air above the nation's most valuable infrastructure.

Due to the absence of restricted airspace and the federal concentration of mitigation technologies, malicious actors can use UAS to enter the airspace directly above or adjacent to critical infrastructure assets uncontested. UAS may then provide reconnaissance in preparation for vandalism, sabotage, and theft or even conduct a kinetic attack. As shared in a recent Environmental Protection Agency National Security Information Sharing Bulletin, UAS equipped with high resolution cameras can gather sensitive security information regarding facility layouts, security perimeters, guard schedules, and access points. [8] Adversaries having significant insight into operations and vulnerabilities enhances the likelihood of successful and damaging crimes.

The growing popularity and risks of UAS usage emphasize the pressing need for a rulemaking enacting Section 2209 of the FAA Extension, Safety, and Security Act of 2016.[9] To mitigate the dangers of UAS misuse, critical infrastructure owners require a clear petitions

[7] Associated Press, Man Pleads Guilty to Planning a Drone Attack on a Nashville Electricity Substation, AP News,[September 9, 2025], Man pleads guilty to planning a drone attack on a Nashville electricity substation | AP News.
[8] U.S. Envtl. Prot. Agency & Water Info. Sharing & Analysis Ctr., A Quarterly National Security Information-Sharing Bulletin (Aug. 13, 2025).
[9] FAA Extension, Safety, and Security Act of 2016, Pub. L. No. 114-190, 130 Stat. 615 (2016).

process, with straightforward approval criteria, to establish a restricted or prohibited area over eligible assets. [10] Owners and operators should receive clear instructions for designating the boundaries of the proposed UAS-restricted airspace and navigating the FAA's process for evaluating and approving petitions. A straightforward process enhances national resilience by promoting successful petitions and expedience in the face of an emerging threat. We are aware the rulemaking is currently at the Office of Budget and Management and request that the FAA provide a fast and clear provision-based process to provide critical insight before finalizing this rule.

d. **Bilateral Airworthiness/Aviation Safety Agreements**

Reference §108.700(b)(1); pp. 38295

As proposed, the rule would require eligibility standards for drone airworthiness acceptance. All drone manufacturers would be required to meet the eligibility requirements prior to submitting a Declaration of Compliance ("DOC"). Proposed 14 CFR §108.700(b)(1) states that: "for the manufacturer to be eligible to apply for a UAS airworthiness acceptance, the UAS must be manufactured in the U.S., or be manufactured in a country with a Bilateral Airworthiness Agreement addressing UAS or a Bilateral Aviation Safety Agreement with associated Implementation Procedures for Airworthiness addressing UAS; or an equivalent airworthiness agreement." The Associations appreciate that the FAA is seeking to ensure that all drones operated in the homeland are both safely manufactured and secure from adversarial influence.

To that end, the FAA seeks public comment on whether there should be any particular manufacturing restrictions on foreign manufacturers intending to manufacture UAS under this rule, such as manufacturing outsourced by a foreign manufacturer to a U.S. manufacturer or a U.S. manufacturer's production of a UAS using foreign designs or parts from a covered country. The FAA is also asking for comments on whether there should be any particular restrictions on the operation of foreign-manufactured UAS by private entities beyond those already provided in law.

The Associations agree that the national security concerns associated with certain foreign drone manufacturers are paramount to safely extending advanced operations in the homeland. It is our position that the U.S. defense and intelligence communities are best positioned to define particular manufacturing restrictions from non-U.S. entities given their highly developed visibility into the supply chain. However, given the very limited domestic drone manufacturing, the Associations encourage the FAA to either/or: clarify and make publicly available the list of eligible foreign manufacturers or provide specific exemptions to this provision based on a defined set of qualifications (*e.g.*, based on certain need, with express security controls in place, etc.); and, provide further details about the process to acquire Bilateral Airworthiness Agreements such that operators can work with drone manufacturers to submit a DOC.

CONCLUSION

[10] 14 C.F.R §73 (2024).

In conclusion, the Associations strongly support the FAA's efforts to establish a comprehensive framework for BVLOS operations under Part 108. Throughout our comments, three key issues are addressed:

1. **Balancing Safety and Flexibility**
   While the proposed rule offers a necessary shift away from waivers toward a scalable, risk-based framework, operators require greater in-flight flexibility. Prescriptive limits on manual control, ECs, reporting burdens, and unclear licensing requirements risk constraining innovation and efficiency. The FAA should ensure that the rule empowers operators to adapt in real time, without undermining safety.
2. **Protecting Critical Infrastructure**
   UAS offer immense value in safeguarding and monitoring energy, chemical, and transportation assets that are vital to national security. To maximize these benefits, the rule must explicitly strengthen protections for both linear and fixed-site facilities, clarify shielded area definitions, and expedite long-delayed Section 2209 processes. A secure BVLOS framework must also respect the operational realities of critical infrastructure sectors.
3. **Ensuring Accountability and Security**
   As the FAA formalizes the role of ADSPs and mandates cybersecurity programs, it is essential to clarify accountability, protect sensitive business information, and avoid duplicative reporting. A balanced governance model, risk-based background checks, and proportionate security measures will ensure that innovation advances alongside robust safety and national security protections.

By addressing these key themes, the FAA can finalize a BVLOS rule that strengthens U.S. resilience, enables innovation, and ensures that advanced UAS operations serve the public interest without compromising security. The Associations look forward to continuing collaboration with the Agency to refine and implement this critical framework.

Respectfully submitted,

Alliance for Chemical Distribution
American Chemistry Council
American Fuel and Petrochemical Manufacturers
American Gas Association
American Public Gas Association
American Petroleum Institute
GPA Midstream Association
Interstate Natural Gas Association of America