AMERICAN ASSOCIATION OF PORT AUTHORITIES

June 29, 2026

Docket Operations
U.S. Department of Transportation
1200 New Jersey Avenue, S.E., Room W58-213
Washington, D.C. 20590-0001

Desk Officer for Federal Aviation Administration
Office of Management and Budget
Office of Information and Regulatory Affairs
New Executive Office Building
725 17th Street, N.W.,
Room 10202
Washington, D.C. 20053

Re: Comments on Docket No. FAA-2026-4558; Notice No. 26-03 – Designation – Restrict the Operation of Unmanned Aircraft in Close Proximity to a Fixed Site Facility

Dear Federal Aviation Administration (FAA) Office of Rulemaking,

The American Association of Port Authorities (AAPA) appreciates the opportunity to comment on the FAA's Notice of Proposed Rulemaking (NPRM) concerning the designation of unmanned aircraft flight restrictions (UAFRs) around eligible fixed site facilities. AAPA represents public port authorities throughout the United States, including many of the nation's largest strategic seaports and critical infrastructure hubs.

AAPA applauds the FAA's efforts to implement Section 2209 of the FAA Extension, Safety, and Security Act of 2016. Establishing a process for eligible facilities to seek drone flight restrictions is a meaningful step toward addressing the growing threat posed by unauthorized unmanned aircraft systems (UAS) operating over critical infrastructure.

America's ports increasingly face drone-related vulnerabilities and operational disruptions. Ports routinely handle hazardous materials, military cargo, cruise passengers, energy products, chemical shipments, and essential consumer goods that are vital to national economic and homeland security. Unauthorized drone activity in the vicinity of any of these facilities raises safety, surveillance, and operational concerns. Moreover, the threat posed by attack drones is particularly acute in the cruise sector, where a single vessel may carry several thousand passengers and crew. A successful attack against a large passenger vessel could result in catastrophic loss of life on a scale rivaling the casualties inflicted during previous terrorist attacks, underscoring the urgent need for stronger protections for America's seaports and maritime gateways.

Strategic seaports are increasingly recognized as high value targets for foreign intelligence collection, cyber-enabled surveillance, and disruptive activities involving UAS. Operational disruptions at major ports can rapidly cascade throughout national and regional supply chains,

affecting fuel distribution, agricultural exports, manufacturing inputs, military readiness, and consumer goods availability. Many ports also support Department of War and Department of Transportation strategic sealift and military outload operations, further elevating their importance to national security.

Because of these unique operational and national security responsibilities, ports warrant special consideration within the FAA's implementation of Section 2209. The consequences of unauthorized drone activity at a port may extend far beyond the immediate facility and impact broader economic resilience, defense readiness, and homeland security objectives.

Given the sensitivity of their operations and proximity to large population centers, ports represent some of the most mature and security-conscious critical infrastructure operators in the nation. Accordingly, many port facilities are regulated under the Maritime Transportation Security Act of 2002 (MTSA), maintain approved Facility Security Plans (FSPs), comply with Maritime Security (MARSEC) requirements, and coordinate closely with the U.S. Coast Guard (USCG) and federal law enforcement agencies.

AAPA strongly supports FAA's recognition that fixed site facilities regulated under MTSA explicitly qualify for UAFRs. We also appreciate the FAA's acknowledgment that unmanned aircraft may pose risks associated with surveillance, cyber intrusion, operational disruption, and physical attacks against critical infrastructure.

AAPA respectfully offers the following recommendations and concerns regarding the proposed rule:

Streamline Eligibility for Maritime Transportation Facilities: AAPA strongly encourages FAA to establish an expedited or presumptive approval pathway for maritime facilities already regulated under MTSA and operating under an active USCG-approved FSP or Alternate Security Plan.

The NPRM appropriately recognizes that maritime transportation facilities regulated under MTSA are eligible to request a UAFR. These facilities already undergo extensive federal security oversight and maintain layered physical and cybersecurity protections. Ports should not be required to duplicate extensive security demonstrations already validated through USCG processes. Further, MTSA-regulated facilities already satisfy many of the security and vulnerability assessment requirements contemplated by the NPRM. FSPs, Facility Security Assessments, Alternate Security Programs, Area Maritime Security Committee participation, and ongoing USCG oversight provide a robust security framework that FAA should leverage wherever possible. Aligning UAFR eligibility with existing MTSA requirements would reduce administrative burden, eliminate duplicative federal review, and advance broader interagency efficiency objectives.

Accordingly, AAPA recommends that:

- MTSA-regulated facilities with approved FSPs automatically qualify to apply for a UAFR;

- The FAA establish a streamlined review process for strategic seaports and maritime critical infrastructure; and
- Existing USCG security documentation be accepted in lieu of duplicative FAA-specific submissions where practicable.

Recognize Port Authorities as Governing Critical Infrastructure Operators: The NPRM currently places substantial emphasis on individual site operators and property interests. However, many public port authorities are governmental entities with statutory authority over complex multi-tenant critical infrastructure environments.

Ports frequently contain multiple energy, cargo, and cruise terminals, chemical facilities, rail operations, and federally regulated maritime facilities operating within a unified security environment. Requiring each tenant individually to apply for separate UAFRs would create inefficiency, inconsistency, and unnecessary administrative burdens.

AAPA recommends that FAA:

- Explicitly recognize port authorities as eligible applicants to apply for UAFRs covering multiple facilities within port jurisdictional boundaries;
- Allow port authorities to coordinate UAFRs on behalf of tenants and operators; and
- Clarify that tenant objections or lack of participation should not prevent a port authority from applying for a UAFR covering publicly governed port property.

As governmental entities responsible for the safety and security of maritime infrastructure, port authorities should retain the ability to coordinate drone security measures across their jurisdiction if they choose.

Allow Flexibility Beyond Strict Property-Line Boundaries: AAPA is concerned that the proposed limitation restricting UAFR lateral boundaries strictly to property lines may create significant operational and security gaps for ports and industrial waterfront facilities. Maritime facilities are fundamentally different from many land-based critical infrastructure sites. Ports by definition include waterside operational areas, including ship berths, mooring dolphins, vessel loading zones, and navigation channels. These maritime assets operate as interconnected facilities with rail corridors and public roadways in a unified security environment. As a result, many ports contain noncontiguous parcels, with public roadways bisecting secure facilities, shared intermodal corridors, or waterside operational areas. Connected energy and chemical infrastructure can also be separated by easements or transportation corridors. Limiting UAFRs to upland property boundaries may leave many of the assets most in need of protection uncovered.

For MTSA-regulated facilities, FAA should consider allowing applicants to define UAFR boundaries consistent with the USCG-recognized security footprint reflected in approved FSPs and related security documentation. Such an approach would better reflect the operational realities of maritime facilities and ensure protection of waterside assets, vessel berths, and adjacent security zones that are integral to port operations.

In addition, modern UAS platforms equipped with advanced optical zoom, thermal imaging, and other surveillance capabilities may collect sensitive information while operating outside a facility's strict property lines. FAA should provide applicants flexibility to justify reasonable security buffer areas to address demonstrated surveillance vulnerabilities and operational risks.

AAPA encourages FAA to:

- Allow reasonable flexibility to extend UAFR boundaries beyond strict property lines when justified by operational security considerations;
- Permit interconnected maritime and industrial facilities to be treated as a unified security site where appropriate;
- Consider operational realities unique to ports and waterfront infrastructure such as flight restrictions over critical navigation channels; and
- Accept USCG-recognized security footprints reflected in approved FSPs.

Address Vertical Boundary Limitations and Aerial Surveillance Risks: AAPA encourages FAA to further evaluate whether the proposed vertical limitations adequately account for the unique characteristics of maritime facilities, existing FAA operational authorities, and the capabilities of modern UAS.

The NPRM generally limits UAFRs to 400 feet above ground level unless a facility contains structures exceeding 300 feet in height. While AAPA appreciates FAA's effort to align UAFR ceilings with existing small UAS operating limitations, this approach may not fully address the security risks facing maritime facilities.

Many port facilities contain ship-to-shore cranes, container handling equipment, refinery structures, loading arms, communications infrastructure, and other industrial assets that routinely exceed 150 to 250 feet in height. Under 14 CFR § 107.51(b), small UAS may operate up to 400 feet above a structure's immediate uppermost limit. As a result, a drone operating near a 250-foot ship-to-shore crane could potentially fly as high as 650 feet above ground level while remaining compliant with existing FAA regulations.

AAPA appreciates the exception proposed in 14 § 74.60(c), which would allow the FAA to raise a UAFR's altitude ceiling when a facility contains a structure exceeding 300 feet in height. However, many maritime facilities contain critical infrastructure below that threshold. Consequently, a port facility with a 250-foot ship-to-shore crane could face a circumstance where drones are authorized to operate substantially above the proposed UAFR ceiling while still maintaining the ability to observe terminal operations and other sensitive activities.

This issue is particularly significant because modern UAS platforms are increasingly capable of conducting detailed surveillance from substantial distances and altitudes. High-resolution cameras, advanced optical zoom capabilities, thermal imaging systems, wireless signal collection technologies, and other commercially available tools may allow operators to observe cargo operations, military vessel movements, security procedures, access control points, hazardous material handling activities, and other sensitive operational information without physically entering a facility's immediate perimeter.

Beyond traditional visual surveillance, UAS may also be capable of collecting information regarding security personnel assignments and patrol patterns, operational movements, facility vulnerabilities, and other indicators of security posture. Certain UAS platforms may also facilitate cyber-enabled reconnaissance activities, including the collection of wireless network information, signal interception, packet capture, or communications disruption attempts. In addition, thermal imaging capabilities may reveal heat signatures associated with critical infrastructure, refrigerated cargo, electrical substations, machinery, vessels, vehicles, or personnel activity, potentially allowing UAS operators to identify active versus dormant facilities, equipment, or operational areas. These concerns are particularly acute at Strategic Seaports and other facilities supporting military deployments, defense logistics, energy transportation, and critical supply chain operations, where collected information could have significant homeland security or national defense implications.

From a security perspective, the risk is not solely the drone's physical presence over a facility, but also its ability to collect intelligence regarding critical infrastructure operations. A drone operating above or adjacent to a facility may be capable of observing many of the same activities that would otherwise be protected by physical barriers, fencing, waterside security measures, and restricted access controls. In many cases, the intelligence collection value of a drone may persist even when the aircraft remains outside the proposed lateral or vertical boundaries of a UAFR.

Accordingly, AAPA recommends that FAA:

- Consider additional flexibility for facilities containing exceptionally tall industrial structures, including ship-to-shore cranes, refinery infrastructure, and other maritime assets;
- Allow applicants to demonstrate a need for expanded vertical protections based on facility-specific security risks and infrastructure characteristics;
- Evaluate whether existing altitude exceptions could create unintended surveillance opportunities that undermine the effectiveness of UAFRs; and
- Consider amending the altitude restriction proposed in 14 § 74.60 to be 400 feet above the tallest structure on the facility.

Improve Coordination and Processing Capacity: The NPRM acknowledges that FAA expects significant application volume and potential delays. AAPA shares concerns regarding whether FAA possesses sufficient staffing and resources to review potentially thousands of applications in a timely manner.

AAPA encourages FAA to:

- Expand interagency coordination with Sector Risk Management Agencies (SRMAs), including USCG and the Department of Homeland Security (DHS);
- Increase reviewer staffing and technical expertise;
- Consider phased or prioritized implementation for nationally significant critical infrastructure sectors, such as for those already maintaining FSPs;
- Develop proposed website-based notice mechanisms to streamline processing while preserving meaningful public comment opportunities; and

- Prioritize review and approval of applications submitted by Strategic Seaports and other nationally significant facilities supporting military deployments, defense logistics, and strategic sealift operations.

Address Authorized Operations and Operational Flexibility: Ports routinely utilize drones for infrastructure inspections, environmental monitoring, emergency response, waterside surveillance, construction management, hazard assessments, and other legitimate operational purposes. AAPA requests clarification that UAFRs will not unintentionally impede authorized and beneficial port-related UAS operations.

AAPA supports FAA's exploration of "whitelisting" Remote ID serial numbers and encourages the development of scalable systems that allow approved operators to conduct legitimate operations within UAFRs efficiently and securely. However, AAPA cautions that serial number-based whitelisting alone may not provide sufficient operational flexibility for large port complexes. At major ports, authorized drone flights may number in the hundreds or thousands annually, and the inventory of approved aircraft may change frequently as drones are added, replaced, retired, or assigned to different operational functions.

To preserve FAA's ultimate authority over the National Airspace System while ensuring timely, risk-based decision making, AAPA recommends that FAA develop localized or streamlined mechanisms for approving authorized UAS operations within UAFRs at complex critical infrastructure environments such as public port authorities. Such mechanisms could include FAA-approved port UAS management plans, streamlined authorization procedures for trusted operators, recurring authorization frameworks, or other scalable processes that recognize port authorities as distinct from individual fixed-site operators.

Many port authorities already maintain mature drone airspace management practices, operational experience, security coordination protocols, and technology-enabled situational awareness capabilities. FAA should consider leveraging these capabilities by allowing port authorities to coordinate authorized UAS operations across multiple facilities within a port-wide UAFR, subject to FAA-approved parameters and appropriate reporting requirements. Quarterly reporting on authorized flight activity, combined with timely notification of unauthorized incursions or mitigation-related incidents, would provide FAA with continued oversight while avoiding unnecessary administrative delays for routine, beneficial port operations.

AAPA also encourages FAA to provide flexibility for port authorities and maritime facilities to satisfy any Remote ID monitoring, notification, or situational awareness requirements through shared or port-wide capabilities. Many ports operate as multi-tenant environments with numerous terminals and operators located within a common security framework. Requiring duplicative systems for each facility could create unnecessary expense while reducing operational efficiency. FAA should allow port authorities or other coordinating entities to provide shared capabilities on behalf of multiple facilities where appropriate.

Protect Sensitive Security Information and Security Documentation: Maritime facility applications for UAFRs may require submission of information already protected under federal

security programs, including FSPs, Facility Security Assessments, vulnerability analyses, security system configurations, and related operational information.

AAPA requests that FAA clearly state in the final rule that Sensitive Security Information and other protected security materials submitted in support of UAFR applications will receive appropriate protection from public disclosure and will not be incorporated into public notices or comment processes in a manner that could compromise facility security.

Continue Advancing Detection and Mitigation Authorities: While AAPA supports the establishment of UAFRs, the NPRM itself acknowledges an important limitation: the proposal does not independently authorize any additional drone detection or mitigation authorities.

While UAFRs represent an important step forward, they are most effective when paired with sufficient detection and mitigation capabilities. Establishing restricted airspace without providing operators and law enforcement adequate means to identify and respond to unauthorized incursions limits the practical effectiveness of the program.

UAFRs are an important legal and airspace management tool, but they alone will not deter malicious actors intentionally disregarding federal law. Ports continue to face real-world drone threats, including surveillance concerns and operational vulnerabilities.

Accordingly, AAPA urges continued federal efforts to:

- Expand authorized counter-UAS detection and mitigation capabilities for critical infrastructure;
- Accelerate the promulgation of approved drone mitigation technologies by federal authorities, including as contemplated under the Safer Skies Act, so that ports and other critical infrastructure operators have adequate lead time to research, test, procure, and deploy mitigation systems appropriate for their individualized operating environments;
- Increase federal training capacity and available seats for authorized counter-UAS operators;
- Strengthen interagency coordination among FAA, DHS, the Department of Justice, the Transportation Security Administration (TSA), and USCG in countering UAS threats;
- Ensure strategic seaports are appropriately prioritized in future counter-UAS initiatives; and
- Evaluate funding mechanisms and support programs for local law enforcement agencies and public port authorities responsible for responding to drone threats affecting critical infrastructure and strategic sealift operations.

America's ports are foundational to national defense, supply chain resilience, energy security, and economic stability. As drone technology evolves, maritime infrastructure operators require practical, scalable, and coordinated tools to address emerging threats while preserving the efficiency of the National Airspace System.

AAPA appreciates the FAA's engagement with stakeholders and its efforts to establish a long-overdue framework for protecting critical infrastructure from unauthorized UAS activity. We look forward to continued collaboration with FAA, DHS, TSA, and USCG to ensure maritime

transportation facilities can effectively utilize this framework while recognizing the unique operational realities of the port environment.

Thank you for considering these comments.

Sincerely,

Sang Yi
President & CEO
American Association of Port Authorities