UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS AVIATION RULEMAKING COMMITTEE

FINAL REPORT

JANUARY 9, 2024

I. Background

Section 383(a) of the *FAA Reauthorization Act of 2018*, airport safety and airspace hazard mitigation and enforcement (Public Law 115-254, Oct. 5, 2018) (Section 383), established 49 U.S.C. Section 44810(a). This section requires the FAA Administrator to work with the Secretaries of the Departments of Defense and Homeland Security and the heads of other relevant federal departments and agencies. Federal partners should ensure that technologies and systems that are developed, tested, or deployed by federal departments and agencies to detect and/or mitigate potential risks posed by errant or hostile unmanned[1] aircraft system(s) (UAS) operations do not adversely impact or interfere with safe airport operations, navigation, air traffic services, or the safe and efficient operation of the National Air Space (NAS). In addition, Section 383[2] requires the FAA to develop a plan for the certification, permitting, authorizing, or allowing of UAS detection and/or mitigation (D/M) systems in the NAS, and to convene an Aviation Rulemaking Committee (ARC) to make recommendations for such a plan.

The ARC Charter was signed in March 2023 and the ARC began its work in May 2023. The ARC is composed of representatives from the manned and unmanned aviation communities, government entities, various subject matter experts (e.g., law, privacy, and environmental), and other stakeholders.

II. Executive Summary

The UAS Detection and Mitigation Systems ARC (the ARC) represented diverse interests and viewpoints. The ARC divided into several working groups and subgroups, working collaboratively to develop the best recommendations with as much consensus as possible. With the safety of the NAS as the ARC's primary focus, several recurring themes began to emerge from the working group discussions, including:

- Concerns surrounding legal authorities and constraints;
- Near-real time ability to share data and to identify verified operators;
- Communication plans, including strategic communications as well as escalation protocols to respond to UAS[3] incursions;
- The need for further research to establish safety standards; and
- Maintaining global leadership in the UAS industry.

A summary of the ARC's recommendations is below. Details and supporting text for all recommendations are in Section VIII of the report. The ARC recommends the FAA, with other relevant federal agencies:

- Ensure that all policy decisions are based on a thorough understanding of the industry and that detection and mitigation issues are considered separately for policy purposes.
- Conduct the necessary research and analysis to establish minimum performance standards, a safety framework, best practices, training programs, and a continually evolving approved list of technologies for UAS D/M systems.
- Establish testing protocols and use approved third parties for system testing and authorization.

[1] The ARC uses "unmanned" throughout this report because that is how the term "UAS" is defined in the law (see, e.g., U.S.C. § 44801). However, the ARC notes that many in the industry prefer "uncrewed" due to the term being more inclusive.

[2] Paragraph (b) of Sec. 383 (49 USC 44810).

[3] For the purposes of this ARC, D/M use on UAS is meant to apply to "small UAS" as defined in the FAA Modernization and Reform Act of 2012 (available at https://www.congress.gov/112/crpt/hrpt381/CRPT-112hrpt381.pdf).

- Establish an entity for airport terminal airspace operations that is responsible for UAS D/M system monitoring and aircraft deconfliction, as deconfliction is an Air Navigation Service Provider (ANSP)[4] function that cannot be adequately managed by a D/M system operator or air traffic control as currently configured.
- Develop a clear approval process for D/M deployment at airports and non-airport facilities and require detection system operators to complete training, and mitigation system operators to complete training and certification. However, acquisition and deployment of D/M by airports should remain optional and never be required by the federal government.
- Create a scalable regulatory framework for operational requirements with privacy protections for UAS operators and for the public. The framework should include verified operator and data sharing programs, noting that any information accessed or exchanged from the agency must have sufficient privacy and security safeguards similar to manned aircraft operators.

The recommendations in this report are intended to provide a framework of actions and policies to promote safe and widespread adoption of UAS D/M systems that does not adversely impact or interfere with the safe and efficient operation of the NAS.

[4] An ANSP is an organization that provides a number of services to airspace users, including aircraft separation. It manages air traffic on behalf of a company, region, or country.

III. Chairs' Comments

The deployment and use of UAS in the NAS is on the verge of a significant breakthrough with many beneficial outcomes for the U.S. economy, industry, and society. At the same time, the deployment of UAS in combat and military applications in conflict zones in 2023 alone has rapidly evolved and changed the threat scenario for facilities across our nation and the globe. This juxtaposition underscores the critical need and timeliness for regulations around UAS detection, identification, and mitigation in the U.S. Additionally, the U.S. is positioned to lead the way for other countries around the world, demonstrating how effective and reasonable implementation of UAS detection, identification, and mitigation systems can ensure the safety of airspace and enable the legitimate application of UAS.

The ARC has worked through a nascent and nebulous topic – one where technologies and techniques are in rapid evolution of capability, but also one where the government and society can ill afford to wait for established equipment and systems. The ARC has brought together more than 50 disparate groups from the UAS industry, traditional aviation groups, public safety organizations, societal interest associations, and others to devise a scalable, fair, reasonable, and transparent set of recommendations to advance the use of these technologies. The ARC has done this as openly as possible, striving to ensure the voices of all parts of the group, and thus all parts of our nation, are heard and understood. Keeping this in mind, it will be critical for the government to continue to consider the evolution of both UAS and the detection and mitigation capabilities as regulations are implemented and expanded.

The original structure of the ARC was designed to ensure each member had a relevant engagement with the subject at hand. Five working groups were created, including one focused on the importance of societal interests, one on systems integration, two on location-specific considerations (airport and non-airport), and one on operational considerations. These five working groups spent several months working through core questions and issues to ensure they were making recommendations relevant and impactful to their areas. After the second in-person plenary, the ARC pivoted to considering four use-case applications related to different scenarios. In these "tabletop-like" exercises over several weeks, the members scrubbed existing recommendations, identified gaps, and held cross-working group meetings to ensure the ARC's recommendations were as holistic as possible.

In the end, the ARC worked over seven months, at three in-person plenary sessions and several more virtual sessions, to craft the recommendations contained in this report. While the ARC recognizes that UAS detection and mitigation is still extremely dynamic, the recommendations have identified several key themes. First, the interplay among relevant government entities regardless of the status of authority is paramount to the safety and security of the NAS. Next, as with many things in the aviation industry, one size does not fit all. Risk tolerance and detection and mitigation capabilities need to be suited for specific missions and vulnerabilities. The aviation industry and society face a herculean challenge of managing legitimate UAS volume while sharing data and information about these operations among interested parties. And, lastly, training and education about UAS detection and mitigation will need to be widely available and shared.

It has been our pleasure to lead this ARC and to break ground on an important and necessary trail for the betterment of our country and of our world. We are appreciative of the members of this ARC who have taken a significant amount of their time and energy to wrestle with a challenging topic which lacks certainty and clarity. Regardless, we believe we have delivered the FAA a flexible and useful set of recommendations that can pave the way to effective and reasonable regulation of the UAS detection and mitigation market, while simultaneously bolstering the safety and security of our NAS.

IV. ARC Charter Summary

A. ARC Objectives

The ARC provided a forum for the U.S. aviation community and UAS security stakeholders to discuss and provide recommendations to the FAA for a NAS-wide plan for certification, permitting, authorizing, or allowing the deployment of UAS D/M technologies or systems, without causing adverse impact to the NAS. The ARC sought to identify opportunities for internal policy and guidance development to ensure adequate FAA oversight over the use of UAS D/M systems. Although current federal law only expressly authorizes certain federal entities to use D/M systems under specified circumstances, the ARC was asked to consider standards and operational uses for these systems in the NAS, regardless of the user of the technology, to ensure the safe integration of this technology into the NAS by any potentially authorized user. The ARC was not meant to address any potential or recommended expansion of FAA authorities by Congress related to the use of these technologies nor the potential expansion of authority by Congress for any other entity to engage in UAS D/M, but did recognize the need for FAA leadership in this area.

B. ARC Tasks

The ARC was tasked to make recommendations for a plan and standards to ensure the use of UAS D/M systems does not adversely impact or interfere with safe airport operations, air navigation, air traffic services, or the safe and efficient operation of the NAS. Where feasible, such recommendations should consider the environmental impact of the research on, testing of, and deployment of these systems. The ARC was asked to address:

- How FAA processes and procedures could ensure UAS D/M systems do not interfere with capabilities such as avionics, communications, radars, lighting, and navigational aids (e.g., spectrum prioritization/hierarchy), considering that these systems vary from site to site.
- How FAA processes and procedures could ensure that UAS D/M systems do not affect aircraft airworthiness; safe navigation; safe operation and use of airspace by compliant operators, existing airspace users, and persons and property on the ground; or NAS infrastructure.
- What additional policies, regulations, and operational procedures the FAA should develop or revise to ensure the use of UAS D/M systems is carried out with minimal disruption to the safety and efficiency of the NAS and maximizes access to the airspace by compliant users.
- Gaps in existing airspace management tools—inclusive of rules and policy for their use—and options for the FAA to alleviate secondary impacts of UAS D/M systems on the safe and efficient operation of the NAS.

The ARC was also tasked to make recommendations on a certification framework and standards in order to minimize risk to the NAS when a UAS D/M system is used, including, at a minimum:

- Possible certification frameworks for UAS D/M systems, including the benefits and drawbacks of certifying systems versus certifying organizations and/or individual operators authorized to use the technology.
- Recommendations for standards for UAS D/M systems, considering the vast number of commercial systems and types of technologies in existence and/or under development, and with consideration for the following:
    - Physical effects of the systems, such as standards related to the safety of, and potential interference with, aircraft in the air and on the ground, airport operations, air traffic control (ATC) facilities, and all aviation-related infrastructure.
    - Communication signals, such as performance standards related to potential interference

with radios, transponders, navigation equipment, and other radio frequency (RF) radios operated by aircraft, ATC facilities, and airports. The ARC was also asked to consider standards related to potential interference with other aviation-related RF spectrum.

- Ensuring systems do not provide erroneous information (e.g., non-UAS false positives, duplicative tracks for the same UAS, incorrect locations) which could threaten the safety of the NAS by instigating inappropriate responses.

V. ARC Activities and Outputs

The ARC took a holistic approach in making its recommendations. It considered the integration of UAS D/M system operations, as well as the safety and security benefits that could be provided to the NAS and to ground-based critical infrastructure facilities and other high-risk events.

The ARC established five working groups to address these issues:

- Working Group 1 – Wider Ecosystem & Public Interests
- Working Group 2 – System Requirements
- Working Group 3A – Site Considerations – Airports
- Working Group 3B – Site Considerations – Non-Airport Environments
- Working Group 4 – Operation Requirements

Each working group developed specific focus questions[5] to guide their work. The groups met for several months to answer the identified focus questions and develop recommendations. The working groups also convened several Tiger Team sub-groups to address technical issues or address particular focus questions in more depth. Members were selected for Tiger Teams based on their experience and expertise. The Tiger Teams generated preliminary recommendations that were presented to the wider working group to obtain feedback and achieve final consensus on the group's recommendations.

In some cases, working groups felt it was necessary to engage with other working groups to resolve conflicting recommendations or avoid duplicating efforts. There were also instances where a member of a particular working group had expertise that was valuable for an alternate working group's focus questions. To facilitate these conversations and information sharing, the working groups held several "Cross Talks" to integrate different perspectives and promote ARC-wide agreement on specific group recommendations. In some cases, the Cross Talks were the impetus for a recommendation. For example, a Cross Talk between WG3A and WG3B identified the need to create a "verified" operator program, which eventually became Recommendation DM4.

A. Working Group 1 – Wider Ecosystems & Public Interests

Working Group 1 (WG1) was tasked with laying the foundation for the ARC Report. The group focused on defining D/M technologies and the relevant marketplace; considering societal interests – including benefits, costs, and risks of D/M integration; and identifying D/M ecosystem needs for success.

B. Working Group 2 – System Requirements

Working Group 2 (WG2) was charged with making recommendations specific to the system requirements of UAS D/M systems to safely integrate into the NAS. The Working Group focused on two premises of UAS systems to reduce the overall risks to the NAS, which included:

- minimizing the impacts that D/M systems present, and
- expanding D/M systems to improve safety, increase security, and reduce economic harm.

WG2 considered a range of factors that would support optimum efficiency and safety in the NAS, including prioritization of the airspace, particularly around critical infrastructure, attributes of current UAS systems and risk profiles, legal authorities, data sharing, and further analysis and testing of systems to futureproof systems and operations. WG2 collaborated with other working groups and consulted

[5] The Focus Questions for each working group are in Appendix C.

subject matter experts, such as representatives from INTERPOL, who provided a summary of lessons learned from operational Use Cases and testing. WG2 also incorporated information from the RTCA SC-238 (Counter Unmanned Aircraft Systems) and EUROCAE WG-115 Counter-UAS Transmission Letter Identifying Terms of Reference in its recommendations.[6]

C. Working Group 3A - Site Considerations-Airports

Working Group 3A (WG3A) was responsible for making recommendations to deploy D/M systems safely in the airport environment. The group focused on safety and security of the NAS, as well as safety and security of the airport facility and business continuity. The group also emphasized the ANSP functions associated with aircraft deconfliction and the gap in existing FAA airspace management tools to deconflict aircraft and alleviate secondary impacts of UAS detection and mitigation systems on the safe and efficient operation of the NAS.

D. Working Group 3B - Site Considerations-Non-Airports

Working Group 3B (WG3B) was responsible for making recommendations to safely deploy D/M systems in non-airport environments and include non-traditional participants in the NAS. The group focused on D/M system usage at critical infrastructure facilities and other high-risk venues, such as chemical plants, prisons, and stadiums. The main goals of WG3B were to increase efficacy in identifying and minimizing the threat of errant or nefarious UAS and to avoid disruption of authorized and compliant operations in non-airport environments.

WG3B began its deliberations by focusing on the safe integration of D/M systems *by sector*. There are 16 critical infrastructure sectors as designated by the Cybersecurity and Infrastructure Security Agency (CISA), which is the national coordinator for critical infrastructure security and resilience.[7] The group initially considered that each sector would require a different D/M system integration plan due to the various operational requirements and specific needs. However, as the group progressed in its work, it became apparent that the core functions of detecting, identifying, and mitigating a UAS would be largely similar regardless of the environment. Therefore, the working group shifted its focus to those three distinct workflows (i.e., Detect, Identify, and Mitigate) and built its recommendations thereon. Detect, Identify, and Mitigate are recognized actions established under DHS' C-UAS Actions authorities and referenced in the C-UAS Tech Guide's processing chain stages that will help properly assess the presence of UAS in proximate airspace.

E. Working Group 4 - Operating Requirements

Working Group 4 was tasked with recommending rules or requirements for safe deployment and operation of D/M technologies, with consideration for safety of the NAS and protection surrounding critical infrastructure and the public, while ensuring that UAS operators are protected in terms of privacy and their ability to lawfully operate freely in the airspace. Special areas of focus for the group included developing a framework for training/certification of D/M operators and exploring what role the FAA should play in establishing guidelines for mitigation of UAS.

[6] See Appendix B for a copy of the RTCA SC-238 (Counter Unmanned Aircraft Systems) and EUROCAE WG-115 Counter UAS Transmission Letter.

[7] There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. *PPD-21: Critical Infrastructure Security and Resilience*, available at https://www.cisa.gov/sites/default/files/2023-01/ ppd-21-critical-infrastructure-and-resilience-508_0.pdf.

VI. Industry Overview

To lay the foundation for this report, the ARC first endeavored to define “counter-UAS system” (C-UAS) technologies and the relevant marketplace. Congress has defined C-UAS as a system or device capable of lawfully and safely disabling, disrupting, or seizing control of an unmanned aircraft (UA)[8] or unmanned aircraft system (UAS or drone).[9] However, as recognized by the Charter for this ARC, the C-UAS marketplace comprises a much broader array of technologies, including UAS detection technologies and systems. Therefore, the ARC uses the terms “C-UAS” and “Detection/Mitigation (D/M)” in this report to encompass a variety of air, ground, and naval platforms for D/M, using laser systems, kinetic systems, electronic systems, and other technologies.

The C-UAS marketplace includes companies from the defense sector, end user critical infrastructure facilities, the growing civil UAS sector, and venture-funded growth and technology companies. To date, the U.S. C-UAS marketplace has suffered from the lack of a clear enabling legal framework. For example, the uncertain and immature legal framework for C-UAS has impacted funding levels for research and development of C-UAS technologies. In addition, many U.S. companies have been compelled to research, develop, and sell their technologies and services abroad, where laws and regulations may be more flexible and mature, and innovation is encouraged.

Even with these challenges, the growing C-UAS technology market has been valued at more than $1 billion, with projections to reach between $8 billion and $10+ billion by 2032. One 2021 study valued the C-UAS market size at $1.1 billion and forecasted that it would grow from $1.4 billion in 2023, to $8.2 billion by 2032.[10] Another report valued the global C-UAS market size at $1.4 billion in 2022, and $1.9 billion in 2023, and forecasted growth at a compound annual growth rate of 28.1% from 2023 to 2030 with a revenue forecast for 2030 of $10.6 billion.[11] These numbers undersell the value of the marketplace, because it is also important to consider the potential effect of security vulnerabilities on the value of the activities the C-UAS equipment protects and enables – such as major sporting events, energy, and utilities.

Notably, although the North American C-UAS marketplace is the largest by revenue,[12] other regions of the world are also active in C-UAS. High-profile events in other countries involving UAS – such as the war in Ukraine, the Israel-Hamas conflict, or the December 2018 Gatwick Airport incident when reported UA sightings essentially closed that major airport – have drawn attention to the need for C-UAS technology internationally.

In defining C-UAS technologies and the relevant marketplace, the ARC noted that many technologies exist that are not defined as C-UAS technologies, but nevertheless promote a safe and secure airspace.

[8] Unmanned aircraft means an aircraft operated without the possibility of direct human intervention from within or on the aircraft. *See* 14 CFR 107.3.

[9] 49 U.S.C. § 44801.

[10] Swapnil Palwe, *Counter UAS Market Research Report Information by Method (Detection and Interdiction), by Platform (Handheld, UAV, and Ground-Based), and by Region (North America, Europe, Asia-Pacific, and Rest of the World) – Market Forecast Till 2032* (February 2021).

[11] Grand View Research, *Anti-drone Market Size, Share & Trends Analysis Report by Component, by Type, by Range, by Technology, by Mitigation Type, by Defense Type, by End-Use, by Region, and Segment Forecasts, 2023 – 2030* (2023), available at https://www.grandviewresearch.com/industry-analysis/anti-drone-market.

[12] Id.

These may be referred to as “enabling technologies.” For example, air traffic management (ATM) and UAS traffic management (UTM) facilitate the monitoring and deconfliction of UA and other aircraft operations, while also helping to enhance operational efficiency among the various operations. These traffic management systems also can support the identification of safety threats from non-conforming UAS operators.

VII. UAS D/M Systems Integration Concerns

A. Legal Constraints

An entity deciding to use D/M systems must not only consider the risks associated with the system's use, but also the legal permissibility. Congress has exclusively authorized the Departments of Defense (DoD), Energy (DOE), Justice (DOJ), and Homeland Security (DHS) to engage in limited UAS D/M activities to counter UAS presenting a credible threat to facilities or assets covered under rulemaking,[13] notwithstanding certain otherwise potentially applicable federal criminal laws, including various laws relating to surveillance.[14] In addition, the FAA is expressly authorized to engage in limited testing activities, notwithstanding certain federal criminal surveillance laws.[15] There are also other categories of federal laws that may apply to UAS D/M capabilities, such as various provisions of the U.S. criminal code enforced by DOJ, and federal laws and regulations administered by the FAA, DHS, and the Federal Communications Commission (FCC).[16] D/M system users should also be mindful of state, local, and tribal laws that may implicate system operations.[17]

In addition to the numerous federal and state laws, D/M system users also need to consider the potential civil liability flowing from the use of UAS D/M technologies (e.g., liability for causing physical damage to other aircraft, persons, or property as a result of mitigating a UAS threat; or civil liability for an unlawful interception of wire, oral, or electronic communications under 18 U.S.C. § 2520). The ARC notes generally that the legal and regulatory implications may vary based on the user and the type of technology used.

B. Regulatory Uncertainty

The ARC also believes legal and regulatory uncertainty currently inhibits progress and undermines investment in the C-UAS industry. Specifically, C-UAS companies are limited in their ability to develop, test, operate, and sell D/M technologies because the legal and regulatory framework for certification, implementation, and operation is unclear and uncertain. In addition, companies, firms, and individuals considering investments in C-UAS companies are less likely to do so because there is no legal or regulatory certainty (or a timeframe for such) regarding the certification, implementation, and operation of D/M technologies or whether any broader application of such systems will be permitted.

The FAA, as evidenced by its continued efforts to address airspace access equity, under-served communities, and standards that foster industry innovation, is very much interested in ensuring

[13] "Covered facility or asset" is defined in the following document: https://ogc.osd.mil/Portals/99/OLC%20FY%202020%20Proposals/10April2019.pdf?ver=moEPMmZvMMu4yNV3Xy5bIg%3D%3D.

[14] DoD and DOE are empowered under 10 U.S.C. § 130i, 50 U.S.C. § 2661. DOJ and DHS get their authority from 6 U.S.C. § 124n.

[15] 49 U.S.C. § 44810(g).

[16] Pen/Trap Statute, 18 U.S.C. §§ 3121-3127, the Wiretap Act (also known as Title III), 18 U.S.C. §§ 2510 et seq., the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, Interference with the Operation of a Satellite, 18 U.S.C. § 1367, Communication Lines, Stations, or Systems, The Aircraft Sabotage Act, 18 U.S.C. § 32(a), The Aircraft Piracy Act, 49 U.S.C. § 46502, 18 U.S.C. § 1362, Marketing, Sale, or Operation of Jammers. 47 U.S.C. § 302a, and Interference with Radio Communications. 47 U.S.C. § 333.

[17] Interagency Legal Advisory on UAS Detection and Mitigation Technologies (https://www.faa.gov/sites/faa.gov/files/uas/resources/c_uas/Interagency_Legal_Advisory_on_UAS_Detection_and_Mitigation_Technologies.pdf).

economic growth opportunities continue to be an important element of its decision-making. As drone technology continues to proliferate, it is also critical that the U.S. has access to security solutions to counter bad actors. Thus, enabling investment in the C-UAS industry is important to all Americans.

In order to provide a suitable legal and regulatory framework, the ARC believes the C-UAS industry needs a federally acknowledged technical validation process, to include a federally released timeline that provides meaningful and actionable information to federal legal and regulatory decision-makers. The ARC also believes the industry needs clear guidelines about what is legal, when, and by whom (in layperson's terms).

C. Public Safety

For the past several decades, the concept of safety surrounding the NAS has primarily focused on safeguarding the flight operations of crewed aircraft, airport operations, and air traffic control. We must now recognize that the rapidly emerging era of UAS is expanding flight operations to include ground control stations and other potential systems that directly control an aircraft from non-airport locations, as well as from airports located within the legal jurisdictions of State, Local, Tribal, and Territorial (SLTT) entities. The U.S. must maintain its leadership role in aviation security while also ensuring the safety and security of the NAS. This will increasingly necessitate the inclusion and cooperation of SLTT public safety partners working alongside federal partners as UAS systems proliferate – especially since there is no current funding or plans to provide federal partners the capability and capacity to manage the NAS in its entirety.

The ARC strongly believes that it is imperative for SLTT partners to have direct, low-cost access to accurate information regarding the volume, frequency, location, and type of low-altitude aviation traffic to properly assess safety and security vulnerabilities within their respective jurisdictions. This requires the capability to detect UAS operations in general, with a specific emphasis on those operations occurring within the vicinity of sensitive or highly vulnerable ground sites, including critical infrastructure, mass gatherings, active public safety, and emergency response incident scenes, as well as other locations requiring enhanced protection from aerial threats.

The ARC strongly supports the creation of shared databases that generally collate and report on the volume of UAS air traffic across the NAS, as well as the frequency and type of suspicious/nefarious operations by these vehicles in specific and vulnerable locations. This data will help establish the baseline required for future assessments of whether SLTT partners should have expanded authorities and capabilities surrounding the technical mitigation of rogue or nefarious UAS vehicles under specific and well-defined rules of engagement.

Additionally, while the present methodology of generally designating airspace at 400 feet Above Ground Level (AGL) and below for part 107 UAS operations has proven to be a reasonable first step towards facilitating safety within the NAS with direct respect to manned air traffic, this solution may not be sufficient to adequately protect non-airport sites with specific and distinct vulnerabilities from unmanned operations. Therefore, the evolution of UAS mandates that stakeholders now assess whether the current paradigm for designating airspace and developing aeronautical charts – predicated primarily on airport location and air traffic type and volume – is sufficient to accommodate projected growth within the UAS traffic segments, while simultaneously ensuring the safety and security of other potentially vulnerable non-airport sites on the ground. Public safety stakeholders believe that the owners and operators of vulnerable, non-airport sites should have an identified and realistic pathway towards having airspace surrounding said sites designated as restricted areas for the operation of certain types of UAS vehicles, especially for those operations conducted at an altitude of 400 feet AGL and below by aircraft that are unregistered, unidentified, or otherwise unknown. The ARC strongly believes that the present environment may represent the best opportunity to reassess the current operational paradigm surrounding how airspace within the NAS is designated above critical infrastructure.

According to the *FAA Aerospace Forecast, Fiscal Years 2023-2043*, at the start of 2023, the U.S. small UAS (sUAS)[18] fleet was estimated to be more than 2.4 million aircraft – more than 10 times larger than the crewed aviation fleet of 216,465 aircraft. The rapid growth of UAS over recent years has increased the potential threat posed by criminal and nefarious UAS operations to the NAS and non-airport sites while also resulting in increased investigatory and enforcement action requiring the timely support of the FAA's Law Enforcement Assistance Program (LEAP). Unfortunately, the LEAP has failed to grow at an appropriate pace to match the growth of the UAS fleet. Presently, there are between 20 and 25 LEAP agents assigned to assist SLTT public safety partners with all types of aviation incidents. This number is insufficient to provide adequate support to SLTT public safety partners tasked with helping to safeguard the NAS. Moreover, approximately 20% of LEAP agents are also reported to be members of a military reserve branch – meaning if they are called to active duty, especially during times of national crisis or war, the gap for LEAP assistance to SLTT public safety partners will widen. The ARC strongly recommends that additional funding and resources be allocated to the LEAP to increase the number of LEAP agents required to provide timely and effective support to SLTT public safety partners as needed.

Finally, the ARC agrees that ensuring the safety and security of the NAS will require a focused educational campaign targeting UAS operators, combined with public information messaging that disseminates accurate regulatory requirements to all remote pilots and UAS operators – with a special emphasis on those that might be classified under "clueless, careless, or criminal" user designations.

D. Intergovernmental Jurisdictional Roles

The ARC notes that intergovernmental jurisdictional roles and cross-jurisdictional boundaries are key issues to resolve. Coordinating multiple jurisdictions provides many opportunities for errors and the pain of communications can significantly hinder the effective deployment of D/M systems in a variety of environments. For example, in the airport environment, there may be instances where airport law enforcement has no authority off-airport and lacks jurisdictional authority to engage with offending UAS operators. In these instances, local law enforcement may be called upon to assist, but safety of the NAS may be a lower priority for non-aviation first responders. Thus, it is critically important to develop comprehensive and coordinated multi-jurisdictional response plans to ensure that errant UAS operations are communicated to the correct entities and to avoid engaging with operators in a way that does not adhere to the accepted protocols, is unlawful, or is not properly documented. The ARC also recognizes that coordination plans alone will not adequately address jurisdictional gaps or the ability to respond to situations without the appropriate Congressional authority.

The ARC also notes that engaging with federal partners to mitigate a UAS can potentially be problematic if escalation and communication protocols are not clearly defined and agreed to in advance. The ARC notes its recommendations in this regard[19] and encourages the FAA to facilitate streamlined

[18] Small unmanned aircraft means an unmanned aircraft weighing less than 55 pounds on takeoff, including everything that is on board or otherwise attached to the aircraft. 14 CFR § 107.3.

[19] See Recommendations AP5, PL11, and SD1.

coordination processes and multi-jurisdictional engagement that supports mutual aid and is scalable and adaptable to a variety of environments. A federal response through TSA/FAA cannot be an FAA mandate for coordination among SLTT entities without the jurisdictional authority and laws in place to enforce.

E. Prioritizing User Communities with Carve Outs

This ARC was asked to solve a challenging problem affecting a variety of stakeholders, where the solutions available are complex. Various themes were deliberated, Use Cases explored, and recommendations generated that have clarified macro-level solutions to ensure the safety of the NAS.

Through the Use Case[20] discussions, it became clear that, while macro-level solutions are complex, some micro-level “carve outs” for D/M authorities may be relatively easier to solve. These examples would include cases such as a prison, where a potential threat is very specific, the location is isolated with limited risks to surrounding airspace and ground assets, existing rules already limit potential exposure, and the proposed solution is constrained.

Because these examples exist and are potentially much easier to solve, the ARC believes that the FAA should utilize these specific Use Cases to more expeditiously implement recommendations made by the ARC. In fact, taking this approach would allow FAA to learn valuable lessons in safe environments, and then expand recommendation implementations over time as Use Cases prove themselves out.

This “spiral development” approach has proven to be effective in other missions and has allowed the U.S. government to ensure safety and security is paramount, while also allowing for faster implementations of emerging solutions to rapidly evolving conditions. The proliferation of UAS in the NAS certainly meets these criteria and, therefore, the need to develop D/M solutions in a timely manner is critical. It is important to note that “spiral development” does not imply that early solutions would gain a priority (e.g., regarding spectrum allocations). Rather, as competing technologies emerge, it is entirely possible that early developments will offer a diminished return or become obsolete altogether. While this ARC believes that the FAA should endorse spiral development, it also recognizes that early adopters must assume the financial risk of their investment.

F. Attributes of D/M Systems and System Operability

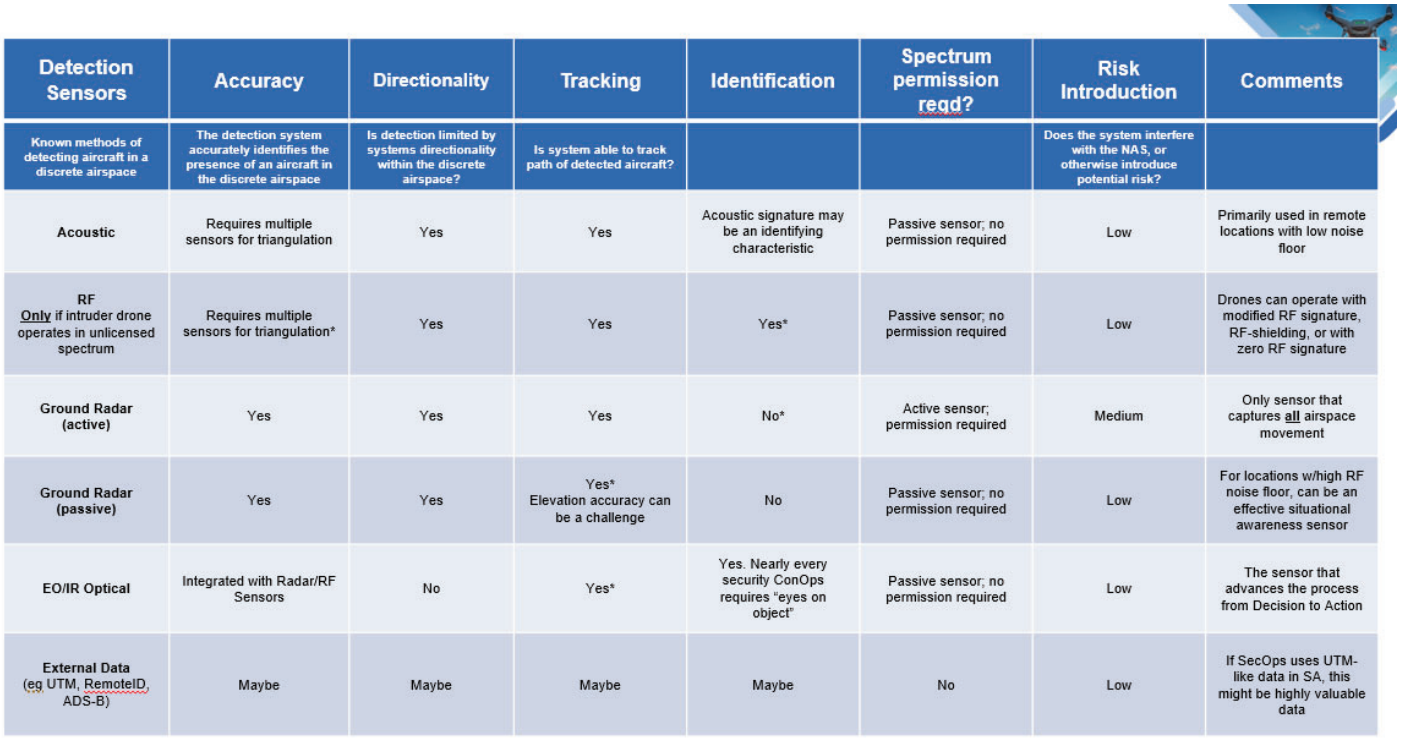
A system-of-systems approach with continual baseline modifications is typically maintained by a large organization such as the federal government. The maintenance of these systems usually requires chief architects, system engineers, continual testing, in-depth knowledge of all participating systems, and a large budget because investment in capital and operational costs and D/M system interoperability programs can be prohibitive. D/M systems will be tailored to site or mission attributes and secured in the same manner as other protected systems. Therefore, any site or mission that is required to evaluate, deploy, and operate D/M systems for compliance or other reasons must have full legal and regulatory capability to do so. Any expansion of authorities beyond current federal entities should consider direct and indirect compliance costs for these entities, as well as any standards or general testing regimes in force.

The charts below list the different types of D/M sensors that would be part of a "system" and in no way have bearing on interoperability. In developing the Detection Chart, the ARC relied on the detection risk

[20] See Appendix D for more information on the ARC’s Use Cases.

levels in RTCA DO-389.[21] As depicted in the chart, the ARC believes risk may be caused by deployed active sensors interfering with each other. The spectrum allocation for ground radar is the same for both Security and Navigation applications, increasing the risk of interference and degradation of both applications. In developing the Mitigation Chart, the ARC relied on the expertise of its members to determine risk level information. The risk levels are not supported by data from a standards body but do provide a helpful notional overview of D/M system risk from an attributes perspective.

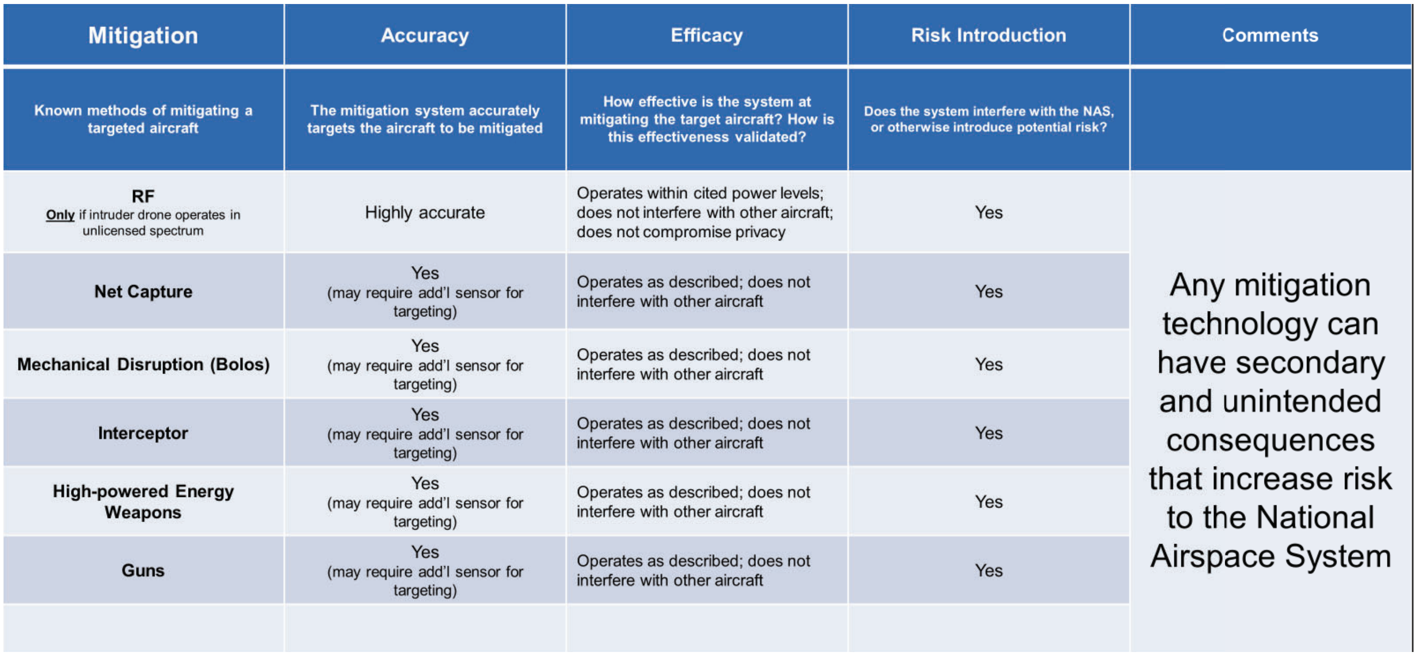
Attributes of UAS Detection Systems⁺



Detection Sensors	Accuracy	Directionality	Tracking	Identification	Spectrum permission reqd?	Risk Introduction	Comments
Known methods of detecting aircraft in a discrete airspace	The detection system accurately identifies the presence of an aircraft in the discrete airspace	Is detection limited by systems directionality within the discrete airspace?	Is system able to track path of detected aircraft?			Does the system interfere with the NAS, or otherwise introduce potential risk?	
Acoustic	Requires multiple sensors for triangulation	Yes	Yes	Acoustic signature may be an identifying characteristic	Passive sensor; no permission required	Low	Primarily used in remote locations with low noise floor
RF **Only** if intruder drone operates in unlicensed spectrum	Requires multiple sensors for triangulation*	Yes	Yes	Yes*	Passive sensor; no permission required	Low	Drones can operate with modified RF signature, RF-shielding, or with zero RF signature
Ground Radar (active)	Yes	Yes	Yes	No*	Active sensor; permission required	Medium	Only sensor that captures **all** airspace movement
Ground Radar (passive)	Yes	Yes	Yes* Elevation accuracy can be a challenge	No	Passive sensor; no permission required	Low	For locations w/high RF noise floor, can be an effective situational awareness sensor
EO/IR Optical	Integrated with Radar/RF Sensors	No	Yes*	Yes. Nearly every security ConOps requires "eyes on object"	Passive sensor; no permission required	Low	The sensor that advances the process from Decision to Action
External Data (eg UTM, RemoteID, ADS-B)	Maybe	Maybe	Maybe	Maybe	No	Low	If SecOps uses UTM-like data in SA, this might be highly valuable data

[21] RTCA DO-389, Operational Services and Environment Definition (OSED) for Counter-UAS in Controlled Airspace, March 18, 2021.

Attributes for UAS Mitigation Systems+*



Mitigation	Accuracy	Efficacy	Risk Introduction	Comments
Known methods of mitigating a targeted aircraft	The mitigation system accurately targets the aircraft to be mitigated	How effective is the system at mitigating the target aircraft? How is this effectiveness validated?	Does the system interfere with the NAS, or otherwise introduce potential risk?	
RF **Only** if intruder drone operates in unlicensed spectrum	Highly accurate	Operates within cited power levels; does not interfere with other aircraft; does not compromise privacy	Yes	Any mitigation technology can have secondary and unintended consequences that increase risk to the National Airspace System
Net Capture	Yes (may require add'l sensor for targeting)	Operates as described; does not interfere with other aircraft	Yes	
Mechanical Disruption (Bolos)	Yes (may require add'l sensor for targeting)	Operates as described; does not interfere with other aircraft	Yes	
Interceptor	Yes (may require add'l sensor for targeting)	Operates as described; does not interfere with other aircraft	Yes	
High-powered Energy Weapons	Yes (may require add'l sensor for targeting)	Operates as described; does not interfere with other aircraft	Yes	
Guns	Yes (may require add'l sensor for targeting)	Operates as described; does not interfere with other aircraft	Yes	

+Tables are for illustrative purposes only: The ARC was not tasked to define all possible attributes of all UAS systems. Rather its task was to consider how D/M systems impact NAS safety and make recommendations. The charts are examples only and are by no means exhaustive or complete. They are included only to illustrate how some systems could be categorized.

**Depends on how the system is designed and deployed.*

VIII. ARC Recommendations - Intent, Rationale, and Approach

This section provides detailed information on each recommendation, including the ARC's intent, supporting rationale, research, examples, and suggested approach. The ARC organized its recommendations into the following categories, noting that the list does not reflect any order of priority.

- Policy
- Risk Management
- System Standards
- Testing
- Training
- Data Management
- System Acquisition
- System Deployment (General)
- System Deployment – Airports
- System Deployment – Non-Airports

A. Policy

The Policy section contains recommendations stressing the importance of a solid industry understanding when making policy determinations, consideration of detection and mitigation as separate issues for policy purposes, research to better enable balancing of risks and benefits, and consideration of costs of D/M integration as well as privacy, environmental, health, and civil liberties interests of the public. In addition, there are recommendations on benefits to security and law enforcement, strategic communications, further study and analysis, privacy protections for UAS operators and the public, and Title 18 relief for UAS mitigation. There are also recommendations on the importance of U.S. leadership and of capitalizing on lessons learned and applying best practices.

PL1 - Policy Recommendations Based on a Thorough Industry Understanding

PL1	**The FAA should incorporate a thorough understanding of the industry and its intricacies, as well as the broader ecosystem, into any policy recommendations.**

INTENT: To ensure that in considering the value of the C-UAS marketplace, the FAA and federal partners consider issues around drone security and specifically tailor recommendations to the C-UAS industry.

RATIONALE: D/M systems and equipment encompass a broad array of technologies and implicate many considerations and unique issues. For example, there are detection technologies (i.e., systems that detect, monitor, and/or track UAS) that often rely on radio frequency, radar, electro-optical, infrared, or acoustic capabilities, or a combination thereof; and mitigation technologies (i.e., non-kinetic and kinetic systems) that disable, disrupt, seize control of, and/or destroy UA or UAS. There are also many "enabling" technologies, such as ATM and UTM, that are not defined as D/M technologies, but facilitate monitoring and deconfliction of UA and other aircraft operations and can support the identification of potential safety threats from UAS operations. In addition, safe and effective use of D/M, and the full UAS integration it will help provide, will have impacts on numerous industries, such as energy and utilities, the defense sector, major sporting events, and venture-funded growth and technology companies. Accordingly, policy recommendations should reflect the full scope of relevant technologies and impacts so they are more specifically tailored to relevant features of UA and C-UAS technology.

APPROACH: The FAA should work with its federal partners to ensure that it thoroughly considers and understands relevant D/M and enabling technologies, as well as the broader ecosystem, when making policy determinations.

PL2 - Separate Policies for Detection & Mitigation

PL2	**Given the differences between detection and mitigation, the FAA should work with its federal partners to consider these two components separately for policy purposes.**

INTENT: To ensure that the FAA and federal partners account for the differences between detection and mitigation when making policy decisions about the appropriate use of D/M technologies and capabilities in different circumstances.

RATIONALE: Congress has defined C-UAS as a system or device capable of lawfully and safely disabling, disrupting, or seizing control of UA or UAS.[22] C-UAS mitigation is a safety and security action to protect people and property from being harmed by nefarious or careless drone operations. Mitigation cannot occur without detection, but detection can occur without mitigation.

As recognized by the ARC Charter, the C-UAS marketplace comprises a broad array of technologies and includes UAS detection-only technologies and systems. The ARC recognizes that many entities will be interested in detection-only systems and will not want systems with mitigation capability due to costs, liability concerns, or other legitimate operational reasons. Accordingly, the ARC recommends the FAA avoid creating rules or policies intended for UAS D/M systems collectively and instead develop policies and rules for UAS detection systems and UAS mitigation systems separately. Entities that only want UAS detection capability should not be marginalized or otherwise negatively impacted by FAA policy decisions or regulatory requirements.

APPROACH: The FAA and federal partners should consider the differences between detection and mitigation and avoid any “one size fits all” approach due to operational and environmental factors.

[22] 49 U.S.C. § 44801.

PL3 - Risk and Benefit Balancing

PL3	**The FAA should work with its federal partners to balance the benefits of authorized D/M technology integration with the potentially detrimental impact of such systems on their surrounding broader ecosystem.**

INTENT: To urge the FAA and federal partners to conduct further research to fully understand the realm of new risks introduced by D/M technology.

RATIONALE: Evaluation of potential risks of D/M integration is necessary so the FAA and federal partners can balance them against potential benefits, yet it is hampered by a lack of research into at least three key areas.

APPROACH: Research must be conducted into the following three policy areas:

- **Impact on the Aviation Community:** This research would involve potential impacts introduced by the variety of D/M systems upon the avionics and other aircraft systems of NAS stakeholders, including military, commercial, recreational, emergency response, and others operating in the NAS. Considerations may include cyber risks, radio frequency interference, kinetic challenges around deployment of mitigation equipment, and more.

- **Impact on Existing Infrastructure:** This research would involve the potential impact of D/M equipment on the NAS and other existing community infrastructure. For example, the ARC discussed how NAS infrastructure may be vulnerable if spectrum frequencies used for air traffic control, position, navigation, timing, and communications are disrupted by D/M technologies. The ARC considers UTM and associated services to be within this realm of vulnerability. Moreover, community infrastructure in congested areas could also be vulnerable if D/M RF emissions “bleed over” into frequencies in use by non-aviation societal functions, such as household items, cell phones, cellular base stations in nearby towers or rooftops, or car navigation.

- **Impact to People on the Ground:** D/M equipment mitigating a drone that subsequently crashes could impact people on the ground. Particularly in populated areas, it is important to consider how the equipment mitigating threats in the air may introduce risks to people and property.

PL4 - Monetary & Non-Monetary Costs of D/M Integration

PL4	**The FAA should account for monetary and non-monetary costs of D/M integration and who will bear costs and externalities.**

INTENT: To ensure that the FAA quantifies and minimizes costs where possible when setting D/M integration policy, including anticipating and addressing potential implementation hurdles.

RATIONALE: Quantifying costs compared to benefits is important for FAA rule promulgation, as well as for the Office of Management & Budget and the Office of Information and Regulatory Affairs. Congressional enactment of any related legislation, while minimizing costs and externalities where feasible, will facilitate implementation.

APPROACH: The FAA will need to consider a range of types of costs and externalities, as well as related issues. Costs may include money spent on the technology itself (including recurring software license fees), integration of D/M technologies into existing workstreams and aviation systems, workforce training, regulatory oversight, and more. Policymakers and stakeholders will need to have an open discussion about who will bear the responsibility, costs, and externalities for D/M equipment. Public safety organizations, state and local governments, the aviation community, professional sports stadiums, telecommunications organizations, and others may all need, or be impacted by, the use of D/M equipment, with corresponding costs. Moreover, as a NAS asset, and in addition to potential equipment costs, implementing D/M systems will require an additional layer of FAA expertise and oversight at minimum, which will incur up-front costs for areas such as new hiring criteria development, hiring an additional class of specialists, regulatory updates, training curriculum development, technical monitoring, maintenance and sustainment coordination, and other indirect costs associated with implementing D/M systems throughout the NAS. Costs to federal agencies, including the FAA, should also be considered. For example, with a decade or more of flat budget resources, the FAA will need to find supporting funding within other programs, thereby potentially prolonging modernization of the NAS infrastructure. This is an indirect but relevant cost to society when NAS modernization is sacrificed for lack of sufficient resources. The challenge of the cost calculus for D/M integration is further complicated by the fact that the effects of D/M technologies have not yet been widely tested in real-world environments.

PL5 - Privacy & Civil Liberties

PL5	**The FAA should work with its federal partners to properly balance D/M end-user safety and security with the privacy, environmental, health, and civil liberties interests of the public.**

INTENT: To avoid privacy, environmental, health, and civil liberties issues arising from the misclassification of legal conduct as a "safety risk."

RATIONALE: If the definition of "safety risk" is unnecessarily broad, enforcement may be discretionary, opening the door for the misuse of safety and security rationales to advance other agendas, such as a desire to block constitutionally protected activities including photography. The ARC acknowledges that there have been instances of different institutions, both governmental and industrial, wishing to block photography in some situations without legitimate legal footing. The ARC recommends that the FAA recognize this dynamic, and that policymakers do not enable institutions to illegitimately utilize security and safety rationales to unjustifiably block constitutionally protected activity.

APPROACH: Checks-and-balances and guardrails may help ensure that rationales like public safety are not used to justify restricting legal UAS activity. To that end, it is important that D/M end-user safety and security is properly balanced with privacy, environmental, health, and civil liberties interests.

PL6 - Strategic Communication

PL6	**The FAA should work with its federal partners, site operators, and other industry stakeholders to develop timely strategic communication plans, allocating roles and responsibilities as needed with respect to engagement and outreach activities. These plans should include direct channels to the public and appropriate timelines to communicate with relevant communities involved in supporting, operating, and using ecosystems that employ D/M technology.**

INTENT: To aid D/M technology integration by taking a proactive role in promoting public acceptance of D/M in a range of circumstances, as well as involvement and understanding among relevant communities.

RATIONALE: A key issue that surfaced in ARC discussions was the need for strategic communication plans to address the changes that will take place due to these new technologies, ensuring that potentially impacted groups and members of the public know what to expect and staying ahead of potential fears and concerns. Public acceptance is key to integrating emerging technology such as D/M into the NAS, as is involvement and understanding from stakeholders in ecosystems which employ D/M. Therefore, authorities and relevant industry stakeholders must ensure they develop and execute robust, timely, and relevant strategic communication plans.

APPROACH: Authorities and relevant industry stakeholders should account for the need for strategic communication from early on in each D/M project or initiative to ensure that they have enough lead time to identify all relevant communities and develop detailed, credible strategic communication plans. Strategic communication plans should also incorporate appropriate timing considerations to ensure that community engagement does not outpace the relevant legal and regulatory approvals. Strategic communication plans should consider incorporating a range of approaches (e.g., outreach to STEM students, educational efforts, and outreach to the UAS user community, allowing community members to report and provide GPS coordinates as part of a national data set) rather than being limited to activities such as town halls, which may not reach all segments of the public. One relevant focus when developing strategic communication plans may be seeking feedback on the public's risk tolerance regarding D/M activities, as balanced with the public benefits of these activities, which may be useful in shaping future communication and outreach approaches.

PL7- Benefits to Security & Law Enforcement

PL7	**The FAA should work with its federal partners to recognize that D/M systems, once properly enabled, will serve as an important tool in the suite of defenses for security and law enforcement, SLTT partners, critical infrastructure owners and operators, and first responders to serve and protect UAS innovation and integration. "Properly enabled" means that authorized protocols include guardrails that balance impacts to surrounding NAS operations, safety, security, and privacy similar to those in current use by regulators that approve large-scale event management.**

INTENT: To recognize the potential benefits D/M systems can provide in security and law enforcement settings and take them into account when developing and implementing C-UAS policies.

RATIONALE: Detection technology will provide many benefits to security and law enforcement, including providing complementary services to UTM, and providing critical infrastructure owners/operators and other end users with knowledge, data, and situational awareness of airspace. Mitigation technology benefits include serving as a deterrent layer of security and enabling safe and secure UAS economic growth by distinguishing and protecting authorized drone operations from unauthorized, nefarious, or careless UAS operations. Balancing a range of interests and impacts to surrounding NAS operations, safety, security, and privacy is required here. The FAA's procedure for considering applications for Temporary Flight Restrictions (TFRs), including for large events, provides a relevant analogy in terms of seeking a similar balance.

APPROACH: The FAA and federal partners should ensure that, where relevant, they account for and enable the benefits that D/M systems can provide to security and law enforcement, SLTT partners, critical infrastructure owners and operators, and first responders.

PL8 - Further Study and Analysis

PL8	**The FAA should commission a cost effectiveness and benefits study to assess the feasibility of mechanisms that improve the ability to differentiate between compliant and non-compliant UAS operations.**

INTENT: To develop and implement practical methods for distinguishing compliant and non-compliant UAS operations to reduce unnecessary mitigation activities and improve the safety of the NAS.

RATIONALE: The ARC believes that the safety of the NAS is enhanced through the minimization of preventable, unnecessary, or erroneous mitigation activities. The ARC supports the safe execution of UAS mitigation when needed and recognizes the potential for mitigation techniques to be conducted safely with minimal risk to persons and property. However, the ARC also believes that avoiding unnecessary mitigation is equally important to NAS safety, especially considering the additional workload associated with non-routine activities. The ability to accurately distinguish between compliant and non-compliant UAS operations will reduce unnecessary mitigation activities and minimize unwarranted threat responses.

The ARC also acknowledges the existing mechanisms that support efforts to distinguish between UAS that present a credible threat and those that may not (e.g., LAANC and Remote ID). However, the ARC also notes that there are emerging mechanisms that could also provide additional benefit, such as implementation of UTM services, and/or modification of Remote ID to include network-based internet transmission (e.g., broadcast or network-based/internet transmission).

APPROACH: The ARC recommends the FAA commission a study to identify and assess existing and emerging technologies that improve the ability to identify and distinguish between compliant and non-compliant UAS operations. The study should consider the effectiveness of these tools, the costs of developing and implementing them, and their anticipated benefit, particularly with respect to reducing unwarranted mitigation activities that jeopardize the safety of the NAS. The ARC believes this research will support investment in D/M system deployment initiatives by both the FAA and industry, and better manage UAS threat response. The findings from the study should be publicly available and include a prioritized list of options based on cost, effectiveness, and safety benefits. The FAA should use the study's findings to take appropriate actions, including issuing guidance material and developing a regulatory framework if needed.

The ARC further recommends the FAA proceed expeditiously to develop a robust C-UAS enterprise architecture, including a conjoined capital investment request that outlines research and development, testing, regulatory infrastructure, system deployment, and other factors that impact UAS integration. The ARC appreciates that this will be a dynamic effort and believes that a D/M enterprise architecture framework that supports an FAA Capital Investment Plan to be an FAA imperative.

PL9 - Title 18 Relief[23] for UAS Mitigation

PL9	**The FAA should work with its federal partners, particularly the DOJ, to identify a clear process and pathway for Title 18 relief for law enforcement officers involved in the mitigation of a UAS.**

INTENT: To provide a degree of Title 18 good faith relief to law enforcement officers who take action to mitigate a UAS that is a clear and imminent threat to life, property, and the public.

Title 18 currently stipulates that punitive measures can be taken for anyone who damages, destroys, or disables aircraft but does not specify any exemption for law enforcement officers taking action against what they have determined, in a good faith effort, to be a nefarious drone.

RATIONALE: While Title 18 relief is debated in Congress, it is anticipated that it may be some time before an official position is taken and there is no clear, effective policy for law enforcement to address real-world hostile UAS threats that exist today. Even if an official Title 18 position is taken, law enforcement across the country may still be faced with the situation of having to address and potentially mitigate a legitimate UAS threat prior to receiving anticipated official and accredited training certification from an approved training authority. Law enforcement officers should not be restricted from acting in the event of an imminent threat to life and property and should not be held to a Title 18 prosecution if they conduct a mitigation that is determined to be reasonable and in good faith with protecting the public.

APPROACH: The FAA, working with partner agencies, should create a concise and understandable procedure with steps of escalation that an official law enforcement officer may take in extraordinary circumstances to address a clear and imminent UAS threat to the public. This procedure should incorporate and adapt existing basic tenets and foundations of law enforcement policy that ensures law enforcement officers are equipped to recognize an extraordinary circumstance, act, and not be prosecuted under Title 18 for good faith efforts to protect the public from harm.[24]

[23] Title 18, U.S.C. - *Crimes and Criminal Procedure*. The main federal criminal code addressing crimes and procedures that fall under federal jurisdiction.

[24] See also Recommendation PL5.

PL10 - Importance of U.S. Leadership

PL10	**The FAA should work with its federal partners to consider the importance of U.S. leadership in this sector.**

INTENT: To ensure that the FAA and federal partners make decisions that facilitate a continued leading role for the U.S. in this sector.

RATIONALE: To date, the U.S. C-UAS marketplace has suffered from the lack of a clear enabling legal framework, impacting funding levels for C-UAS R&D and leading many U.S. companies to research, develop, operate, and sell their technologies and services abroad. This is a national security issue for the United States. A continued strong U.S. role in this industry will help ensure that relevant U.S. stakeholders have access to a full range of C-UAS tools, rather than being limited in what tools are available to them. There are also Congressional concerns about the security implications of using UAS and C-UAS tools originating in certain countries.[25]

APPROACH: The ARC recommends the FAA and federal partners establish a mature legal and policy framework for C-UAS that provides sufficient certainty and flexibility to encourage U.S. companies to develop C-UAS domestically and to seek out U.S. customers.

[25] For example, Senators Warner and Blackburn introduced legislation (Stemming The Operation of Pernicious and Illicit (STOP Illicit) Drones Act) focused on limiting funding to covered foreign entities for any "project related to UAS" which arguably includes C-UAS equipment and operations.

PL11 - Adapting Best Practices & Lessons Learned to Non-Aviation Environments

PL11	**The FAA should work with its federal partners to put forth lessons learned, guidance, recommendations, and best practices for deploying detection systems in non-airport environments.**

INTENT: To adapt existing knowledge and experience regarding the placement and usage of detection systems to non-airport/non-aviation environments.

RATIONALE: Adapting existing practices to non-airport/non-aviation environments will save considerable time, funding, and resources, and enable the FAA to capitalize on proven and established methods.

APPROACH: The FAA should work with relevant federal agencies to develop guidance for the deployment of D/M systems in non-airport/non-aviation environments. The guidance should be based on the existing best practices associated with the deployment of D/M systems in airport settings. While the ARC cannot make recommendations to agencies beyond the FAA, the ARC requests that other federal agencies partner with the FAA to collate and disseminate data and information regarding best practices to end users and stakeholders. This collaboration is intended to be a mutually beneficial knowledge sharing partnership between the FAA and other federal departments and agencies. The ARC further recommends that the FAA create a knowledge management framework to ensure that new information is captured and shared with its federal partners and with the thousands of non-federal end users and stakeholders that may be impacted by UAS operations and D/M technology.

B. Risk Management

The Risk Management section contains recommendations on defining an acceptable level of risk for D/M systems and implementing a safety framework, as well as considering the risks associated with enabling the deployment of D/M systems and establishing operating rules.

RM1 - Safety Framework (Acceptable Level of Risk)

RM1	**The FAA should create an acceptable level of risk and a safety framework for UAS D/M systems and integration.**

INTENT: To establish an Acceptable Level of Risk (ALR) that balances resulting benefits against potential harms.[26]

RATIONALE: The FAA defines risk as the composite of predicted severity and likelihood of the potential effect of a hazard. Hazard is defined as a condition that could foreseeably cause or contribute to an aircraft accident. It is a source of danger. The future impact of a hazard that is not eliminated or controlled is also referred to as risk.[27] The ARC identified multiple risks associated with D/M systems and recommends that the FAA, in partnership with other federal agencies, define an ALR that considers both strategic and tactical risk reductions. Strategic risk reductions are those that are anticipated in the application, planning, and deployment stages, while tactical risk reductions are those that are responded to in operations and during special events. The ARC believes that a balanced approach is essential to risk identification and response and recommends the FAA use UTM/Remote ID/LAANC to reduce the unnecessary use of mitigation capabilities or otherwise interfere with approved UAS operations.

The FAA and other agencies should develop and implement an ALR for D/M systems that is consistent across similar types of systems and operations. The ARC envisions a common set of policies and guidance for D/M system owners and operators, as well as the flexibility to meet the ALR through qualitative or quantitative methods, and/or a hybrid approach. D/M systems vary by location, weather, and other factors, and their performance can fluctuate based on topology, background electronic emissions, physical obstacles, population centers, and many other variables. A single set of rules binding all systems and locations would be untenable. Therefore, a safety framework based on risk level will allow for more flexibility and fewer constraints.

The use of mitigation systems poses inherent risks to aircraft operating in the surrounding area. Notifications to aircraft and operators and risk/liability assumed by mitigation system operators are important to the safety of the NAS. A flood of unaffirmed data can increase risk and create a mischaracterization of the situation that results in an unwarranted response. For example, multiple

[26] The ARC notes that an ALR for UAS operations is also necessary to ensure that D/M systems are used appropriately based on UAS threats. The ARC commends the Adoption and Implementation of a Target Level of Safety (TLS) for Drone Operations being added to the FY23 Portfolio of Goals July 2023.pdf (faa.gov). The ARC also highlights exemptions recently granted for UAS BVLOS operations which contain conditions and limitations (C&L) prescribing the risk mitigations and levels of safety the FAA expects for these types of operations. The C&Ls also include safety data reporting requirements. The FAA will use the safety data obtained through this reporting requirement to establish safety metrics. See Exemptions 19110A and 19111B.

[27] https://www.faa.gov/documentLibrary/media/Order/FAA_Order_8040.4B.pdf.

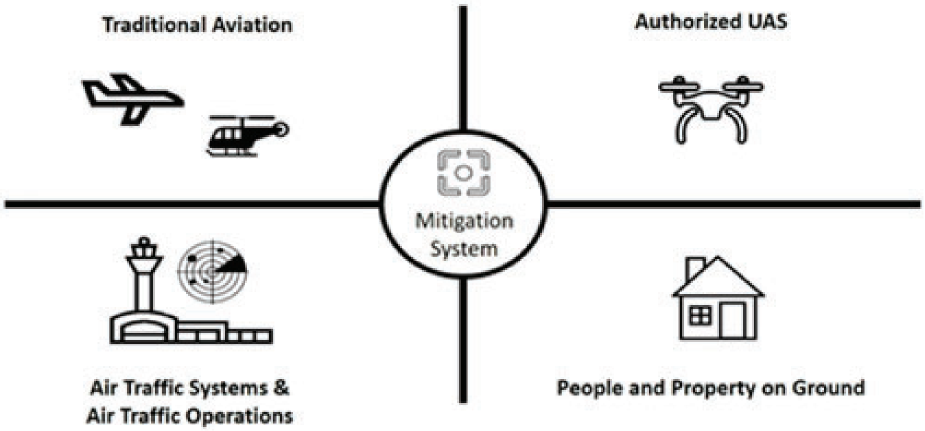
systems with independent sensors each registering a single UAS could appear to be multiple UAS in the same area instead of the same UAS being identified numerous times. This creates a risk of response at a higher threat level than warranted for a single UAS (i.e., artificially high-volume). The FAA should ensure that its ALR approach anticipates these types of anomalies and does not needlessly disrupt lawful and authorized UAS operations (see Recommendations RM2 and SD1).

APPROACH: The ARC determined that a risk-based approach was the most suitable mechanism for assessing the appropriate type of D/M system to be deployed, if at all, in response to a potential UAS threat. The ARC also relied heavily on the Beyond Visual Line of Sight System Requirements and subject matter expertise input to identify three types of risk to the NAS:

- Spectrum interference or non-availability, including and beyond the NAS (e.g., airport lighting, a local cellular network, adjacent hospital equipment, emergency response systems).
- Mitigation systems jeopardizing aviation safety.
- Detection systems providing erroneous information that could lead to an unsafe action and jeopardize aviation safety. It may also create increased workload.

The ARC also identified three types of risk associated with utilization choice:

- Spectrum interference or non-availability related to non-NAS systems.
- Mitigation systems jeopardizing systems, other aircraft (manned and unmanned), people, or property on the ground (including consideration of population density).[28]
- Risk threats and criticality associated with infrastructure based on a security threat as determined by the DHS' *Government Coordinating Council (GCC)*.
  - Is the asset important enough to warrant mitigation authorities and, if so, what type?
  - If mitigation authority is granted, are the previously identified NAS and non-NAS risks addressed?

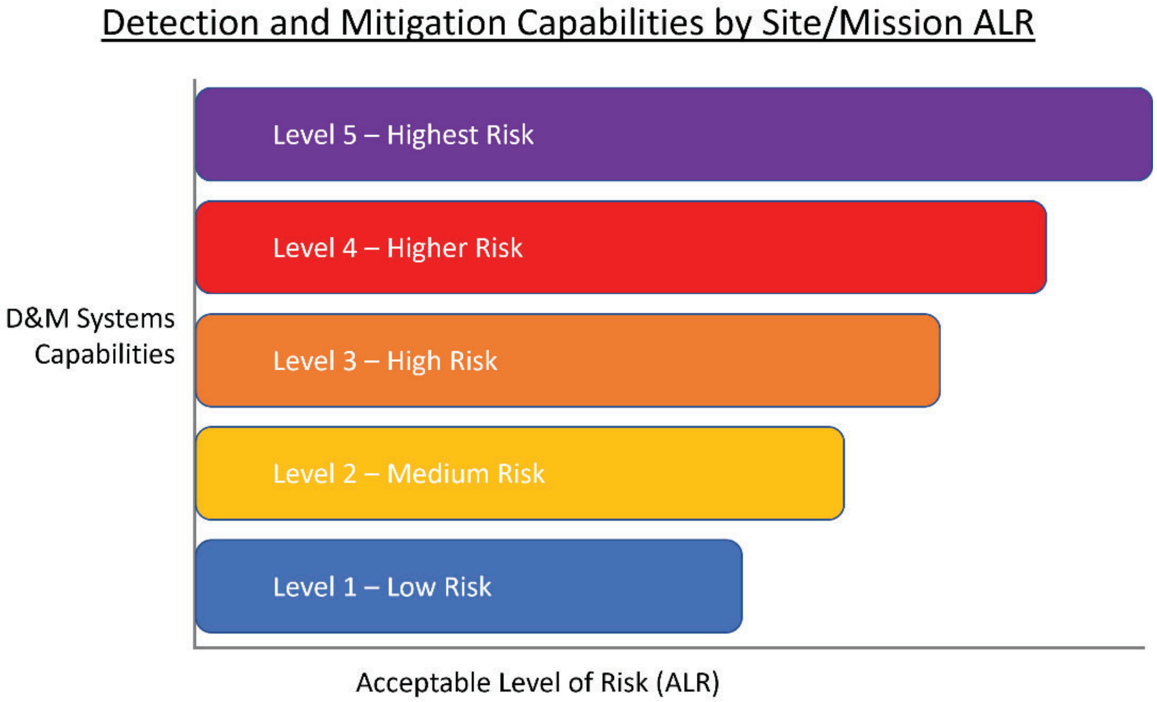

Traditional Aviation
Authorized UAS
Mitigation System
Air Traffic Systems & Air Traffic Operations
People and Property on Ground

[28] Congress has further directed the FAA to "prescribe air traffic regulations on the flight of aircraft (including regulations on safe altitudes)" for navigating, protecting, and identifying aircraft; protecting individuals and property on the ground; using the navigable airspace efficiently; and preventing collision between aircraft, between aircraft and land or water vehicles, and between aircraft and airborne objects. 49 U.S.C. § 40103(b)(2).

The GCC's membership Working Groups span 16 market sectors and coordinate action across agencies. Extending the GCC's scope to manage this coordinated ALR creates a governmental D/M framework for deployment, operations, and adherence. The ARC recommends the FAA coordinate with DHS GCCs to be the primary means to:

- Define risk
- Determine acceptable levels of risk
- Prioritize missions
- Consider cyber concerns
- Ensure operational security parameters can be contained
- Coordinate amongst industry
- Coordinate across agencies

The ARC recommends that guidelines and restrictions be created for each ALR that are best suited for the site/mission-specific level of risk. Approval of C-UAS D/M system, operator certification, operator training, and reporting requirements should follow a risk continuum, aligned with the risk framework, with the goal of meeting the ALR. For example, a site or mission with a Level 3 designation might be prescribed less powerful detection technologies and mitigation capabilities with lower emissions than a Level 4 or Level 5 site. A Level 5 site or mission might be required to adhere to system approval based on risk mitigation and safety plans, and robust and ongoing training for high emissions mitigation systems. Considerations are found in the following table.



Examples of Site or Mission ALR Requirements: [29] This example assumes that all ALR are based on fixed sites or preplanned events, when the reality is that operations may be emergent or mobile and that gatherings can become mass without forewarning.

Site or Mission ALR	Interference Priority	Detection Capabilities	Mitigation Capabilities	Training	Reporting
Level 5	Cannot tolerate interference	No limitations	No limitations	Certificate-based and Continuing	Daily
Level 4	Moderate (5 has priority)	No limitations	Enhanced mitigation	Required and Continuing	Weekly
Level 3	Low (5 and 4 have priority)	Active emitters allowed	Enhanced RF (takeover, interfere)	Required and Continuing	Monthly
Level 2	No	Passive sensors only	RF-only (identify operator)	Required	Quarterly
Level 1	No	Passive sensors only	Restricted	Recommended	Quarterly

Tables are for illustrative purposes only: The ARC was not tasked to define all possible attributes of all UAS systems. Its task was to consider how D/M systems impact NAS safety and make recommendations. The charts are examples only and are by no means exhaustive or complete. They are included only to illustrate how some systems could be categorized.

[29] The ARC believes the determination of how sites or missions are categorized is outside its scope, but factors beyond safety of the NAS, such as proximity to population centers, critical natural and man-made resources, and national security locations, were considered in these examples.

RM2 - Enabling Method Risks

RM2	**The FAA should consider the risks associated with the method it chooses to enable the deployment of D/M systems. Specifically, the different risks associated with whether systems are certified, permitted, authorized, or allowed.**

INTENT: To facilitate a streamlined, timely, and cost-effective method to enable the deployment of D/M systems in a manner that is commensurate with the system's risk and the operational environment.

RATIONALE: Section 383 requires the FAA to formulate a plan to certify, permit, authorize, or allow UAS D/M systems into the NAS. The terms "certify, permit, authorize, and allow" are not legally defined but are interpreted by the FAA in their traditional sense unless legislative intent suggests otherwise. These terms also do not have a defined hierarchy but are usually categorized based on the extent of the associated FAA processes. For example, a product or operation that is "certified" by the FAA will likely have undergone a more rigorous assessment process than a product or operation that is "allowed" by the FAA. Certification is generally viewed as the FAA's most stringent enabling method and is a key tool in how the FAA manages risk through safety assurance.[30] According to the FAA's website, certification provides confidence that a proposed product or operation will meet FAA safety expectations to protect the public and affirms that FAA requirements have been met.[31] The FAA will decide which enabling method is most suitable for deploying D/M systems. However, the ARC advises that the chosen enabling method should correspond to the level of risk, recognizing that risks and burdens will significantly vary based on the system type deployed and the chosen enabling method.

APPROACH: Enabling Method for Detection-Only Systems versus Detection and Mitigation Systems

The ARC anticipates that operators will use a range of different D/M system types. Systems may be detection only, mitigation only, or a combination of both. They may be used in a wide range of environments for a variety of purposes, with some operators prioritizing security of the facility and continuity of operations, while others focus more on protecting the airspace.

Under the existing regulatory scheme, only a limited number of authorized government entities have the authority to mitigate UAS. This is partly due to the excessive threat that an errant or nefarious UAS can create in the NAS, and partly due to the inherent dangers of mitigation. As such, the ARC is firmly of the opinion that mitigation is at the highest level of risk for *whoever* is operating the system and should be enabled in accordance with the FAA processes and procedures that are reserved for that level of risk. Accordingly, the ARC recommends that mitigation systems have an enabling method that is more stringent than the enabling method used for detection-only systems. While both types of systems require an enabling method that provides the FAA with the assurances necessary to honor its safety mission, the ARC considers systems with mitigation capability to require an enabling method of a higher order due to the greater risks associated with mitigation. The ARC further notes that nothing in this report should be interpreted to require an enabling method that generates the need for a federal

[30] Federal Aviation Administration, Certification of Advanced Unmanned Aircraft Systems, available at https://www.faa.gov/uas/advanced_operations/certification.

[31] Id.

action,[32] and the ARC recommends that the FAA adopt enabling methods that are flexible, promote innovation in technological advancements, and appropriately balance benefits with costs (see Recommendation RM1).

[32] This ARC specifically does not intend for any of the contents of this report to constitute a major federal action triggering environmental review under the National Environmental Policy Act (NEPA). National Environmental Policy Act Review Process | U.S. EPA (The NEPA process begins when a federal agency develops a proposal to take a major federal action. These actions are defined at 40 CFR 1508.1).

RM3 - Operating Rules to Minimize Risks

RM3	**The FAA should work with its federal partners to establish operating rules for D/M operators across all sites to minimize risks to the NAS and traditional air traffic operations.**

INTENT: To define operating rules that minimize risk to the NAS.

RATIONALE: Deploying D/M technologies carries varying levels of risk to the NAS and air traffic operations, which necessitates federal standards to better assess these risks and D/M operating rules to minimize collateral impacts in these critical areas.

APPROACH: The FAA should define operational requirements for D/M systems and create a mechanism for systems to be reviewed and certified in order to minimize risk to the NAS and air traffic operations. This would include designating areas deemed too high-risk for D/M technology use and restricting D/M equipment use in those areas.

The FAA should promote, and each site should adopt, a comprehensive UAS response plan. This plan can be developed in a site-specific manner and will determine the appropriate level of technology and information needed by approved D/M operators to address anticipated UAS traffic. At each stage in the Detect, Identify, and Mitigate workflow, D/M operators may have access to a continuum of capabilities that will enable them to properly assess the presence of UAS in proximate airspace.[33] For purposes of the ARC, the workflows are defined as follows:

> Detect. The technological means by which an operator discovers what is determined to be a UAS.
>
> Identify. Electronically accessing information associated with the assignment by the D/M technology (either autonomously or by an operator) of a potential target UAS to a high-level category such as UAS type or group.
>
> Mitigate. When necessary, utilizing appropriate methods to reduce the potential of a detected UAS from interference or harm.[34]

A range of potential capabilities and options reside within each workflow. Some of the options would be considered low-level while other options would be considered high-level. For instance, basic Detection may be satisfied through visual confirmation or accomplished by an array of UAS detection systems (e.g., radio frequency). Identification may consist of sharing a unique UAS identifier with local law enforcement or, in more sensitive cases, additional information may be necessary to quickly discern the potential UAS risk, such as correlated operator and UAS registration/authorization information. Similarly, Mitigation may consist of a low-level intervention, such as a verbal request to the UAS operator to cease operations, or could be accomplished by higher level methods, such as electronically

[33] As stated above Detect, Identify, and Mitigate are recognized actions established under DHS' C-UAS Actions authorities and referenced in the C-UAS Tech Guide's processing chain stages. Counter Unmanned Aircraft Systems (C-UAS) Tech Guide (dhs.gov).

[34] For purposes of the ARC, the terms may be understood to correlate with these DHS definitions with some additional context. This is particularly true with the definition for "Identify", as this term has been expanded beyond the technology aspects of the DHS definitions to include, as appropriate for the facility level of risk, a more complete spectrum of additional information that is available outside of the tactical data transmission focus of the DHS definition and is particularly helpful for the Verified Operator UAS.

disrupting or disabling the UAS. The overall nature of the risk and the facility will determine which option is most appropriate and when capabilities need to be escalated. Recommendations in RM1 related to D/M system capabilities and site or mission ALR requirements should be used to support these determinations.

Beyond these requirements, the industry and FAA should also take other proactive steps to protect the safe and efficient operations of the NAS, specifically:

- Harmonize an open protocol for message routing that supports technical specifications to promote consistency and facilitate systems integration for end users across the NAS (see Recommendation NP2).

- Establish an oversight committee to regularly review the use of D/M technologies and recommend changes to policies or procedures as technology evolves. The oversight committee should be composed of representatives from the FAA, airports, aircraft operators, airlines, relevant national associations, public safety departments, and D/M operators.

C. System Standards

The System Standards section contains recommendations for minimum performance standards for UAS D/M systems and use of existing C-UAS standards organizations. It also includes recommendations for a list of approved D/M technologies and vendors and for detection-only system standards tailored to the airport environment.

ST1 - Minimum Performance Standards

ST1	**The FAA should work with its federal partners and standards organizations to develop minimum performance standards (MPS) for UAS D/M systems in a comprehensive, coordinated manner that supports aviation safety.**

INTENT: To create MPS for UAS D/M systems adopted by all relevant and appropriate agencies and authorities.

RATIONALE: UAS D/M systems should have standard capabilities and a common performance threshold that can be adapted to a variety of environments. As UAS operations in airspace continue to grow and UAS technology continues to mature, there is a need for industry and government to work together to develop standards on D/M technology. A public-private partnership developing consensus among diverse and often competing interests on critical aviation modernization issues in an increasingly global enterprise is imperative.

The ARC recommends the FAA fully engage with the appropriate subject matter experts to quickly adopt standards. The ARC also stresses the importance of distinguishing between standards and specifications. These terms are often used interchangeably, but they represent two different concepts.

- A *standard* is documentation established by consensus of subject matter experts and approved by a standards authority that provides rules, guidelines, or characteristics for activities or their results.
- A *specification* is documentation of a precise requirement or list of requirements, which has not necessarily received approval by an official standards authority.

The ARC considers standards to be most appropriate for D/M integration to ensure they will provide adequate fidelity and support the safe integration of D/M systems into the NAS.

Standards should be robust enough to provide operators with confidence that the systems are safe and fit for purpose, while also being flexible enough to foster innovation and competition. They should prescribe requirements for system performance and contain information about hazards or other limitations to be aware of, such as siting, frequency conflicts, power levels, radar separation to avoid blocking radar range, and other performance characteristics. Standards should also accommodate a range of operational environments and the FAA should be mindful of smaller and less resourced operators when setting MPS. Affordable options should also be approved so that any operator that desires a system has reasonably priced options to choose from and is not priced out of the market. Once standards are set, systems must be vetted to ensure they meet the standard, function as advertised, and are appropriate for the particular environment.

APPROACH: Collaboration between FAA and Other Federal Agencies for MPS - The FAA and its federal partners should work together to create MPS for UAS D/M systems to minimize safety risks to the NAS. The FAA and related federal agencies all have a stake in the safe deployment and use of D/M technologies, but no single agency has full authority or understanding of D/M systems' capabilities and performance in unique environments.[35] The ARC recommends the FAA and partner agencies:

- Support standards bodies establishing a UAS D/M MPS technology categorization framework and consider system monitoring based on technology type.
- Adopt or accept standards bodies UAS D/M MPS.
- Develop a streamlined process to update and adopt new UAS D/M MPS.
- Ensure agencies and standards bodies are coordinating amongst themselves to prevent duplication of work.
- Collaborate with wireless operators, D/M manufacturers, and other stakeholders to minimize interference on systems and enable more efficient spectrum use through FCC and NTIA. For example, coordination with operators near airports where D/M systems may be deployed should those systems interfere with wireless operators.[36]

Collaboration between FAA and Standards Organizations for MPS - The ARC recommends the FAA task RTCA SC-238 Counter UAS (RTCA SC-238)[37] to develop standards to ensure D/M systems continually meet required safety thresholds. The ARC also urges the FAA to continue active participation on the RTCA SC-238 and create risk-based and performance-based MPS recommendations. As advances in technology and safety/threat determinations change, the FAA should make appropriate adjustments to the RTCA SC-238 Charter to reflect these changes. MPS should be Use Case defined and based on DHS' GCC definitions (see Recommendation RM1).

The FAA in conjunction with RTCA SC-238 and other Standards Bodies, such as ASTM and 3rd Generation Partnership Project (3GPP), should also develop MPS related to:

- The efficacy of systems,
- Spectrum emissions and receivers, and
- Interference predicate on known and unknown variables such as: environment, weather, and other factors determined by further testing (possibly resulting in varying minimum performance standards).

The ARC urges the FAA, as part of the RTCA SC-238, to modify terms of reference and applicability to include Use Cases and mitigation as part of the RTCA ARC Charter's[38] scope. The RTCA ARC should reconvene, as necessary, to provide risk-based MPS as advances in technology and safety/threat

[35] See Legal Constraints discussion above at Section VII.A.

[36] IF12046 (congress.gov), Congressional Research Service, *National Spectrum Policy: Interference Issues in the 5G Context* (noting that the "FCC and NTIA coordinate spectrum allocations, which are not perpetual and may be reassigned. By statute (47 U.S.C. § 922), the agencies must meet regularly to conduct joint spectrum planning. They maintain a memorandum of understanding (MOU) setting terms of coordination"). February 14, 2022.

[37] RTCA SC-238 was established on December 6, 2019, and operates as a joint committee with EUROCAE Working Group (WG) 115. *See* https://www.rtca.org/sc-238/ SC-238 collaborates with EUROCAE WG-115 to develop standards C-UAS technology, focusing on detection and mitigation standards to ensure the safe integration of UAS into the aviation ecosystem.

[38] https://www.faa.gov/regulations_policies/rulemaking/committees/documents/media/RTCA%20Charter%20Order1110.77V.pdf.

determinations change. Outputs would include individual systems MPS and system of systems Minimum Aviation System Performance Standards (MASPS). For example:

- A highly populated area may require high safety levels of performance.
- Critical infrastructure may require over-the-horizon capabilities at a certain distance based on industry standards.
- A Core 30[39] airport may require minimum detection by two integrated systems for authentication at a certain distance from a touch down location (vertically), and out to a certain distance beyond the fence line (horizontally). The distances should be set in accordance with industry standards.

Impact of Newly Developed MPS on Existing D/M System Operators

D/M systems have been deployed in a range of environments for several years, and the FAA should consider the impact of newly developed standards on existing D/M system users. Existing systems should be assessed against the minimum standards to determine if they meet the requirements. If an existing system meets the new standards and does not otherwise present a threat to the NAS, it should be allowed to remain in operation for as long as it meets the standards. The ARC does not intend for the new standards to automatically render existing systems obsolete if there is no spectrum interference or other threat to the NAS. However, the ARC also does not intend for systems that do not meet the minimum standards to be "grandfathered" or otherwise allowed to continue operating. Every system, regardless of its current approval status, capability, or purpose must meet the minimum standards set by the FAA to ensure safe integration into the air traffic control and air traffic management systems. Systems that do not meet the minimum standards should be decommissioned, upgraded, or replaced to avoid negatively impacting the NAS.

The ARC acknowledges the impact this may have on some operators but considers this necessary to ensure a baseline level of capability for all systems and minimize anomalies that may arise from incompatible systems. The ARC anticipates that the degrees of incompatibility will vary across existing systems, resulting in the need to disable some systems earlier than others. Thus, the ARC recommends that the FAA establish a transition pathway for non-compliant systems to ensure that they are decommissioned, upgraded, or replaced within a timeframe that is conducive to NAS safety. For systems that will be upgraded or replaced, the FAA should establish reasonable sunset provisions to allow adequate time for users to meet the new standards, similar to the uptake periods allowed for other technologies, such as ADS-B and Remote ID.

It is the ARC's desire that very few operators of existing systems will be required to decommission, upgrade, or replace their systems, but this can only be achieved if the FAA sets standards that include as many existing systems as possible. Standards should be developed based on a range of technologies and complexities so that the vast majority of existing systems will be able to meet them.

[39] Core 30 - ASPMHelp (faa.gov). Core 30 airports are a group of airports in the United States that are considered to be the busiest airports in the country. These airports are used by millions of passengers every year and are critical to the functioning of the national air transportation system.

ST2 - FAA Approved D/M Technologies & Vendors

ST2	**The FAA should work with its federal partners to evaluate and approve a set of D/M technologies from which approved users may select.**

INTENT: To develop a list of approved D/M technologies and vendors allowing operators to select systems in a streamlined and efficient manner.

RATIONALE: Operators should be able to easily identify and select approved D/M technologies and vendors that are proven effective and reliable. FAA evaluation and approval will incorporate safeguards for operators that will contribute to the safety of the NAS, compliant UAS operations, and protection of critical infrastructure.

APPROACH: The ARC considers U.S. government agencies to be best situated to coordinate on evaluation and approval of D/M technologies and systems. The ARC recommends the FAA coordinate with partner agencies to:

- Establish appropriate performance criteria to evaluate and approve each type of D/M technology.
- Create an approved list of vendors and technologies to centralize and streamline the process for entities to choose and acquire D/M technology.
- Work in coordination with DHS to establish and maintain:
    - An anonymous/non-punitive database to capture operational data, performance issues, required updates, and other information for shared use by the participating stakeholders.
    - A D/M approved user and asset location database for shared use by the participating stakeholders.
    - A secure database of all D/M systems, especially those with active emitters and/or mitigation authority to avoid interference between fixed, mobile, or ad hoc D/M systems and navigation/navigation-related equipment.

System capability and performance standards should be prescribed in an FAA Engineering Brief or Advisory Circular. Systems that meet the standard and the corresponding approved vendors would be added to an FAA approved list. The list would essentially be a “menu” of vendors and options for operators to choose from based on what is most compatible with their location and operational needs. The advantages of an FAA approved list is that it creates a catalog of vendors and systems that have been vetted by the FAA in advance and removes the burden on operators to determine system capability and compatibility on site. It also facilitates partnership with other federal agencies that may be required to assist with developing technical standards, such as the FCC or DHS, and streamlines the incorporation of new technology types as systems evolve.

Once a system or vendor is assessed as meeting the standard and added to the FAA’s approved list, it will remain on the list unless there is a substantial change that warrants a review of their status. The ARC notes that a determination of whether a change is substantial or not will vary based on the type of change and the type of technology. However, the ARC’s expectation is that the FAA would make that assessment in accordance with existing guidance material, such as AC 21.101-1B, Establishing the

Certification Basis of Changed Aeronautical Products.[40] System changes that would be considered substantial and requiring FAA review include changing the radar frequency, changing the antenna, or upgrading the equipment such that a new FCC license is required. System changes that would not be considered substantial include updating the system library. The ARC does not intend to require vendors to undergo recurrent assessments or other types of re-validation. Instead, the ARC recommends the FAA rely on usage reports, operator feedback, and other verification methods, such as comparison testing, to confirm that the product functions as it did when originally tested and should remain approved.

[40] AC 21.101-1B, Establishing the Certification Basis of Changed Aeronautical Products, available at https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_21.101-1B.pdf., para. 2.1.2: Changes that require a substantial re-evaluation of the product's compliance findings are referred to as "substantial changes."

ST3 - System Standards – Special Considerations for Airports

ST3	**The FAA should develop detection-only system standards that are tailored to the airport environment.**

INTENT: To ensure that standards are developed based on empirical testing and operational experience in airport environments.

RATIONALE: The Airport Safety and Airspace Hazard Mitigation and Enforcement Program (383 Program) was launched in 2021 to test and evaluate technologies and systems that could detect and mitigate potential safety risks posed by unmanned aircraft at and near airports.[41] The 383 Program tested several technologies, including radar, radio frequency, electro-optical, infrared, acoustic, and combined sensors.[42] The 383 Program has demonstrated that simple systems, such as radar, can be easily incorporated into many airport environments, while other more sophisticated systems are unsuitable for airport use due to interference or other performance characteristics that could negatively impact the NAS. The ARC considers it critical to incorporate these experiential findings into the standards for detection systems that will be used in the airport environment.

The ARC is also mindful of Airport Emergency Plan (AEP) obligations for Part 139 certificated airports and believes that robust and comprehensive standards based on empirical testing will be helpful in this regard. The ARC further notes that under the existing regulatory scheme, airports do not have mitigation authority. Thus, standards based on detection-only operating scenarios will be beneficial to airport system operators, as well as to other system operators that do not have or want mitigation authority.

APPROACH: The ARC recommends that in addition to the standards developed in accordance with Recommendations ST1 and ST2 above, the FAA also partner with a standards organization to develop detection-only system standards based on the 383 Testing Program and other airport-specific empirical data or information to address the unique airport environment and the need to simultaneously protect the airport and the airspace.

[41] https://www.faa.gov/uas/critical_infrastructure/section_383.

[42] Center for the Study of the Drone at Bard College, *Counter-Drone Systems (2nd ed.),* (2019), available at https://dronecenter.bard.edu/files/2019/12/CSD-CUAS-2nd-Edition-Web.pdf.

D. Testing

The Testing section contains recommendations to enable coordination of D/M system testing across relevant stakeholders, including authorizing/delegating third-party testers, system monitoring, and system efficacy testing.

TE1 - D/M Systems Testing in Varied Environments

TE1	**The FAA should work with its federal partners to enable and coordinate D/M systems testing across relevant stakeholders.**

INTENT: To enable broader testing, and better leverage existing testing of D/M systems and components in a variety of real-world environments.

RATIONALE: To comprehensively detail and assess the benefits and costs of D/M technologies, it is necessary to safely enable broader testing while fully leveraging testing opportunities and available testing data. While various federal agencies have been conducting testing, it is often not coordinated across partner agencies and the broader ecosystem, including the private sector.

APPROACH: The FAA and federal partners should seek opportunities to safely expand the ability to test D/M technology within real-life environments. The FAA, TSA, DoD, DHS' Science and Technology Directorate, and other relevant agencies should coordinate testing and share testing opportunities to allow other relevant stakeholders to take advantage of lessons learned, as well as to potentially use testing frameworks in more efficient ways.

TE2 - Testing, Authorization, Monitoring

TE2	**The FAA should work with its federal partners to develop criteria for D/M system and component efficacy testing to be conducted by approved third-party entities.**

INTENT: To approve and support third party testing, authorization, and monitoring for UAS D/M systems to minimize safety risks to the NAS.

RATIONALE: The ARC is mindful that the FAA has limited resources and testing could be significantly delayed if the FAA is the only entity permitted to carry it out. Accordingly, the ARC recommends that the FAA approve and delegate testing authorities to assist with testing systems and approving new technologies. Vendors that want to be on the FAA approved list could have their systems tested by either the FAA or an approved third-party certification company to confirm that they meet FAA specifications. This is consistent with the FAA practice of using third-party companies to assess other types of approved vendors (e.g., airfield lighting equipment). Some ARC members expressed concern about the inherent risks and shortcomings of delegating this type of authority to third parties. However, the ARC believes that the FAA can and must continue to ensure adequate oversight of entities with delegated authority. Third party testing is also necessary because the FAA may not have the availability of requisite expertise to meet the needs should D/M authorities be expanded and bestowed to SLTT entities or private operators in critical infrastructure market segments. Thus, the ARC recommends the FAA ensure system integrity (efficacy) and include third party testing to avoid introducing components or systems whose operation may increase risk to the NAS.

APPROACH: The ARC recommends the FAA work with other U.S. government agencies to create testing environment(s) that document actual D/M system and component performance, and that the information is made available to approved D/M systems operators.

The FAA should engage with FCC and DOJ to establish research-specific field testing outside of current FCC restrictions. The testing should explore fully exercised performance efficacies of D/M systems, including mitigation capabilities. The ARC recommends the FAA approve the following entities for testing, authorization, and monitoring:

- Federally Funded Research Corporations (e.g., MITRE and Aerospace Corp.),
- The FAA William J. Hughes Technical Center independent testers,
- Volpe, and
- The UAS Test Sites as mandated by the FAA Modernization and Reform Act of 2012 (FMRA 2012) and expanded by the FAA Extension, Safety and Security Act of 2016 (FESSA 2016) (Griffiss International Airport, NY; New Mexico State University, NM; North Dakota Department of Commerce, ND; State of Nevada, NV; Texas A&M University Corpus Christi, TX; University of Alaska Fairbanks, AK; Virginia Polytechnic Institute & State University, VA).

Authorized third party testing entities may make test plans, conduct testing, make findings of compliance, and recommend approval of D/M systems and their operations to the FAA. However, the final approval of the D/M systems and their operations should remain with the FAA.

Special Considerations for Detection System Testing in Airport Environments - The ARC is aware of the FAA's reluctance to delegate airport detection system evaluations to third parties due to the sensitive nature of the problems encountered during the 383 Program and their potential impact on the safety of the NAS. Specifically, the 383 Program revealed delicate issues with respect to spectrum compliance and performance, such as radar frequencies operating on a wider band than the vendor advertised or other types of spurious emissions. The FAA has expressed hesitancy in delegating the management of these types of issues to a third party.

There is also concern that an airport operator will not fully know if a system is going to perform in accordance with the standard unless the testing program mimics the 383 Testing Program. However, no company exists today that can mimic the 383 Testing Program, and even if such a company existed in the future, testing in situ is a high-risk activity that should not be delegated. To address these concerns, the ARC recommends the FAA establish testing protocols for airport environments that restrict the types of tests delegated testing authorities can perform. For example, the FAA could delegate testing of detection-only systems and basic technologies (e.g., passive RF or cameras), but not allow delegated testers to evaluate complex systems (e.g., radar) or systems with mitigation capabilities. Limiting the types of systems that delegated authorities can test would ensure that the most sophisticated and complex systems were tested exclusively by the FAA in the airport environment. The ARC considers this sufficient to provide adequate safeguards for the introduction of new and novel technologies into the NAS. The ARC recognizes, however, that even the most basic or technologically benign system can generate complex, or safety sensitive anomalies due to the unique environment in which it is deployed. For example, a passive RF system at a joint-use military airport would prompt a different set of concerns than a passive RF system at a rural airport. While the technology may be identical, the operational environment warrants a different approach. To meet these challenges, the ARC recommends that the FAA identify categories of airports or operational environments that cannot be delegated. For example, the FAA could decide that system testing at Core-30 airports or joint use military airports cannot be conducted by delegated testers and can only be carried out by the FAA. The ARC further recommends that regardless of the technology type or environment, if certain anomalies arise during testing, the delegated tester must terminate the evaluation and refer the assessment to the FAA. An example of an anomaly that might trigger FAA intervention is the airport surface detection radar experiencing interference that has not previously been an issue. The FAA should also establish procedures for testing to be properly socialized so that community members and spectrum users in the area are aware of the tests and able to inform and report on any interference anomalies.

The ARC is sensitive to the argument that limiting delegated testers to certain types of technology or environments defeats the purpose of having delegated testers, which is to decrease the backlog for the FAA and bring technologically advanced products to market faster. However, the ARC expects the universe of technologies that delegated authorities can test to expand rapidly as the FAA and industry gain more experience and confidence with the systems. The complex systems of today will be the basic systems of tomorrow, allowing delegated testers to provide testing support across a broader range of equipment and environments. Therefore, the ARC considers it prudent in these early stages to limit the scope of delegated authority to balance safety concerns against the need to gain experience. The ARC further recognizes that there may be occasions where the FAA needs to partner with a delegated entity to conduct tests that the entity would be prohibited from conducting on its own (e.g., a mitigation system). This may be due to a lack of expertise within the FAA of new cutting-edge technology or other reasons that make the FAA's execution of the testing impractical. The ARC does not intend to hinder the FAA's ability to engage in these partnerships and encourages a flexible approach that allows the tests to be conducted in a safe, timely, and efficient manner.

TE3 - System Efficacy Testing – Special Considerations for Airports

TE3	**The FAA should consider expanding the 383 Testing Program or creating a new program to test the efficacy of systems to an acceptable performance standard to avoid erroneous information that could jeopardize the NAS.**

INTENT: To assess the efficacy of detection systems to build confidence in the information they provide and avoid false alarms or other erroneous information.

RATIONALE: The ARC agrees that accurate data from detection sensors is essential in any environment for operators to assess whether a drone impacts the safety of the NAS. A system that sends erroneous data jeopardizes the NAS because it could result in shutting down an airport, dispatching law enforcement to the wrong location, or taking other actions based on erroneous information. The ARC was advised that the 383 Program did not test the efficacy of detection system output. Instead, its testing was limited to whether the system interferes with spectrum. The ARC asserts that efficacy and spectrum prioritization and interoperability are equally important, and detection systems need to be tested to ensure that they do not provide erroneous information which also creates a threat to the NAS.

Under the current FAA practice, when a UAS detection event occurs, the FAA assesses the circumstances to determine the actions necessary to reduce the risk. Detection equipment information is considered "one source" of information, but it is not the *primary s*ource. Instead, the FAA prefers to obtain visual or other confirmation of the UAS from either the pilot or from someone on the ground. Visual verification is necessary because detection systems have not been tested to confirm their efficacy, so the FAA cannot rely on them for aircraft separation. However, visual verifications are also inaccurate and difficult to obtain in certain conditions (e.g., at night).

The FAA advised that the 383 Program was not intended to confirm that detection systems meet the surveillance requirements necessary for aircraft separation. Rather, it was intended to confirm that there was no spectrum interference that would impact the safety of the NAS. Primary surveillance equipment, such as short-range radars, must meet specific standards for latency, accuracy, and other separation criteria. Secondary systems, like ADS-B, are also required to meet certain separation standards. However, detection systems tested under the 383 Program were not tested to meet specific standards or data points, which is why secondary visual verification is necessary. The FAA cannot make aircraft separation or air traffic flow decisions based on equipment that does not meet the technical separation standards.

System efficacy, performance fidelity, and confidence in a detection system's ability to provide accurate information is extremely important. Bad data can be just as dangerous as no data, and there are human factors concerns associated with repeated false alarms, such as the potential for an operator to ignore the alarm when the threat is valid. Visual confirmation of the UAS detection is not ideal because there are numerous situations where visual verification cannot be confirmed, such as during inclement weather.

APPROACH: The ARC submits that if the primary goal is safe integration of detection systems into the NAS, then the 383 Program should be expanded to include efficacy testing, or a different program should be initiated to test and confirm that detection systems perform to a satisfactory or expected degree. The ARC further recommends that detection system standards have sufficient fidelity such that they can be relied on for higher order tasks, similar to the standards for short-range radars or ADS-B. Detection systems need to be as reliable as technologically possible, and the FAA should require manufacturers to demonstrate that system performance meets an FAA accepted performance standard because erroneous information jeopardizes the NAS.

E. Training

The Training section contains recommendations for training and operational requirements for detection-only system operators, training requirements and completion certifications for designated Identification Data Managers in non-airport environments, and training and certification for personnel performing mitigation functions.

TR1 - Training Requirements

TR1	**The FAA should work with its federal partners to develop and maintain training requirements to ensure the safe deployment of D/M systems across all sites and should differentiate this training based on the needs of the operational environment.**

INTENT: To define training requirements for the safe operation of D/M systems, including a standard that provides a minimum level of qualifications and understanding so that end users across the United States may be interoperable with one another and speak the same language when collaborating for D/M missions.

RATIONALE: Joint agency operations are the normal course of action on a daily basis across the country. All end users must have a common understanding, built through a standard of operation, to successfully execute the D/M mission. A standard of training minimizes risk to the NAS and general public while providing a common framework of understanding across all approved authorities.

APPROACH: Operators should be trained and qualified before deploying D/M systems. Operators of passive detection systems (Category 1) should obtain a basic qualification comparable to a TRUST certificate,[43] while operators of higher-risk technologies like active D/M equipment should acquire more advanced qualifications or authorizations to ensure sufficient understanding of UAS rules and regulations. Additionally, certification requirements should be developed in collaboration with federal partners and SLTT stakeholders for mitigation (Category 3) system operators to ensure they meet minimum federal standards before operating mitigation equipment.

Rather than start from scratch, a common curriculum should be developed from best practices that exist today across the U.S. government and allied nations. These best practices should be synthesized into training modules that build to a training standard that the FAA can accept and authorize for widespread training. Instructors should ensure that students meet the standard and provide confirmation of course completion. The FAA should model its training approach on existing federal agency methods, such as the Federal Bureau of Investigation's (FBI) Hazardous Devices School (HDS). HDS trains all local, state, and federal bomb technicians across the United States to a uniform standard. This ensures consistency of operations, application of authorized techniques, and safety procedures that minimize the public risk as well as the risks to critical infrastructure and first responders. A standardized approach also provides the opportunity to build a culture of safe and proactive end users that enhances joint interoperable missions. A single source of training, continuing education, and recurrency/recertification (as needed) ensures that those designated to perform these duties maintain a high degree of professionalism and maintain currency on emerging threats, technologies, and procedures.

[43] The Recreational UAS Safety Test (TRUST) | Federal Aviation Administration (faa.gov). An aeronautical knowledge and safety test for recreational flyers.

In particular, the FAA should require mitigation personnel to complete training developed by DHS/DOJ as part of the certification process. Although the FAA would not be responsible for delivering the training, they would retain safety oversight by ensuring that the training complies with FAA requirements and is delivered in a manner that ensures ongoing quality of performance. Given the common goals of protecting critical infrastructure facilities, the training and performance criteria should be consistent across all entities vested with mitigation authority. Individuals or entities that have been granted mitigation authority must be fully informed about the range of mitigation measures available to deploy, and which scenarios warrant a mitigation action. It is also critical that they know when and how to escalate issues to the FAA or other relevant authorities to prevent undue harm to compliant operators or bystanders.

Additionally, the ARC recommends requiring equipment-specific training for D/M operators prior to using any D/M technology. An internal training program should be developed based on the equipment manufacturer's recommendations to ensure all relevant personnel are trained on the equipment and associated risks. This training should cover system capabilities, UAS threat identification, legal considerations, privacy concerns, rules of engagement (for mitigation equipment), and risk assessment techniques. To support these efforts, the FAA should update its Risk Management Handbook[44] to include risk mitigation techniques and a UAS D/M risk matrix to provide operators with a resource for standardized risk assessment. The FAA Safety Team should also develop free online courses on passive UAS detection to provide zero cost training for detection system operators.

Prior to operating D/M equipment at fixed-site locations, the ARC also recommends that organizations deploying the equipment provide operators with site-specific training that identifies local air traffic patterns, nearby infrastructure, and risks to property and people on the ground in the surrounding area. This will promote familiarity with their operating environment and improve real-time risk assessments. Mobile D/M operations can present challenges based on the unique locations where they are deployed. Therefore, training should enhance operators' ability to make dynamic airspace assessments and consider the impact of unique terrain or geographical features that could impact D/M equipment performance. The ARC recommends that the FAA provide a checklist with guidance on what areas should be included in site-specific training, including (but not limited to) promoting awareness of permanent flight restrictions, LAANC areas, airspace features (including airports/vertiports/heliports), and drone delivery corridors.

To accomplish this, the FAA should develop training guidelines through public-private partnerships to ensure that personnel performing UAS identification functions at a qualifying facility can access and correctly identify UAS operators. These personnel should have access to reliable sources of information, such as waivers, LAANC data, Certificates of Authorization, Remote ID, aircraft and operator registration, and other approved commercial solutions available in the marketplace. The training objectives should include an in-depth understanding of standardized processes for identifying, reporting, and escalating UAS identity information as needed in a timely manner. Personnel must also be trained in privacy protocols and the facilities must have robust systems in place to protect UAS Identification Data. Finally, the ARC recommends annual recurrent training to be conducted for all authorized D/M equipment operators to ensure they maintain proficiency. Recurring training topics should include the latest developments in the relevant technology, emerging UAS threats, policy changes, and any new legal considerations.

[44] FAA-H-8083-2A, available at https://www.faa.gov/regulationspolicies/handbooksmanuals/risk-management-handbook-faa-h-8083-2a.

F. Data Management

The Data Management section contains recommendations for data sharing, an industry-led data access management system, and correlation of detection information with identification data. It also includes recommendations on a verified operator program, digital forms of airspace information, incentives for Remote ID equipage, and communication on appropriate use and identification of Remote ID.

DM1 - Data Sharing

DM1	**The FAA should establish D/M system data retention protocols.**

INTENT: To ensure that D/M systems only capture information necessary to ensure the safety of the NAS, and only retain that information for as long as reasonably necessary to meet UAS threats.

RATIONALE: D/M systems are capable of capturing a range of information, which may include personally identifiable information (PII) or other types of information that is sensitive in nature. The ARC recommends the FAA establish clear rules prescribing the types of data that D/M systems can acquire, how that data should be secured, and how the data can be shared. Privacy and civil liberties concerns should be key elements of these rules, including a requirement for D/M system operators to complete specific training programs in these areas. This will help ensure legal, responsible, and reasonable data retention and sharing. This will support the critical need to capture UAS operator information while also ensuring that the capability is not overly broad or needlessly intrusive.

APPROACH: The ARC recommends the FAA promulgate rules for retaining and sharing data acquired from D/M systems. The regulatory requirements should be based on how sensitive the data is. For example, D/M technologies should be limited in the types of data they can collect beyond drone telemetry or command and control (C2) information. The FAA should also approve and disseminate guidance about how to recognize and protect PII. PII should be captured only for legitimate stated purposes and closely guarded. Data should be deleted if no longer needed for its stated purpose and should never be shared with sources that cannot guarantee its protection. In contrast, UAS sensor datapoints such as UAS altitude, UAS latitude/longitude, and other non-personally identifiable information should not have data retention or sharing restrictions.

Privacy considerations, civil liberties, and First & Fourth Amendment education should be key considerations in the regulatory framework and incorporated into D/M system operator training and certification to ensure responsible and effective data retention and sharing. Written policies (consistent with law enforcement and other agencies' duties) should also be required to address privacy considerations. Authorizations to perform functions relating to Detection, Identification, or Mitigation, should be rescinded for D/M system operators that repeatedly violate these requirements or otherwise harass or unlawfully interfere with UAS operations.

DM2 - Broader Access to Identification Data & an Industry Led Data Access Management System

DM2	**The FAA should provide greater access to Identification Data and support a decentralized, industry led data access management system.**

INTENT: To establish access to UAS and operator registration and identification information, which will serve as a valuable tool to quickly and more effectively identify UAS.

RATIONALE: The FAA and its partner agencies hold UAS information that can be leveraged to increase situational awareness and security in the NAS. However, security personnel and other entities currently lack access to this information, which prevents them from fulfilling the time-critical responsibility of identifying compliant UAS in the NAS. The ARC recommends that this information, collectively referred to as "Identification Data," [45] should be digitized and appropriately accessible by authorized entities. The ARC notes specifically that Identification Data such as LAANC, Remote ID, and UTM are important tools for C-UAS initiatives, and can augment the Detection, Identification, and Mitigation capabilities for airports, facility operators, and law enforcement officers. Remote ID is particularly useful because it is intended to act as a digital license plate for UAS operators, making it extremely valuable for UAS identification in real time. The ARC asserts that broader access to Identification Data will support UAS threat assessment and NAS safety by potentially avoiding an unwarranted threat response. This is particularly beneficial for UAS operations that are *unintentionally* non-compliant (e.g., "clueless and careless") because the ability to identify and contact the UAS operator could avoid the use of kinetic and non-kinetic mitigation responses.

APPROACH: The ARC recommends that the FAA:

- Provide greater access to Identification Data from multiple data sources, and
- Support industry-led access to Identification Data to improve UAS identification in real time.

<u>Broader Access to Identification Data</u> - The ARC recommends that FAA provide greater access to Identification Data from multiple data sources, including LAANC and Remote ID. Identification Data should be accessible to specifically authorized individuals/entities to more effectively identify proximate UAS. These individuals/entities, hereinafter referred to as Identification Data Managers (IDMs), would have access to current, comprehensive, and digitized information on UAS and operator registration and identification. The degree of access and type of data available to IDMs will vary based on the risks and operational needs of the facility. For example, IDMs at critical infrastructure facilities may have a higher level of access than IDMs at other types of facilities. Similarly, some IDMs will be able to validate the existence and accuracy of certain information, while other IDMs will be able to access and correlate data with basic identifying information from approved detection equipment in situations where a timely response is required.

The FAA should direct and empower IDMs to leverage identity and access management tools when evaluating proximate UAS, including UTM, Broadcast Remote ID, **and** Network Remote ID (should it be available). IDMs should be trained to correctly interpret Identification Data and quickly correlate available

[45] Identification Data is a generic term for government datasets containing information about a UAS operator's identity. The government datasets may contain sensitive or personally identifiable information that would be made available to Identification Data Managers based on their facility's risk level.

information to determine the identity of a UAS that has been detected and remotely identified. This will prevent compliant operations from being misidentified as non-compliant and avoid situations where resources are wasted investigating compliant UAS activities. IDMs should also be trained in privacy and data protection requirements when accessing or exchanging Identification Data.

Industry Led Identification Data Management System – The FAA should support a digital network of UAS registration information. The ARC submits that industry is best positioned to construct and maintain access points and ensure that it is comprehensive and current. The data sets should include basic identifying information associated with an aircraft and provide UAS registration and contact information to be used when necessary (see Recommendation DM3).

DM3 - Detection Correlated with Identification

DM3	**The FAA should ensure that detection information is correlated with identification data whenever possible.**

INTENT: To ensure that D/M systems have the technical and/or operational ability to correlate detection information with UAS identification data to enhance situational awareness and decision making.

RATIONALE: Detect, Identify, and Mitigate are the basic blocks of combatting a UAS threat, and identification is a core component in the rules of engagement. As such, detection information should be correlated with identification data whenever possible to provide accurate information to determine a UAS threat response. Insight from detection information alone is valuable, but information correlated with identification data provides a more robust view of a detection event and will lead to better decision making. The ARC recognizes that the *need* to correlate data will vary based on facility risk, but the *ability* to do so should be a standard feature of D/M systems, and every system should be technically and/or operationally capable of performing this function as needed.

APPROACH: Remote ID provides a means to correlate detection and identification data. The ARC acknowledges that it is not the only method, and that UAS Identification can be accomplished by other means, such as a law enforcement officer positively identifying an operator through in-person communication. The ARC contends, however, that Remote ID is a fundamental tool that can be used to positively identify a UAS and its operator. It is also affordable and capable of integrating with a wide variety of detection systems through application program interfaces (APIs). Thus, the ARC recommends that whenever possible, detection information be correlated with identification data, and that D/M system operators consider utilizing Remote ID (where available) to support these efforts.[46]

[46] Remote Identification of Drones | Federal Aviation Administration (FAA.gov), noting that "[d]rone pilots are expected to comply with the September 16, 2023, compliance date for Remote ID. However, the FAA understands that some drone pilots may not be able to comply because of limited availability of broadcast modules and lack of approved FAA-Recognized Identification Areas. In those instances, the FAA will consider all factors in determining whether to take enforcement action through March 16, 2024."

DM4 - Verified Operator Program

DM4	**The FAA should establish a Verified Operator Program (VOP) to quickly and correctly identify proximate UAS that are VOP qualified.**

INTENT: To create a modern and digitized database, accessed as needed by designated IDMs, in which qualifying UAS operators voluntarily provide identifying information so they can be readily identified in the event of detection.

RATIONALE: Given that the vast majority of UAS operators are lawful, the ARC recommends that a Verified Operator Program (VOP) be created to serve as a repository of operators that have established safety programs and are authorized to conduct legitimate UAS operations. This repository of information will enable D/M system operators to confirm that the UAS is operating as intended (i.e., in accordance with its FAA authorized activities), to more easily and quickly grant these operators access to airspace. A VOP will also help D/M system operators to narrow their focus on potentially disruptive or dangerous UAS activity.

APPROACH: The VOP is intended to be similar to the TSA Pre-Check program where participants voluntarily submit information that is shared with appropriate authorities (e.g., TSA and the FAA). The ARC envisions the FAA would lead the efforts to establish and maintain the program and liaise with other federal partners as needed. VOP qualified operators would be required to meet certain criteria and provide information to the relevant entities. Once granted, VOP status would support a UAS operator's request for increased airspace access whenever possible.

Under the VOP, information would be shared with authorized entities (e.g., FAA and IDMs), and used to provide additional context to UAS operations, while also providing operator identification and contact information.[47] For example, if a VOP qualified UAS was detected, the IDM (or other approved government agency/entity) could use Remote ID (or another approved correlation method) to identify the UAS operator and confirm that their information is in the VOP database. This would expedite UAS identification and assessment of the operation.

Eligibility to participate in the VOP should mirror existing models, such as the DOT Economic Authority, Known Crew Member, and Gateway, and should incorporate an assessment of the operator's managerial competence, safety culture, and overall compliance posture (e.g., regulatory violations or fraudulent activities). These characteristics provide insight into UAS operations and capability on many fronts, and would serve as an appropriate model for VOP eligibility and qualification.

[47] As stated above in Recommendation DM2, the degree of access and the type of data would be based on the facility risk and the IDM's authorization.

DM5 - Digital Forms of Airspace Information

DM5	**The FAA should ensure that digital forms of airspace information are available to the public.**

INTENT: To provide airspace information in a publicly available, digital format that can be accessed by UAS operators and D/M system operators.

RATIONALE: While the majority of UAS operators are compliant, there are a considerable number of non-compliant UAS that operate in restricted areas. Many of these non-compliant operations are unintentional ("clueless and careless"), as opposed to deliberate unlawful behavior. To address this issue, the ARC recommends the FAA provide clear information to the public regarding operations in restricted areas and special use airspace (e.g., TFRs). The ARC further recommends that the information be made available in a digital format for easy access by UAS and D/M system operators as well as the general public. With better and more effective communication, the FAA can significantly reduce the number of UAS operating in restricted airspace near airports, critical infrastructure facilities, or other high-risk areas or events.

APPROACH: As part of its stakeholder engagement efforts, the FAA should highlight flight planning resources and other relevant airspace information that should be referenced when planning UAS operations. These resources should contain information about restricted airspace and the safety implications of violating TFRs. The FAA should also ensure that airspace information is current. For example, the FAA's B4UFLY[48] tool does not consistently list all restricted operating areas, which makes it difficult for UAS operators to be aware of or comply with the restrictions. This lack of clear communication contributes to non-compliant UAS incidents and creates safety concerns for UAS operators and the public, particularly with respect to unscheduled events.

The ARC also emphasizes the importance of modernized FAA systems to improve compliance, and recommends the FAA set a near-term goal of 100% digital TFRs that can be publicly accessed. This is necessary because TFR coordinates can sometimes be incomplete and are often unavailable in a machine-readable format. This hinders the ability to process up-to-date information about airport restrictions, critical infrastructure, or large gatherings. The ARC further notes that TFRs can be rapidly processed by UAS service suppliers and made available to subscribers following guidance from the FAA's UAS Volume Reservations under UTM Pilot Program Phase 1 (UPP).[49] The ARC reiterates that the availability of this information in a digitized format would improve UAS operator compliance.

[48] B4UFLY provides a clear "status" indicator that informs the operator whether it is safe to fly or not. The program is available as a mobile app or as a desktop version to support preflight planning and research. It contains information about controlled airspace, special use airspace, critical infrastructure, and TFRs. B4UFLY App | Federal Aviation Administration (faa.gov).

[49] The UPP was designed to enable the development, testing, and demonstration of a set of UTM capabilities, including sharing of operational intent between operators, establishing a UAS Volume Reservation (UVR) program, and providing access to FAA Enterprise Services to support shared information. Microsoft Word - UPP Summary Report FINAL 20191028.docx (faa.gov).

DM6 - Incentivize Remote ID Equipage

DM6	**The FAA should create a Remote ID incentive program.**

INTENT: To provide financial and operational incentives to increase Remote ID compliance and adoption rates.

RATIONALE: Remote ID compliance is a critical component to UAS Detection and Identification. When the Remote ID Final Rule was adopted, the FAA estimated that the incremental cost to the consumer would range between $20 USD and $50 USD per unit. However, the actual costs have been more than double these estimates, with nearly all Remote ID modules carrying a price tag in excess of $100 USD, and in some cases, exceeding $300 USD. As a result, Remote ID uptake has proven cost prohibitive for many UAS operators, and compliance is not at the expected levels. In addition to the financial barriers, the ARC notes that compliance rates have also languished due to lack of awareness and minimal FAA educational efforts and outreach to the UAS recreational community.

APPROACH: To increase Remote ID compliance, the ARC recommends the FAA create a Remote ID incentive similar to the ADS-B Out initiatives.[50] The Remote ID incentive program should include a rebate program, education campaigns, and public-private partnerships to publicize Remote ID benefits and encourage compliance.

[50] FAA ADS-B Out Rebate Program for General Aviation | Federal Aviation Administration.

DM7 - Use & Interpret Remote ID

DM7	**The FAA should provide information about how to use and interpret Remote ID data.**

INTENT: To clearly communicate Remote ID usage requirements to UAS operators, and provide the UAS community and the general public with information about how to use and interpret Remote ID data.

RATIONALE: The FAA's requirement for non-exempt UAS operators to install Remote ID[51] will aid the detection of proximate UAS. The public can also access basic Remote ID information, so it is important to have sufficient education about how to use and interpret Remote ID data. This will ensure that UAS operators are compliant and will also avoid undue alarm among the general public regarding nearby lawful and authorized UAS operations.

APPROACH: The ARC recommends the FAA provide educational resources about Remote ID installation and usage. The educational campaign may consist of FAA community engagement as well as widely distributed digital information on the FAA website and other industry focused websites. The FAA should also provide adequate training for D/M system operators to perform their duties correctly and effectively. These efforts will provide assurance to the public that the presence of a UAS is not often cause for alarm and that facilities have protections against nefarious actors.

The ARC further recommends that the FAA highlight the potential use of additional detection and identification opportunities for Beyond Visual Line-of-Sight capability to D/M system operators and the general public.

[51] 14 CFR Part 89, Remote Identification of Unmanned Aircraft.

G. System Acquisition

The System Acquisition section contains recommendations on acquisition and use of detection systems and on a structured 7460 process for review and assessment of detection-only systems at airports.

AQ1 - Acquisition & Use of Detection Systems

AQ1	**The FAA should facilitate the voluntary acquisition and use of detection systems in a manner that accommodates rapid technological changes.**

INTENT: To ensure that systems do not become outdated quickly due to technological changes.

RATIONALE: The ARC considers it prudent to assess the various options for acquiring and using detection systems to determine if safety outcomes are impacted by whether a system is leased, purchased as standard equipment, or acquired through a competitive bidding process.

APPROACH: The ARC acknowledges that organizations desiring to deploy D/M systems may not have the resources to purchase systems outright, and that leasing may be the only option. This is especially true when considering how rapidly the technology evolves and the likelihood that better solutions will continue to emerge over time. The ARC also understands that in some cases, multiple systems may be required, such as for a state or regional municipality with multiple airports and/or critical infrastructure facilities that could all benefit from a D/M system. The ARC considers that most entities will probably opt for short term D/M system leases (e.g., two years) to provide an opportunity to test a variety of technology types and upgrade or alter their systems as technology advances. Thus, the ARC supports D/M system acquisition processes that can be easily integrated into existing procurement practices and that do not deviate significantly from how other advanced security and operational technology systems are acquired. D/M system operators will also need to ensure that systems are acquired and operated in accordance with any applicable regulations and guidelines.

<u>Buying v. Leasing</u>

The ARC also considered various methods for acquiring systems and their potential impacts on the safety of the NAS. Specifically, whether detection systems should be purchased or leased, and whether leasing allows users to more easily keep pace with technology changes. Users that are considering purchasing a system outright may be concerned about the system being quickly outdated, while users that are contemplating leasing may be concerned about the ongoing financial burden and increased costs associated with upgrading every few years or when new technology is released. In both cases, there will be security, maintenance, and technical support costs, leaving many potential users grappling with whether to purchase a system and use it until it becomes unusable, or lease a system and periodically upgrade. This decision is also impacted by the technology type. For example, library-based radio frequency systems require frequent library updates, which are more akin to a subscription service; while radar-based systems do not change as frequently, but the changes may be significant, and updates will still be required. Users need to carefully assess their needs to seek cost effective solutions that provide the best capability for the environment, and the FAA needs to provide a range of options with clear information on performance and capability so that operators can make an informed choice.

AIP Funding

The ARC notes that D/M system operators in an airport environment face different challenges with respect to Airport Improvement Program (AIP) funding. The ARC recommends that airports should continue to be permitted to buy or lease systems depending on their budgets and operational priorities. The ARC notes, however, that there are limited federal dollars in the AIP program to support system purchases, and that the existing federal funding model makes leasing systems impossible.

Nearly all U.S. commercial service airports are public agencies with competitive bidding requirements, so it is expected that D/M systems will be acquired in this manner. Detection systems that are eligible for federal grant funding would follow the existing grant application processes, but that process is only available to users that want to *purchase* systems. Under the current AIP requirements[52], AIP dollars cannot be used to *lease* airport equipment. This creates a tremendous financial obstacle for many airports, especially smaller, non-Core 30 airports with budgets that would never allow them to purchase a system and leasing is the only option. The ARC recommends the FAA engage with Congress to amend the legislation so that AIP funding can be used for leasing systems.

The ARC is mindful, however, that even if the statute was amended to allow AIP funded leases, federal AIP dollars are so incredibly oversubscribed that funding would likely not be available. Therefore, the ARC further recommends that the FAA partner with DOT, TSA, and other federal agencies to explore alternative funding sources for airports to acquire systems either through purchase or lease. The financial burden should not rest solely on the airport's shoulders for systems that benefit the NAS as a whole.

State aeronautics agencies interested in supporting the deployment of detection systems across their state should also be considered eligible for AIP funding not only for implementing these systems but also for conducting regional and statewide studies that can lay the groundwork for their implementation. Current mechanisms already allow state aeronautics agencies to receive AIP funding as eligible sponsors, and numerous block grant states effectively manage the AIP program within their jurisdiction. Effective collaboration with local communities, airport sponsors, and non-airport critical infrastructure facilities that stand to gain from a regional or statewide implementation would be critical throughout this process.

[52] https://www.faa.gov/airports/aip/overview.

AQ2 - 7460 Process for Detection System Review at Airport

AQ2	**The FAA should use a structured 7460 evaluation process to review and assess the installation of D/M systems.**

INTENT: To ensure that the 7460 process is structured and enhanced to provide streamlined, cost effective, and timely review and assessment of D/M system installations that could affect the safety of the NAS.

RATIONALE: FAA Form 7460-1 is titled "Notice of Proposed Construction or Alteration" and must be filed by any person proposing construction or alteration that may affect navigable airspace.[53] Filing the form initiates the "7460 process," which is a structured evaluation process for temporary or fixed equipment in an airport environment or in a non-airport environment that could affect the safety of the NAS. The evaluations are necessary to ensure that the proposed equipment, construction, or alteration will not endanger existing airport equipment, critical infrastructure, or otherwise jeopardize the safety of the NAS.

The FAA used the 7460 process to facilitate the deployment of detection-only systems at airports that were pioneering the technology. The 7460 process was also used to support the FAA's 383 Testing Program. This allowed the FAA to obtain information about detection system capability, siting, and performance using its existing notification and review processes. Because the 7460 process had been used to support airports that were early adopters of detection systems, the ARC considered whether the process was suitable for D/M system evaluations going forward (in both airport and non-airport environments), or whether an alternative evaluation method should be used.

APPROACH: The ARC found the 7460 process to be reasonably comprehensive, flexible, and suitable for addressing electronic interference and physical obstructions. However, there were concerns expressed about the lengthy timeframe to complete the process and the level of transparency regarding submission requirements. These concerns prompted the ARC to explore other processes that might be less plagued by timeframe and transparency shortcomings. Specifically, the ARC considered the DoD's Joint C-UAS program, which was established to lead, synchronize, and direct C-UAS activities, and create joint solutions with a common architecture to address current and future emerging UAS threats.[54] However, the ARC concluded that the DoD program was more suitable for military missions and objectives, as opposed to facilitating the airspace analyses that the FAA must complete for temporary or permanent structures that might interfere with navigable airspace. The ARC further determined that developing and implementing a new airspace evaluation process would be duplicative and equally or, in some cases, more difficult to manage. Thus, the ARC recommends that the 7460 airspace evaluation process should continue to be used for D/M system installations provided the FAA continues its efforts to improve transparency and reduce processing time.

The ARC notes that some of the improvement initiatives are already underway, such as the 7460-guidance document issued in June 2023 during the ARC's deliberations. The guidance document contains best practices regarding how to submit UAS D/M system information into the FAA's

[53] https://www.faa.gov/forms/index.cfm/go/document.information/documentID/186273.

[54] U.S. Department of Defense, *Counter-Small Unmanned Aircraft Systems Strategy,* available at https://media.defense.gov/2021/Jan/07/2002561080/-1/-1/0/DEPARTMENT-OF-DEFENSE-COUNTER-SMALL-UNMANNED-AIRCRAFT-SYSTEMS-STRATEGY.pdf (p 11).

Obstruction Evaluation / Airport Airspace Analysis (OE/AAA) portal.[55] The guidance also provides case details, supporting documentation requirements, and preferred presentation formats. The ARC commends the FAA's efforts, noting that one of the stated objectives in the guidance material was to reduce the 7460 processing time to 90 days. The ARC recommends that the FAA evaluate the effectiveness of the guidance material, the related processes and procedures, and staff training to reduce the processing time even further to a maximum of 45 days.

[55] 88 FR 30640.

H. System Deployment (General)

The System Deployment & Integration (General) section contains recommendations on a policy framework for operational requirements and coordination and communication plans for system operations. It also includes recommendations on a scalable framework for airspace density and usage, rules of engagement for D/M operations, and spectrum interference or non-availability.

SD1 - Policy Framework for Operational Requirements

SD1	**The FAA should develop a policy framework that establishes D/M operational requirements to ensure the safe deployment of D/M systems across all sites.**

INTENT: To provide clear direction for facilities on the requirements and process necessary to operate a D/M capability that meets all FAA requirements. This is particularly important since some facilities are not likely to be familiar with FAA requirements and processes.

RATIONALE: D/M technologies, or the methods in which they are utilized, pose risks to the areas in which they are deployed. Training and other operational requirements are necessary to ensure D/M operators safely deploy their systems, with requirements based on the type of technology being used and the level of risk it poses.

APPROACH: The FAA will be instrumental in ensuring that sites have an approval process for all parts of the Detection, Identification, and Mitigation workflow. Several items would need to be considered as part of the compliance determination of the facility operator, such as:

- A determination that the D/M technology does not interfere with NAS systems. This determination could be made by selecting, installing, and operating equipment and systems that have been previously evaluated by the FAA, as determined by Recommendation ST2.
- An assessment of the airspace above the facility and an understanding of all considerations and designations for that airspace with respect to the desired D/M operation by the facility.
- Requiring completion of an FAA-approved training program and, for mitigation personnel, completion of a DHS/DOJ-developed certification program (see Recommendation TR1).
- Implementation of DHS/DOJ-developed normal and non-normal D/M operational procedures that are appropriate for the authorized technology and functions.
- Procedures to prevent mitigation of lawful UAS.

The FAA should approve D/M technologies in one of three established categories based on their associated risks in order to provide standardized training for operators. Category 1 would encompass low-risk technologies, namely passive UAS detection systems.[56] Category 2 would be considered medium-risk and include active detection systems (i.e., radar). Category 3 would be reserved for high-risk technologies such as mitigation systems. Subcategories within these categories may be required based on site location, airspace, and technology type.

[56] DHS CUAS-T-G-1, available at https://www.dhs.gov/sites/default/files/publications/c-uas-tech-guide_final_28feb2020.pdf, for categorizations of detection (passive and active) and mitigation systems.

The FAA should also define site categories for mitigation technology installation based on risk level and proximity to airports. For example, sites that are closer to airports might be in a higher risk category than sites that are further away. Similarly, lower altitude operations would be in a higher risk category than higher altitude operations. Additional factors could also be considered for designating sites under higher risk categories, such as proximity to critical infrastructure or dense urban environments. Non-airport sites such as critical infrastructure that are more vulnerable to UAS threats should have a pathway for designating airspace surrounding the site as restricted areas for UAS operations, especially for unregistered UAS operating below 400 feet AGL.

D/M operators should be required to register their D/M system with the FAA to provide a mechanism for authorizing and overseeing D/M systems in use. Registration information would include the technology category, manufacturer, location, capabilities, and risk level. Category 1 systems could be immediately authorized, while Categories 2 and 3 would require approval based on a risk mitigation and safety plan presented by the operator when registering the system. A national registry, similar to the FAA's Airmen Registry, would also provide a mechanism to track D/M operator compliance.

SD2 - Communication Plans (General)

SD2	**The FAA should require detection system operators to develop a coordination and communication plan for system operations.**

INTENT: To ensure that system operators develop and implement a robust communication plan that accounts for coordination with multiple users, stakeholders, jurisdictional issues, and law enforcement engagement.

RATIONALE: A comprehensive communication plan is essential to ensure coordination between internal and external entities during D/M operations.

APPROACH: The ARC recommends the FAA require a comprehensive cross-communication plan or “open mic” system that allows information to be shared quickly and simultaneously across the full range of stakeholders. The plan must facilitate a coordinated response, ensuring that actual or perceived threats at a location are shared with the system operator and relevant stakeholders. The plan should be tailored to the specific operational environment and be developed following a tabletop exercise where various scenarios are explored, and communication protocols are tested. Standard and consistent phraseology should also be developed and used across all stakeholder groups, including site personnel, first responders, UAS operators, D/M system operators, and members of the public. An FAA developed CONOP would be helpful in this regard.

The communication plan should consider a range of factors, such as site staffing, law enforcement considerations both on and off site, military engagement protocols for co-located facilities, responsibilities to assist and provide mutual aid, and notification for other critical infrastructure facilities, if necessary. The plan should also outline how the site will engage with its federal partners for cases where mitigation is warranted.

SD3 - Scalable Framework for Airspace Density & Usage

SD3	**The FAA should establish and maintain a flexible, scalable regulatory framework that can accommodate increases in airspace density or usage.**

INTENT: To establish a D/M framework that can accommodate the future growth of airspace usage.

RATIONALE: As airspace becomes denser and more complex due to many manned and unmanned aviation initiatives, it will be important for D/M operators to build and maintain situational awareness of and effective coordination with manned and unmanned aircraft operators.

APPROACH: The ARC recommends that the FAA form a standing advisory committee comprised of UAS and C-UAS industry representatives, federal agencies, airport and aircraft operators, community members, and international partners to share best practices and establish common D/M protocols that are scalable. Recognizing that not all geographic regions will experience density increases at the same rate, this diverse committee would ensure a measured approach consistent with varying air density levels across local regions. Achieving a common interoperability protocol for D/M systems could benefit the advisory committee's work and will be necessary to promote safe deployment of UAS D/M strategies as airspace density increases.

Additionally, the ARC recommends that reviews of fixed-site locations with D/M systems be conducted to periodically reassess local traffic density and other relevant attributes. This practice follows existing methods that identify changing conditions over time, such as Joint Vulnerability Assessments that are conducted every three years by the FAA, FBI, and TSA at large airports. Further, the FAA should work with other agencies to maintain a database of UAS breaches in sensitive sites (e.g., airports, critical infrastructure) that can be monitored to determine whether D/M activity is proportionate to the site’s risk profile. The ARC also recommends that the FAA support periodic interagency tabletop exercises anticipating future threats that could arise from increased airspace usage at a particular site.

SD4 - Rules of Engagement for C-UAS Operations

SD4	The FAA should play a role in developing "rules of engagement" for C-UAS operations

INTENT: To obtain input from the FAA on rules of engagement (ROE) for UAS mitigation to protect the safe, lawful use of UAS in the NAS while minimizing any potential collateral effects caused by its deployment.

RATIONALE: Mitigation operations currently present significant challenges and uncertainties around liability and collateral risks. C-UAS operators will require clear, concise guidelines for safe mitigation protocols.

APPROACH: Rules of engagement should ensure that all D/M equipment is vetted for potential collateral impacts. The ARC recommends the FAA collaborate with the FCC to determine mitigation systems' effects on manned and unmanned aircraft and anything aloft in the NAS. These agencies should also collaborate to develop a process for conducting site surveys on fixed-site installations to determine long-term effects and anticipate any changes to the site environment and its risk profile. While ROE are generally considered through the lens of mitigation technology, they may also need to be considered for detection systems that can provide UAS pilot location information, which could lead to law enforcement locating the pilot and requesting a halt to the UAS operation that poses a threat.

The ARC recommends ROEs incorporate a law enforcement style threat assessment approach that weighs the threat posed by a drone against the safety of deploying the mitigation technology. Due to the potential for extremely short timeframes between detection and the need to mitigate, mitigation decisions should rest with a legally authorized, trained, and certified operator who will need to factor in the site environment and system-specific risks.

Prior to engaging in mitigation of UAS, operators should conduct an FAA established C-UAS risk assessment based on standardized scenarios to reduce the risk of collateral impacts to nearby aircraft, infrastructure, and the public. Considerations for threat analysis could include a range of factors, such as whether:[57]

- The operator has determined the UAS is nefarious;
- The UAS is in violation of a TFR;
- The operator believes the UAS poses an imminent threat to the NAS, aircraft (on the ground or in the NAS), airport infrastructure or persons on airport grounds;
- The UAS is impeding with airborne firefighting efforts;
- The UAS is interfering with air ambulance operations;
- The UAS is impeding with law enforcement aviation operations;
- The UAS is interfering with public safety aircraft operations during a search and rescue event or disaster response; ***and/or***
- The mitigated drone's response can be reliably determined.

[57] The following list assumes the proper checks and balances are embedded in the missions of all entities conducting UAS operations such that UAS operators would only be subject to airspace restrictions or risk of mitigation when interfering with legitimate public safety efforts.

Ultimately, due to the inherent risks involved in deploying mitigation technology, the ARC views mitigation as a last-resort option to protect the safety of the NAS, critical infrastructure, or the public. The FAA can take steps to reduce instances where engaging UAS is necessary. Public educational campaigns on legal and proper UAS operations, including fostering awareness of part 107 requirements and Special Government Interest Certificates of Authorization, could curb the number of careless or clueless UAS operators in the NAS. Real time airspace awareness tools (including an easily accessible LAANC database and overlay of authorized flights) and whitelisting[58] known authorized and compliant operations would also help C-UAS operators communicate with drone operators or assess the likelihood that a drone presents a threat.

The ARC also recommends implementing tabletop exercises for mitigation operations. Conducting these exercises will enable local operators to walk through rules of engagement as applied to potential real-world scenarios and improve the likelihood of good decision-making during an actual event.

[58] Whitelisting refers to identifying authorized drones that fly in otherwise restricted airspace. The ARC also notes its recommendations in section VIII.F. above that are intended to educate UAS operators about restricted airspace (DM5), create the ability to identify and contact UAS operators as needed (DM3), and establish a Verified Operator Program (DM4).

SD5 - Spectrum Interference or Non-Availability

SD5	**The FAA should prioritize spectrum usage in coordination with its federal partners and adopt a common lexicon defining the uses of spectrum allocated for D/M purposes.**

INTENT: To ensure FAA harmonization with spectrum allocation protocols to support a fair and manageable approach to spectrum approval and utilization.

RATIONALE: The International Telecommunication Union (ITU) defines radiodetermination spectrum for navigation as a safety service and distinct from allocations for more general radiolocation.[59] These definitions have been adopted under U.S. regulations by both the FCC and National Telecommunications and Information Administration (NTIA), but not by the FAA. This hinders the ability to create a hierarchy for spectrum approval and utilization. This situation is further exacerbated by the fact that, in some cases:

- D/M components may also be consumers and interrogators of the radio frequency spectrum:
- D/M components, such as radar, include active emitters in the granted spectrum allocation(s), and
- Permission for D/M system radar is sourced from the same spectrum allocation as ground station radar for UAS (in all cases).

APPROACH: The ARC recommends the FAA adopt the definitions that have been adopted by both the FCC and NTIA and included in other U.S. regulations.[60] The ARC further recommends FAA, FCC, and NTIA incorporate the following approval definitions related to spectrum allocation:

Radionavigation Approval (Relative to D/M and UAS integration) is an allocation for detection systems that are used for separation assurance; including for dual-purpose use—UAS integration as well as detection of non-cooperative aircraft.

Radiolocation Approval (Relative to D/M and UAS integration) is an allocation for detection systems that are exclusively used for detection of non-cooperative aircraft (i.e., no separation assurance).

The ARC also recommends GCC prioritize spectrum approval based on criteria other than "first-come-first serve" to include UAS integration and D/M activities.

[59] ITU Radio Regulations, 2020 Edition https://www.itu.int/en/publications/ITU-R/pages/publications.aspx?parent=R-REG-RR-2020&media=electronic.

[60] 47 CFR § 2.1.

I. System Deployment – Airports

This section contains recommendations that are specific to airport environments. As such, the recommendations are limited to detection-only systems because under the existing regulatory scheme, airports do not have mitigation authority.[61] The ARC clarifies that it is not opposed to mitigation authority for airports, but limited its recommendations to detection-only systems to remain consistent with the current mitigation authorities. The ARC notes that mitigation at airports, as at any other location, would need to be properly negotiated and coordinated in advance with the authorized entities, ATC, and any co-located users (e.g., military installations). This could be achieved through CONOPs and should include procedures for escalating the threat as well as for communicating when the threat has been contained and operations can be restored.

The System Deployment – Airports section contains recommendations for clarification that detection systems are optional in the airport environment, protocols for D/M system interoperability, and airport and airspace boundaries. It also includes recommendations on training and operational requirements for detection-only systems, communication plans for the airport environment, empowering the correct entity to perform monitoring and response functions, guidance and updates to operational procedures at airports that will allow for the safe deployment of C-UAS equipment, and federal liability immunity protections for airport operators.

AP1 - D/M Systems Should be Optional in the Airport Environment

AP1	**The FAA should clarify that detection systems are not mandatory in the airport environment.**

INTENT: To clarify that detection systems are voluntary for airports, even though they are included in an AEP or a Drone Response Plan (DRP).

RATIONALE: Operators in an airport environment should be allowed, but not required, to obtain and use detection systems to assist with responding to UAS incidents, securing critical airport infrastructure, and ensuring continuity of operations. The detection system procedures should be consistent with FAA requirements and other airport practices.

Detection systems are currently optional in the airport environment, and the ARC acknowledges the FAA's present assurances that they will remain so. However, even if the FAA never mandates detection systems at airports, the ARC contends that the existing regulatory requirements for certificated airport operators who voluntarily deploy systems, have largely the same effect.

Under Part 139, certificated airport operators are required to have an AEP and a DRP. The plans must describe how a detection system will be used in the airport environment, even if the system is voluntarily deployed. Some ARC members are concerned that the mandatory requirement to incorporate the voluntary system into the AEP/DRP has the practical effect of making the system itself regulated, despite its optional deployment. Indeed, an airport operator that deviates from its AEP/DRP with respect to a voluntarily deployed detection system could be subject to FAA enforcement action.

[61] Congress has exclusively authorized the DoD, DOE, DOJ, and DHS to engage in limited UAS D/M activities to address UAS presenting a credible threat to covered facilities or assets. 10 U.S.C. § 130i, 50 U.S.C. § 2661, and 6 U.S.C. § 124n.

When this concern was shared with the FAA during the ARC's deliberations, the response was that certificated airport operators have always been required to comply with their AEP/DRPs, and the inclusion of a detection system would not alter that. Moreover, airport operators are empowered to draft their plans in a way that unambiguously demonstrates that the systems are not compulsory. For example, the plans could state that the system will only be operated during business hours or that the system will be checked twice per day by the airport manager at the start and end of the shift. Therefore, while it is true that the airport operator would be required to include the system in the plans, the airport operator is free to establish system protocols that are as onerous or effortless as the airport operator sees fit. The FAA further advised that it does not currently mandate specific requirements for how the systems should be monitored or operated, and there is no intent to do so in the future. The FAA only requires the operator to document how it intends to safely incorporate a system into its operations and to follow that documented process.

Some members of the ARC countered that the inclusion of a voluntary system into the mandatory plan does constitute a departure from the status quo because for all other activities in an AEP/DRP, the airport manager has responsibility ***and authority*** to manage the activity from beginning to end. This is not the case for detection system operations where much of what happens following a detection event is beyond the airport operator's control, legal authority, and in some cases, beyond the airport operator's knowledge. Indeed, jurisdictional restrictions may prohibit the airport operator from dispatching law enforcement to respond to a detection event, or ATC may be engaged for real time aircraft deconfliction, neither of which are within the airport manager's control. Thus, the concern remains that incorporating the detection system into the mandatory plans will inevitably create obligations that the airport cannot practically meet. Moreover, while the ARC members may agree with the FAA's assertion that, *theoretically,* plans can be drafted to limit the airport's responsibilities, the limitation may be insufficient to shield the airport from liability.

APPROACH: For these reasons, the ARC recommends that the FAA confirm (as it did with the SMS rule) that it does not intend the integration of detection systems at airports to create or modify state tort liability law, create a private right of action under federal or state law, or otherwise subject airport operators to certificate action or civil penalty. The ARC considers this "liability caveat" necessary to minimize liability concerns that may cause airports to refrain from deploying systems, and to clarify that no new or additional grounds for liability should arise under *federal or state law* as a result of the FAA's actions in this space. [62]

In addition to liability concerns from a state and local law perspective, the ARC also challenges potential FAA enforcement actions for voluntarily deployed detection systems. Unlike detection system users in non-airport environments, airport system operators face potential FAA enforcement action for their systems, making the deployment of a system in an airport environment one of the few activities where voluntary actions undertaken to improve safety can be penalized. Moreover, airport operators that voluntarily deploy a system can face certificate action and civil penalties for deviating from the voluntary aspects in their AEP, *even if no harm occurs*, because the deviation itself could constitute a violation of the Federal Aviation Regulations. [63]

[62] The ARC acknowledges that the FAA is jurisdictionally limited to enforcing its own regulations and can offer no opinion on an airport's liability exposure under federal or state law. However, the ARC considers the liability caveat to be necessary, and notes that it is consistent with language the FAA used in other rulemaking initiatives. https://www.federalregister.gov/d/2016-16596/p-217.

[63] 14 CFR 139.325.

To be clear, the ARC recognizes that detection systems need to be regulated by the FAA to ensure the safety of the NAS. The ARC does not object to an airport operator being required to comply with the 7460 process, nor does the ARC object to an airport operator documenting the type of detection system that will be used at the airport in the AEP. As noted above, airspace evaluations under the 7460 process, as well as siting, interference, and other safety concerns warrant FAA surveillance of airport-based detection systems. What the ARC objects to, however, is airport operators potentially facing an FAA enforcement action for a voluntary system simply because there is a safety need to include the voluntary system in the AEP. In the ARC's view, a better approach would be a framework that provides all of the safety benefits associated with having a system while removing the liability concerns for operators and the reluctance to voluntarily assume additional FAA obligations. To that end, the ARC recommends that if an airport voluntarily deploys a system, everything about that system from an FAA regulatory perspective should also be voluntary to the greatest extent possible. Again, the ARC recognizes that there are certain laws and rules that the airport would always have to follow for safety, security, or privacy purposes, but the system, processes, and procedures should not be "mandated" or "regulated" by virtue of the AEP.[64]

This is not to suggest that there is less commitment on the part of airports to follow safety procedures. It simply means that the airport operators should not face additional enforcement jeopardy because their system is at an airport. Taking this regulatory posture incentivizes airport operators to deploy systems, provides adequate FAA oversight, and ensures that airspace safety considerations are addressed, while eliminating the FAA enforcement concerns for airport operators. This will also level the playing field between airport and non-airport operators that are operating the same systems with only the airport operators being subject to FAA enforcement action.

[64] See also Recommendation AP8 discussing federal liability immunity for voluntarily deployed detection systems.

AP2 - Protocols for D/M System Interoperability

AP2	**The FAA should establish interoperability protocols for situations where more than one entity has a D/M system in or around the same airport environment.**

INTENT: To establish a hierarchy of systems that avoids interference and supports interoperability.

RATIONALE: Where an airport has deployed a D/M system and one or more other entities (e.g., DoD, TSA) have also deployed a system, the airport should incorporate prioritization and interoperability protocols into their AEPs that are appropriate for the unique environment and facilities. The airport will need to work collaboratively with other authorized entities to develop a comprehensive plan that addresses the concerns of all stakeholders. FAA support may be required to assist airports as they engage with federal partners or other authorized entities to ensure that detection system procedures are consistent with FAA requirements and other airport practices. A detailed system that establishes a hierarchy and protocols is especially necessary for entities that are not subject to the Federal Aviation Regulations.

APPROACH: There is no "one size fits all" approach to safely implementing multi-system operations in an airport environment, and the ARC does not want to be overly prescriptive about how airports should achieve this objective. However, the ARC believes that there are some universal factors that should be considered appropriate for each airport, recognizing that it will be highly dependent on how the roles and responsibilities for UAS detection are allocated. They include:

- Hazards associated with the type of UAS operations, such as proximity to critical airport infrastructure, passenger safety, security risks, and the potential impact on air traffic operations.
- Capabilities and coverage areas of the different D/M systems deployed by various entities, including range, accuracy, response time, and mitigation effectiveness. Consideration should be given to limiting D/M system operations within a certain distance of the airport (e.g., five miles).
- AEP requirements for certificated airports and airport system protocols, specifically regarding information sharing or data exchange, system interoperability, threat prioritization, and threat resolution. Systems must be linked for communication and able to be handed off to other detection sectors.
- Personnel training on the D/M system and the specific airport procedures.
- FAA ATC procedures for sharing potentially sensitive data with operators of authorized UAS operations and deconfliction procedures with crewed aircraft.

a. Is one system trusted more than the other?

The ARC considered the safety concerns associated with creating a trust hierarchy in multi-system environments. Some ARC members believed that the D/M system operated by the airport should be the most trusted system with the highest priority, while other members believed that prioritizing systems equally provides the most comprehensive operating picture and a broader information base for better decision making. Where members agree is on the need to develop response plans that are tailored to the unique needs of the airport and contain protocols to manage conflicting information from multiple systems. ARC members also emphasized the importance of working collaboratively with non-airport entities, especially those over whom the airport has limited influence or control (e.g., military, SLTT). Coordination with these entities will be essential in creating a response plan and procedures for assessing the reliability of information and ensuring its proper dissemination. The ARC also noted that, regardless of priority, only systems that meet minimum standards should be accepted in the airport environment.

b. Are detection alarms from systems shared?

The ARC generally agrees that alarms from D/M systems should be shared among the various stakeholders in a multi-system environment. However, the ARC stresses the importance of adequately assessing the reliability of an alarm/alert before sharing it with a wider audience. There is a strong desire to avoid the panic and eventual complacency that develops from repeated “false alarms.” The alarm should be tagged to the specific UAS whenever possible and should continue alerting until the matter is resolved.

c. How are potential interference issues addressed?

- Systems should be tested for the specific airport environment, weather, terrain, aircraft systems, and potential interference from buildings or other structures near the airport.
- UAS Response Plans should include mitigation measures for potential risks and should incorporate recommendations from the Blue Ribbon Task Force on UAS Mitigation at Airports.[65]
- If multiple systems are in place, each should have direct communication with each other and ATC. If safe to deploy, each should follow their directives on training and mitigation while communicating intent with ATC and other system users.
- Potential electromagnetic interference issues must be evaluated and resolved prior to deployment.
- Interference questions and issues should be addressed through the standards development process. The detection system installation specifications should be defined to remove the interference issues prior to operation. If interference issues arise after installation, the detection system should be recalibrated to resolve the interference or undergo a new 7460 process to identify if subsequent construction will cause interference. An operator may also be required to complete a frequency interoperability assessment or process if the interference constitutes a substantial change.[66] This is most likely to occur with system upgrades or changes that alter the operational frequency band or otherwise create interference where none previously existed.

[65] https://uasmitigationatairports.org/wp-content/uploads/2019/10/BRTF-Report2019.pdf, 2019.

[66] See discussion of substantial changes in ST2 above.

AP3 - Airport & Airspace Boundaries

AP3	**The FAA should set the standards for detection systems in the airport environment to ensure that the systems are able to detect UAS from the area immediately inside the airport fence line out to a specified radius around the airport property that provides sufficient time to respond to UAS threats.**

INTENT: To ensure that detection systems have sufficient capability to detect UAS in the critical areas of the airport environment, including the airport perimeter and the Air Operations Area (AOA) to promote the safety of the NAS, the security of the airport facility, and continuity of operations.

RATIONALE: The goal of every detection system is to:

- Obtain information about UAS traffic in the area; and
- Develop a plan to relay that information to the person or entity ultimately responsible for threat management and incident response.

To achieve this goal, detection system operators will need to determine which areas they intend to monitor to obtain the most pertinent information. For operators in the airport environment, this means assessing the airport boundary, the volume of airspace, and how far the detection range needs to be to avoid negatively impacting the NAS and ensure that there will be sufficient time to effectively engage with the UAS as needed.

APPROACH: The ARC recommends that the detection range for D/M systems in the airport environment be able to detect UAS from the immediate area inside the airport fence line out to a distance that encompasses the critical areas of the airport property. The ARC acknowledges that these distances will vary across airports. For example, the area inside the fence line will be very large for some airports (e.g., Denver International Airport) and very small for others (e.g., Chicago Midway International Airport). However, for all systems, the detection range should include at a minimum the AOA, final approach fixes, and the departure corridors.

The ARC clarifies that the recommended detection range requirements are intended to prescribe the system's capability, not the airport's responsibility. The system operator may desire to monitor a wider radius or a smaller radius depending on why the system was deployed; but the system itself should be able to detect out to the critical areas of the airport.

In considering what should constitute the "airport environment" for monitoring, the ARC drew upon other airport activities that require similar boundary determinations, such as avian radar for wildlife management. The ARC noted that, similar to detection systems, avian radar is not intended to provide direct wildlife mitigation. Instead, it is used for indirect mitigation to establish wildlife flight patterns and increase the effectiveness of wildlife mitigation programs. Detection systems could serve a similar purpose in identifying areas where UAS activity is most prevalent so that those areas could be more closely monitored. Once the primary monitoring areas are identified, they could be further classified as high, medium, or low risk to ensure resources are appropriately allocated. This would essentially establish a risk continuum for areas to be monitored in the airport environment, which is consistent with recommendations made by the RTCA and EUROCAE in their standards document entitled RTCA DO-

403 / EUROCAE ED-322 “System Performance and Interoperability Requirements for Non-Cooperative UAS Detection Systems”.[67] Section 4 of the report classifies “airport critical zones” as high criticality, medium criticality, and low criticality. High Impact areas are inside the airport perimeter. Medium Impact areas are within the airport boundary and extend to the take-off climb/approach flight segments, and Low Impact areas are near the airport boundary or in areas where the likelihood or severity of a drone disruption is minimal. These boundaries align with the ARC’s recommendations for defining the airport environment, which allows the operator to determine who should be responsible for executing certain functions in that environment.

The ARC clarifies that it does not intend the installation of an airport detection system to imply responsibility for engaging in any kind of mitigation. However, the ARC is sensitive to the fact that when a system is deployed, there will be some consideration given to how the operator should respond to a detection. The ARC recognizes that each airport will need to decide whether and how it will respond to a detection event, and that “mitigation” can have a broad range of meanings – from something as simple as dispatching law enforcement to an offending operator’s location, to something far more complex, such as engaging with federal partners for kinetic or electronic UAS interdiction. Whatever the airport decides to do, it must ensure that it is within their authority to do it. Therefore, the ARC was careful to consider the airport’s jurisdictional authority when recommending the range of areas to be monitored.

Jurisdictional authority varies across airport facilities and can be difficult for some airport operators to manage. For example, at some airports, the airport law enforcement officers have “off airport” jurisdiction, making it easier for them to engage with offending UAS operators. At other airports, however, the airport police do not have jurisdiction outside of the airport so offending UAS operators are managed by local law enforcement. This can be challenging because the safety of the NAS may be a lower priority for non-airport first responders due to the other criminal matters competing for their resources and attention. Moreover, many local law enforcement entities may not appreciate the severe and immediate threat that an unauthorized UAS can present in the airport environment, and in some cases, may be dismissive of the threat or lack the staff to prioritize the threat even if they do appreciate the danger. This is especially so for smaller airports or in cities with limited law enforcement personnel.[68] From the airport’s perspective, the person or entity responding to the detection event should have the ability and authority to execute the actions necessary to meet the threat, including aircraft deconfliction and UAS interdiction if required. The ARC’s specific recommendations on this matter are more fully explained below in Recommendation AP6.

[67] *ED-322 - System Performance and Interoperability Requirements for Non-Cooperative UAS Detection Systems - Eurocae,* December 2023 available at https://www.eurocae.net/news/posts/2023/december/ed-322-system-performance-and-interoperability-requirements-for-non-cooperative-uas-detection-systems/.

[68] For instance, the Airport Use Case scenario evaluated by the ARC dealt with a small town with just two officers in the police force, often (depending on the time of day) with only one officer on duty. See Appendix D for more information on the ARC's Use Cases.

AP4 - Training & Operational Requirements for Detection-Only Systems/Airports

AP4	**The FAA should establish training and operational requirements for detection-only system operators**

INTENT: To ensure that operators of detection-only systems are adequately trained in the equipment and operational environment for detection-only systems.

RATIONALE: The ARC seeks to avoid unnecessarily constraining the pool of potential detection-only system operators, allowing a broad range of people to operate the systems provided they are appropriately trained.

APPROACH: The ARC recommends that the FAA allow any appropriately trained person to operate a detection-only system, including airport staff, law enforcement personnel, and contractors. The training should be tailored to the specific system and airport to ensure that the operator is well versed in the airport environment and procedures as well as the functionality and capability of the system. The training should also include detailed instructions on appropriate escalation procedures that focus on ensuring critical information is relayed efficiently to all relevant stakeholders in a timely manner. System operators should also be trained in low-level intervention or mitigation techniques, such as dispatching law enforcement to the UAS operator's location, if needed.

While the ARC encourages a broad range of individuals being allowed to operate detection-only systems in the airport environment, the ARC recognizes that training requirements will vary based on who is operating the system and the primary purpose for the system's deployment. For example, the training provided to an airport operator will likely differ from the training provided to law enforcement personnel or a similar security related organization. In airports where the system is deployed primarily for airport security purposes, the training would likely emphasize the law enforcement aspects of a monitoring program, to ensure appropriate and lawful engagement with offending UAS operators. In these airport environments, the monitoring program could include fixed-site systems and mobile systems equipped with a portable detection device allowing a law enforcement team to be deployed to respond to UAS sightings. In contrast, if the system is deployed for airspace management purposes, the training would likely prioritize escalation protocols and appropriate engagement with ATC. In these airports, the system would typically be operated by airspace management operations personnel with a display or mobile device that receives the detection. The operations personnel would then follow the standard operating procedures to escalate the issue for others to respond.

Considering these varied training needs, the ARC recommends system operators be allowed great flexibility in determining what is appropriate for their airport. The FAA should provide basic guidelines, such as that training and maintenance programs should be in writing or have different levels based on the technology of the products or the complexity of the system, but the airport should be allowed to develop a training program that is suitable for its needs. The ARC emphasizes that systems should be bespoke in nature, focusing on a specific operator, the specific type of equipment or technology, and the specific airport environment. The ARC discourages off-the-shelf training packages that do not adequately address the unique needs of the operating environment.

AP5 - Communication Plans (Airport)

AP5	**The FAA should require detection system operators to develop a communication plan that addresses the unique airport operational environment.**

INTENT: To establish communication plans and SOPs for the airport environment that are jointly crafted with ATC and other stakeholders in the airport environment.

RATIONALE: Recommendation SD2 above is the ARC's recommendation for communication plans for system operators. It contains guidelines that are generally applicable to most operating environments. However, the ARC considers it prudent to also recommend communication protocols specifically for the airport environment due to the need for system operators to engage with the airport and ATC to simultaneously protect both the airport and the airspace. An airport-specific recommendation is also needed because the communication plan for a Part 139 certificated airport operator will be included in the airport's AEP, and thus, subject to regulatory oversight and, as proposed by the ARC, not subject to enforcement.

APPROACH: Consistent with Recommendation SD2, the ARC reiterates the need for a comprehensive communication plan based on tabletop exercises and an FAA CONOP. The plan should:

- comply with relevant regulations,
- contain standard and consistent phraseology,
- include notification requirements for other critical infrastructure, and
- contain escalation protocols to engage with federal mitigation authorities, if required.

The ARC acknowledges, however, that in some cases, an airport may have limited influence over other entities or an inability to require them to comply with an AEP. Thus, the FAA should support the efforts of system operators in airport environments to engage with other federal and local entities, including TSA, FAA, local law enforcement, or military installations for co-located airports. Memorandums of understanding (MOU) should also be executed between the airport and these entities, specifically the entities that are not subject to FAA requirements. Executing an MOU will make the non-aviation parties aware of the airport's obligations with a view toward securing their cooperation in assisting the airport to meet FAA requirements.

In addition, the communication plan must allow for a coordinated response, ensuring that actual or perceived threats at the airport are jointly shared by the system operator with the airport and with ATC. The plan should be incorporated into ATC's SOPs as well as into the airport's AEP and other response plans. The plan should also highlight how notifications will occur for authorized operations, such as runway inspections using UAS or UAS deployed for wildlife mitigation. The plan should be renewed on a regular basis and updated whenever new equipment is installed at the airport, or new airport tenants/users are added.

AP6 - Monitoring & Response are ANSP Functions

AP6	**The FAA should work with its federal partners to empower the correct entity to perform the ANSP functions of monitoring detection systems and responding to UAS threats in the airport environment.**

INTENT: To ensure that the person or entity monitoring a detection system has the ability and authority to appropriately respond to a detection event and execute all of the actions necessary to meet an immediate threat.

RATIONALE: One of the ARC's tasks is to "identify gaps in existing airspace management tools and provide options for the FAA to alleviate secondary impacts of UAS detection and mitigation systems on the safe and efficient operation of the NAS."[69] The ARC has identified a "gap in the airspace management tools" with respect to monitoring detection systems and responding to a UAS detection event in the airport environment. The gap exists because currently, neither airports nor air traffic controllers are tasked or equipped to perform both of these functions. As more fully explained below, this is due to a range of factors, including limited access to information and liability concerns.

Controlling the Airspace v. Controlling the Airport

Airport managers at towered airports have a partnership with ATC. The airport manager is primarily responsible for the airport environment and ATC is primarily responsible for the safety and security of the NAS. These different focus areas create different priorities, with airport managers prioritizing the security of the airport facility and the continuity of airport operations, while ATC prioritizes the airspace and air traffic management.

A detection system deployed at an airport can serve both airport security and NAS safety functions, but issues may arise regarding who should be responsible for monitoring the system and responding to a threat. If the monitoring function rests with the airport manager, it could be problematic from an air traffic management perspective because airport managers cannot deconflict aircraft. Similarly, if the monitoring function rests with ATC, it could be problematic due to the consuming nature of active traffic management and limited bandwidth for an air traffic controller to monitor the system and respond in a timely manner. As a result, the operational environment is one in which the airport manager may have the ability to monitor the system, but would not have the authority to respond to a threat; and ATC has the ability to respond to the threat in real time, but is unable to adequately monitor a system due to task saturation. The ability to monitor *and* address conflict does not fit squarely within any of the functions that ATC or airport managers currently perform, and both functions need to be executed **simultaneously and by the same entity** to effectively secure the NAS.

The ARC considered whether ATC and the airport manager could simultaneously share the monitoring and response functions, with the airport monitoring and ATC responding to perceived threats. However, this would not be a comprehensive solution because latency in communication could result in ATC being

[69] Federal Aviation Administration, *UAS Detection and Mitigation Systems Aviation Rulemaking Committee Charter,* (Mar 2023), available at https://www.faa.gov/regulations_policies/rulemaking/committees/documents/index.cfm/document/information?documentID=5844.

advised too late to mitigate effectively, and because data cannot be freely shared between ATC and the airport manager. For example, certain air traffic operations are not disclosed outside of ATC due to national security concerns (e.g., FBI law enforcement sensitive operations). ATC is aware of secret/sensitive aircraft operations because they have responsibility to deconflict, but ATC would be prohibited from informing an airport manager about these operations or otherwise indicating that they are authorized. The ARC also notes ATC cannot meaningfully assist with thwarting errant or nefarious UAS operations below 400 feet AGL, which would likely be a greater threat to the airport facility than the airspace (e.g., a UAS attack on an airport fuel farm). Thus, even attempts by airport managers and ATC to work collaboratively would be insufficient to meet the broad, and sometimes disparate, needs in the airport environment.

APPROACH: The ARC recommends that the FAA engage with Congress and other federal partners to create a new entity, or empower an existing entity, with the ability and authority to monitor detection systems and respond to detection events in the airport environment. This authority should be adequate to meet every potential UAS threat and should include crewed aircraft deconfliction advisories and UAS interdiction if required. The ARC considers the FAA best positioned to lead this effort as it has oversight of both airports and air traffic controllers, and can ensure a comprehensive regime to manage these functions. FAA oversight is also necessary to avoid the proliferation of divergent state and local requirements that would inevitably emerge if detection monitoring and UAS threat response was managed at the airport or local level. While the ARC believes the FAA should lead these efforts, the ARC cautions the FAA against defaulting to using the existing ATC workforce and increasing their already demanding workload. Indeed, task saturation is a major factor in why ATC cannot currently effectively perform in this space. Monitoring drone activity is simply not a part of what controllers currently do, and it would be impossible for their work practices or workload to accommodate this function. Monitoring drone operations is a separate and distinct activity that needs to be handled by a separate and distinct entity. Perhaps that “other” entity exists today or perhaps it will exist in the future (e.g., supplemental data service providers), but it is not ATC in its current form. Thus, the ARC recommends that ATC be reconstituted to better accommodate those functions, or that those functions be transferred to a different entity that can better manage them. Any newly created or newly empowered entity should have access to all information currently held within the FAA and ATC, including information and relevant data about secret aircraft operations and national security operations.

The ARC reiterates that ATC/FAA, through its ANSP functions, is responsible for providing crewed aircraft separation services in controlled airspace. As such, they have immunity from some of the liability concerns that airports do not enjoy.[70] This contributes to a reluctance to engage in D/M activities that may increase the airport’s liability exposure, and some airports may not want to assume these responsibilities. However, the ARC is also well aware of several airports with detection systems in place that have expressed a desire to conduct D/M activities at their airports, up to, and in some cases, including mitigation authority. The ARC reiterates that the deployment of D/M systems should remain a voluntary undertaking for airports that desire to perform these activities. The FAA should facilitate and support airports that want to deploy D/M systems, but the systems should never be mandated or required.

[70] This was the case for Boston Logan following the 9/11 attacks where Congress had to enact the Sabotage and Terrorist Act Protection Act to insulate the airport from the multibillion-dollar lawsuits it faced; but airports would not generally be eligible for that protection because they are not under a terroristic threat *per se* with respect to UAS operations.

AP7 - Detection & Mitigation at Airports

AP7	**The FAA should update operating rules at airports to accommodate deployment of D/M technologies.**

INTENT: To provide guidance and updates to operational procedures at airports that will allow for the safe deployment of D/M equipment in the airport environment.

RATIONALE: Airports across the country have varying levels of experience with D/M technologies and currently lack substantive guidance on implementing or conducting D/M operations at their facilities.

APPROACH: The ARC recommends that the FAA coordinate with TSA on UAS mitigation technologies at airports and continue to support TSA as the lead federal agency for CONOPS for Core 30 airports.

Local Flight Standards District Offices should update the local airport Tactical Response Plan (TRP) for C-UAS to include new C-UAS mitigation technology. The TRP for C-UAS should clearly indicate chain of command and decision-making protocols. Approval from the DHS Secretary for C-UAS mitigations must be on file for specific airport locations with C-UAS mitigation technology (with notification being the only follow-up requirement). Safe mitigation of deadly, dangerous, or persistent and disruptive UAS should occur as soon as safely practicable to minimize the duration of ground stops issued by the FAA. It is essential to mitigate these UAS as soon as practical because prolonged ground stops not only impact the safety of the NAS, but are also disruptive and costly for airlines and airport operations and create lost economic opportunities for communities. Safe mitigation would include determining whether the UAS is authorized in the NAS, ensuring appropriate safety protocols are conducted, and having a trained, authorized C-UAS operator available on site.

The FAA should work with TSA to ensure Federal Air Marshals are dedicated to supporting new C-UAS mitigation technology. Federal Air Marshals should be trained and available on site, and prepared for C-UAS mitigation response in accordance with the local TRP for C-UAS and any related policies or procedures developed as a result of the tabletop exercises.

The ARC also recommends that the FAA coordinate with TSA and other relevant stakeholders to conduct advanced tabletop exercises to manage D/M operations and UAS threat response. Interagency tabletop exercises should be conducted at appropriate intervals to ensure effective multi-stakeholder engagement and response. Tabletop, functional, and full-scale exercises are well-established practices in aviation and have a track record of bringing diverse perspectives to improve safety in the operational environment and the safety of the NAS. Moreover, when done at the local level, these exercises are also effective in establishing and maintaining critical relationships. Tabletop exercises should explore high risk scenarios or events, such as visual detection of UAS, which can be highly inaccurate (especially at night) and has led to the temporary closures of airports worldwide. The FAA should provide guidance on improving visual detection procedures and ensuring an appropriate response.

The guidance material and collaboration efforts described above should occur as part of a broader partnership between the FAA and airport industry associations to update D/M policies for Part 139 regulated airports. The updated policies should explicitly describe how D/M procedures will be incorporated into AEPs and confirm that the FAA does not intend the integration of UAS detection systems at airports to create a new legal obligation that would subject airports to Part 139 enforcement action, or otherwise be punitive in nature. The ARC notes a similar initiative from the FAA in 2021[71] where the FAA issued guidance to airports about updating their AEPs to include response plans for unauthorized UAS activity. This process brought stakeholders together and provided a common understanding of roles, responsibilities, and authorities. That same framework should be used here to ensure safety, collaboration, and effectiveness for D/M operations.

[71] https://www.faa.gov/sites/faa.gov/files/airports/airport_safety/part139_cert/what-is-part-139/part-139-cert-alert-21-04-AEP-139.325(b)(7)-Clarification.pdf.

AP8 - Federal Liability Immunity Protections for Airport Operators

AP8	**The FAA should petition Congress to expand federal liability immunity protections to airport operators that voluntarily deploy UAS detection systems.**

INTENT: To avoid penalizing airport operators that voluntarily deploy a detection system and are required under the Federal Aviation Regulations to include the optional detection system in their AEP.

RATIONALE: Part 139 requires certificated airports to develop and maintain an AEP to minimize the possibility and extent of personal injury and property damage on the airport in an emergency, and to address other unlawful interference with operations.[72] As stated above in Recommendation AP1, airport detection systems should be regulated by the FAA, and the ARC does not object to including detection systems in the airport's AEP. However, the ARC recommends that airports with voluntarily deployed systems should have the same liability protections that other detection system operators enjoy, including federal partners who are insulated from liability and detection system operators in non-airport environments who are not subject to FAA regulatory requirements.

APPROACH: To address the potential hazard of an unauthorized UAS operation on the airport that could interfere with operations, the airport operator is required to develop a response plan and coordinate with federal agencies, law enforcement, and other stakeholders. To meet this FAA requirement, airport operators must annually train airport staff on the UAS response plan protocols to manage the response to unauthorized UAS activity at the airport. The training applies to all airport staff, and includes a wide range of roles and responsibilities, all of which may have some obligation for performing the duties defined in the AEP. These employees could be airfield maintenance personnel, operations agents, or law enforcement, or they could be carpenters, plumbers, electricians, or administrative personnel.

An airport employee performing their core function could receive notification about a UAS in the airport environment. If that employee is unable to immediately follow the notification steps prescribed in the response plan and a catastrophic incident or accident ultimately occurs that causes loss of life, the airport operator may be legally liable for failure to notify or execute the responses identified in the response plan. The individual may also be liable in their personal capacity.

The FAA's expectation is that certificated airports will comply with everything in their response plan. Failure to do so exposes the airport to a potential investigation and enforcement action. The airport has a great degree of control over what is included in the plan, but it is expected to be reasonable. There is no requirement to include detection systems in an AEP, and the airport may omit any reference to it. However, if the airport plans to use the detection system as a UAS response tool, then the detection system must be included in the response plan. This requirement places airports in the unique position of having their voluntarily deployed systems become mandatory by virtue of the AEP. An airport that wants to use a detection system for any reasonable purpose, including general awareness of UAS activity in the vicinity, is required to include the system in the response plan, making it subject to enforceable action under FAA requirements. Moreover, even in situations where the employee executes all the actions as prescribed in the response plan, there would still be time required to relay information to the airport

[72] 14 CFR 139.325.

operations center, the dispatch facility, the public safety answering point, and the FAA air traffic control – time that could be used to deconflict the UAS from other aircraft and avoid an accident.

Additionally, using D/M equipment for a UAS, the FAA's hazard identification requirement may detect a UAS that is located **OFF** the airport. The airport operator does not control airspace nor non-airport property and may not have jurisdiction for law enforcement off the airport. Even prior coordination with SLTT agencies will not guarantee an immediate response to investigate the UAS or locate the UAS operator. In many cases SLTT agencies may be challenged with adequate staffing for policing their own communities and will need to prioritize calls for service. Consequently, the airport operator may be expected by the FAA to provide a role or function that is beyond the control of the airport operator's function of managing an airport.

Therefore, due to the airport's limited ability to manage a detection system event, coupled with the latency in the time required to coordinate with those who can, the ARC recommends that airport operators that voluntarily employ UAS detection equipment and have an FAA requirement for an AEP response plan, be included under federal liability immunity protections.

J. System Deployment – Non-Airports

The System Deployment – Non-Airports section contains recommendations for the FAA to support expanded mitigation authority, system interoperability and integration, and airspace policies in non-airport facilities.

NP1 - FAA Support for Expanded Mitigation Authority

NP1	**The FAA should support the Congressional authorization of specific credentialed staff in facilities and law enforcement as mitigation authorities. This authority should be developed based on experience gained at non-airport facilities on a temporary basis, initially via a pilot program.**

INTENT: To provide sufficient mitigation support necessary to counter UAS threats at non-airport critical infrastructure facilities.

RATIONALE: There is a current deficit in mitigation authorities to effectively protect critical infrastructure, and this deficit will become more pronounced as the UAS industry continues to grow and evolve. Law enforcement and staff charged with overseeing critical infrastructure facilities should be designated as mitigation authorities. Once designated, they would fall under the FAA's jurisdiction because their mitigation capabilities involve interfering with aircraft.

APPROACH: Longstanding legal precedent has established that all airspace is managed at a federal level under the FAA's regulatory authority. Given this precedent, the ARC recommends that the FAA lead efforts to establish national policy for mitigation oversight and management. However, as necessary or advisable, the FAA must do so in cooperation and partnership with other appropriate federal agencies.

One notable gap of authority that could endow critical infrastructure facilities with effective mitigation tools is implementation of Section 2209. Section 369 of the FAA Reauthorization Act of 2018 requires the FAA to establish a process for critical infrastructure facilities to manage airspace relative to UAS operations that may be in close proximity to their facilities. This will support critical infrastructure facilities in identifying any unauthorized UAS flying over a designated area, and enable them to implement safety and security measures, which may decrease the number of unauthorized UAS encounters.

The perimeters established via Section 2209 could serve as one indirect mitigation measure, though it will be important to grant waivers or permit lawful UAS operators, as appropriate. Effective implementation of this measure would not only facilitate restrictions for these facilities, but also rapidly enable access in an automated fashion to legitimate UAS operators flying in those areas.

NP2 - System Interoperability & Integration

NP2	**The FAA should direct industry to develop a harmonized protocol for applicable detection systems to route messages in non-airport environments to promote systems interoperability and integration.**

INTENT: To harmonize an open protocol message routing system that supports multiple D/M system types and eases D/M system integration across the NAS.

RATIONALE: Numerous vendors produce D/M equipment, and it is envisioned that multiple types of systems will be deployed to ensure mission success in a variety of environments. Accordingly, there is a need to ensure that these varied systems can communicate with one another because seamless communication will promote the highest degree of technical relevancy for end users who maintain and potentially layer multiple systems. The ARC recommends the FAA facilitate and support industry efforts to update and refine an existing common protocol, or define a protocol for this purpose. For example, the Cursor-on-Target (CoT) message router protocol, as defined in MIL-STD-6090, has been utilized as a *de facto* interoperability standard for C2 systems, especially in DoD environments. CoT provides a means to integrate many systems into a Common Operating Picture (COP) or C2 system utilized by end users. Many C2 systems are capable of ingesting CoT, which further enhances the overall end user sight picture – even if a variety of end users choose different C2 or COPs for their various Use Cases. The ARC also notes that prioritizing interoperability provides wider market opportunities for vendors, and incentivizes innovative solutions.

APPROACH: The FAA should maintain an interagency cross functional team, with industry representation, to adopt a technical standard (e.g., CoT Message Router) or work with industry to align on another common protocol for detection systems to communicate. This industry means of communication should include appropriate privacy and data retention safeguards, and should be adopted and maintained via consortium of the government and industry cross functional team.

NP3 - Defining Airspace Policies in Non-Airport Facilities

NP3	**The FAA should work with its federal partners to develop processes and eligibility criteria for airspace restrictions to be granted to non-airport critical infrastructure facilities with a qualifying safety need. The FAA should also develop a process that allows verified UAS operators to access these restricted airspaces.**

INTENT: To ensure that certain non-airport critical infrastructure facilities and large outdoor gatherings (i.e., "non-aviation entities") can obtain airspace restrictions as needed, and to provide a pathway for qualified UAS operators to access these restricted airspaces.

RATIONALE: Current airspace requirements for UAS operations below 400 feet AGL are set on an all-or-nothing basis, with the airspace being either completely restricted or completely unrestricted. As UAS operations increase and become more complex, this binary approach to airspace management will be ill-suited to meet the security needs of non-aviation entities. For example, a prison may need an airspace restriction to prohibit a nefarious UAS operator from dropping contraband into the prison yard. However, the prison may also want a verified UAS operator to monitor the prison yard for safety and security purposes. Under the existing regulations, there is no clear process for a prison to request an airspace restriction from the FAA. Moreover, even if a process was developed, the restriction would likely prohibit UAS operations above the prison (up to 400 feet AGL), which would hinder the prison's ability to deploy a UAS for safety and security purposes. Accordingly, the ARC recommends that, similar to airspace system allocations for crewed aircraft in the ATM, the airspace environment below 400 feet AGL should include access to various types of airspace based on operator qualifications, navigational capabilities, flight plans, and other relevant factors.

The ARC further recommends that non-aviation entities should be able to obtain a tailored airspace restriction if there is a credible risk of an unsafe or unlawful UAS incursion. The ARC notes, however, that there may be instances where lawful, safe, and qualified UAS operations should be allowed to continue despite the non-aviation entity's airspace restriction. Thus, the ARC also recommends the FAA develop a process that allows qualified UAS operators access to restricted airspaces granted to non-aviation entities. The ARC considers this to be a more sophisticated approach to UAS airspace management that accommodates safety and security needs while preserving available airspace access for verified and compliant operators.

APPROACH: The FAA should work with partner agencies to establish a process and determine appropriate criteria that non-aviation entities must follow to be eligible to request and obtain airspace restrictions as needed. This approach is related to and inspired by the concept of airspace management in Section 2209 of the FAA Extension, Safety, and Security Act of 2016, the implementation of which would also aid specificity and progress on this recommendation.

The FAA should publicize information about the airspace restriction application process, including the criteria that non-aviation entities must meet to qualify for an airspace restriction. Any airspace restrictions that are granted should be considered based on their temporal or permanent nature, and an application for restrictions of prolonged duration must describe the continued safety need. These types of airspace restrictions should also consider an altitude ceiling to avoid restricting commerce from traditional forms of aviation as appropriate based on risk.

In addition to providing a pathway for non-aviation entities to request an airspace restriction, the FAA should also develop a method for qualified UAS operators to access these restricted airspaces. Access should be granted so that verified UAS operations can continue without unnecessary impediments. Given their recognized status of operating in a lawful and responsible manner, UAS operators that have been designated as verified operators through the VOP should be granted access to these restricted airspaces via the timely digital exchange of the requisite credentials.

IX. Definitions and Glossary of Terms

The following definitions apply specifically within the context of the ARC Final Report and associated documents.

A. Abbreviations and Acronyms

AEP - Airport Emergency Plan

AGL - Above Ground Level

AIP - Airport Improvement Program

ALR - Acceptable Level of Risk

ANSP - Air Navigation Service Provider

ATM - Air Traffic Management

BVLOS - Beyond Visual Line of Sight

CISA - Cybersecurity & Infrastructure Security Agency

C2 - Command and Control

CONOP - Concept of Operations

C-UAS - Counter-UAS

DAR - Designated Airworthiness Representative

D/M - Detection and/or Mitigation

DHS - Department of Homeland Security

DoD - Department of Defense

DOE - Department of Energy

DOJ - Department of Justice

DRP -Drone Response Plan

EO - Electro-optical

FAA - Federal Aviation Administration

FCC - Federal Communications Commission

FESSA - FAA Extension, Safety and Security Act

GCC - Government Coordinating Council(s)

GPS - Global Positioning System

IDM - Identification Data Manager

IR - Infrared

ITU - International Telecommunication Union

MOS - Manual of Standards

MPS - Minimum Performance Standards

NAS - National Airspace System

NTIA - National Telecommunications and Information Administration

RF - Radio Frequency

SLTT - State, Local, Tribal, and Territorial

sUAS - Small Unmanned Aircraft System(s)

UA - Unmanned Aircraft

UAS - Unmanned Aircraft System(s)

UTM - Unmanned Aircraft System Traffic Management

VOP – Verified Operator Program

B. Definitions

1. Current Definitions

Counter-UAS - UAS detection and mitigation activities to counter UAS (C-UAS) [Note: For this ARC, C-UAS is only attributable to sUAS.]
(https://www.faa.gov/sites/faa.gov/files/uas/resources/c_uas/Interagency_Legal_Advisory_on_UAS_Detection_and_Mitigation_Technologies.pdf)

Counter-UAS System - A system or device capable of lawfully and safely disabling, disrupting, or seizing control of an uncrewed aircraft (UA) or uncrewed aircraft system (UAS or drone).
(49 U.S.C. § 44801)

Mitigation Capabilities - Fall into two general categories: non-kinetic and kinetic. Non-kinetic solutions use non-physical measures to disrupt or disable UAS, including RF, WiFi, or Global Positioning System (GPS) jamming; spoofing; hacking techniques; and non-destructive directed energy weapons. Kinetic solutions may employ a variety of measures capable of physically disrupting or disabling a UAS, including nets, projectiles, and lasers.
(https://www.faa.gov/sites/faa.gov/files/uas/resources/c_uas/Interagency_Legal_Advisory_on_UAS_Detection_and_Mitigation_Technologies.pdf)

2. Recommended Amendments to Existing Definitions

Detection Capabilities - Systems that detect, monitor, or track [and identify] UAS often rely on radio frequency (RF), radar, electro-optical (EO), infrared (IR), or acoustic capabilities, or a combination thereof. These capabilities detect the physical presence of UAS or signals sent to or from the UAS

(https://www.faa.gov/sites/faa.gov/files/uas/resources/c_uas/Interagency_Legal_Advisory_on_UAS_Detection_and_Mitigation_Technologies.pdf)

3. Recommended New Definitions

Identification Data - A generic term for government datasets containing information about a UAS operator's identity. The government datasets may contain sensitive or personally identifiable information that would be made available to Identification Data Managers based on their facility's risk level.

Identification Data Manager – An organization or individual approved by the FAA to have access to Identification Data.

Radionavigation Approval (Relative to D/M and UAS integration) - An allocation for detection systems that are used for separation assurance; including for dual-purpose use—UAS integration as well as detection of non-cooperative aircraft.

Radiolocation Approval (Relative to D/M and UAS integration)- An allocation for detection systems that are exclusively used for detection of non-cooperative aircraft (i.e., no separation assurance).

Verified Operator – A UAS operator that, after voluntarily submitting relevant information to the Verified Operator program, has been officially recognized as meeting certain criteria of lawfulness and responsibility to merit access to special use airspace.

X. Out of Scope Issues

This section contains the ARC's views on matters that were out of scope per the ARC Charter or that should be considered for future rulemaking initiatives.

A. Geofence

Geofence systems may provide UAS operators with up-to-date information on airspace restrictions. Geofence systems may also provide warnings to UAS that are approaching or operating within geofence boundaries; and, in some cases, prohibit UAS from flying across or initiating takeoff within a geofence boundary. Yet there are many limitations and potential unintended consequences associated with geofence technology that could negatively impact the safety of the NAS. The ARC makes no recommendations on geofence, but urges the FAA to thoughtfully consider the utility of this technology and its safety and security implications for the NAS and for UAS and UAS D/M system integration.

B. Network Remote ID

The FAA's Remote ID Final Rule[73] represented a major change from its Proposed Rule.[74] In the Final Rule, compliance requirements for network-based internet transmission were eliminated, allowing only broadcast-based systems for compliance.

Network Remote ID has the potential to provide additional airspace awareness that could positively inform UAS detection efforts beyond what is currently available with broadcast-only Remote ID, as the FAA has presently scoped the rule. Several ARC members relayed that eliminating network-based systems was proving problematic on several operational fronts. Other ARC members, however, were of the view that network-based systems would create problems of their own, specifically with respect to privacy, security, Remote ID module pricing, safety, availability, and module weight. Moreover, all ARC members acknowledge that network-based Remote ID is not currently viable in certain environments due to the lack of infrastructure or unreceivable transmissions. This is especially true in rural areas that are unserved or underserved with internet access.

Although the implementation of Network Remote ID was beyond the scope of the ARC Charter, the ARC found it necessary to discuss the issue because it is significantly connected to matters that were within scope, such as data sharing/correlation and how to interpret Remote ID data whether broadcast or network based (see Recommendations DM2, DM3, DM6, and DM7). The ARC also notes that the problems identified above warrant further study and analysis as stated in Recommendation PL8. Thus, the ARC considers it prudent to inform the FAA of the views that emerged from its deliberations.

The ARC members held three distinct views regarding Network Remote ID and the FAA's Final Rule. Specifically, the ARC members consider that the rule should either:

- change to *include* a network-based / internet transmission compliance option,
- change to *require* a network-based / internet transmission capability, or
- remain unchanged.

The ARC appreciates the FAA's consideration of its views.

[73] *Remote Identification of Unmanned Aircraft*, 86 FR 4390, (Mar 16, 2021).

[74] *Remote Identification of Unmanned Aircraft Systems,* 84 FR 72438, (Dec 31, 2019).

XI. Appendices

Appendix A - Recommendations List

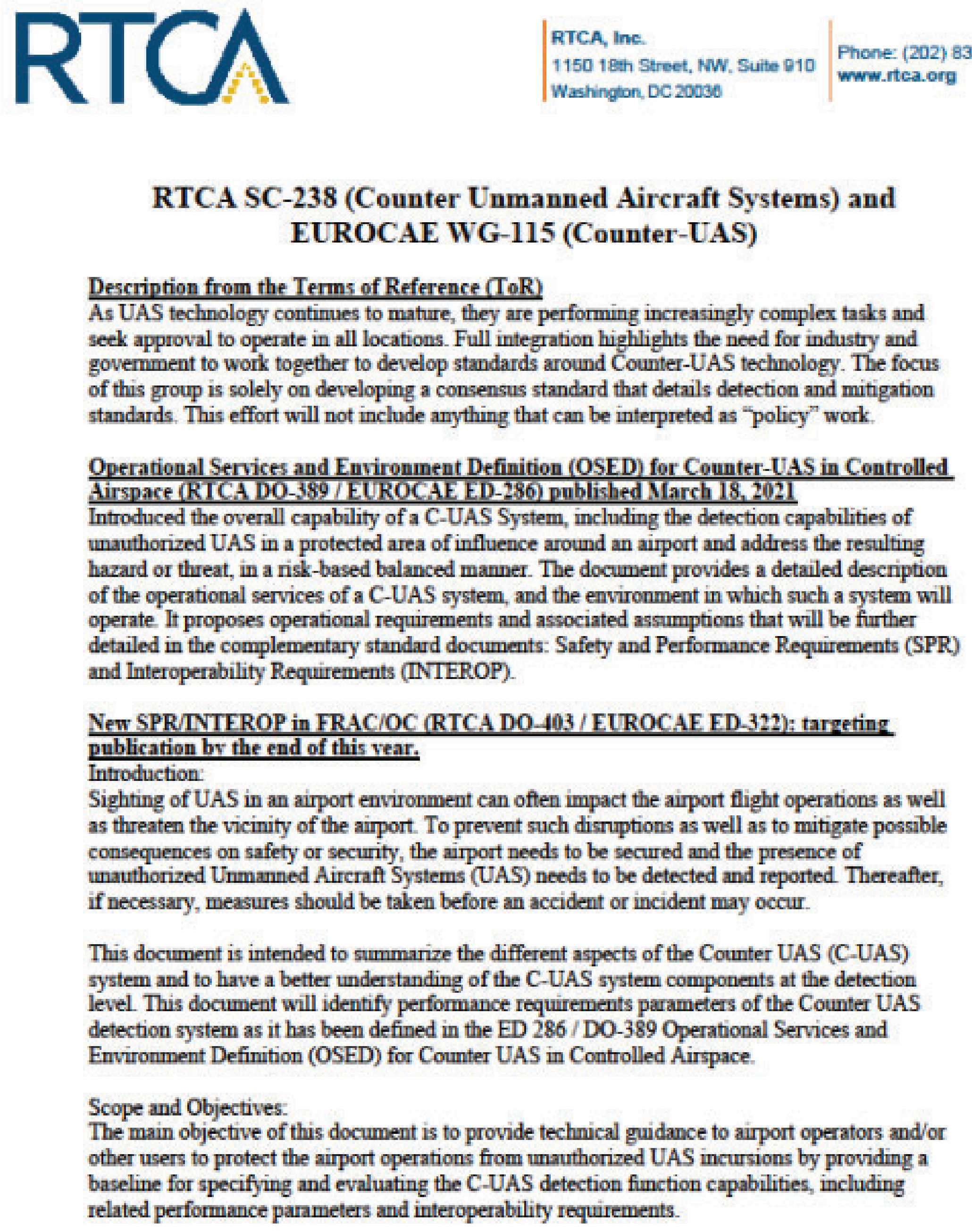
Policy Recommendations (PL)	
PL1	The FAA should incorporate a thorough understanding of the industry and its intricacies, as well as the broader ecosystem, into any policy recommendations.
PL2	Given the differences between detection and mitigation, the FAA should work with its federal partners to consider these two components separately for policy purposes.
PL3	The FAA should work with its federal partners to balance the benefits of authorized D/M technology integration with the potentially detrimental impact of such systems on their surrounding broader ecosystem.
PL4	The FAA should account for monetary and non-monetary costs of D/M integration and who will bear costs and externalities.
PL5	The FAA should work with its federal partners to properly balance D/M end-user safety and security with the privacy, environmental, health, and civil liberties interests of the public.
PL6	The FAA should work with its federal partners, site operators, and other industry stakeholders to develop timely strategic communication plans, allocating roles and responsibilities as needed with respect to engagement and outreach activities. These plans should include direct channels to the public and appropriate timelines to communicate with relevant communities involved in supporting, operating, and using ecosystems that employ D/M technology.
PL7	The FAA should work with its federal partners to recognize that D/M systems, once properly enabled, will serve as an important tool in the suite of defenses for security and law enforcement, SLTT partners, critical infrastructure owners and operators, and first responders to serve and protect UAS innovation and integration. “Properly enabled” means that authorized protocols include guardrails that balance impacts to surrounding NAS operations, safety, security, and privacy similar to those in current use by regulators that approve large-scale event management.
PL8	The FAA should commission a cost effectiveness and benefits study to assess the feasibility of mechanisms that improve the ability to differentiate between compliant and non-compliant UAS operations.
PL9	The FAA should work with its federal partners, particularly the DOJ, to identify a clear process and pathway for Title 18 relief for law enforcement officers involved in the mitigation of a UAS.
PL10	The FAA should work with its federal partners to consider the importance of U.S. leadership in this sector.
PL11	The FAA should work with its federal partners to put forth lessons learned, guidance, recommendations, and best practices for deploying detection systems in non-airport environments.

Risk Management Recommendations (RM)	
RM1	The FAA should create an acceptable level of risk and a safety framework for UAS D/M systems and integration.
RM2	The FAA should consider the risks associated with the method it chooses to enable the deployment of D/M systems. Specifically, the different risks associated with whether systems are certified, permitted, authorized, or allowed.
RM3	The FAA should work with its federal partners to establish operating rules for D/M operators across all sites to minimize risks to the NAS and traditional air traffic operations.
System Standards Recommendation (ST)	
ST1	The FAA should work with its federal partners and standards organizations to develop minimum performance standards (MPS) for UAS D/M systems in a comprehensive, coordinated manner that supports aviation safety.
ST2	The FAA should work with its federal partners to evaluate and approve a set of D/M technologies from which approved users may select.
ST3	The FAA should develop detection-only system standards that are tailored to the airport environment.
Testing Recommendations (TE)	
TE1	The FAA should work with its federal partners to enable and coordinate D/M systems testing across relevant stakeholders.
TE2	The FAA should coordinate with their federal partners to develop criteria for D/M system and component efficacy testing to be conducted by approved third-party entities.
TE3	The FAA should consider expanding the 383 Testing Program or creating a new program to test the efficacy of systems to an acceptable performance standard to avoid erroneous information that could jeopardize the NAS.
Training Recommendation (TR)	
TR1	The FAA should work with its federal partners to develop and maintain training requirements to ensure the safe deployment of D/M systems across all sites and should differentiate this training based on the needs of the operational environment.
Data Management Recommendations (DM)	
DM1	The FAA should establish D/M system data retention protocols.
DM2	The FAA should provide greater access to Identification Data and support a decentralized, industry led data access management system.

DM3	The FAA should ensure that detection information is correlated with identification data whenever possible.
DM4	The FAA should establish a Verified Operator Program (VOP) to quickly and correctly identify proximate UAS that are VOP qualified.
DM5	The FAA should ensure that digital forms of airspace information are available to the public.
DM6	The FAA should create a Remote ID incentive program.
DM7	The FAA should provide information about how to use and interpret Remote ID data.
System Acquisition Recommendations (AQ)	
AQ1	The FAA should facilitate the voluntary acquisition and use of detection systems in a manner that accommodates rapid technological changes.
AQ2	The FAA should use a structured 7460 evaluation process to review and assess the installation of D/M systems.
System Deployment (General) Recommendations (SD)	
SD1	The FAA should develop a policy framework that establishes D/M operational requirements to ensure the safe deployment of D/M systems across all sites.
SD2	The FAA should require detection system operators to develop a coordination and communication plan for system operations.
SD3	The FAA should establish and maintain a flexible, scalable regulatory framework that can accommodate increases in airspace density or usage.
SD4	The FAA should play a role in developing “rules of engagement” for C-UAS operations
SD5	The FAA should prioritize spectrum usage in coordination with its federal partners and adopt a common lexicon defining the uses of spectrum allocated for D/M purposes.
System Deployment (Airports) Recommendations – (AP)	
AP1	The FAA should clarify that detection systems are not mandatory in the airport environment.
AP2	The FAA should establish interoperability protocols for situations where more than one entity has a D/M system in or around the same airport environment.
AP3	The FAA should set the standards for detection systems in the airport environment to ensure that the systems are able to detect UAS from the area immediately inside the airport fence line out to a specified radius around the airport property that provides sufficient time to respond to UAS threats.
AP4	The FAA should establish training and operational requirements for detection-only system operators

AP5	The FAA should require detection system operators to develop a communication plan that addresses the unique airport operational environment.
AP6	The FAA should work with its federal partners to empower the correct entity to perform the ANSP functions of monitoring detection systems and responding to UAS threats in the airport environment.
AP7	The FAA should update operating rules at airports to accommodate deployment of D/M technologies.
AP8	The FAA should petition Congress to expand federal liability immunity protections to airport operators that voluntarily deploy UAS detection systems.
System Deployment Non-Airports Recommendations (NP)	
NP1	The FAA should support the Congressional authorization of specific credentialed staff in facilities and law enforcement as mitigation authorities. This authority should be developed based on experience gained at non-airport facilities on a temporary basis, initially via a pilot program.
NP2	The FAA should direct industry to develop a harmonized protocol for applicable detection systems to route messages in non-airport environments to promote systems interoperability and integration.
NP3	The FAA should work with its federal partners to develop processes and eligibility criteria for airspace restrictions to be granted to non-airport critical infrastructure facilities with a qualifying safety need. The FAA should also develop a process that allows verified UAS operators to access these restricted airspaces.

Appendix B - RTCA SC-238 (Counter Unmanned Aircraft Systems) and EUROCAE WG-115 Counter-UAS Transmission Letter



RTCA, Inc.
1150 18th Street, NW, Suite 910
Washington, DC 20036

Phone: (202) 833-9339
www.rtca.org

RTCA SC-238 (Counter Unmanned Aircraft Systems) and EUROCAE WG-115 (Counter-UAS)

Description from the Terms of Reference (ToR)

As UAS technology continues to mature, they are performing increasingly complex tasks and seek approval to operate in all locations. Full integration highlights the need for industry and government to work together to develop standards around Counter-UAS technology. The focus of this group is solely on developing a consensus standard that details detection and mitigation standards. This effort will not include anything that can be interpreted as "policy" work.

Operational Services and Environment Definition (OSED) for Counter-UAS in Controlled Airspace (RTCA DO-389 / EUROCAE ED-286) published March 18, 2021

Introduced the overall capability of a C-UAS System, including the detection capabilities of unauthorized UAS in a protected area of influence around an airport and address the resulting hazard or threat, in a risk-based balanced manner. The document provides a detailed description of the operational services of a C-UAS system, and the environment in which such a system will operate. It proposes operational requirements and associated assumptions that will be further detailed in the complementary standard documents: Safety and Performance Requirements (SPR) and Interoperability Requirements (INTEROP).

New SPR/INTEROP in FRAC/OC (RTCA DO-403 / EUROCAE ED-322): targeting publication by the end of this year.

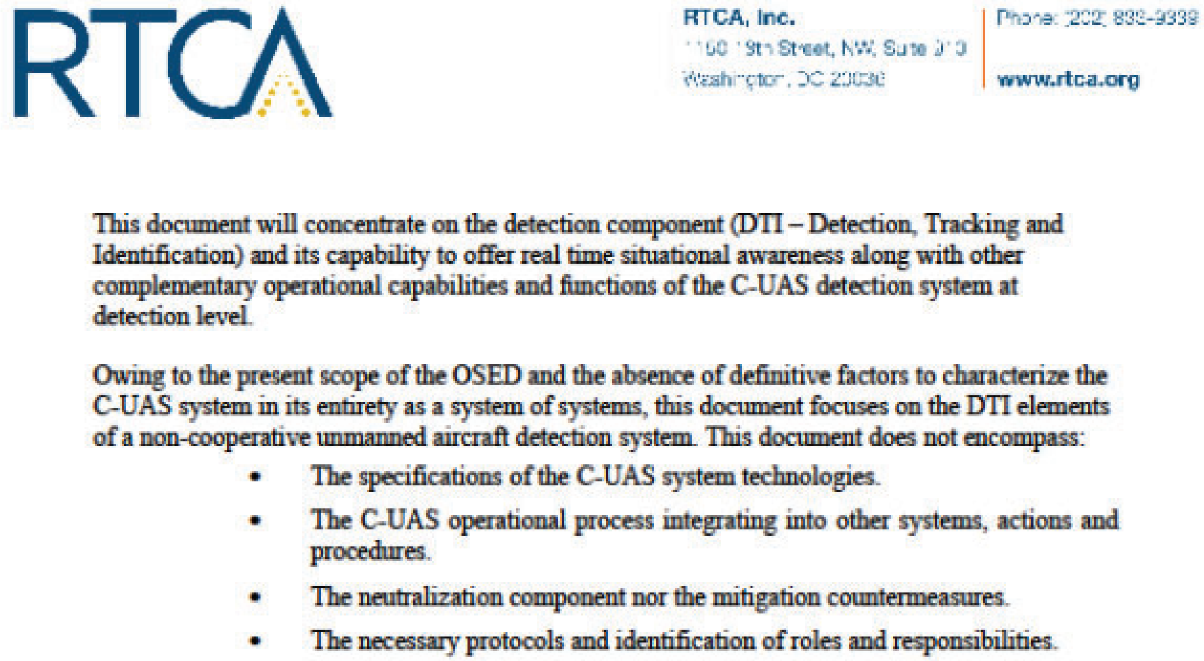
Introduction:

Sighting of UAS in an airport environment can often impact the airport flight operations as well as threaten the vicinity of the airport. To prevent such disruptions as well as to mitigate possible consequences on safety or security, the airport needs to be secured and the presence of unauthorized Unmanned Aircraft Systems (UAS) needs to be detected and reported. Thereafter, if necessary, measures should be taken before an accident or incident may occur.

This document is intended to summarize the different aspects of the Counter UAS (C-UAS) system and to have a better understanding of the C-UAS system components at the detection level. This document will identify performance requirements parameters of the Counter UAS detection system as it has been defined in the ED 286 / DO-389 Operational Services and Environment Definition (OSED) for Counter UAS in Controlled Airspace.

Scope and Objectives:

The main objective of this document is to provide technical guidance to airport operators and/or other users to protect the airport operations from unauthorized UAS incursions by providing a baseline for specifying and evaluating the C-UAS detection function capabilities, including related performance parameters and interoperability requirements.



This document will concentrate on the detection component (DTI – Detection, Tracking and Identification) and its capability to offer real time situational awareness along with other complementary operational capabilities and functions of the C-UAS detection system at detection level.

Owing to the present scope of the OSED and the absence of definitive factors to characterize the C-UAS system in its entirety as a system of systems, this document focuses on the DTI elements of a non-cooperative unmanned aircraft detection system. This document does not encompass:

- The specifications of the C-UAS system technologies.
- The C-UAS operational process integrating into other systems, actions and procedures.
- The neutralization component nor the mitigation countermeasures.
- The necessary protocols and identification of roles and responsibilities.

Appendix C - Working Group Focus Questions

Working Group 1 Focus Questions:

1. What societal interests should be addressed in expanding the integration of D/M systems?
2. What are the benefits of full integration of UAS into the NAS?
3. How will the expanded use of D/M systems facilitate the full integration of UAS into the NAS?
4. What are the general benefits of the various types of C-UAS equipment?
    a. Detection – is detection enough?
    b. Mitigation
    c. Integration v. isolation
5. What are the specific potential societal and economic benefits (to users of D/M systems) vs. the risk of inaction to:
    a. Security partners and law enforcement agencies?
    b. Critical infrastructure?
    c. Airports?
    d. Communities and the public?
6. What societal concerns should be addressed in expanding the integration of D/M systems?
7. What new risks could be introduced to the NAS and the public through further integration of D/M systems?
    a. Traditional aviation community
    b. UAS community
    c. Infrastructure
    d. Spectrum
    e. Communication
    f. ATM interface – Radar, ILS, Navigation, RF
    g. Mitigation risks to people on the ground
    h. Other
8. What privacy and civil liberties concerns may be introduced by the expanded use of D/M systems and how can they be addressed?

Working Group 2 Focus Questions:

The Working Group developed the following Focus Questions to guide its work:

<u>How should the FAA oversee UAS D/M systems to minimize safety risks to the NAS?</u>

1. What standards should be developed to ensure D/M systems meet the required safety thresholds?
    a. Will FAA approve/accept minimum performance standards (MPS) and if so, based on spectrum or more?
2. What constitutes safety?
    a. Spectrum interoperability
    b. NAS safety hazards

c. The efficacy of the systems (to avoid introducing erroneous information that may have safety and efficiency implications)
d. Cyber security
e. Supply chain concerns

3. Should the FAA and their partner agencies establish an anonymous/non-punitive database to capture:
    a. A continuum of updates
    b. Synthesized data
    c. What other information might be important - data beyond performance:
        i. Initial and full-lifecycle execution implications
        ii. Initial and full-lifecycle costs
4. Should the FAA oversee D/M systems by technology type? What categorization framework does the ARC recommend?
5. Should the FAA develop and maintain an "approved systems list" for D/M systems? If so, how might that list be established and updated to expeditiously approve new systems and technologies?
6. Will FAA only approve systems that do not interfere with the spectrum or impact safety as defined?
7. Will separate systems be deployed for counter-UAS (C-UAS) versus UAS integration activities?
8. If so, is spectrum prioritization based on the current method of first come-first serve for approval (to include integration, D/M activities)? What system integration concerns are relevant?
9. What other C-UAS groups we should be coordinating with?

Working Group 3A Focus Questions:

The Working Group developed the following Focus Questions to guide its work:

1. Should operators in an airport environment receive certification, authorization, approval or be allowed to manage the deployment of a UAS detection system in their facility?
2. Representing the airport ecosystem, what risks should be considered in "approving, authorizing, certifying, or allowing" detection-only or detection and mitigation systems?
    a. Are there different risks depending on whether a system is authorized versus certified?
3. What process should users use to seek FAA review of the installation of detection-only systems?
4. With rapid changes in UAS technology, how will operators acquire and use detection-only technologies?
5. How will detection system operators identify UAS operations enabled by FAA? What is the data sharing mechanism?
6. What personnel will be allowed to operate and maintain a detection-only system at an airport?
7. How would priorities, data sharing and interoperability be established and managed for situations where more than one entity has detection-only or detection and mitigation technologies in or around the same airport environment?
    a. Is one system trusted more than the other?
    b. Are detection alarms from systems shared?
    c. How are potential interference issues addressed?

8. What other risks are associated with the integration of detection and mitigation systems in the airport environment that could impact the safety of the NAS, such as:
    a. the terminology used for authorizing, approving, certifying, or allowing systems,
    b. the existing laws about who has the authority to mitigate UAS activities,
    c. coordination requirements between multiple entities (i.e., the entity operating the system, the entity controlling the airspace, and the entity responsible for mitigation activities),
    d. systems that are not monitored 24/7 – what happens when the people are not on site,
    e. latency of notification streams – is there a risk if the person who receives the detection is not in a position to affect air traffic or otherwise communicate with crewed aircraft?
    f. What if the notifications are sent to someone engaged in other duties and ATC finds out too late?

Working Group 3B Focus Questions:

The Working Group developed the following Focus Questions to guide its work:

1. What elements should be considered in allowing Detection/Mitigation systems in a non-airport environment?
    a. To the NAS?
    b. To the environment of the surrounding community?
2. What risks should be considered for non-airport facilities and what entities should provide input, information, and authorizations?
3. How should the FAA address these risks at non-airport sites?
4. Are there different authorization and operating levels for facilities based on risk considerations?
5. What process should non-airport sites use to apply for site approval (FAA review process)?
6. What are the challenges for traditionally non-aviation related facilities operating equipment in the NAS?
7. What personnel will be responsible for operating and maintaining the equipment at the facility?
    a. What are the training, education, certification requirements?
8. With the rapidly changing technology environment, what are the challenges and impact to facilities?

Additional Focus Questions include:
Using the successful example of the TSA Pre-Check program for airline passengers, how could the FAA promote "Verified Operators" for the purpose of increasing the available resources to more effectively monitor airspace to identify and discern the intent of "Other" UAS?

1. What are the necessary criteria for operators to be deemed as "verified" operators?
2. How do "verified" operators and regulators participate in concept of identity and access management?
3. What is the process for non-airport sites to coordinate with security agencies to verify operator identity and access?
    a. Who are the agencies and what data-sharing will be required?

What distinction should the FAA make between detecting versus tracking UAS and ensure that mitigation is reserved only as a last resort?

Working Group 4 Focus Questions:

1. What operator requirements should the FAA consider for the safe operation of D/M systems? (By technology type? Site category? Risk category?)
2. Based upon these requirements, what are the levels of initial and recurring training that operators should meet?
3. What operating rules should the FAA establish for D/M operators to:
    a. Minimize risks to the NAS?
    b. Minimize risks to traditional air traffic operations?
    c. Account for future increases in airspace density or usage?
    d. Minimize risks of potential collateral effects to authorized UAS?
    e. Protect the privacy of UAS operators and the public?
    f. Minimize risks to persons or infrastructure on the ground?
4. What role should the FAA play in establishing and overseeing mitigation "rules of engagement" to protect the safety of lawful UAS in the NAS?
5. What additional operating rules are necessary to establish at airports?

Appendix D - Use Case Scenarios

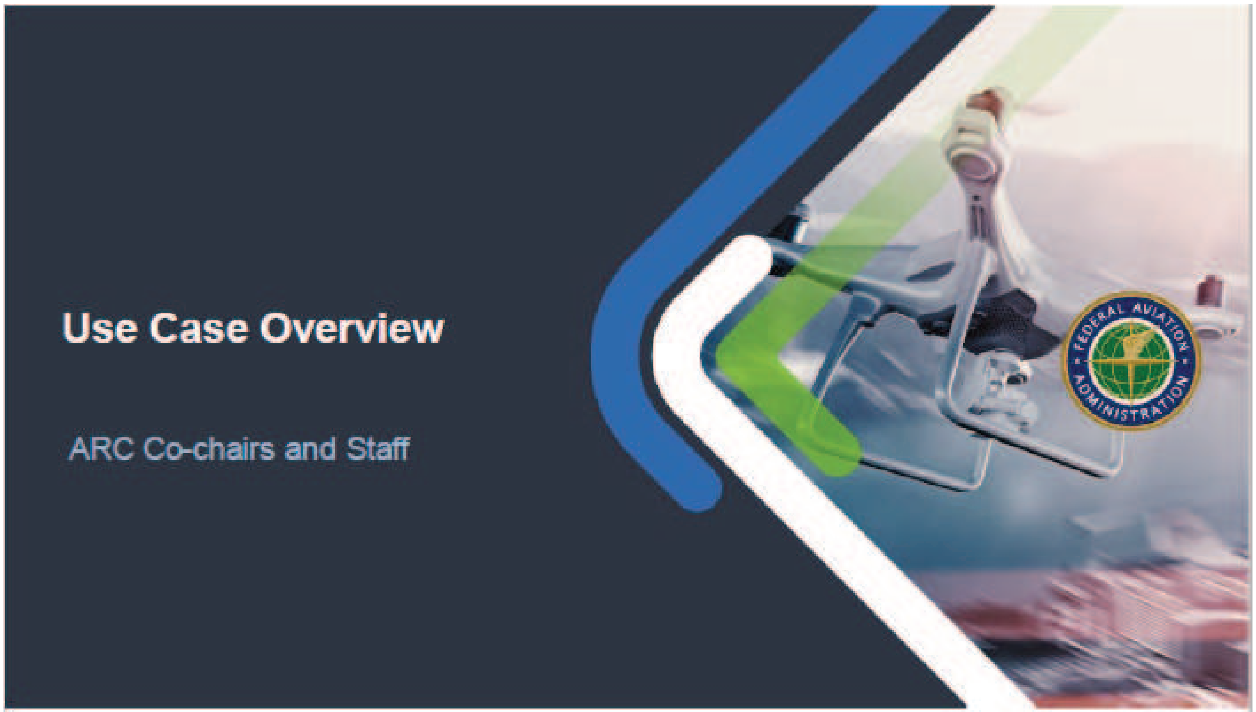
As part of the process of developing and refining its recommendations, the ARC formed teams to examine four different Use Case scenarios designed to present a variety of realistic D/M issues relevant to different sites and settings. The Use Cases were intended as a thought tool for stress-testing the ARC's recommendations, shifting the focus from general issues to very specific contexts and fostering collaboration across working groups.

The four Use Case scenarios[75] were:

- State prison (UAS dropping contraband or direct delivery to inmates).
- Stadium (UAS over parking lots and in seating bowl during games).
- Law enforcement for disaster response (UAS interference in firefighting response).
- Airport (installation of D/M system at a Part 139 Airport certificated airport that is co-located with a military installation with kinetic mitigation authority and equipment).

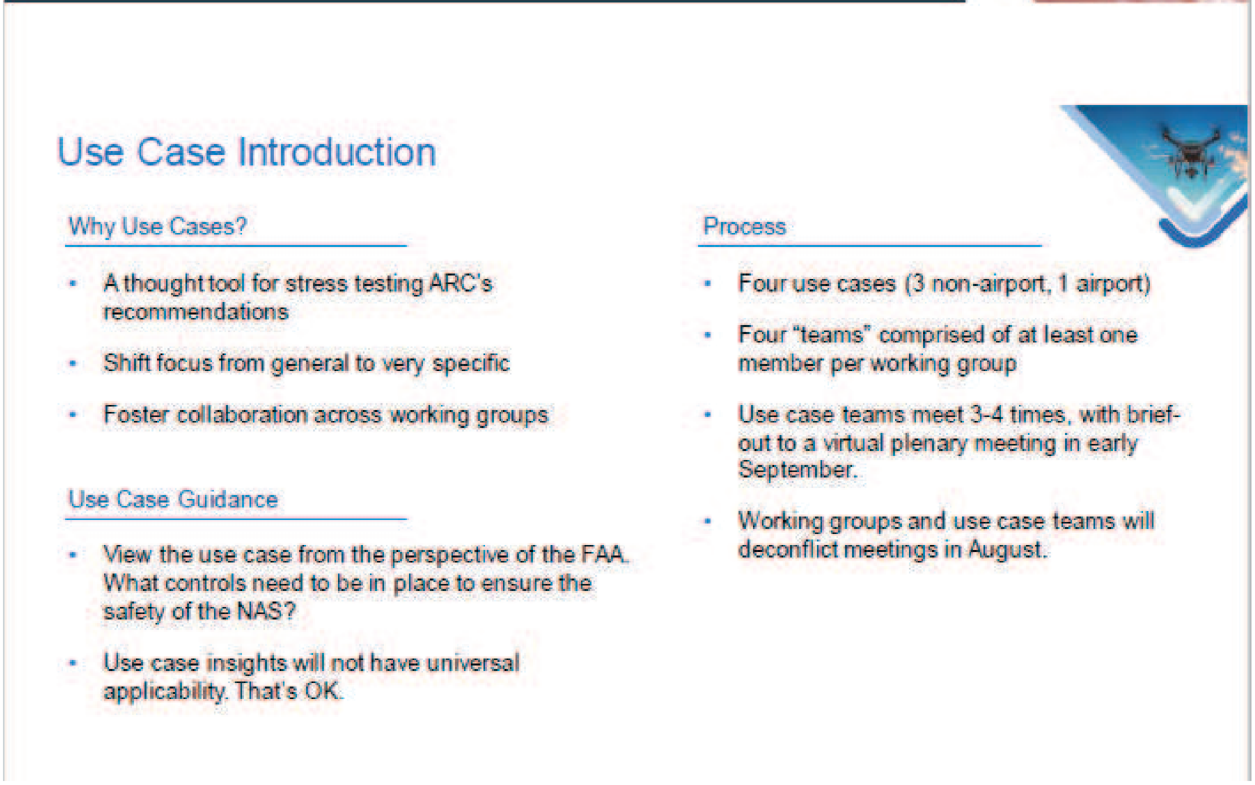
Detailed information on each Use Case is below in the full briefing slides.

[75] The Use Case presentation slides are in Appendix D.



Use Case Overview

ARC Co-chairs and Staff



Use Case Introduction

Why Use Cases?

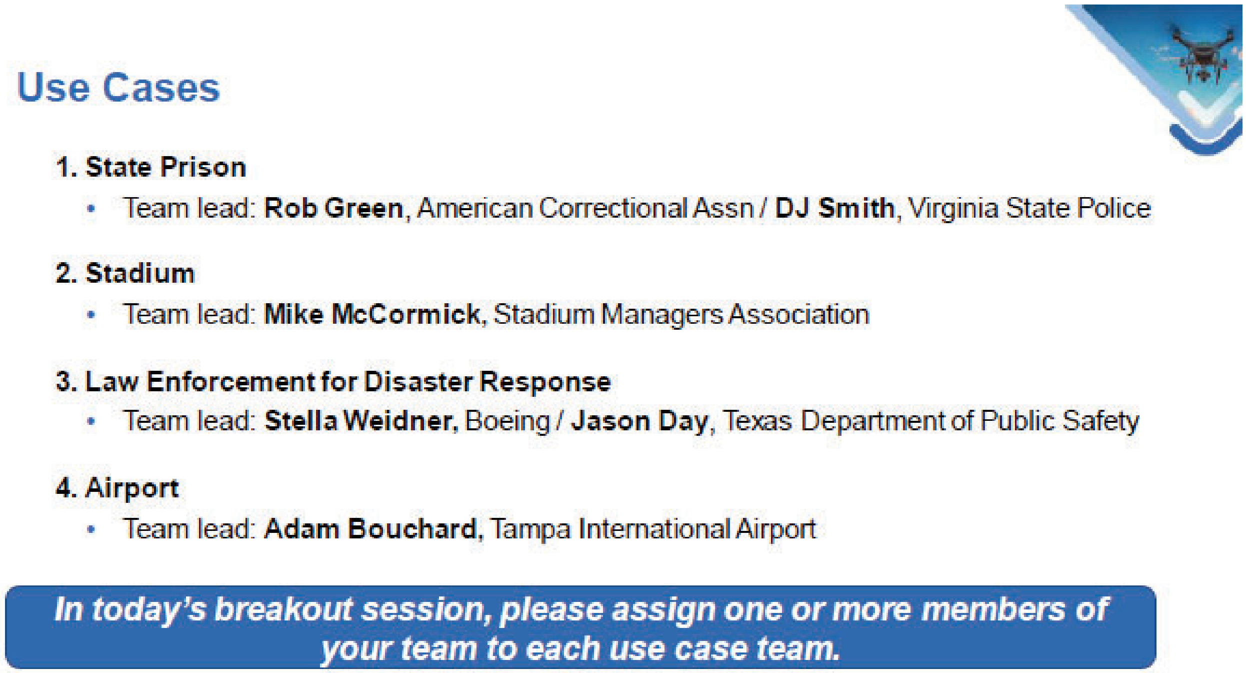
- A thought tool for stress testing ARC's recommendations
- Shift focus from general to very specific
- Foster collaboration across working groups

Use Case Guidance

- View the use case from the perspective of the FAA. What controls need to be in place to ensure the safety of the NAS?
- Use case insights will not have universal applicability. That's OK.

Process

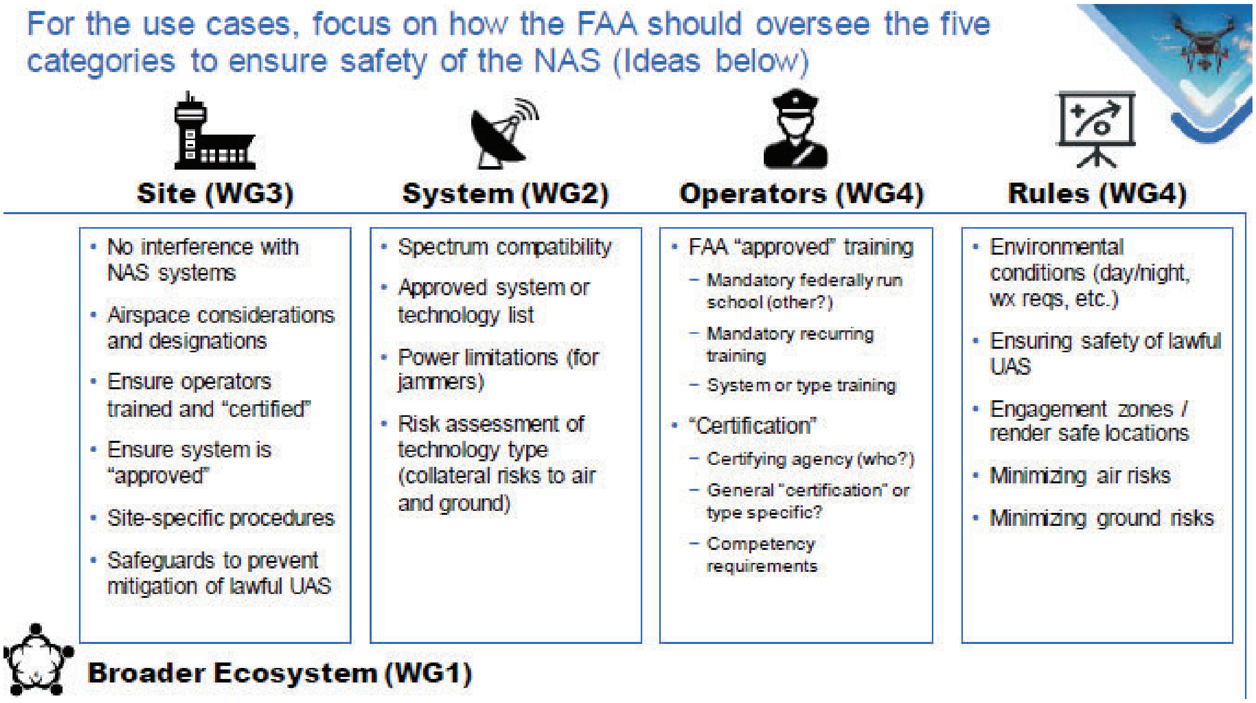
- Four use cases (3 non-airport, 1 airport)
- Four "teams" comprised of at least one member per working group
- Use case teams meet 3-4 times, with brief-out to a virtual plenary meeting in early September.
- Working groups and use case teams will deconflict meetings in August.



Use Cases

1. **State Prison**
   - Team lead: **Rob Green**, American Correctional Assn / **DJ Smith**, Virginia State Police
2. **Stadium**
   - Team lead: **Mike McCormick**, Stadium Managers Association
3. **Law Enforcement for Disaster Response**
   - Team lead: **Stella Weidner,** Boeing / **Jason Day**, Texas Department of Public Safety
4. **Airport**
   - Team lead: **Adam Bouchard,** Tampa International Airport

In today's breakout session, please assign one or more members of your team to each use case team.



For the use cases, focus on how the FAA should oversee the five categories to ensure safety of the NAS (Ideas below)

Site (WG3)

- No interference with NAS systems
- Airspace considerations and designations
- Ensure operators trained and "certified"
- Ensure system is "approved"
- Site-specific procedures
- Safeguards to prevent mitigation of lawful UAS

System (WG2)

- Spectrum compatibility
- Approved system or technology list
- Power limitations (for jammers)
- Risk assessment of technology type (collateral risks to air and ground)

Operators (WG4)

- FAA "approved" training
  - Mandatory federally run school (other?)
  - Mandatory recurring training
  - System or type training
- "Certification"
  - Certifying agency (who?)
  - General "certification" or type specific?
  - Competency requirements

Rules (WG4)

- Environmental conditions (day/night, wx reqs, etc.)
- Ensuring safety of lawful UAS
- Engagement zones / render safe locations
- Minimizing air risks
- Minimizing ground risks

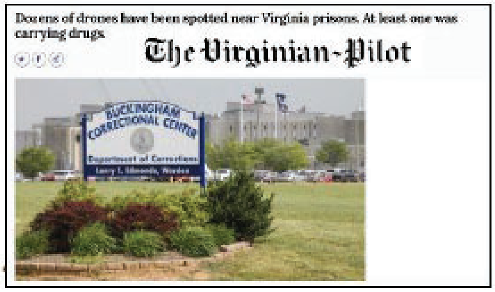
Broader Ecosystem (WG1)

Use Case 1: State Prison

Prison Use Case:

Buckingham Correctional Center

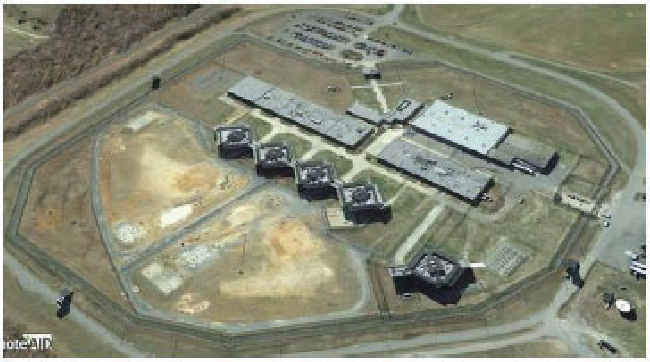
- State prison operated by the Virginia Department of Corrections
- Buckingham County, Virginia
- Average population: 1,000 inmates
- Security Level 3-4
- Airspace considerations: Richmond Class C, 40 miles east
- No drone restrictions nearby
- History of UAS smuggling contraband

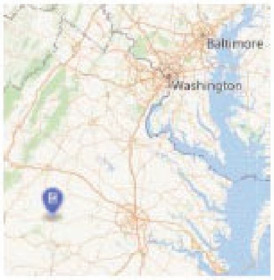


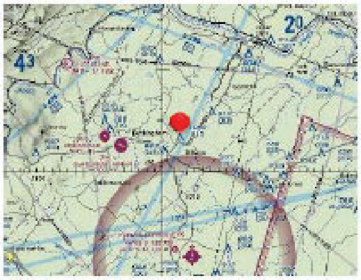
Dozens of drones have been spotted near Virginia prisons. At least one was carrying drugs.

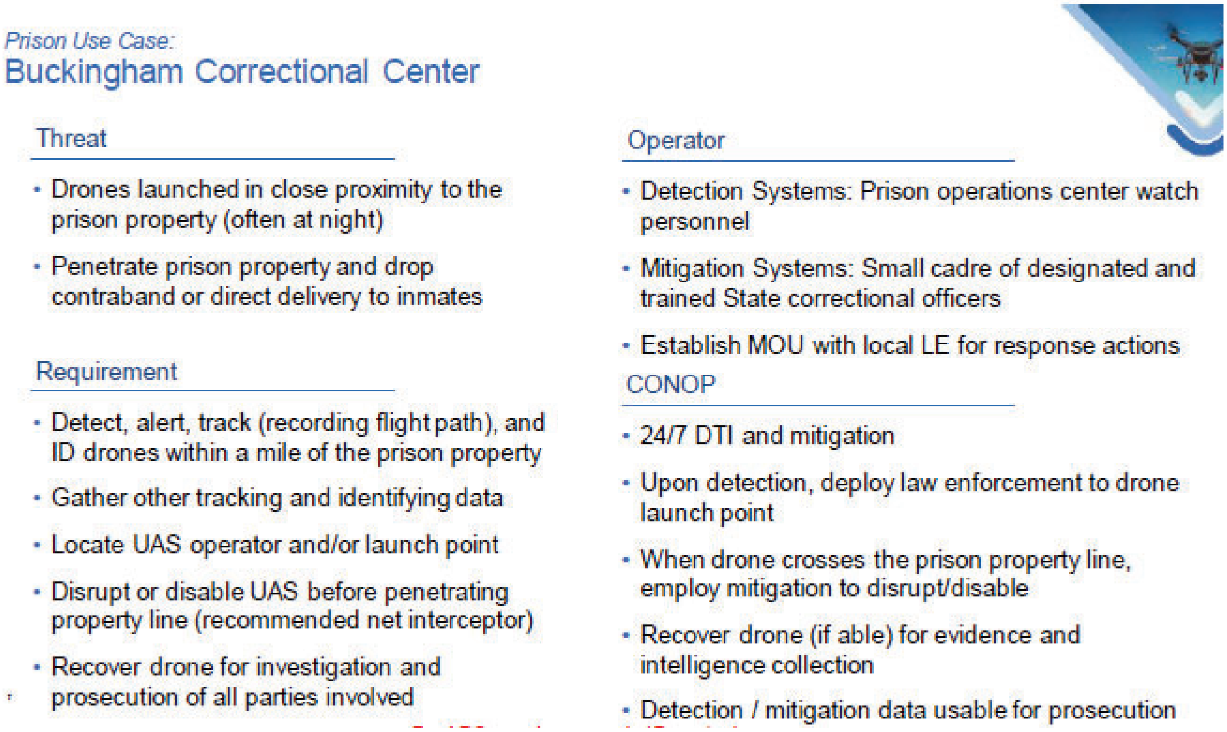
The Virginian-Pilot

BUCKINGHAM CORRECTIONAL CENTER
Department of Corrections
Larry L. Edmonds, Warden









Prison Use Case:

Buckingham Correctional Center

Threat

- Drones launched in close proximity to the prison property (often at night)
- Penetrate prison property and drop contraband or direct delivery to inmates

Requirement

- Detect, alert, track (recording flight path), and ID drones within a mile of the prison property
- Gather other tracking and identifying data
- Locate UAS operator and/or launch point
- Disrupt or disable UAS before penetrating property line (recommended net interceptor)
- Recover drone for investigation and prosecution of all parties involved

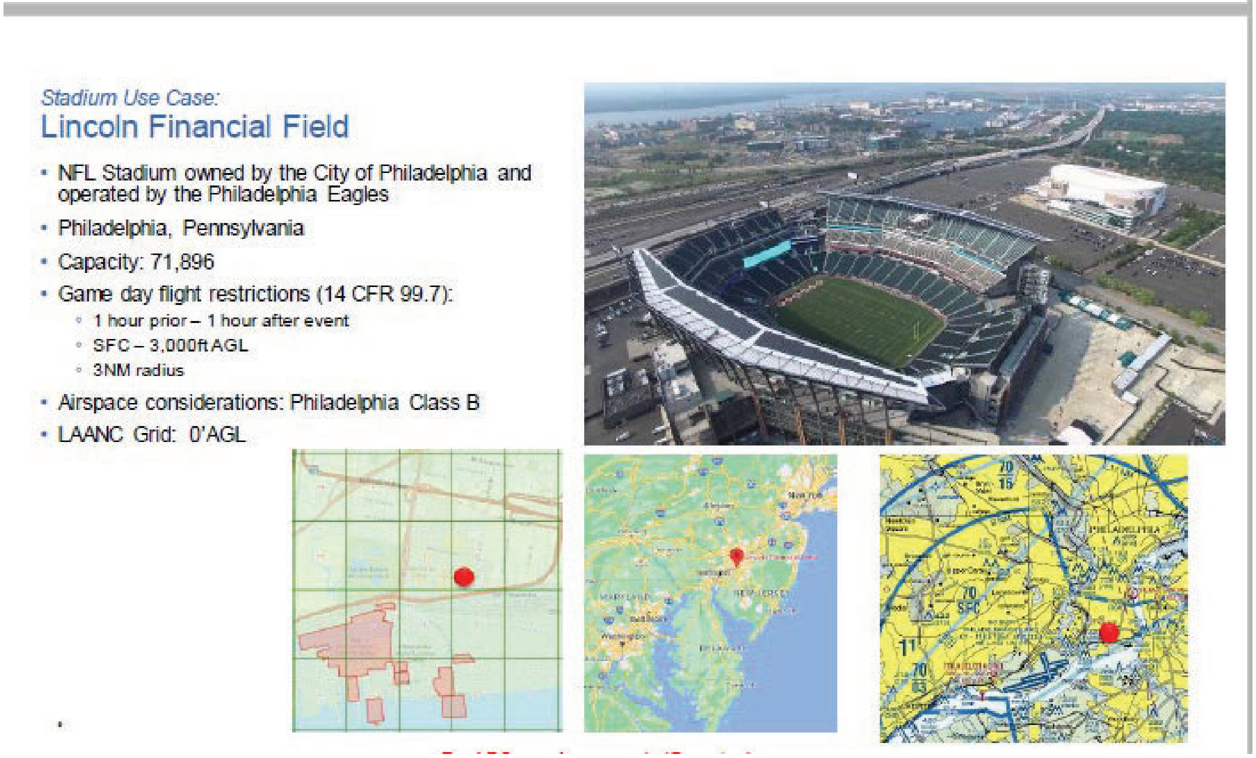
Operator

- Detection Systems: Prison operations center watch personnel
- Mitigation Systems: Small cadre of designated and trained State correctional officers
- Establish MOU with local LE for response actions

CONOP

- 24/7 DTI and mitigation
- Upon detection, deploy law enforcement to drone launch point
- When drone crosses the prison property line, employ mitigation to disrupt/disable
- Recover drone (if able) for evidence and intelligence collection
- Detection / mitigation data usable for prosecution

Use Case 2: Stadium



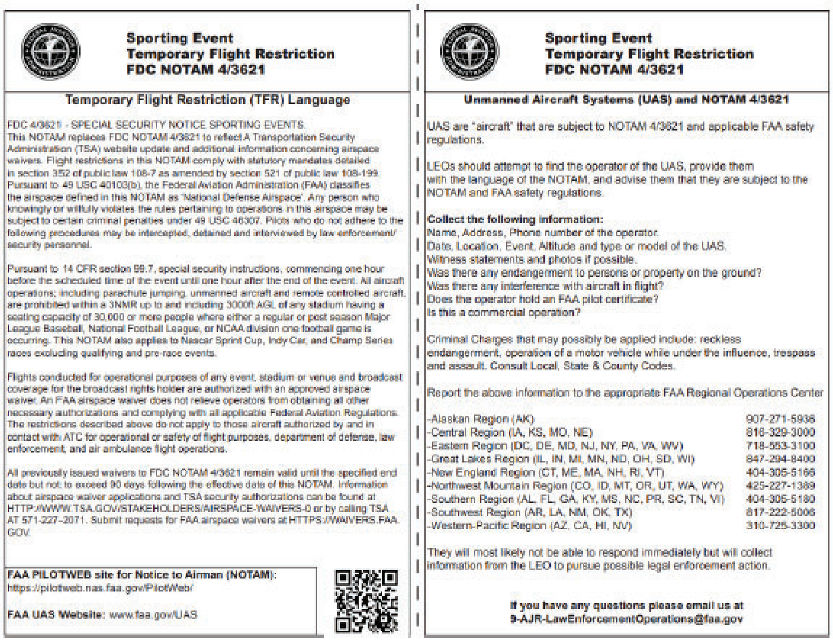
Stadium Use Case:

Lincoln Financial Field

- NFL Stadium owned by the City of Philadelphia and operated by the Philadelphia Eagles
- Philadelphia, Pennsylvania
- Capacity: 71,896
- Game day flight restrictions (14 CFR 99.7):
  - 1 hour prior – 1 hour after event
  - SFC – 3,000ft AGL
  - 3NM radius
- Airspace considerations: Philadelphia Class B
- LAANC Grid: 0'AGL

[illegible]

Sporting Event Temporary Flight Restriction (FDC NOTAM 4/3621)



Sporting Event
Temporary Flight Restriction
FDC NOTAM 4/3621

Temporary Flight Restriction (TFR) Language

FDC 4/3621 - SPECIAL SECURITY NOTICE SPORTING EVENTS.
This NOTAM replaces FDC NOTAM 4/3621 to reflect A Transportation Security Administration (TSA) website update and additional information concerning airspace waivers. Flight restrictions in this NOTAM comply with statutory mandates detailed in section 352 of public law 108-7 as amended by section 521 of public law 108-199. Pursuant to 49 USC 40103(b), the Federal Aviation Administration (FAA) classifies the airspace defined in this NOTAM as 'National Defense Airspace'. Any person who knowingly or willfully violates the rules pertaining to operations in this airspace may be subject to certain criminal penalties under 49 USC 46307. Pilots who do not adhere to the following procedures may be intercepted, detained and interviewed by law enforcement/ security personnel.

Pursuant to 14 CFR section 99.7, special security instructions, commencing one hour before the scheduled time of the event until one hour after the end of the event. All aircraft operations; including parachute jumping, unmanned aircraft and remote controlled aircraft, are prohibited within a 3NMR up to and including 3000ft AGL of any stadium having a seating capacity of 30,000 or more people where either a regular or post season Major League Baseball, National Football League, or NCAA division one football game is occurring. This NOTAM also applies to Nascar Sprint Cup, Indy Car, and Champ Series races excluding qualifying and pre-race events.

Flights conducted for operational purposes of any event, stadium or venue and broadcast coverage for the broadcast rights holder are authorized with an approved airspace waiver. An FAA airspace waiver does not relieve operators from obtaining all other necessary authorizations and complying with all applicable Federal Aviation Regulations. The restrictions described above do not apply to those aircraft authorized by and in contact with ATC for operational or safety of flight purposes, department of defense, law enforcement, and air ambulance flight operations.

All previously issued waivers to FDC NOTAM 4/3621 remain valid until the specified end date but not to exceed 90 days following the effective date of this NOTAM. Information about airspace waiver applications and TSA security authorizations can be found at HTTP://WWW.TSA.GOV/STAKEHOLDERS/AIRSPACE-WAIVERS-0 or by calling TSA AT 571-227-2071. Submit requests for FAA airspace waivers at HTTPS://WAIVERS.FAA.GOV.

FAA PILOTWEB site for Notice to Airman (NOTAM):
https://pilotweb.nas.faa.gov/PilotWeb/

FAA UAS Website: www.faa.gov/UAS

Sporting Event
Temporary Flight Restriction
FDC NOTAM 4/3621

Unmanned Aircraft Systems (UAS) and NOTAM 4/3621

UAS are "aircraft" that are subject to NOTAM 4/3621 and applicable FAA safety regulations.

LEOs should attempt to find the operator of the UAS, provide them with the language of the NOTAM, and advise them that they are subject to the NOTAM and FAA safety regulations.

Collect the following information:
Name, Address, Phone number of the operator.
Date, Location, Event, Altitude and type or model of the UAS.
Witness statements and photos if possible.
Was there any endangerment to persons or property on the ground?
Was there any interference with aircraft in flight?
Does the operator hold an FAA pilot certificate?
Is this a commercial operation?

Criminal Charges that may possibly be applied include: reckless endangerment, operation of a motor vehicle while under the influence, trespass and assault. Consult Local, State & County Codes.

Report the above information to the appropriate FAA Regional Operations Center

-Alaskan Region (AK)	907-271-5936
-Central Region (IA, KS, MO, NE)	816-329-3000
-Eastern Region (DC, DE, MD, NJ, NY, PA, VA, WV)	718-553-3100
-Great Lakes Region (IL, IN, MI, MN, ND, OH, SD, WI)	847-294-8400
-New England Region (CT, ME, MA, NH, RI, VT)	404-305-5166
-Northwest Mountain Region (CO, ID, MT, OR, UT, WA, WY)	425-227-1389
-Southern Region (AL, FL, GA, KY, MS, NC, PR, SC, TN, VI)	404-305-5180
-Southwest Region (AR, LA, NM, OK, TX)	817-222-5006
-Western-Pacific Region (AZ, CA, HI, NV)	310-725-3300

They will most likely not be able to respond immediately but will collect information from the LEO to pursue possible legal enforcement action.

If you have any questions please email us at 9-AJR-LawEnforcementOperations@faa.gov

Stadium Use Case:
Lincoln Financial Field

Threat

- Drones have been spotted on game days over the parking lots and in the seating bowl during the game
- Safety concern for players and fans due to nefarious acts or mass gathering panic

Requirement

- Local law enforcement will provide enforcement of local regulations
- Fixed detection system to detect and identify UAS and operators within 3 miles of stadium
- Active RF mitigation to repel UAS deemed a threat to the safety of individuals at the stadium

Operator

- Detection Systems: Stadium security or local law enforcement officer
- Mitigation Systems: Local law enforcement officer

CONOP

- Event specific DTI and mitigation
- Upon detection, local law enforcement to drone launch point
- When drone flies directly over the stadium, playing area, or seating area, employ mitigation to disrupt/disable
- Recover drone (if able) for evidence collection

Use Case 3: Law Enforcement Application

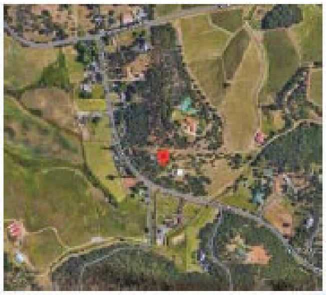
Law Enforcement Use Case:

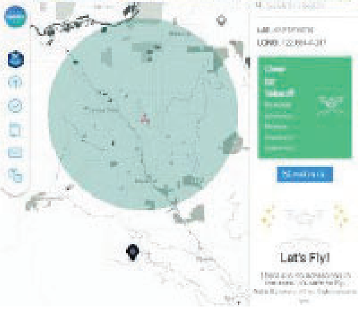
UAS interference in Fire Fighting Response

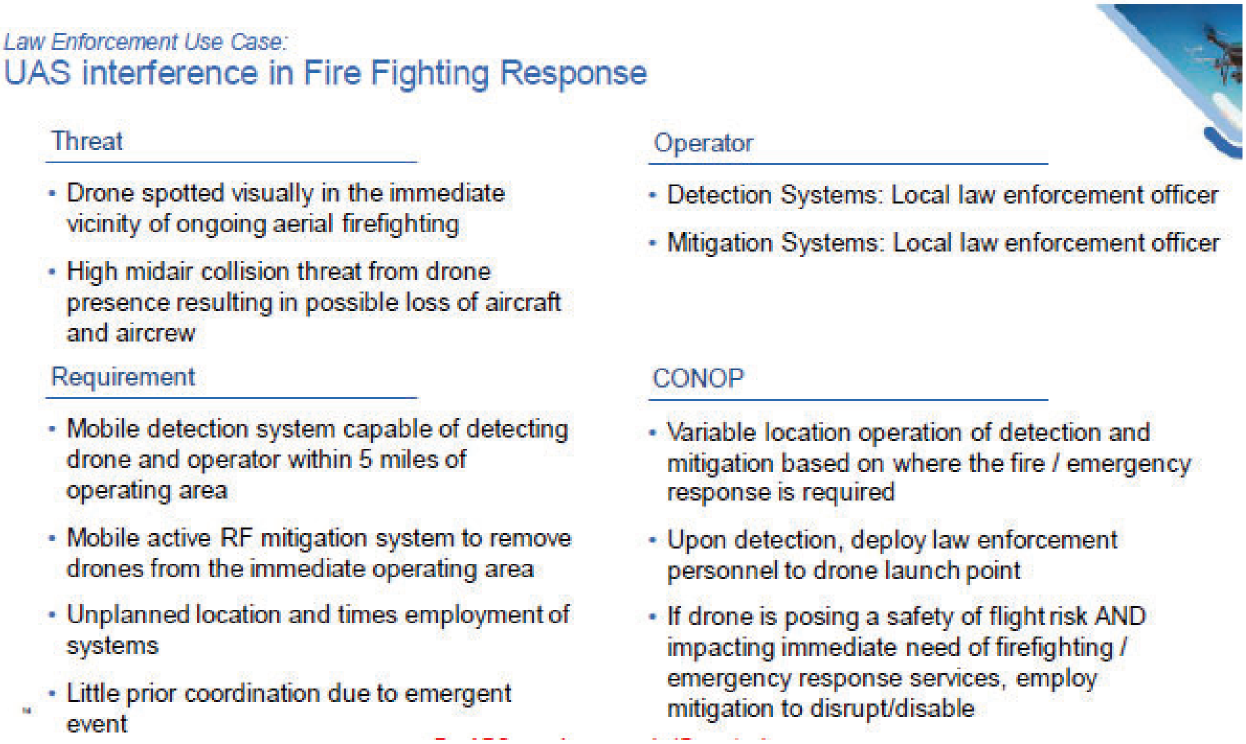
- Structure fire spreading to local forest in Medford, Oregon
- Dept of Forestry helicopter engaged in dropping water on the structure fire
- Drone in the area forced firefighting helicopter to land
- Airspace: Class G

Drone near Talent fire puts firefighting aircraft at risk

by John McMahon | Tue, September 13th 2022, 2:34 PM EDT







Law Enforcement Use Case:

UAS interference in Fire Fighting Response

Threat

- Drone spotted visually in the immediate vicinity of ongoing aerial firefighting
- High midair collision threat from drone presence resulting in possible loss of aircraft and aircrew

Operator

- Detection Systems: Local law enforcement officer
- Mitigation Systems: Local law enforcement officer

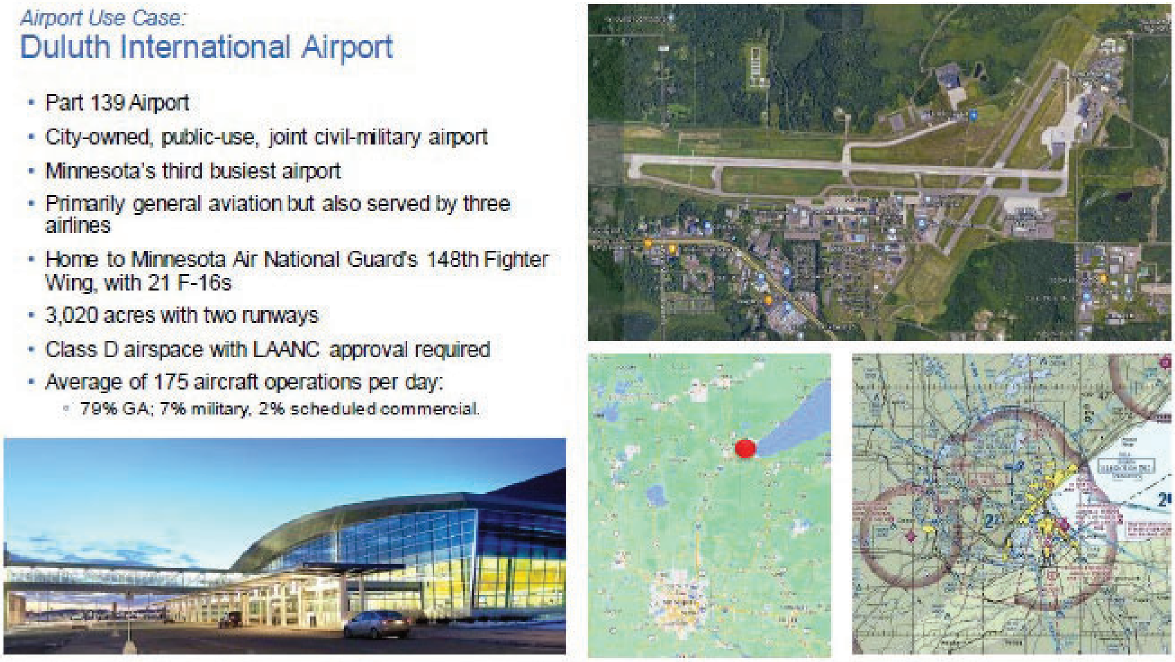
Requirement

- Mobile detection system capable of detecting drone and operator within 5 miles of operating area
- Mobile active RF mitigation system to remove drones from the immediate operating area
- Unplanned location and times employment of systems
- Little prior coordination due to emergent event

CONOP

- Variable location operation of detection and mitigation based on where the fire / emergency response is required
- Upon detection, deploy law enforcement personnel to drone launch point
- If drone is posing a safety of flight risk AND impacting immediate need of firefighting / emergency response services, employ mitigation to disrupt/disable

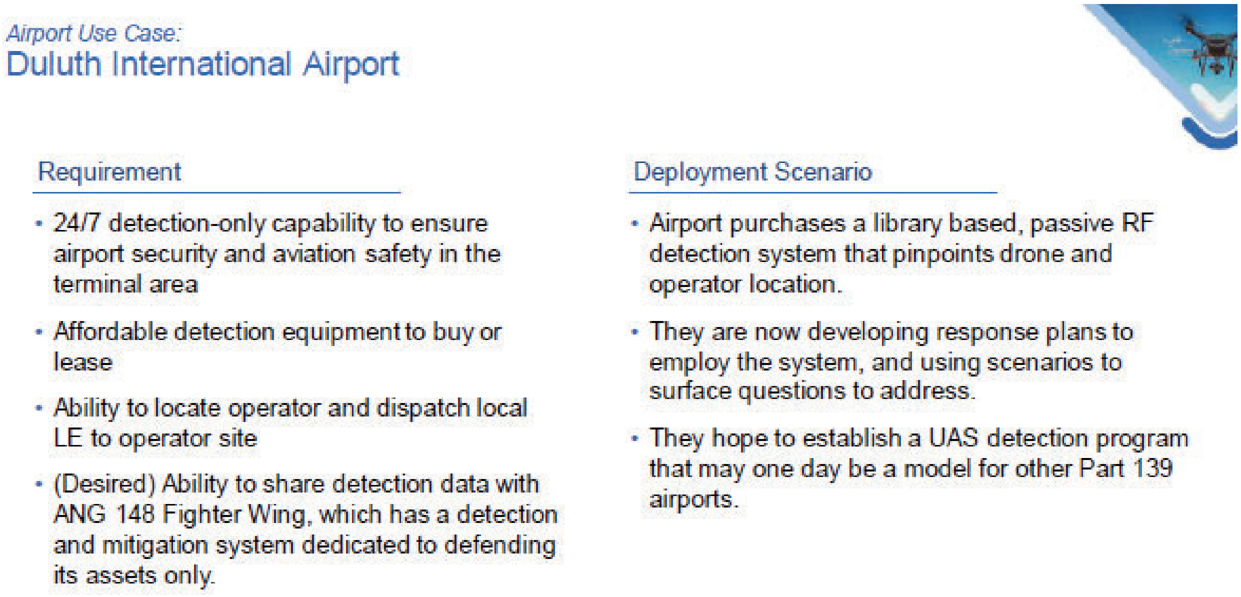
Use Case 4: Airport Detection Scenario



Airport Use Case:

Duluth International Airport

- Part 139 Airport
- City-owned, public-use, joint civil-military airport
- Minnesota's third busiest airport
- Primarily general aviation but also served by three airlines
- Home to Minnesota Air National Guard's 148th Fighter Wing, with 21 F-16s
- 3,020 acres with two runways
- Class D airspace with LAANC approval required
- Average of 175 aircraft operations per day:
  - 79% GA; 7% military, 2% scheduled commercial.



Airport Use Case:

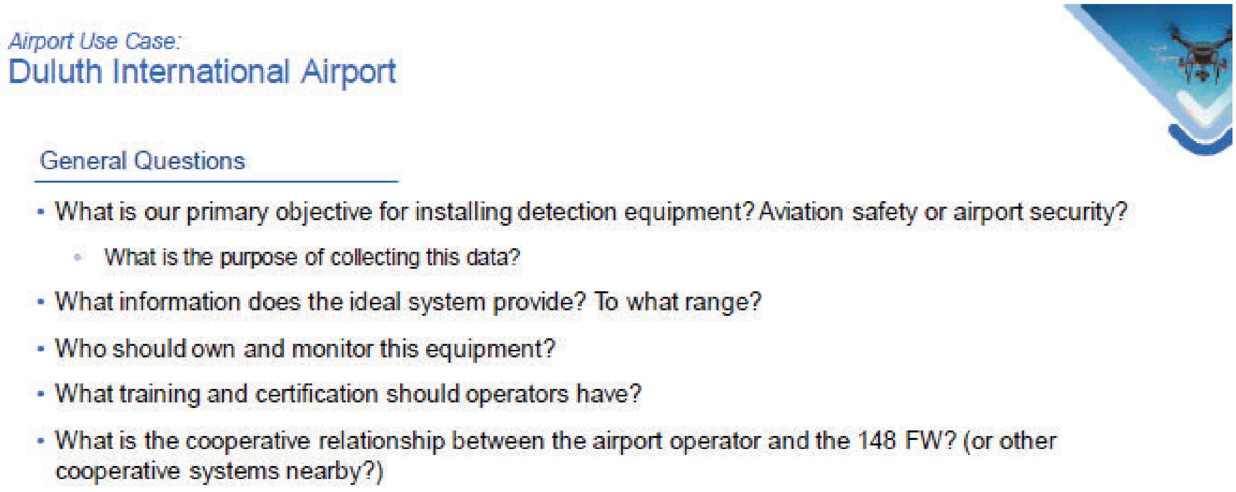
Duluth International Airport

Requirement

- 24/7 detection-only capability to ensure airport security and aviation safety in the terminal area
- Affordable detection equipment to buy or lease
- Ability to locate operator and dispatch local LE to operator site
- (Desired) Ability to share detection data with ANG 148 Fighter Wing, which has a detection and mitigation system dedicated to defending its assets only.

Deployment Scenario

- Airport purchases a library based, passive RF detection system that pinpoints drone and operator location.
- They are now developing response plans to employ the system, and using scenarios to surface questions to address.
- They hope to establish a UAS detection program that may one day be a model for other Part 139 airports.



Airport Use Case:

Duluth International Airport

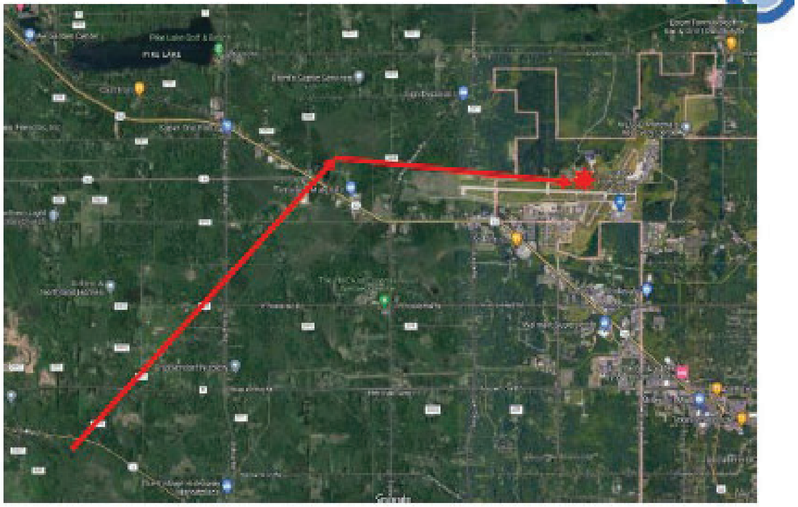
General Questions

- What is our primary objective for installing detection equipment? Aviation safety or airport security?
  - What is the purpose of collecting this data?
- What information does the ideal system provide? To what range?
- Who should own and monitor this equipment?
- What training and certification should operators have?
- What is the cooperative relationship between the airport operator and the 148 FW? (or other cooperative systems nearby?)

Airport Use Case:

Duluth International Airport

Scenario Input 1: The system detects a drone (and launch point) 3 miles southwest of the airport, traveling northeast at 20 knots at 500 ft. As it travels toward the airport, the drone strays north into the approach corridor of Rwy 9 (the active runway) at 1 mile. Turning due east, the drone flies near the runway centerline and penetrates the field boundary. The detection system indicates that it is now hovering within the airport fence line, approximately 100 meters north of Rwy 9.



Airport Use Case:

Duluth International Airport

Scenario Input 1: The system detects a drone (and launch point) 3 miles southwest of the airport, traveling northeast at 20 knots at 500 ft. As it travels toward the airport, the drone strays north into the approach corridor of Rwy 9 (the active runway) at 1 mile. Turning due east, the drone flies near the runway centerline and penetrates the field boundary. The detection system indicates that it is now hovering within the airport fence line, approximately 100 meters north of Rwy 9.

Scenario-based Questions

- Both the airport and the 148 FW have interest in this potentially nefarious drone. How do they share data and jointly address the threat?
- The drone launch point is outside airport property. What are the jurisdictional lines between the airport and local LE?
- How is local LE notified, and what is the desired response?
- The drone is posing a potential hazard to aircraft on approach to Rwy 9. What are the procedures to address this situation?
- If the airport is first to see this drone, who should they notify?
- What are the various trigger points for action? Does the airport define various rings around the airport that trigger escalating actions?
- What is ATC's responsibility to ensure the safety of the NAS? What is the airports responsibility? What role does TSA play?

Airport Use Case:

Duluth International Airport

Scenario Input 2: The drone continues to hover north of Rwy 9. After 15 minutes, the drone crashes on airport property.

Scenario-based Questions

- During the time the drone is hovering, what coordination should take place between the airport operator, FAA, TSA, and 148 FW?
- How is the situation resolved? Who determines when to resume normal operations?
- Who takes possession of the drone and leads the investigation?

Appendix E - ARC Members by Working Group

WG	Organization	Primary	Alternate
	Co-Chairs		
Co-chair	Association of Uncrewed Vehicle Systems International (AUVSI)	Michael Robbins	Max Rosen
Co-chair	UAS and Emerging Entrants Security, FAA	Abby Smith	
Co-chair	Airports Council International – North America (ACI-NA)	Matt Cornelius	Chris Oswald

WG 1: Wider Ecosystem and Public Interests			
1	Airplane Owners and Pilots Association (AOPA)	Jim McClay	Murray Huling
1	Aloft	Jon Hegranes	Brad Llewellyn
1	American Civil Liberties Union	Jay Stanley	
1	Choctaw Nation	James Grimsley	Karen DiMeo
1	Commercial Drone Alliance	Lisa Ellman	Pat Rizzi
1	Conference of Minority Transportation Officials (COMTO)	Terrence Hicks	April Rai
1	Helicopter Association International (HAI)	Christopher Martino	Greg Brown
1	International Association of Fire Chiefs (IAFC)	Christopher Sadler	
1	National League of Cities	Brittney Kohler	McKaia Dykema
1	Society of Chemical Manufacturers and Affiliates	Joe Dettinger	Genevieve Strand
1	The MITRE Corporation	Michelle Duquette	Art Branch

WG 2: System Requirements			
2	Airborne Public Safety Association	Daniel Schwarzbach	Terry Palmer
2	ASRI	Andy Roy	Kris Hutchinson
2	Boeing	Stella Weidner	Ben Ivers
2	Dedrone	Ben Wenger	Mary Lou Smoulders
2	Echodyne	Leo McCloskey	Tom Krogh
2	Honeywell	David Karsch	Sapan Shah
2	Northrop Grumman	Curt Ames	Randy Willis
2	NUAIR	Ken Stewart	Lee Nguyen
2	Raytheon Technologies	Elizabeth Soltys	JJ Johnson
2	RTCA	Terry McVenes	Brandi Teel
2	Skydio	Jenn Player	
2	CTIA	Avonne Bell	Raj Sengupta
WG 3: Sites			
3	National Football League (NFL)	Cathy Lanier	GB Jones

WG 3A: Airports			
3A	Air Line Pilots Association (ALPA)	Eric Herman	Shea Byom
3A	Airport Law Enforcement Agencies Network (ALEAN)	Kevin Murphy	Mike Eversom
3A	Airport Minority Advisory Council (AMAC)	Ernest Huffman	John Sulsona
3A	American Association of Airport Executives (AAAE)	Stephanie Gupta	Justin Barkowski
3A	D-Fend	Ilana Brodesky	Brett Fedderson
3A	Minneapolis-Saint Paul Metropolitan Airports Commission	Roy Fuhrmann	
3A	NATCA	Melvin Davis	Kevin Maney
3A	National Association of State Aviation Officials (NASAO)	Kyle Wanner	Kenji Sugahara
3A	Tampa Airport	Adam Bouchard	
3A	WiMax Forum	Declan Byrne	

WG 3B: Non-airports			
3B	Academy of Model Aeronautics (AMA)	Chad Budreau	Tyler Dobbs
3B	American Correctional Association	Rob Green	Jeffrey Washington
3B	Chula Vista Police Department	Roxana Kennedy	Miriam Foxx
3B	DRONERESPONDERS /Airborne International Response Team (AIRT)	Christopher Todd	Charles Werner
3B	Florida Power and Light	Eric Schwartz	Heath McLemore
3B	International Association of Amusement Parks and Attractions (IAAPA)	Keith Stephenson	Tracy Taylor
3B	Major League Baseball (MLB)	David Thomas	
3B	Pierce Aerospace	Aaron Pierce	Gary Bullock
3B	SkySafe	Grant Jordan	Sam Cook
3B	Stadium Managers Association	Mike McCormick	Angie Nix
3B	WING	Matt Satterley	Steve Fulton

WG4 Operating Requirements			
4	AeroVigilance	Tom Adams AeroVigilance/ High Point Aerotechnologies	Casey Flanagan AeroVigilance /Dedrone
4	Airlines for America	Craig Lowe	
4	Airport Consultants Council (ACC)	Dave Fleet	T.J. Schultz
4	Amazon	Francisco Castillo	
4	ASTM International	Philip Kenul	Ajay Sehgal
4	Cherokee Nation	John Coffey	
4	DFW Airport	Chris McLaughlin	Jon (JT) Taylor
4	Hidden Level	Jeff Cole	
4	Port of Long Beach	Casey Hehr	Michael Goldschmidt
4	Texas Department of Public Safety	Jason Day	Captain Aaron Fritch
4	Virginia State Police	Richard Boyd	David Smith

Appendix F - ARC Member Responses and Voting Results

The ARC believes this report fulfills the tasks in the mission of the Charter. The recommendations contained in this report were robustly debated and the report was accepted by the full ARC prior to submission to the FAA.

In support of a transparent ARC process, members were offered the opportunity to include a (2 page) concurrence or non-concurrence on the final document. All submissions are included in this report.

The ARC completed its deliberations and report drafting on January 9, 2024. Voting ballots were distributed to the 58 voting members. The tally is as follows:

Concur as Written - 53
Concur with Exception - 3
Non-Concur - 1
Ballot Not Submitted - 1

Organization	Primary	Alternate	Voting Response
Academy of Model Aeronautics (AMA)	Chad Budreau	Tyler Dobbs	Concur with Exception
AeroVigilance	Tom Adams AeroVigilance/ High Point Aerotechnologies	Casey Flanagan AeroVigilance /Dedrone	Concur as Written
Air Line Pilots Association (ALPA)	Eric Herman	Shea Byom	Concur as Written
Airborne Public Safety Association	Daniel Schwarzbach	Terry Palmer	Concur as Written
Airlines for America	Craig Lowe		Concur as Written

Airplane Owners and Pilots Association (AOPA)	Jim McClay	Murray Huling	Concur as Written
Airport Consultants Council (ACC)	Dave Fleet	T.J. Schultz	Concur as Written
Airport Law Enforcement Agencies Network (ALEAN)	Kevin Murphy	Mike Eversom	Concur as Written
Airport Minority Advisory Council (AMAC)	Ernest Huffman	John Sulsona	Concur as Written
Airports Council International – North America (ACI- NA)	Matt Cornelius	Chris Oswald	Concur as Written
Aloft	Jon Hegranes	Brad Llewellyn	Concur as Written
Amazon	Francisco Castillo		Concur as Written
American Association of Airport Executives (AAAE)	Stephanie Gupta	Justin Barkowski	Concur as Written
American Civil Liberties Union	Jay Stanley		Concur with Exception
American Correctional Association	Rob Green	Jeffrey Washington	Concur as Written
Aviation Spectrum Resources Inc. (ASRI)	Andy Roy	Kris Hutchinson	Concur as Written

Association of Uncrewed Vehicle Systems International (AUVSI)	Michael Robbins	Max Rosen	Concur as Written
ASTM International	Philip Kenul	Ajay Sehgal	Concur as Written
Boeing	Stella Weidner	Ben Ivers	Concur as Written
Cherokee Nation	John Coffey		Concur as Written
Choctaw Nation	James Grimsley	Karen DiMeo	Concur as Written
Chula Vista Police Department	Roxana Kennedy	Miriam Foxx	Concur as Written
Commercial Drone Alliance	Lisa Ellman	Pat Rizzi	Concur as Written
Conference of Minority Transportation Officials (COMTO)	Terrence Hicks	April Rai	Concur as Written
CTIA	Avonne Bell	Raj Sengupta	Concur with Exception
Dedrone	Ben Wenger	Mary Lou Smoulders	Concur as Written
D-Fend	Ilana Brodesky	Brett Fedderson	Concur as Written

DFW Airport	Chris McLaughlin	Jon (JT) Taylor	Concur as Written
DRONERESPONDERS / Airborne International Response Team (AIRT)	Christopher Todd	Charles Werner	Concur as Written
Echodyne	Leo McCloskey	Tom Krogh	Concur as Written
Florida Power and Light	Eric Schwartz	Heath McLemore	Concur as Written
Helicopter Association International (HAI)	Christopher Martino	Greg Brown	Concur as Written
Hidden Level	Jeff Cole		Concur as Written
Honeywell	David Karsch	Sapan Shah	Concur as Written
International Association of Amusement Parks and Attractions (IAAPA)	Keith Stephenson	Tracy Taylor	Concur as Written
International Association of Fire Chiefs (IAFC)	Christopher Sadler		Concur as Written
Major League Baseball (MLB)	David Thomas		Concur as Written
Minneapolis-Saint Paul Metropolitan Airports Commission	Roy Fuhrmann		Concur as Written

National Air Traffic Controllers Association (NATCA)	Melvin Davis	Kevin Maney	Concur as Written
National Association of State Aviation Officials (NASAO)	Kyle Wanner	Kenji Sugahara	Concur as Written
National Football League (NFL)	Cathy Lanier	GB Jones	Ballot Not Submitted
National League of Cities	Brittney Kohler	McKaia Dykema	Non-Concur
Northrop Grumman	Curt Ames	Randy Willis	Concur as Written
NUAIR	Ken Stewart	Lee Nguyen	Concur as Written
Pierce Aerospace	Aaron Pierce	Gary Bullock	Concur as Written
Port of Long Beach	Casey Hehr	Michael Goldschmidt	Concur as Written
Raytheon Technologies	Elizabeth Soltys	JJ Johnson	Concur as Written
RTCA	Terry McVenes	Brandi Teel	Concur as Written
Skydio	Jenn Player		Concur as Written

SkySafe	Grant Jordan	Sam Cook	Concur as Written
Society of Chemical Manufacturers and Affiliates (SOCMA)	Joe Dettinger	Genevieve Strand	Concur as Written
Stadium Managers Association	Mike McCormick	Angie Nix	Concur as Written
Tampa Airport	Adam Bouchard		Concur as Written
Texas Department of Public Safety	Jason Day	Captain Aaron Fritch	Concur as Written
The MITRE Corporation	Michelle Duquette	Art Branch	Concur as Written
Virginia State Police	Richard Boyd	David Smith	Concur as Written
WiMax Forum	Declan Byrne		Concur as Written
WING	Matt Satterley	Steve Fulton	Concur as Written

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS
Aviation Rulemaking Committee (ARC)
Statement of Concurrence / Non-Concurrence

Voting Member Name	Chad Budreau
Voting Member Organization	Academy of Model Aeronautics

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: ________________________________ Date: ________________

2. Concur with the following exception(s):

AMA appreciates that edits were made to make the final report more concise and to improve readability. Unfortunately, the tone of geofencing within the out-of-scope section can now be incorrectly interpreted as an implied endorsement, which does not reflect the attitude of all ARC participants or previous drafts of the report. For example, there was no consensus from the ARC to “urge” the FAA to consider geofencing. In fact, there was much opposition about geofencing noting concerns about practicality, cost, compliance, liability, safety, and inefficiencies with the technology. As written, perceived benefits now overshadow these geofencing concerns.

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: Chad Budreau Date: Jan 16, 2024

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ________________________________ Date: ________________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	Tom Adams
Voting Member Organization	AeroVigilance/High Point Aerotechnologies

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: Tom Date: 1/16/2024

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ______________________ Date: ____________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ______________________ Date: ____________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	Daniel B. Schwarzbach
Voting Member Organization	Airborne Public Safety Association (APSA)

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: ____________________ Date: 15-Jan-2024

2. Concur with the following exception(s):

__Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.__

Voting Member Signature: ____________________ Date: ____________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ____________________ Date: ____________

__Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.__

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	Jim McClay
Voting Member Organization	Aircraft Owners and Pilots Association (AOPA)

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: ______________________ Date: 1/11/2024

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ______________________ Date: ____________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ______________________ Date: ____________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	Eric Herman
Voting Member Organization	Airline Pilots Assoociation, International

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: ____________________ Date: 01/15/2024

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ____________________ Date: ____________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ____________________ Date: ____________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	CRAIG S. LOWE
Voting Member Organization	AIRLINES FOR AMERICA - (A4A)

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: ______________________ Date: 1/11/2024

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ______________________ Date: ______________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ______________________ Date: ______________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	Kevin Murphy
Voting Member Organization	Airport Law Enforcement Agencies Network (ALEAN)

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: ______________________ Date: 01/14/2024

2. Concur with the following exception(s):

□

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ______________________ Date: ______________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ______________________ Date: ______________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	Ernest Huffman
Voting Member Organization	Airport Minority Advisory Council

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: ______________________ Date: 1/12/24

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ______________________ Date: ______________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ______________________ Date: ______________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	Dave Fleet
Voting Member Organization	Airports' Consultants Council

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

David M. Fleet

Voting Member Signature: David M. Fleet Date: January 18, 2024

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ______________________ Date: ____________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ______________________ Date: ____________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	MATTHEW J. CORNELIUS
Voting Member Organization	AIRPORTS COUNCIL INTL - NORTH AMERICA

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: ______________________ Date: 01/16/2024

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ______________________ Date: ______________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ______________________ Date: ______________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	Jon Hegranes
Voting Member Organization	Aloft Technologies, Inc.

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: Jon Hegranes

box SIGN 1V7Z39QP-1JP8Q5K5

Date: Jan 16, 2024

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ______________________________ Date: ______________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ______________________________ Date: ______________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	Francisco E. Castillo
Voting Member Organization	Amazon Prime Air

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: ____________________ Date: January 19, 2024

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ____________________ Date: __________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ____________________ Date: __________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	Stephanie K. Gupta
Voting Member Organization	American Association of Airport Executives

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: Stephanie K Gupta Date: 1/16/24

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ______________________ Date: ____________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ______________________ Date: ____________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	Jay Stanley
Voting Member Organization	American Civil Liberties Union (ACLU)

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: ______________________________ Date: ________________

2. Concur with the following exception(s):

Please see separate statement.

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ______________________________ Date: Jan. 16, 2024

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ______________________________ Date: ________________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

ACLU
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION

Jay Stanley
Senior Policy Analyst
Speech, Privacy and Technology Project
ACLU National Legal Department

ACLU statement of partial concurrence

As the ARC's lone representative that advocates for privacy and First Amendment rights, the ACLU finds much to agree with in this report, including the need for reasonable drone security measures; clear and regular processes by which rules prohibiting drones from flying in certain spaces can be enforced; and rules governing when and how counter-UAS technology can be applied to deal with illegal drone operations. We agree on the need for public communication, performance standards for C-UAS systems, and vigorous protection of airports, among other recommendations.

We embrace the inclusion of recommendation PL5, which urges that security imperatives be properly balanced against the privacy and civil liberties of the public, and the crucial recommendation that the agency be mindful that "security" has been and likely will again be used to try to block legal photography. We endorse the recommendation [PL7] that the FAA carefully balance the benefits for security against a range of other interests including privacy; the recommendation that the FAA establish protocols for limits on data collection, retention, and sharing [DM1]; and the ARC's recognition that drone "mitigation" (the destruction or incapacitation of a drone) should be "a last resort option" [line 1952].

There are also several recommendations that run contrary to our views. Overall, we urge the FAA to support a limited C-UAS system that that avoids unnecessary complexity and focuses on the most significant security threats from drones.

- We do not agree with recommendations that the FAA build complex infrastructures for tracking drone use and drone users and invest heavily in an identity-based approach to security [DM3]. The report generally fails to recognize the importance of preserving access to the use of drones by ordinary people, and the harm to such access that C-UAS may pose to that access as applied by a very troubled U.S. law enforcement establishment.

- We are strongly opposed to the creation of a vaguely defined "verified operator program" [DM4 and NP3 lines 2568-69], aka "PreCheck for Drones." Given the practical, administrative, privacy, due process, and security problems that would result, we strongly urge the FAA to decisively reject this un-American attempt to create first- and second-class drone operators. Such a program would have limited security utility, since knowing someone's identity doesn't reveal their intent. It would introduce additional complexity into the C-UAS system, which is bad for security, and the reduced scrutiny paid to those who are "in the club" would open up vulnerabilities to be exploited. Other questions abound: Who would administer the program? What data would qualification or rejection be based on? Indeed, just how much information would have to be gathered and verified about an operator to mean they're "trusted" — and where would that data collection stop? What would the due process procedures be for those who are rejected from "trusted" status? Would it apply to individuals or companies? If the latter, would individual employees be vetted? How and in what circumstances, exactly, would a "trusted" operator receive different treatment from other drone operators?

- The "verified operator" and other portions of the report seem to contemplate that mitigation will be a routine activity, rather than an extraordinary one. We recognize that drones may pose a legitimate security threat to crowded stadiums or nuclear power plants, but “Critical Infrastructure” is a very elastic term, many definitions of which sweep in a significant portion of land in the United States. We don’t want law enforcement officers to end up with what amounts to a plenipotentiary power to take down any drone they wish. All too often we have seen expansive powers granted to security agencies based on extreme terrorism scenarios, only to be used and abused in everyday life. Although the report recommends that the FAA expand [NP3] and lobby Congress to expand [NP1] mitigation authority, it contains no commensurate recommendations on how C-UAS can be properly limited so that mission creep doesn’t close out much of our airspace to ordinary people. The danger of sweeping, comprehensive C-UAS systems is that they will be overused, with just this result.

- The report also contemplates giving industry special access to the drone equivalent of license plate data, and potentially other data collected about drone operations [DM2]. We strongly believe that any drone data provided to companies should also be provided to members of the public, who, after all, may also find a suspicious drone hovering over their property.

- Not included in the report is a recommendation — vital in our view — that the FAA be mindful in its policymaking of the importance that individual drone owners receive due process from a neutral disinterested party should their drone be improperly damaged, destroyed, or seized by law enforcement or other party exercising mitigation authority. Mistakes and abuses are inevitable, and innocent drone operators in such cases have the right to fair treatment.

- Finally, the report incorporates the concept of mitigating drones through “takeover” [line 954] of a targeted aircraft. Assuming that such a takeover would only be possible based on security vulnerabilities in the drone's software, aka “zero days,” that raises a number of problems that the ARC declined to comment upon. We recommend the FAA work to require that discovery of any security vulnerabilities in drones be immediately shared with drone manufacturers so they can be patched, and not kept secret for C-UAS purposes. As with personal computers and other devices, failure to do so leaves the drones vulnerable to hacking not just for legitimate C-UAS operations but also by nefarious actors. For the same reason, we recommend a ban on the creation of backdoors in drone security systems.

Jay Stanley
ACLU

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	Rob Green
Voting Member Organization	American Correctional Association

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: Rob Green Date: January 18, 2024

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ______________________ Date: ____________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ______________________ Date: ____________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	Philip Kenul
Voting Member Organization	American Society for Testing & Materials (ASTM International)

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: Philip Kenul Date: January 17, 2024

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ______________________ Date: ____________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ______________________ Date: ____________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	Michael Robbins
Voting Member Organization	Association for Uncrewed Vehicle Systems International (AUVSI)

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: Michael Robbins

Date: 12 JAN 2024

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ____________________ Date: ____________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ____________________ Date: ____________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	Andrew Roy
Voting Member Organization	Aviation Spectrum Resources Inc. (ASRI)

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: ______________________ Date: 18 Jan 2023

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ______________________ Date: ______________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ______________________ Date: ______________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	John "JC" Coffey
Voting Member Organization	Cherokee Nation Federal

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: ____________________ Date: 01/16/2024

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ____________________ Date: ____________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ____________________ Date: ____________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	James Grimsley
Voting Member Organization	Choctaw Nation of Oklahoma

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: ______________ Date: Jan 12, 2024

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ______________ Date: ______________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ______________ Date: ______________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	Roxana Kennedy
Voting Member Organization	Chula Vista Police Department

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: Roxana Kennedy ____________________ Date: 1/17/2024

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ____________________ Date: ____________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ____________________ Date: ____________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	Lisa Ellman
Voting Member Organization	Commercial Drone Alliance

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: Lisa ______________________ Date: January 16, 2024

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ______________________ Date: ____________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ______________________ Date: ____________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	Terrence M. Hicks
Voting Member Organization	Conference of Minority Transportation Officials

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: ____________ Date: 01/17/24

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ____________ Date: ________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ____________ Date: ________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	Avonne Bell
Voting Member Organization	CTIA

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: ______________________ Date: ____________

2. Concur with the following exception(s):

CTIA appreciates the opportunity to participate and contribute to the important work of the D&M ARC. We applaud the efforts of the FAA team, ARC co-chairs, and all participants to find consensus on the key issues. While the discussion of networked remote ID was deemed out of scope, we take exception with the characterization of the capabilities of this technology. Cellular networks are secure, reliable and available in most parts of the country with increasing coverage in exurban and rural areas. We recommend that, as the FAA looks to adopt policies from the ARC's report, it more broadly considers the potential that enabling technologies like UTM and remote ID supported by networked communication present for improving awareness of the NAS.

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: Avonne Bell Date: 1/16/2024

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ______________________ Date: ____________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	Benjqmin Wenger
Voting Member Organization	Dedrone

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: ______________________ Date: 1/16/24

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ______________________ Date: ______________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ______________________ Date: ______________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	Ilana Bodesky
Voting Member Organization	D-Fend

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection And Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: Ilana Bodesky Date: 1/17/24

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ____________________ Date: ____________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ____________________ Date: ____________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	CHRIS McLAUGHLIN
Voting Member Organization	DFW AIRPORT

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: ______________________ Date: 1/11/24

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ______________________ Date: ______________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ______________________ Date: ______________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	Christopher Todd
Voting Member Organization	AIRT / DRONERESPONDERS

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: ______________________ Date: 1/16/2024

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ______________________ Date: ______________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ______________________ Date: ______________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	Leo McCloskey
Voting Member Organization	Echodyne

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: Leo McCloskey Date: 01/15/2024

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ______________________ Date: ____________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ______________________ Date: ____________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	Eric Schwartz
Voting Member Organization	Florida Power and Light Company

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: Eric Schwartz Date: 1-10-2024

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ______________________ Date: ____________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ______________________ Date: ____________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	Christopher A. Martino
Voting Member Organization	Helicopter Association International

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: C.A. Martino Date: 15 January 2024

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ______________________ Date: ____________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ______________________ Date: ____________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	Jeff Cole
Voting Member Organization	Hidden Level Inc

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: ______________________ Date: 01/15/2024

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ______________________ Date: ______________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ______________________ Date: ______________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	Adam Bouchard
Voting Member Organization	Hillsborough County Aviation Authority

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: ______________________ Date: 1-15-24

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ______________________ Date: __________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ______________________ Date: __________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	David Karsch
Voting Member Organization	Honeywell

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: ______________________ Date: 1/16/24

2. Concur with the following exception(s):

Honeywell

BUILDING TECHNOLOGIES

Dave Karsch
Director of Regulated Markets

1583 Gregory Drive
Warrington, PA 18976-1570
215-266-3473 Mobile

honeywell.com
@honeywell

dave.karsch@honeywell.com

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ______________________ **Date:** ______________

3. Non-Concur. Letter of Dissent must be provided.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)
Statement of Concurrence / Non-Concurrence

Voting Member Name	Keith Stephenson, Director of Public Affairs
Voting Member Organization	IAAPA, the Global Association for the Attractions Industry,

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written:

Voting Member Signature: ________________________________ Date: ________________

2. Concur with the following exception(s):

IAAPA, the Global Association for the Attractions Industry, concurs with the final report since fixed-site amusement parks are defined as one of the 16 critical infrastructure sectors, and by extension, are defined as a high-risk venue on page 11 (sentence 320-339) within the final report.

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: **Date:** 1/22/2024

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ________________________________ Date: ________________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	Christopher W. Sadler
Voting Member Organization	International Association of Fire Chief's

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: Christopher W. Sadler Date: January 12, 2024

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ____________________ Date: __________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ____________________ Date: __________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	David L. Thomas
Voting Member Organization	Major League Baseball

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: ______________________ Date: 1.17.2024

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ______________________ Date: ______________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ______________________ Date: ______________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	Roy Fuhrmann
Voting Member Organization	Metropolitan Airports Commission

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: ______________________ Date: _January 15, 2024_____

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ______________________ Date: ______________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ______________________ Date: ______________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	Melvin S. Davis
Voting Member Organization	National Air Traffic Controllers Association

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: Melvin S. Davis Date: 1/16/2024

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ____________________ Date: __________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ____________________ Date: __________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	Kyle Wanner
Voting Member Organization	National Association of State Aviation Officials (NASAO)

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: Kyle Wanner Date: 1/12/2024

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ____________________ Date: ____________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ____________________ Date: ____________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA Section 383 UAS Detection and Mitigation Systems Aviation Rulemaking Committee

Statement of Concurrence / Non-Concurrence

Voting Member Name	Brittney Kohler
Voting Member Organization	National League of Cities

As a voting member and full participant of the FAA Section 383 UAS Airport Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the ARC Recommendations Final Report and make the following declaration regarding the Report:

1. Concur with the Final Document as written

Voting Member Signature: ________________________Date: _________________

2. Concur with the Final Document with the following exception(s): **(Fully explain the areas of exception below, providing specific page and line number. Submission of separate paper is acceptable).**

Voting Member Signature: ___________________________________ Date: _________________

3. Non-Concur with the Final Report. Letter of Dissent on company letterhead must be provided.

Voting Member Signature: Brittney Kohler Date: 1/16/24

NATIONAL LEAGUE OF CITIES

CITIES STRONG TOGETHER

January 16, 2024

RESPONSE TO THE FINAL REPORT OF THE FAA UAS DETECTION AND MITIGATION SYSTEMS AVIATION RULEMAKING COMMITTEE

The National League of Cities (NLC) appreciates the work of this Aviation Rulemaking Committee (ARC) to advance meaningful dialogue with FAA on the potential use of Counter UAS (C-UAS) systems in the U.S. airspace. However, the limitations of the charter for the ARC led to recommendations which overstate the benefits and need for large-scale deployment of C-UAS by both government and non-governmental actors while minimizing the costs and relevant overlapping policies, which could limit the homeland security risks that are deeply concerning to local governments.

Enabling vast UAS users without appropriate limits, policy, and respect for the capacity of air traffic management today puts the safety and security of our nation's airspace, and more importantly, residents at risk. Furthermore, coalescing around C-UAS mitigation military-grade technology as a primary solution to manage errant UAS and airspace safety when it is banned by the Federal Communication Commission (FCC) from operating in the U.S. due to interference in 9-1-1 and other public safety systems begs the question of whether the cure is worse than the disease our current federal policy has unleashed. No federal agency has expressed confidence that C-UAS mitigation technology has been appropriately tested in modern American cities with complex telecommunication landscapes - including airports and heliports, emergency response systems and various security and communications systems.

In addition to any damages to local systems by C-UAS use, of particular concern to local governments is that both federal legislation offering the ability to purchase C-UAS technology to select local governments is as stark an unfunded federal mandate as the current directions of FAA for local first responders to engage with all the clueless, careless, and criminal UAS operators being reported by the public. Therefore, NLC concurs with the ARC that the FAA must account for the monetary and non-monetary costs of the C-UAS detection and mitigation policy including Title 18 liability protections.

With appropriate local government support, reasonable law enforcement entities concerned for the public's welfare are actively soliciting C-UAS tools in the absence of rational federal action. But NLC must reiterate that a more holistic policy review is needed to mitigate the risks and rewards of UAS and Advanced Air Mobility (AAM), in light of the current stark international conflicts highlighting UAS and C-UAS capabilities. The escalating demand for detection and mitigation of C-UAS equipment is directly related to a permissive policy on UAS today, but even with authority, it is possible our individual localized purchases may not create the same benefits as a collective C-UAS system or a distributed C-UAS authority structure.

For reference, NLC would like to express several significant policy reflections based on the recommendations of the final ARC report:

- NLC believes that UAS detection technology should be adapted into a national shared resource by the FAA that integrates with airspace management immediately, or it should be developed and managed exclusively by DHS with access for authorized users such as air traffic control, local law enforcement and critical infrastructure owners. Either option requires Congressional mandates and appropriate support.

- NLC disagrees with the ARC that the FAA has the authority or technical capacity to deploy C-UAS mitigation or its performance standards, best practices, or training. However, FAA should organize the aviation industry stakeholders to have DHS ingest and test aviation specific concerns with various C-UAS technologies before deployment. With this approach, FAA will not need to approve C-UAS system as DHS should ensure that they will not impact aviation or the entirety of ground-based local safety systems. To be effective, Congress must direct DHS to expeditiously confirm legal authority for testing of C-UAS technologies, including in complex environments, before expanding operations which would establish the regulatory certainty that industry seeks.

- NLC concurs with the ARC that it is impossible to have a safe NAS without also having a secure one. Therefore, pilots and aircraft must be responsible for the safety of the airspace and deconfliction in flight, and with the size of UAS and number of operations expected, operator privacy must be secondary to responsible and appropriate transmission of identity to FAA, location of the operator and UAS, and flight plans that can deconflict traffic as well as limit nuisance and privacy concerns of the greater public.

- NLC is concerned by the ARC’s user-agnostic approach to the C-UAS user, given the damage, risk to residents on the ground, and the threat to aircraft. Access to C-UAS should be intentionally granted to responsible entities that protect our national interests and all C-UAS systems should be registered at point of sale and retired to the DHS or other appropriate entity. A spiral development approach could be valuable to national coverage.

- NLC concurs with the public safety community that strongly believes that now is the best opportunity to reassess the current operational paradigm surrounding how airspace within the NAS is designated and controlled for future use by all stakeholders, as well as the communication system to pilots that both deserve appropriate federal resources to address. We also strongly encourage FAA to substantially ease the burden on local governments to utilize Temporary Flight Restrictions and provide notices to pilots on recommended routes to minimize risks to the public.

In summary, NLC encourages the FAA to advance detection capabilities expeditiously into their air traffic management mandate and share these tools with local government emergency response, as well as prioritize the ways their current policy and procedures can be amended to more economically fill security gaps that lead to a more secure and advanced airspace and deferring technical approval and use of C-UAS mitigation to DHS and FCC. The National League of Cities welcomes the opportunity to work with the FAA, DHS and FCC to accomplish these goals and continue to encourage a safe and secure airspace for all communities across the country.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name Curtis Ames

Voting Member Organization Industry

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: ____________________ Date: 1/16/24

2. Concur with the following exception(s):

N/A

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ____________________ Date: ____________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ____________________ Date: ____________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	KENNETH STEWART
Voting Member Organization	NUAIR Inc.

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: Ken Stewart Date: 1/17/2024

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ____________________ Date: ____________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ____________________ Date: ____________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	Aaron Pierce
Voting Member Organization	Pierce Aerospace Inc

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: ____________________ Date: 18 JAN 2024

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ____________________ Date: __________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ____________________ Date: __________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	Casey Hehr
Voting Member Organization	Port of Long Beach

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: ______________________ Date: 1/18/2024

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ______________________ Date: __________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ______________________ Date: __________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	Elizabeth Soltys
Voting Member Organization	Raytheon Technologies

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: ______________ Date: 1/15/2024

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ______________ Date: ______________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ______________ Date: ______________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	Terry L. McVenes
Voting Member Organization	RTCA, Inc.

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: Terry L McVenes Date: January 15, 2024

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ______________________ Date: ______________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ______________________ Date: ______________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	Jenn Player
Voting Member Organization	Skydio, Inc.

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: ______________________ Date: 1/15/2024

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ______________________ Date: ____________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ______________________ Date: ____________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	Grant Jordan
Voting Member Organization	SkySafe

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: ______________________ Date: 01/16/2024

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ______________________ Date: ______________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ______________________ Date: ______________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	Joe Dettinger
Voting Member Organization	SOCMA

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: ____________________ Date: 1-18-24

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ____________________ Date: ____________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ____________________ Date: ____________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	Mike McCormick
Voting Member Organization	Stadium Managers Association

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: ________________________ Date: 1/16/2024

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ________________________ Date: ____________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ________________________ Date: ____________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	Jason L. Day
Voting Member Organization	Texas Department of Public Safety

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: ______________________ Date: 1/16/24

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ______________________ Date: __________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ______________________ Date: __________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	Stella Weidner
Voting Member Organization	The Boeing Company

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: /s/ Stella Weidner Date: January 12, 2024

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ______________________ Date: ____________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ______________________ Date: ____________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	**Michelle A Duquette**
Voting Member Organization	**The MITRE Corporation**

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: ______________ Date: **16 JAN 2024**

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ______________ Date: ______________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ______________ Date: ______________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	DJ Smith
Voting Member Organization	Virginia Department of State Police

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: ______________ Date: 01/16/2024

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ______________ Date: ______________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ______________ Date: ______________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	Declan Byrne
Voting Member Organization	WiMAX Forum

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection And Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: Date: _______January 18, 2024____

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ___________________________________ Date: _________________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ___________________________________ Date: _________________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

FAA UNMANNED AIRCRAFT SYSTEMS DETECTION AND MITIGATION SYSTEMS

Aviation Rulemaking Committee (ARC)

Statement of Concurrence / Non-Concurrence

Voting Member Name	Matthew Satterley
Voting Member Organization	Wing Aviation LLC

As a voting member and full participant of the FAA Unmanned Aircraft Systems Detection and Mitigation Systems ARC, I hereby acknowledge that I have reviewed the Final Report and recommendations and make the following statement:

1. Concur with the Final Report as written

Voting Member Signature: Matthew P Satterley Date: 01/16/2024

2. Concur with the following exception(s):

Fully explain the area(s) of exception in the text box above and include the specific line number from the document. Member may submit a separate paper on company letterhead if additional space is required. Separate papers may not exceed 2 pages in length.

Voting Member Signature: ______________________ Date: ______________

3. Non-Concur. Letter of Dissent must be provided.

Voting Member Signature: ______________________ Date: ______________

Letters of Dissent must be on company letterhead and may not exceed 2 pages in length.

Wing

First and foremost, thank you to the FAA for the opportunity to engage with a diverse group of stakeholders on the multifaceted issue of counter-UAS, which is becoming increasingly relevant and important. The Non-Airports Working Group 3B - in which Wing participated - was emblematic of the wide-ranging applicability of counter-UAS, with representation that included law enforcement, utilities, correctional institutions, public arenas, sporting facilities and the commercial drone industry. Each member provided unique insights that were essential to shaping our recommendations on how to best prevent errant or nefarious drone activity while permitting airspace access for authorized and compliant UAS operations. Both our commonalities and distinctive perspectives enabled us to produce thoughtful and forward-looking recommendations. We appreciate the FAA's leadership and time in their coordination with our working group's efforts. From this engagement, we feel that we have had the opportunity for our voice to be heard.

We look forward to the FAA's further action on the report's recommendations for data management, as we believe they represent an initial priority that will improve the ability of drones to be perceived in a trusted and secure manner. An industry-led data access management system will be particularly instrumental in ensuring that security personnel and other entities have access to information that will enhance situational awareness, threat assessment and security in the NAS. These entities can have greater access to digitized information, including from LAANC, Remote ID and UTM, that can enable them to more effectively perform the time-critical responsibility of identifying compliant operators.

Another recommendation in the report that will support these identification efforts is the establishment of a voluntary Verified Operator Program (VOP) in which qualified operators that choose to opt into this program can be more readily identified as credentialed and granted airspace access that might not be otherwise accessible.

In all ARC initiatives, including those pertaining to data management, ARC members place paramount importance in safeguarding user and aviation data. These protections should place particular emphasis on providing appropriate privacy, data protection and data retention safeguards for personally identifiable information (PII). The introduction of sUAS into our everyday lives has evolved the relationship of aviation and aircraft with the average citizen. In this new dynamic, customer behaviors and personal preferences (eg, drone delivery from specific retailers) may be exposed in certain data collection activities that were previously unseen under conventional aviation policies. As such, the FAA should consider the extension of privacy and data protection policies through to the end user.

The report initiates an important conversation on the roles and responsibilities of counter-UAS entities and technologies. While counter-UAS can act as a valuable tool in enhancing security and situational awareness in the NAS, it would be beneficial to clarify that D/M technologies are not a traffic deconfliction tool. As stated in other recommendations in the report, the diverse suite of D/M technologies provide targeted information to enable the effective identification of compliant UAS operators.

We appreciate the ARC's concerted efforts to clearly define and differentiate the counter-UAS workflow terms of Detection, Identification and Mitigation which introduces a deliberate and proportional methodology when considering the risk of proximate drones. Recognizing the unique purpose and scope of each stage of the counter-UAS processing chain, the ARC as a whole emphasized tailored training, policies and rules for the testing and implementation of these counter-UAS actions. The ARC's analysis was targeted and nuanced in both distinguishing between these roles and also demonstrating how they relate to one another, as evidenced in a recommendation to correlate detection with identification whenever possible. We believe this clarification and direction will help prevent the undue mitigation or restriction of lawful UAS activity.

We joined several members of the ARC in voicing support for the FAA to embrace future opportunities for Network Remote ID as a valuable Detection and Identification asset for the upcoming era of routine BVLOS flights; and would further suggest its consideration as an alternative means of compliance for the Remote ID rule. This technology would enhance the identification of UAS at extended ranges, beyond what is technically feasible with current Broadcast Remote ID transmissions, and provide additional safeguards preventing data from unauthorized access or becoming compromised.

Given the dynamic nature of the UAS industry, we realize that the sector's associated technology will continue to evolve. As such, there are certain technologies today that have outpaced the applicability or efficacy of current UAS regulation, while there may be opportunities for existing and potential future technologies to improve situational awareness prior to FAA regulatory activity. We appreciate and encourage the FAA's continued evaluation of UAS technology as this will be critical to the responsible and effective growth of the UAS and counter-UAS industry.

We look forward to further action from the FAA on this very timely topic and stand ready to continue supporting the FAA and industry as a whole however appropriate and necessary.