

UAS Identification and Tracking (UAS ID) Aviation Rulemaking Committee (ARC)

ARC Recommendations Final Report

September 30, 2017

Page intentionally left blank

Table of Contents

1. BACKGROUND.....	1
2. OBJECTIVES AND SUMMARY OF ACTIVITIES OF THE ARC.....	1
3. EXECUTIVE SUMMARY	2
4. DEFINITIONS.....	7
5. DISCUSSION.....	9
5.1. Available and emerging technologies for remote ID and tracking of UAS	9
5.1.1. Identifying viable technology solutions.....	10
5.1.2. Criteria for reviewing and rating viable technology solutions	11
5.1.3. Analysis of viable technology solutions	23
5.2. Requirements for meeting the security and public safety needs of the public safety officials, homeland defense, and national security communities for the remote identification and tracking of UAS .	27
5.2.1. Identifying the needs of public safety officials.....	27
5.2.2. Impacts to safety and security from unmanned aircraft.....	28
5.2.3. Applicability of ID and tracking requirements	29
5.3. Feasibility and affordability of available technical solutions, and the ability of those technologies to address the needs of public safety and air traffic control communities.....	31
6. ARC RECOMMENDATIONS	31
6.1. Applicability of the ID and tracking requirements	31
6.2. Direct broadcast and network publishing requirements for remote ID and tracking.....	33
6.2.1. Direct broadcast (locally)	33
6.2.2. Network publishing (to an FAA-approved internet-based database).....	33
6.3. Tiered UAS direct broadcast and network publishing requirements for remote ID and tracking....	35
6.3.1. Tier 0 – No ID and tracking requirement.....	36
6.3.2. Tier 1 – Direct broadcast (locally) <i>or</i> Network publish to FAA-approved internet-based database	37
6.3.3. Tier 2 – Direct broadcast (locally) <i>and</i> Network publish to FAA-approved internet-based database	37
6.3.4. Tier 3 – Flight under part 91 rules	37
6.4. Implementation approach to direct broadcast and network publishing requirements for remote ID and tracking.....	38
6.4.1. Pre-Rule.....	38
6.4.2. Before final rule is enacted	38
6.4.3. After final rule enacted.....	38
6.5. Types of data related to direct broadcast and network publishing requirements for remote ID and tracking	39
6.5.1. Unique identifier of the UA	39
6.5.2. Tracking information for the UAS.....	40

6.5.3.	Identifying information of the UAS owner and remote pilot.....	41
6.5.4.	Mission type (optional).....	42
6.5.5.	Route data (optional).....	42
6.5.6.	Operating status (optional).....	42
6.5.7.	Table of data elements, time of data provision, and requirements	42
6.6.	Key implementation considerations from ATC and for critical infrastructure and airports.....	44
6.6.1.	Air Traffic Control.....	44
6.6.2.	Airports and Critical Infrastructure.....	45
7.	OTHER RECOMMENDATIONS AND CONSIDERATIONS.....	46
7.1.	Access to data related to direct broadcast and network publishing requirements for remote ID and tracking.....	46
7.1.1.	Public access	46
7.1.2.	Designated public safety and airspace management officials access	47
7.1.3.	Federal, State, and local agency and FAA access.....	47
7.1.4.	Data authentication and retention.....	47
7.1.5.	Privacy considerations.....	47
7.1.6.	Governmental UAS operations	48
7.2.	Interoperability with current & future systems/programs.....	48
7.3.	First Amendment.....	49
7.4.	Education.....	49
7.5.	Pending Federal legislation	49
7.6.	Pending State/local legislation	49
7.7.	Global harmonization.....	49
7.8.	Children and minors.....	49
7.9.	Effect on other laws.....	50
7.10.	Trusted Operator System	50
8.	CONCLUSION	50
9.	APPENDICES	51

1. BACKGROUND

The Federal Aviation Administration (FAA or the Agency) chartered the Unmanned Aircraft Systems (UAS) Identification (ID) and Tracking Aviation Rulemaking Committee (ARC) (UAS-ID ARC) to provide recommendations to the FAA regarding technologies available for remote identification and tracking of UAS.

In December 2015, the FAA issued an interim final rule entitled “Registration and Marking for Small Unmanned Aircraft.” This rule implemented recommendations from the Registration Task Force by creating an online registration portal for commercial and recreational small UAS. It also required owners to mark their aircraft with a unique identifier, but it did not include provisions for identifying unmanned aircraft during operations. The FAA recognizes the potential value remote identification would have to public safety and the safety of the National Airspace System (NAS). The FAA chartered the UAS-ID and Tracking ARC to inform the FAA on available technologies for remote identification and tracking, shortfalls in available standards, and make recommendations for how remote identification may be implemented.

2. OBJECTIVES AND SUMMARY OF ACTIVITIES OF THE ARC

ARC Membership

The UAS-ID ARC was composed of members representing aviation community and industry member organizations, law enforcement agencies and public safety organizations, manufacturers, researchers, and standards bodies who are involved in the promotion of UAS, the production of UAS, and security issues surrounding the operation of UAS. A complete list of ARC members is included in Appendix A to this report.

ARC Objectives

The FAA charged the UAS-ID ARC with the following three objectives:

1. Identify, categorize and recommend available and emerging technology for the remote identification and tracking of UAS.
 - a. Factors to consider include, but are not limited to: technical and operational capabilities such as size, weight, speed, payload, and equipage; appropriate requirements for different classifications of unmanned aircraft system operations, including public and civil; technology readiness levels (TRL); operational range; and reliability.
2. Identify the requirements for meeting the security and public safety needs of the law enforcement, homeland defense, and national security communities for the remote identification and tracking of UAS. The ARC should consider and evaluate the need to provide information that could assist in threat discrimination and determination of hostile intent.

3. Evaluate the feasibility and affordability of available technical solutions, and determine how well those technologies address the needs of the law enforcement and air traffic control communities. The ARC should develop evaluation criteria and characteristics for making decisions, and rate the available technical solutions provided.

During its deliberations, the ARC considered all UAS operations in all airspace.

ARC Working Groups

The members of the UAS-ID ARC were organized into three working groups:

- Working Group One (WG1) – Existing and Emerging Technologies
- Working Group Two (WG2) – Law Enforcement and Security
- Working Group Three (WG3) – Implementation

ARC Plenary Meetings

The full UAS-ID ARC met on June 21-23, 2017, and July 18-19, 2017, for the purpose of education and information gathering. The full UAS-ID ARC met again on August 16-17, 2017, and September 7-8, 2017, for the purpose of discussions and deliberations.

3. EXECUTIVE SUMMARY

The UAS-ID ARC membership represented diverse interests and viewpoints. During the course of ARC activities described above, the three working groups met on several occasions to address specifically assigned objectives. The individual working group efforts and analyses were captured in separate working group reports that are included as appendices to this report. These findings and conclusions were presented to, and considered by, the full UAS-ID and Tracking ARC. Although some decisions were not unanimous, the ARC reached general agreement on many of their recommendations to the FAA. Working group discussions and divergent views are noted both in the report (section 5) and in the Working Group Appendices to the report. The recommendations in this report reflect the final statements of the ARC. A summary of the ARC's recommendations (which appear in section 6 of this report) is included below.

The ARC did not reach consensus on an applicability threshold for ID and tracking requirements. ARC members discussed two options, which are presented in section 6.1 (p. 31) of this report. The ARC recommends the FAA give due consideration to both of those options.

The ARC recommends that, regardless of which option for applicability the FAA chooses, the following UAS be exempt from remote ID and tracking requirements:

- UAS operated under ATC and contains the equipment associated with such operations (including ADS-B, transponder, and communication with ATC).
- UAS that are exempted from ID and tracking requirements by the FAA (e.g., for the purposes of law enforcement, security or defense, or under an FAA waiver).

The ARC further recommends the FAA do the following regarding the applicability of remote ID and tracking requirements:

- Include a waiver mechanism in the remote ID and tracking rule, to allow individual operations or classes of UAS to deviate from the requirements of the rule if operations are conducted under the terms of a certificate of waiver.
- Apply the remote ID and tracking requirements to the remote pilot, not to the manufacturer of the UAS.
- Require manufacturers to label their products to indicate whether they are capable of meeting applicable remote ID and tracking requirements. If a product is labeled as capable of meeting remote ID and tracking requirements, such capabilities must be enabled by default and the manufacturer must not present the user with an option to turn off the ID and tracking.
- Consider whether unmanned aircraft equipped with advanced flight system technologies that are strictly for safety purposes and that keep the aircraft within visual line of sight of the remote pilot, such as a “return to home” feature, should be exempt from remote ID and tracking requirements, provided the safety features cannot be readily altered or reprogrammed.

The ARC recommends two methods for UAS to provide remote ID and tracking information – (1) direct broadcast (locally, e.g., ADS-B, Low-Power Direct RF, Unlicensed Integrated C2, and Visual Light Encoding); and (2) network publishing (e.g., Networked Cellular, Satellite, and SW-based Flight Notification w/ Telemetry) to an FAA-approved internet-based database. (Sec 6.2, p. 33)

- *Direct broadcast* means to transmit data in one direction only with no specific destination or recipient. Data can be received by anyone within broadcast range. With regard to direct broadcast capabilities, the ARC recommends the FAA adopt an industry standard for data transmission, which may need to be created, to ensure UA equipment and public safety receivers are interoperable, as public safety officials may not be able to equip with receivers for all possible direct broadcast technologies.
- *Network publishing* means the act of transmitting data to an internet service or federation of services. Clients, whether Air Traffic Control (ATC) or public safety officials, can access the data to obtain ID and tracking information for UAS for which such data has been published. With regard to network publishing, the ARC recommends that information held by Third Party Providers (TPP) or UAS Service Suppliers (USS) be governed by restrictive use conditions imposed on the TPP/USS related to the use and dissemination of any data and information collected.

The ARC recommends a tiered approach to direct broadcast and network publishing requirements (Sec 6.3, p. 35).

- *Tier 1 – Direct broadcast (locally) or Network publish:* UAS in this tier would be required to direct broadcast both ID and tracking information so that any compatible receiver nearby can receive and decode the ID and tracking data. If a network is available, network publishing to an FAA-approved internet-based database satisfies this requirement. A UAS would fall into Tier 1 if it does not qualify for an exemption from remote ID and tracking requirements (such UAS are referred to as Tier 0) and does not meet the conditions for Tier 2 or Tier 3, for example UAS conducting most part 107 operations.
- *Tier 2 – Direct broadcast (locally) and Network publish:* UAS in this tier would be required to broadcast (locally) ID and tracking data *and* network publish ID and tracking data to an FAA-approved internet-based database. An example of UAS that may fall into would be UAS that are conducting waivered operations that deviate from certain part 107 operating rules, and where the FAA determines that Tier 2 ID and tracking are required as a condition of the waiver.
- *Tier 3 – Flight under part 91 rules:* UAS in this tier must adhere to the rules of manned aircraft as defined in 14 CFR part 91. This tier is intended for aircraft that are integrated into the manned aircraft airspace. An example of UAS that may fall into Tier 3 are those weighing above 55 pounds and operating BVLOS, in IFR conditions, or operating in controlled airspace.

The ARC offers recommendations and suggestions for the three stages of implementing a remote ID and tracking rule. (Sec 6.4, p. 38)

- *Pre-rule:* To help address the concerns of public safety officials before an ID and tracking rule is finalized, the Agency could broaden UAS safety education efforts and continue the UAS detection pathway research with industry.
- *Before final rule is enacted:* Before the final rule is enacted, the Agency could work to scope standards needed to enable direct broadcast and network publishing technologies for implementing the remote ID and tracking requirement on new equipment and existing equipment. The ARC recommends the FAA ensure that standards for ID and tracking technology move forward at a rapid pace. The ARC further recommends the FAA work closely with industry on developing the ideal architecture for the PII System.
- *After final rule enacted:* After the remote ID and tracking rule is enacted and standards are in place, all UAS manufactured and sold within the United States that are capable of meeting the threshold for compliance should be labeled if ID and tracking capable. FAA should allow a reasonable grace period to carry out retrofit of UAS manufactured and sold within the United States before the final rule. The grace period should end when retrofit options are inexpensive and easy to implement.

The ARC recommends a set of minimum data requirements for remote ID and tracking of UAS. (Sec 6.5, p. 39) The following types of data related to the UA or associated control station *must* be made available:

- *Unique identifier of the UA*: This should be specific to the UA, continuously available in near-real time, electronically and physically readable, tamper resistant, and easily accessible.
- *Tracking information for the UAS*: This should include aircraft position and control station location (or take-off location if ground control station location is not available).
- *Identifying information of the UAS owner and remote pilot*: This information would not be broadcast or published, but would be available from the PII System (see definition below in section 4).

The following types of data related to the UA or associated control station are *optional*:

- *Mission type*: This characterizes the flight path of the UA.
- *Route data*: This includes pre-programmed navigation or flight plans.
- *Operating status of the UA*: This refers to operational information that may provide some insight into the current operations of the UA.

The ARC recommends the following as to how ATC should interoperate and maximize the benefits of ID and tracking equipage (Sec 6.6, p. 44):

- The FAA should identify whether BVLOS operations will routinely occur (i.e. without a waiver) without an IFR flight plan, and if so, under what operational conditions (e.g. airspace, altitudes, speeds, etc.).
- Any proposal for using ADS-B frequencies in the solution for UAS ID and tracking must be analyzed for the impact on the performance of current and future SSR, ACAS, and ADS-B.
- The UAS ID and tracking system should interoperate with the ATC automation, such that target information from the ID and tracking ground system, including ID and position, can be passed to ATC automation.
 - FAA automation should be able to accept target information from the UAS ID and tracking ground system.
 - End-to-end latency from UA position report to ATC automation should ideally be low enough to be of use in the tactical ATC environment.
- FAA automation should by default filter out UAS ID and tracking system targets from the ATC display that fall outside of adapted airspace deemed to be of interest to ATC (i.e., away from typical manned aviation flight paths).
 - FAA automation should be able to alert ATC personnel (e.g. Certified Professional Controller or Front-Line Manager) when an unexpected UAS enters airspace of interest to ATC operations.

- The FAA should define standard criteria for identifying airspace that should be adapted as being of interest to ATC operations in this context, and ensure that the UAS ID and tracking ground system has coverage in these areas.
- FAA automation and the UAS ID and tracking system should be able to display designated UAS targets of interest (e.g. by a public safety official, in the UAS ID and tracking system) to ATC personnel.

The ARC recommends the FAA do the following regarding airports and critical infrastructure (Sec 6.6.2, p. 45):

- Incorporate implementation costs of critical infrastructure facilities into rulemaking analysis, including physical (e.g., radio receivers) and digital (e.g., networked software solutions) infrastructure, and any financial burdens associated with planning and capability requirements for critical infrastructure facilities to implement UAS ID and tracking systems and security procedures.
- Identify an approach and timeline to designating approved technologies for airports and critical infrastructure facilities, and address any legal barriers to implementing approved technologies. If a period of optional equipage is defined, the requested approach and timeline should support testing and deployment of systems at facilities during this phase
- Provide guidance to airports on any impact or interference to safe airport operations including how UAS ID and tracking may impact definition of UAS Facility Maps, security procedures, and risk assessments of UAS operations.

In the process of this effort, the ARC also identified a number of related issues that were deemed to have potential impact on the implementation of effective UAS ID and tracking solutions. These recommendations are provided for FAA considerations:

- Regarding access to data related to direct broadcast and network publishing, the ARC recommends the FAA implement at least three levels of access to the information that is either broadcast or captured and contained in the appropriate database. Those levels of access are: (1) information available to the public; (2) information available to designated public safety and airspace management officials; and (3) information available to the FAA and certain identified Federal, State, and local agencies. (Sec 7.1, p. 46)
 - *Information available to the public:* The UA unique identifier should be available to the public.
 - *Information available to designated public safety and airspace management officials:* Access to personally identifiable (PII) information should be limited to public safety officials and similarly regulated public safety entities, including airspace management officials.
 - *Information available to the FAA and certain identified Federal, State, and local agencies:* All relevant tracking data should be retained for a reasonable period of time to allow

public safety officials and other authorized users to have access to information critical to investigations.

- The ARC recommends that the United States government be the sole keeper of any PII collected or submitted in connection with new UAS ID and tracking requirements.
- The ARC recommends that the remote ID and tracking system include reasonable accommodations to protect the operational security of certain governmental UAS operations, consistent with accommodations provided to governmental operations in the manned space.

4. DEFINITIONS

Beyond Visual Line of Sight (BVLOS) means UAS operating beyond the visual line of sight (as that term is defined in 14 CFR 107.31 and below) of the remote pilot, remote pilot in command, and visual observer (if one is used).

Configuration is the process by which the owner/operator sets up a device to communicate the appropriate unique ID.

Control station means an interface used by the remote pilot to control the flight path of the unmanned aircraft.¹

Federated Approach is a framework that allows for interoperability and information sharing among systems from different vendors to deliver a common, seamless service to users.

Historical tracking information is tracking information compiled over a period of time that reflects the flight activities of unmanned systems.

Identity refers to a data set that can be traced to a unique UAS, its owner and/or operator.

Identify means the ability to establish the identity of a specific UAS and its associated owner and remote pilot.

Interoperability is the ability of systems to exchange and make use of information.

Low Altitude Authorization and Notification Capability (LAANC) is the broad term for an enterprise capability to automate to the maximum extent possible the ability for FAA to grant authorization to 14 CFR part 107 operators under § 107.41 and to allow for model aircraft operators to notify Air Traffic Control (ATC) of planned operations within 5 miles of an airport as described at Pub. L. 112-95 § 336. LAANC major elements include the FAA's provision of authenticated map data for use in determining authorization, the use of Third-Party Providers (TPP) to provide services to operators, and the ability for multiple TPP to provide services.²

¹ 14 CFR 107.3.

² For a detailed description of LAANC, see FAA ATO LAANC Concept of Operations V 0.93. For a description of how LAANC could be used to publish to an FAA-approved internet-based database, see section 6.2.2 of this report.

Original Equipment refers to solutions that are integrated into the UAS by the manufacturer at the time of manufacture.

Owner refers to the person or organization possessing legal ownership of the aircraft.

Operator refers to the person or organization responsible for ensuring compliance with the ID and tracking regulation.

PII means personally identifiable information.

The PII System includes processes and technology (direct broadcast or network publishing) that enables approved users to associate UAS ID with the FAA System of Records. This system would include the database where remote pilot/owner/operator PII is housed for access by authorized users.

Provision is the process of enabling a communications device to participate in a network service.

Public unmanned aircraft system means an unmanned aircraft system that meets the qualifications and conditions required for operation of a public aircraft (as defined in 49 U.S.C. 40102).³

Registration is the process by which the owner/operator associates himself/herself (including contact information and other PII) and aircraft (e.g., make, model, modifications) with an assigned, unique identifier.

Remote Identification means discerning identity from a distance.

Remote Pilot means the person who manipulates the flight controls of the UAS.⁴

Remote Pilot in Command means a certificated airman that has the final authority and responsibility for the operation and safety of a UAS operation.⁵

Retrofit is the installation of an ID and tracking solution on an existing UAS. This may include items physically attached to the airframe, connected to the existing subsystems, or software updates.

Technical Readiness Level (TRL) is defined by NASA/DoD as a method of estimating technology maturity of critical technical elements.

Technology Alternative is defined as a broad, non-industry member specific category proposed solution for UAS ID and tracking.

Tracking is the process of following the dynamic location of UAS components over time.

³ Section 331(4) of the FAA Modernization and Reform Act of 2012, Public Law 112-95, 126 Stat. 72.

⁴ See 14 CFR 107.12.

⁵ Operation and Certification of Small Unmanned Aircraft Systems, June 28, 2016, 81 FR 42064, 42087.

Unmanned aircraft (UA) means an aircraft operated without the possibility of direct human intervention from within or on the aircraft.⁶

Unmanned aircraft system (UAS) means an unmanned aircraft and associated elements (including communication links and the components that control the unmanned aircraft) that are required for the pilot in command to operate safely and efficiently in the national airspace system.⁷

UTM (UAS Traffic Management) is a developmental system for UAS operations that are not receiving ATC services, which is separate but complementary to the FAA's Air Traffic Management (ATM) system. UTM development will ultimately identify services, roles/responsibilities, information architecture, data exchange protocols, software functions, infrastructure, and performance requirements for enabling the management of low-altitude uncontrolled UAS operations.

Visual Line of Sight (VLOS) aircraft operation is one where, with vision that is unaided by any device other than corrective lenses, the remote pilot in command, the visual observer (if one is used), and the person manipulating the flight control of the small unmanned aircraft system must be able to see the unmanned aircraft throughout the entire flight in order to: (1) know the unmanned aircraft's location; (2) determine the unmanned aircraft's attitude, altitude, and direction of flight; (3) observe the airspace for other air traffic or hazards; and (4) determine that the unmanned aircraft does not endanger the life or property of another.⁸

5. DISCUSSION

In addition to the four meetings of the full UAS-ID ARC, each working group met separately to address the specific issues they were tasked to consider. This section includes a summary of each working group's analysis of those issues, as well as a summary of each working group's findings and conclusions, which were presented to and considered by the full UAS-ID ARC. More detailed reports summarizing the activities and findings of WG1 and WG2 can be found in the Appendix.

The ARC's final recommendations related to what is discussed in this section are included below in section 6.

5.1. Available and emerging technologies for remote ID and tracking of UAS

WG1 was tasked with identifying, categorizing, and recommending available and emerging technologies for the remote ID and tracking of UAS. WG1 considered technologies for near-term retrofitting of existing UAS, as well as technologies for longer-term integration into new UAS by the manufacturer at the time of manufacture.

WG1 used data needs identified by WG2 as guidance in determining how well various technology alternatives may satisfy the "requirements" for remote ID and tracking. Those data needs include: (a) the unique identifier of the unmanned aircraft (UA); (b) the position of the UA; and (c) the location of the ground control station (if possible). These data needs are discussed in greater detail in section 6.5.

⁶ *Id.*

⁷ Section 331(9) of the FAA Modernization and Reform Act of 2012, Public Law 112-95. 126 Stat. 72.

⁸ 14 CFR 107.31(a).

WG1 considered the wide variety of potential operating environments in which an ID and tracking solution will need to operate. In particular, WG1 noted that a UAS may be operating along the following dimensions:

- Remote areas to urban areas.
- Outside of surveillance and communication networks to overlapping surveillance and communications networks.
- Areas with minimal buildings and obstructions to urban canyons.
- Areas with little spectrum usage to areas with heavy spectrum congestions.

WG1 determined that different technology solutions, or combinations of solutions, may be appropriate for different operating environments.

5.1.1. Identifying viable technology solutions

AUVSI, a member of WG1, solicited ideas from industry on remote ID and tracking solutions. A total of 53 white paper proposals were received. At the request of the FAA, the MITRE Center for Advanced Aviation System Development analyzed these proposals and presented its findings (without revealing proprietary information) to WG1. WG1 also received briefings from various working group members. Using this information, WG1 identified the following eight viable technology solutions:

1. **Automatic Dependent Surveillance Broadcast (ADS-B):** Two alternatives are discussed related to a rule-compliant version (i.e., adheres to current ADS-B rules/standards on licensed ADS spectrum) and a lower-power alternative that leverages the message, protocols, and frequency but uses a significantly lower transmit power to address concerns about potentially overwhelming existing ADS-B services.
2. **Low-Power Direct RF:** Includes a variety of RF based protocols leveraging unlicensed spectrum including Bluetooth, WiFi, RFID, and others.
3. **Networked Cellular:** Leverages the existing cellular network and network-connected devices on licensed spectrum.
4. **Satellite:** Leverages existing satellite tracking services.
5. **SW-based Flight Notification with Telemetry:** Leverages existing and developing UAS services that enable UAS operators to exchange operational information during flight. Depends upon a network connected device coupled with a ground control station that many small UAS operators use today.
6. **Unlicensed Integrated C2:** Modulates ID and tracking packets on existing C2 communication channels on unlicensed spectrum.
7. **Physical Indicator:** Consists of unique and categorical physical markings (e.g., etched numbers, streamers) that will need to be visually observed. Some concepts do not provide remote identification.

8. **Visual Light Encoding**: Leverages software controlled LEDs to digitally encode information that can be decoded by a device connected to a visual sensor.

Fundamentally, the eight technology alternatives fall into two broad categories: (1) *direct broadcast solutions* (e.g., ADS-B, Low-Power Direct RF, Unlicensed Integrated C2, and Visual Light Encoding); and (2) *network publishing solutions* (e.g., Networked Cellular, Satellite, and SW-based Flight Notification w/ Telemetry). *Direct broadcast solutions* transmit data in one direction only with no specific destination or recipient. For *network publishing solutions*, there will be the need for technology to collect and distribute the ID and tracking data. This may be in the form a single server/database or a federated database on distributed servers. It is envisioned that the users of the ID and tracking data (e.g., public safety officials) will have integrated access.

The assumption was made that the FAA would be responsible for maintaining a PII System which correlates unique electronic ID with owner/operator contact information and other PII. The FAA would be responsible for the procedural and technical access controls to such data and thus was not considered as a comparison point in characterizing the technology alternatives.

WG1 analyzed the eight technology alternatives identified above using five criteria. The five criteria are identified and discussed below in section 5.1.2. Following that discussion, in section 5.1.3, are four tables that summarize WG1's analysis of the eight technology alternatives against the five criteria. More details associated with the characterizations of each technology alternative can also be found in WG1's report in Appendix B.

5.1.2. Criteria for reviewing and rating viable technology solutions

WG1's analysis of potential technology solutions was based on the following five prioritized criteria:

1. Ease of compliance for the owner/remote pilot.
2. Readiness for implementation.
3. Operational performance and security.
4. Costs.
5. Interoperability.

5.1.2.1. Ease of compliance

To be effective, any regulation associated with UAS ID and tracking will need a high degree of UAS owner/operator compliance. If sightings of unidentified UAS are routine, significant time and energy will be expended in both responding to potential threats and attempting to identify the owner/operator through current means. Thus, broad compliance is critically important for an ID and tracking solution to have value.

The assumption is that most owner/operators want to be compliant. The likelihood that they will comply depends upon the relative ease of complying, the perceived costs of complying, the penalties for non-compliance, and any potential rewards from compliance. One could think of the "Likelihood of Compliance" to include the "Motivation to Comply" along with the "Deterrence of Compliance."

Motivation to Comply

There are two major factors which would motivate compliance with ID and tracking regulations: (1) negative consequences associated with enforcement actions for non-compliance; and (2) the positive benefits of complying. Enforcement actions for non-compliance could be especially challenging since it will be difficult to hold an owner/operator accountable if they are not identifiable. The second factor, benefits that an owner/operator receives from conducting operations in compliance with the ID and tracking regulation (i.e., positive reinforcement), should be explored. The benefit could take the form of increased airspace access, reduced safety oversight (because the owner/operator can be more easily held accountable for unsafe actions), or tangible proof that they are complying with other aviation safety regulations (e.g., proof that they did not violate an airspace restriction).

Potential Deterrence to Compliance

There are many factors that may deter owner/operator compliance with ID and tracking regulations. Deterrence to compliance falls into two broad categories: (1) Burdens of Compliance; and (2) Perceived Detriments of Compliance.

Assuming that most owners/operators want to comply, the easier it is for them to comply with the regulation, the more likely they are to comply. The burden of compliance will be lower if the owner/operator can comply with the regulation with minimal or no additional tasks – i.e., the fewer tasks to forget or overlook the better. Automatic or seamless compliance is preferable, for example with ID and tracking capabilities built into new original equipment with ID associated with the owner included in other routine configuration tasks. Depending upon specifics of the technology alternatives and their associated business models, there may be different burdens of compliance on retrofit aircraft than for original equipment. Compliance burdens refer to the impact on the owner/operator to comply with the ID and tracking regulation. Examples of potential burdens on the owner/operator include the time, effort, and costs to purchase, install, and configure new equipment and additional tasks associated with each flight to ensure ID and tracking equipment is functioning. Industry may have competitive motivations to reduce compliance burdens.

Concern was expressed that a technology solution that requires the establishment and maintenance of a subscription service may increase the real and perceived burden even if costs are minimal. Factors could include the need to choose a service provider, establish and maintain payment and contact information, remain aware of coverage and contract terms of service, etc. There are also issues associated with minors who may operate under 14 CFR part 101 having difficulty entering a contractual arrangement for a subscription service. Solutions that have a potential for a subscription service may be perceived as a burden for owner/operators who only operate their UAS on occasion or who may be visiting the United States for a short duration.

There may also be perceived detriments associated with compliance. Some of these are material and others relate to the reduced operational utility. There are also perceived risks associated with sharing information.

Material – Material costs include expense of equipment or services that may be incurred as part of complying with ID and tracking requirements. Examples may include electronic radio beacons, subscription services, integration of new equipment, etc.

Operational – Given the relative small size of many UAS, integrating additional equipment that requires space, adds weight, and consumes power may reduce the operational utility of the UAS (e.g., reductions in flight duration, payload, range).

Disclosure of Operationally Sensitive Information – Owner/operators may view negatively the loss of control of information associated with their flight operations. Even without disclosure of PII, the widespread availability of operational sensitive information (e.g., time, location, duration, flight frequency) could have an impact on an owner/operator's perceived privacy and/or commercial interests. The holding of such information by a third party may be concerning to some UAS owner/operators, whereas some may prefer it. If broad operational data is available, it may be archived and mined for information which could be perceived as detrimental to the owner/operator. Even if access to such information is limited to public safety officials or through use agreements, the perception may be detrimental to the willingness to comply.

The ARC discussed the fact that tracking occurs in some circumstances for manned aviation. For those aviation activities receiving Air Traffic Control (ATC) services there is routine tracking today. At the same time, there are also thousands of flight operations a day in the NAS where the aircraft are not tracked. The ARC discussed that privacy concerns may arise from a requirement to track nearly every UAS flight. A perception that UAS are burdened more than manned aircraft may be a disincentive to compliance.

The “ease of compliance” criterion was scored (high/medium/low) based on the time and effort to install and configure the UAS, and on the size, weight, and power (SWaP) impacts to the UAS.

Scoring for retrofits:

- High – Involves no-to-minimal time and effort to install and configure, and the weight impact to the UAS is less than 10g.
- Medium – Requires installation and configuration of a separate piece of hardware, which would either require integration into the aircraft system power or would have to have its own batteries which would require separate recharging. Weight impact to the UAS is less than 250g.
- Low – Requires either installation that involves physical connections to existing sub-systems, a weight impact to the UAS of greater than 250g, or specific operational tasks required for each flight (e.g., participation in a flight notification program).

Scoring for original equipment:

- High – Installed by manufacturer upon purchase and requires minimal additional tasks by the owner/operator to comply with the ID and tracking requirements, other than those associated with registration and minimal configuration (<10 mins).
- Medium – Requires complex configuration tasks by the owner/operator upon setup (>10 mins).
- Low – Requires specific operational tasks for each flight (e.g., submitting a flight plan).

Another critical consideration for this criterion was whether establishing the ID and tracking capabilities requires involvement of a third-party intermediary to either provide communications services or to otherwise facilitate the delivery of information.

5.1.2.2. Readiness for implementation

This criterion considers the time and effort necessary to implement the technology solution for remote UAS ID and tracking. This criterion was scored as a “yes” or a “no” based on whether the technology solution can meet the following conditions:

- Available as a retrofit for existing UAS in less than 1 year.
- Available for integration into new original equipment in less than 1 year.
- Available to public safety officials in less than 1 year.
- Required infrastructure and data management capabilities will be established in less than 1 year.
- No significant changes in FAA/FCC policies specific to the use of the technology solution are needed.

NASA/DoD Technology Readiness Levels, a commonly used measure of technology maturity, were used to inform the ratings. However, Table 2 (on page 24) shows a simplification of the ratings based on industry input.⁹

Not all technology solutions evaluated by the ARC were standards-based. Technology standards that have been rigorously evaluated, tested, and agreed upon by industry offer a firm foundation upon which to introduce new technologies and innovations, ensuring that products, components, and services supplied by different companies will be compatible and interoperable over the long term. The availability of agreed-upon standards also provides industry with the level of knowledge required to develop products and services that will seamlessly interact with one another.

Standards-based technology solutions offer a number of benefits, including rapid introduction of innovative products to market, interoperability among existing, new and future products and services, global economies of scale (with attendant cost reductions), compliance standards, competition by a greater number of companies to develop the technology, and a baseline to evolve the technology and add new features over time. Standards-based technology solutions also offer specifications that ensure that all implementations of a technology meet certain performance expectations.

The typical standardization process involves multiple companies making contributions and performing reviews. The final specification for a technology may be different from the initial suggestions made by a company about a proprietary solution. Standardizing technologies can be either a lengthy or short process depending on the nature of the technology that needs to be standardized. The UAS-ID ARC has had the benefit of input from standards-setting bodies as members, who have indicated that the standardization process could take between 6 months to 2 years. When the need for a standard is urgent, the timeline could be shortened.

⁹ This scale ranks the maturity of technology from basic research (1) to operational system (9).

Beyond ensuring that each technology is standards-based, and has gone through a standardization process, other standards will need to be agreed upon for remote ID and tracking of UAS specifically. For example, standards will be needed for data transmission and publishing, and standards will be needed for broadcast technologies to ensure receivers are interoperable.

5.1.2.3. Operational performance and security

Operational performance

The operational performance criterion evaluates how well the technology solution is expected to perform in an operational setting. In its analysis, WG1 considered the following factors:

- **Meets criteria for direct broadcast or network publishing (yes/no)** – Each alternative has a Primary method of operation that maps into one of the two basic requirements of WG2: (1) Direct Broadcast; or (2) Networked (Publishing). Although some solutions could have secondary means of meeting a second requirement, the Primary method is identified and it is noted how the secondary requirements could be achieved, if applicable.
- **Update Rate $\geq 1\text{Hz}$ (yes/no)** – Can transmit to public safety officials ID and tracking information at an update rate of a minimum of once per second. Update rate is discussed below in greater detail.
- **Latency $<3.5\text{ s}$ (yes/no)** – Can transmit to public safety officials ID and tracking information that is delayed in delivery by less than 3.5 seconds (time from transmission of the message to receipt on a display). Network solutions require “right-sized” server capacity and bandwidth. Direct broadcast solutions are likely to have $< 1\text{s}$ latency. Latency is discussed below in greater detail.
- **Range** – Effective range of the solution, considering four broad categories:
 - **Radio Range:** Solution works to the radio transmission range of the equipment involved. Varies by power, propagation effects, and communications environment.
 - **Network Range:** Communicates if the unmanned aircraft and/or ground control station (GCS) are in an area served by the network.
 - **Satellite Range:** Communicates if the unmanned aircraft and/or GCS are in an area served by the satellite.
 - **Visual Range:** Individual/Receiver must be able to see the unmanned aircraft.
- **Licensed Spectrum (yes/no)** – Spectrum that is likely free from interference from other applications implying a higher quality of service. Spectrum is discussed below in greater detail.

Update rate and latency

An important performance criterion in any ID and tracking system is the update rate and end-to-end latency associated with information delivery. For the purposes of this document, the update rate will refer to how often the ID and tracking information is updated in a communicated transmission. End-to-end latency refers to the time it takes for an event to happen (e.g., position of the aircraft) to when that information is available for use by a public safety official (e.g., displayed on a smart device). End-to-end latency could include the processing time associated with message generation, message transmission time, transit time, message receive time, processing to decode, network

routing, database propagation, other radio transmissions, and processing associated with display rendering.

For the purposes of this discussion, the combination of update rate and latency will be referred to as “total latency.” Assuming worst case, the total latency (i.e., the lag between event occurrence and what is communicated to the public safety official) would be the sum of the interval between updates and the total latency.

To determine the desired update rate and end-to-end latency we used the following overall approach:

- Identified potential public safety officials/UAS interaction scenarios.
- Identified which public safety officials/UAS interaction scenario was the most demanding in terms of requirements for total latency.
- Identified precedents in existing standards for similar applications.
- Compared precedent standards to the most demanding public safety officials/UAS interaction scenario using some assumptions with regard to UAS performance.

At least four public safety officials/UAS interaction scenarios exist:

1. Public safety officials are providing security to critical infrastructure or venue and spot a “suspicious drone” that is currently operating and need to determine whether it is a direct threat or not in order to respond accordingly.
2. Public safety officials are responding to a citizen report of a “suspicious drone” that is currently operating.
3. Public safety officials are responding to a citizen report of a “suspicious drone” that had been operating recently (e.g., within the past 15 minutes).
4. Public safety officials are responding to a citizen report of a “suspicious drone” that had been operating in the past (longer than 15 minutes ago).

In terms of total latency requirements, the most demanding situation is Scenario 1. If the ID and tracking solution satisfies the total latency requirements of Scenario 1, the demands of Scenarios 2-4 would be met. With that in mind, the remainder of the discussion will address maximum total latency acceptable to meeting Scenario 1 needs.

While a maximum total latency of 0 seconds is desirable, it is not technologically feasible. The recommendation regarding maximum total latency is based upon the following considerations and precedents of similar technologies

The ARC considered two different established RTCA standards. The first was RTCA DO-362, Command and Control (C2) Data Link Minimum Operational Performance Standards (MOPS) (Terrestrial). This standard defines parameters associated with the C2 link between the UA and the GCS. The standard specifies that target data should be updated once per second as part of the C2 downlink to the GCS (*see* RTCA DO-362, Appendix J).

The second was DO-317B, Minimum Operational Performance Standards (MOPS) for Aircraft Surveillance Applications (ASA) Systems. This standard defines requirements associated with ADS-B applications. Specifically, the ARC examined latency requirements associated with messages eventually displayed as part of cockpit display of traffic information (CDTI) and used by pilots for

visual acquisition of aircraft. The ARC felt that visual acquisition of aircraft by public safety officials on the ground was an analogous function, and that we could leverage latency requirements defined in this standard as precedent for the ID and tracking domain. WG1 evaluated technology against a maximum “creation to transmit” delay of 2 seconds and a maximum “transmit to display” delay of 3.5 seconds. Combined, these two delays result in a 5.5 second end-to-end latency. ADS-B has a minimum update rate of at least once a second.

Using these two standards as precedents leads to the conclusion that for ID and tracking purposes a minimum of once per second update rate and maximum end-to-end latency of 5.5 seconds should be considered. Adding these two factors together results in a maximum total latency of 6.5 seconds.

Nearly all technology solutions examined by the ARC met this standard. This could warrant a reexamination of whether this standard meets public safety officials and other needs in various operational scenarios.

Using scenario 1 as the most demanding use case, the ARC then explored whether the total latency would be appropriate using some assumptions with regard to aircraft performance. Although 14 CFR part 107 permits a maximum small UAS (sUAS) velocity of 100 mph, the average small sUAS is not capable of a sustained velocity of more than 50 mph. Assuming a total latency of 6.5 seconds, the average small UA would travel approximately 160 yards at 50 miles/hour. Based upon public safety subject matter expertise, it was determined this would meet the needs implied by Scenario 1.

Licensed Spectrum

As noted above, the spectrum or frequency on which a technology functions was one of the factors WG1 considered when evaluating the merits of the technologies available for remote ID and tracking of UAS. There was not, however, full consensus within WG1 on the operational performance value of technology solutions that may or may not use licensed spectrum. The spectrum provides the communications link from the UA or the ground control station through which ID and tracking information is transmitted to public safety officials, the public, and/or the contemplated centralized database. The technology solutions studied by the ARC included solutions that rely on licensed spectrum and unlicensed spectrum.

Licensed and unlicensed communications links have different characteristics and protections that can impact the operational performance, reliability and security of a technology solution. Spectrum interference is not likely to thwart the ability of an ID and tracking system to work, although reception of the information may be, at times, less predictable than reception of such information via licensed spectrum. There are a number of questions to consider when evaluating the quality of the communications link, including: whether the spectrum is protected from interference by regulation; how much spectrum is available to support the communications link; if the spectrum is shared with other users for similar or dissimilar uses in controlled or uncontrolled environments; and if the FAA has, or will have, any requirements for use of licensed spectrum or unlicensed spectrum in certain UAS operating environments or for certain UAS functions.

WG1 had a robust discussion about spectrum issues in relation to the technologies that are available for remote tracking and identification of UAS, including the following perspectives:

1. Unlicensed spectrum is generally used by small UAS today for visual line of sight control links, and manufacturers report that unlicensed bands have proved to be reliable for visual line of sight operations as they are conducted today.
2. When considering use of unlicensed spectrum for remote ID and tracking in populated operational environments, where the density of users is high in relation to public safety officials attempting to capture UAS transmitted data, interference should be expected.
3. All radio technologies could be impacted by uncontrolled interference and therefore regulatory protection of spectrum is a key consideration. In contrast with licensed spectrum rights, devices or systems operating on an unlicensed basis have no regulatory protection against interference from users in the band and therefore there is no assurance of link performance. *See* FCC regulation 47 CFR 15.5.
4. Technology standards are evolving to improve coexistence among users of unlicensed spectrum through protocols such as “listen before talk” which seek to mitigate interference impact as uses of unlicensed spectrum continuously increase.
5. The level of impact on the technology solution due to interference to the communications link will vary and needs to be assessed against the performance requirements for remote identification and tracking technology, which may tolerate an occasional dropped or delayed packet or mitigated by transmitting at a higher update rate. Interference to the communications link manifests in range reduction, lost or delayed data, lost link (either because of congestion or jamming), etc.
6. When considering suitable spectrum for technology performing various functions for UAS, the expected evolution of the UAS market should be considered, with the projected ramp up in the number of UAS and UAS applications across all environments (rural, suburban and urban).

These factors and the performance tradeoffs between technologies deployed on licensed and unlicensed spectrum were considered and assessed against the operational requirements of public safety officials.

Security

WG1 also considered whether each technology solution contains the following security measures:

- **Spoofing Security (yes/no)** – A mechanism is in place that would make it more difficult for mischievous/malicious electronic intervention.
- **Tamper Proof (yes/no)** – A mechanism is in place that would make it more difficult for mischievous/malicious physical intervention.
- **Tracking Verification (yes/no)** – A mechanism is in place that could independently correlate location information received in the ID and tracking messages.

5.1.2.4. Interoperability

The interoperability criterion was used to identify whether the technology solution would enable interoperability, including serving as a data source for ATC or being able to be federated as a

potential source of information for a low-altitude traffic management capability (e.g., UAS Traffic Management (UTM)). In its analysis, WG1 considered the following factors:

- Whether the technology solution could serve as a data source for ATC without significant changes to ATC infrastructure.
- Whether the technology solution is compatible with solutions that may be employed internationally.
- Whether the technology solution supports a federated approach where multiple vendors can provide the same service in a manner that is seamless to owner/operators and public safety officials. And whether the technology solution leverages data exchange created for LAANC, SWIM, or other low-altitude traffic management capability.

5.1.2.5. Costs

WG1 also evaluated each technology solution based on the initial and recurring costs of the Primary solution to the owner/remote pilot, public safety officials, manufacturers, the Agency, and other third parties.

Overview of Cost Factors

Each of the eight technology alternatives categorized by WG1 has associated costs. Although the goal is to provide “relative costs” between the alternatives, there are many cost factors to consider:

- Costs may vary significantly in how a technology alternative meets one or both requirements (“direct broadcast” and “networked”). In some cases, the solution natively applies to one but not both requirements, thus a secondary solution would be required to meet both. And in some cases, like SW-based Flight Notification w/Telemetry, the category itself relies on other technology solutions.
- Each technology alternative category has a varying level of scope. For instance, Low Power Direct RF covers multiple technical solutions while the Physical Indicator category is “technically” narrow.
- The industry representatives in WG1 are from a finite number of companies and might not statistically represent the entire category. For instance, a consumer-focused manufacturer or service provider might have a very different cost structure and target market than a commercial-focused one.
- In some technology alternative categories, some costs may float between entities that could be burdened by such costs. For example, a data subscription cost could be seen directly by the end user, *or* fully included in the UA costs for the life of the product and borne by the manufacturer, *or* split between entities.
- Retrofit costs could be very similar or very different from an integrated product solution.
- Development costs, particularly but not limited to hardware based solutions, will need to be amortized over applicable volume. One manufacturer’s cost structure may be entirely different from another.
- There is an inherent time-based ambiguity to any costs. A manufacturer or service provider that has a solution already in development, or can slip-stream behind an existing implementation for something similar, may have a very different cost structure from a provider that will commence development once the FAA issues guidelines or a NPRM. And

more simply, some technology alternatives with low TRL's have ambiguous cost structures as the solutions are still in development.

Assumptions

To reach consensus on the relative costs of each technology alternative and where the costs are being incurred, an aligned assumption set is required. No assumption set is perfect or fully inclusive. Here are the baseline assumptions for this analysis of relevancy:

- The consideration of costs is entirely monetary. Emotional costs, such as willingness to comply for varied reasons, including privacy, are not considered as relevant cost factors. Furthermore, Ease of Compliance, Readiness for Implementation, Operational Performance/Security, and Interoperability were not considered as relevant factors in these cost assumptions, but are discussed elsewhere.
- Each technology alternative has a primary implementation, direct broadcast or networked. Although almost all technology alternatives could technically address both requirements, a primary implementation is assigned and only the primary is considered for cost relevancy. For example, Visual Light Encoding could technically provide a networked solution if the receiver is a device capable of transmitting the decoded message across the Internet. However, the primary implementation is direct in that it is the main thesis of the technology.
- Fixed infrastructure receivers, although important to the overall ARC, are not considered. The focus is on mobile/portable receivers for public safety officials and the public; however there is no doubt that fixed infrastructure receivers could be built to accommodate most solutions.
- Some general cost items are beyond the scope of the technology alternatives as defined. The FAA, for instance, would need to maintain the registration database and PII System for all solutions. Additionally, the ARC has called out two separate requirements, "direct broadcast" and "networked." To meet the "networked" requirement there is general acknowledgement that some entity(ies) will need to build out the database, API's, security, and access controls required to realize ID and tracking for networked based solutions. These databases are assumed as common costs and are not reflected in the chart, but are discussed below in the Database Costs subsection. Finally, regulatory costs and regulatory timeframe to enable a technology alternative are out of scope as well.

Analysis

Table 4 (on page 26) provides relevant costs associated with the creation of solutions across each technology alternative's primary implementation and under the assumptions set above. The costs are grouped into three categories: Transmitter, Receiver, and Development Costs.¹⁰ Individual components are broken out and the bearer(s) of each cost is identified. As there are many factors in the determination of actual amounts, **\$'s are used to show relative costs within a row and are not keyed to any dollar figure.** The relative scale used here is from \$ to \$\$\$\$, with each \$ roughly reflecting a doubling (e.g., \$\$ is relatively 2x the cost of \$).

¹⁰ Does not include the cost to setup, maintain, and provide access control for the database which connects owner contact information and other PII with the unique ID.

WG1 considered the following critical factors:

- **Transmitter HW** – This represents the cost of hardware to add the transmission capability for the solution. This cost is assumed to be borne by the owner of the UA, the purchaser. This is a per-unit cost.
- **Transmitter Data** – For some solutions there may be a cost associated with the transmission of data from the UA. The burden of this cost can be applied to either the manufacturer or the owner, as it may be bundled entirely in the cost of the UA or may be a separate cost. This cost may be one-time or reoccurring. This is a per-unit cost.
- **Receiver HW (Non-Internet Device)** – This represents the cost of a receiver that is not a smartphone or other Internet connected device.
- **Receiver Internet Device** – This represents whether an Internet device, like a smartphone, is required to be the receiver. Internet-enabled devices do not need to be smart-phones, and investment may need to be made to purchase Internet-enabled devices. Some statistics suggest that only 30% of patrol officers currently have department-issued smartphones,¹¹ while others suggest that 84% of public safety agencies use mobile field technologies “ranging from rugged laptops, tablets and handhelds to consumer-grade devices.”¹² Some agencies also may have “bring your own device” policies that allow officers to use personal devices for official purposes, and other agencies have strict policies against such use. Additionally, when a public safety official is not equipped with such a device, it is acknowledged that existing radios could be used to communicate with an individual, perhaps at dispatch, who has a receiver internet device connected to the internet and can provide relevant ID and tracking information. *Required* indicates that it is required to complete the solution. *Optional* indicates that it can add value to the solution, like the ability to query a database, but is not required to complete the solution. Costs are not explicitly detailed as there is range of possibilities for procurement and use or non-use of personal devices by public safety officials, and costs for devices and service are well known.
- **Receiver Internet Data** – This represents whether an Internet Device data plan is required to complete the receiver solution. *Optional* indicates that it can add value to the solution, like the ability to query a database, but is not required to complete the solution.

Note: Regardless of Receiver solution, for public safety officers in the field to directly retrieve owner contact information and other PII, a device connected to the network (e.g., handheld smartphone, laptop in patrol car) will be required.¹³

- **Development Costs** – This is a relative guide to include all costs (per unit, non-recurring HW+SW engineering [NRE], certifications, distribution, etc.) for all pieces necessary for the manufacturer and third parties, collectively, to complete the solution (transmitters and receivers).

¹¹ https://www.washingtonpost.com/news/true-crime/wp/2017/08/02/firstnet-broadband-network-to-enable-police-and-fire-responders-to-talk-to-each-other-ready-to-launch/?utm_term=.bd12dfcbe3c6.

¹² <http://www.policemag.com/channel/technology/articles/2016/10/a-guide-to-understanding-law-enforcement-field-technology.aspx>.

¹³ A radio call to a dispatcher may be sufficient.

Database Costs

Networked solutions require a central database to allow the incoming ID and tracking data to be accessed by the recipients such as public safety officials, security agencies, airport authorities, air traffic controllers, emergency responders, and members of the public. Under certain operations, direct broadcast solutions may also be required to provide a method to publish to this database, or may want to optionally offer this ability. Furthermore, all solutions require a central database for hosting registration and PII. The costs and complexities of such database(s) should be weighed carefully by the FAA. The ongoing development or existence of other authenticated FAA databases that have similar functionality, or could be expanded, may mitigate some of these costs.

In particular, the FAA should consider whether LAANC could be expanded to address the requirements of the real-time networked ID and tracking database. According to the FAA, LAANC is “the first step of a UTM system.” The task of evolving the LAANC system to provide real-time networked ID and tracking will require the establishment of a telemetry API. If the FAA uses the telemetry API protocol already tested and created by NASA, some costs could be mitigated. The costs for the expanded development and service of providing real-time networked ID and tracking with LAANC, while borne by UAS Service Suppliers (USS’s), may be passed on to the end user. The nature and extent of these costs are currently unknown. It is also possible that the FAA could forgo relying on LAANC or third parties for the development of the real-time networked ID and tracking database and resulting service, bearing all costs itself.

5.1.3. Analysis of viable technology solutions

Table 1. Summary Characterization of Technology Alternatives

Technology Alternatives: Summary	ADS-B	Low Power Direct RF	Networked Cellular	Satellite	SW-Based Flight Notification w/ Telemetry	Unlicensed Integrated C2	Physical Indicator	Visual Light Encoding
Primary Requirement Met	Direct Broadcast	Direct Broadcast	Networked	Networked	Networked	Direct Broadcast	Direct Broadcast	Direct Broadcast
Retrofit Transmitter	External device attached to UA	External device attached to UA	External device attached to UA	External device attached to UA	Manual flight planning	Integrated with C2 (may not be possible for all UA)	Physical	Integrated w/lights (may not be possible for all UA)
Integrated Transmitter	Integrated	Integrated	Integrated	Integrated	Integrated Flight Planning	Integrated with C2	Physical	Integrated
Mobile Receiver	Device that can decode ADS-B	Device that speaks same transport as transmitter, e.g. Bluetooth	Connected Internet Device	Connected Internet Device	Connected Internet Device	Device that can decode special channel in C2 link	Eyes	Smartphone Camera

Table 2. Characterizations of Technology Alternatives Related to Ease of Compliance and Technology Readiness

Technology Alternatives: Ease of Compliance and Technology Readiness		ADS-B	Low Power Direct RF	Networked Cellular	Satellite	SW-Based Flight Notification w/ Telemetry	Unlicensed Integrated C2	Physical Indicator	Visual Light Encoding
Ease of Compliance for Owner / Operator	Retrofit	Medium	Medium	Medium	Medium	High, if GCS sends telemetry via Internet connected device	High, if device capable	Low - High (varies)	High, if device capable
	Integrated	High	High	Med-High	Med-High	High (same caveat as Retrofit)	High	High	High
	Requires 3rd Party	No	No	Yes	Yes	Yes	No	No	No
Readiness for Implementation	Retrofit in < 1yr	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
	Integrated in < 1yr	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No

Table 3. Characterizations of Technology Alternatives Related to Operational Performance, Security, and Interoperability

Technology Alternatives: Operational Performance, Security and Interoperability		ADS-B	Low Power Direct RF	Networked Cellular	Satellite	SW-Based Flight Notification w/ Telemetry	Unlicensed Integrated C2	Physical Indicator	Visual Light Encoding
Performance Against Requirements	1:Direct Broadcast	Yes	Yes	No	No	No	Yes	Yes	Yes
	2:Networked Database	No	No	Yes	Yes	Yes	No	No	No
	Notes	Could be networked from receiver	Could be networked from receiver		Network only needed for receiver	Telemetry requires Internet connected GCS	Could be networked from receiver		Could be networked from receiver
	Update Rate $\geq 1\text{Hz}$	Yes	Yes	Yes	No	Yes	Yes	N/A	No
	Latency $<3.5\text{s}$	Yes	Yes	Yes	Yes	Yes	Yes	N/A	Yes
	Range	Radio Range	Radio Range	Network Range	Network Range	Network Range	Radio Range	Visual Range	$<$ Visual Range
	Licensed Spectrum	Yes	No	Yes	Yes	Varies by HW	No	N/A	N/A
Security	Spoofing Security	No	Solution dependent	Yes	Yes	No	Yes	No	No
	Tamper Resistance	Yes, Integrated; No, for Retrofit	Yes, Integrated; No, for Retrofit	Yes, Integrated; No, for Retrofit	Yes, Integrated; No, for Retrofit	No	Yes	No	No
	Tracking Verification	No, except ATC	No	Yes	No	No	No	No	No
Interoper- ability	ATC	Yes	No	No	No	Yes	No	No	No
	International	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Federated	Yes	No	Yes	Yes	Yes	No	No	No

Table 4. Characterizations of Technology Alternatives Related to Costs

Technology Alternatives: Costs (Primary Implementation Only)		ADS-B	Low Power Direct RF	Networked Cellular	Satellite	SW-Based Flight Notification w/ Telemetry	Unlicensed Integrated C2	Physical Indicator	Visual Light Encoding
Costs Item	Cost To								
Transmitter HW	Owner	\$\$\$\$ (rule compliant), \$\$ (low power)	\$-\$	\$\$	\$\$	None - \$\$	None	<\$	\$
Transmitter Data	Manufacturer and/or Owner; one-time or recurring; bundled with hardware or separate	None	None	\$-\$	\$-\$	None - \$\$	None	None	None
Receiver HW (Non Internet Device)	Public Safety Officer	\$\$	None (existing device); \$\$ (stand alone)	None	None	None	\$\$\$\$	None	None
Receiver Internet Device		Optional	Optional	Required	Required	Required	Optional	Optional	Required
Receiver Internet Data		Optional	Optional	Required	Required	Required	Optional	Optional	Optional
Development Costs	Manufacturer and/or 3rd Party	\$-\$	\$-\$	\$-\$	\$-\$	Near Zero - \$	Near 0-\$ (OEM); \$-\$ (receivers)	Near Zero	\$-\$

5.2. Requirements for meeting the security and public safety needs of the public safety officials, homeland defense, and national security communities for the remote identification and tracking of UAS

WG2 was tasked with identifying “the requirements for meeting the security and public safety needs of the law enforcement, homeland defense, and national security communities for the remote ID and tracking of UAS.”

WG2 considered the need to identify specific requirements while at the same time attempting to account for technology advancements in the future regarding UAS equipment, payload capacity, size, speed, and capabilities.

While its focus was on the needs of public safety officials, WG2 nevertheless understood the importance of also considering the needs of the numerous stakeholders served by public safety officials. To that end, WG2 considered the following factors:

1. The safety and security of the National Airspace System (NAS).
2. Protection of the public.
3. Accountability of UAS manufacturers and consumers.
4. Ease of use for UAS remote pilots, manufacturers, owners, and public safety officials.
5. Privacy concerns.
6. Ease for specific stakeholders (media, government agencies, etc.) to enter airspace otherwise off-limits to UAS.
7. Service to the public.
8. Protection of critical infrastructure.

5.2.1. Identifying the needs of public safety officials

WG2 explored dozens of potential scenarios and use cases to determine the information that public safety officials and other designated officials need to identify and track UAS. Through this process, WG2 identified two general categories of UAS ID and tracking needs: (1) incident investigation, to include both the local incident sight and tracking of entire flight profile outside the immediate local incident location, as well as historical tracking information to assist in pre- and post- incident investigations and surveillance of suspected criminal or terrorist activity; and (2) active monitoring of heightened awareness areas.

1. Incident investigation.

This category includes all scenarios in which an individual wishes to inquire about the identity and purpose of a sighted UA. The information an individual could obtain would depend on the authorization level of the individual making the inquiry.

2. Active monitoring of heightened awareness areas.

This category addresses the need to have dynamic and active awareness of UAS near heightened awareness areas. These areas could include: airports, heliports, prisons, military installations, nuclear facilities, large stadiums, and other critical infrastructure locations where a UAS could potentially

pose an imminent threat to public safety and security. Stakeholders representing some of these locations expressed the need to have a system in place that would allow certain entities to be alerted when a UAS enters designated airspace near these heightened awareness areas. This would facilitate immediate identification, authentication, communication, and mitigation in areas where timely response is critical.

To achieve the goals of both categories, WG2 determined that all UAS meeting certain threshold requirements would need to be tracked, whether passively or actively, from commencement to termination of each operation. WG2 further concluded that information regarding the position of the aircraft, the location of the ground control station, and the identity of the remote pilot will help maintain a safe and secure environment for the general public and public safety officials.

5.2.2. Impacts to safety and security from unmanned aircraft

While the majority of UAS will be operated in compliance with operational regulations, non-compliant or unauthorized UAS operations must be adequately addressed to ensure the safety and security of the NAS, critical infrastructure, and people on the ground.

At the core of the concern regarding UAS operations is accountability. With manned aircraft there is a pilot who is easily identifiable, and often in two-way communication with air traffic control. The intent of the pilot may be ascertained. However, with UAS operations, identifying the remote pilot to determine intent may be more problematic, especially if the remote pilot is operating beyond line of sight, or if the UAS is operating in an autonomous mode. The anonymity of the remote pilot is the central concern. In addition, manned aircraft is sometimes equipped with a transponder that is transmitting a unique flight code, which allows ATC to track the aircraft electronically. At present, the primary method for public safety officials to track a UA in flight is visually. A unique identifier that is available electronically would support both identification and tracking.

The key considerations of WG2 in determining the requirements necessary for identifying and tracking a UAS were:

1. **Public safety**: Assist responding public safety officials in identifying the owner and operator of UAS being used to harass others, or rogue UAS over crowds during large events or at disaster or crash scenes where manned aircraft are responding.
2. **Aviation safety**: Avoid conflict with manned aircraft and safely integrate UAS into the NAS by providing the UA the ability to operate beyond visual line of sight or autonomously within a UTM architecture.
3. **National security**: Support security for critical infrastructure, such as nuclear power plants or military sites, where there has been evidence of UA attempting to perform persistent surveillance. Similarly, where there is evidence of UA being used autonomously, or flown beyond visual line of sight to fly drugs across the southern border, or to deliver contraband inside prisons.

5.2.3. Applicability of ID and tracking requirements

At a threshold level, WG2 considered to which UAS the remote ID and tracking requirements should apply. WG2 determined that UAS with either of the following characteristics should comply with remote ID and tracking requirements:

1. Ability of the aircraft to navigate between more than one point without direct and active control of the pilot.
2. Range from control station greater than 400' *and* real-time remotely viewable sensor.

In addition to the capabilities of the UAS, WG2 also considered other factors such as weight, inertia, speed, payload, classification as toys, and waivers (R&D, experimental, etc.) as potential discriminators to define thresholds requiring ID and tracking. However, WG2 concluded that applicability should be based upon capabilities of the UAS versus other factors such as weight or the operational use of the UA.

It should be noted that there was a robust discussion of the full ARC about whether the ARC should recommend a capabilities-based or, in contrast, a weight-based approach to applicability. Some stakeholders expressed strong preference for a weight-based threshold. Arguments in favor of this approach stressed simplicity, adaptability, and familiarity, which would promote compliance and thereby enhance the security, safety and efficiency of the NAS; comprehensiveness to support robust UTM systems; future-proofing to encompass technological developments without need to constantly revisit the applicability threshold; and closing ID and tracking gaps inherent in the capabilities-based applicability threshold. With a 250-gram threshold (as used for the existing sUAS registration requirement), these stakeholders urged that this approach would also properly focus on risk of the operation, as well as capacity to pose a threat via a payload, rather than operator intent, and streamline implementation.

The ARC's discussions concerning the WG2 threshold reflected on the scenario of a UA that does not have a real-time remotely viewable sensor or is not autonomous but that is still capable of flying beyond 400 feet from the remote pilot via manual controls, perhaps due to its large size and high visibility at a distance. Such UA would include a significant number of "traditional" model aircraft, which present a different risk profile, leading the ARC to discuss that expanding the threshold in this way might also compel an exemption for model aircraft operators who are in compliance with 14 CFR part 101. This exemption would not include model aircraft that have advanced flight functions. As a result of these discussions, the recommended threshold requirement was expanded beyond what WG2 proposed, and a proposal to exempt certain part 101 (model aircraft) operations emerged (see section 6.1, Option 1). For several members of the ARC, the expansion of the threshold beyond what WG2 proposed was linked to the need for an exemption of some kind for part 101 model aircraft.

The ARC discussed recommending exemptions from remote ID and tracking requirements for the following:

- Unmanned aircraft that are operated in compliance with 14 CFR part 101.

- Unmanned aircraft that are operated in compliance with 14 CFR part 101 *and* are:
 - operated within 400' of the remote pilot, regardless of capability (navigation and sensors); *or*
 - range limited to less than 1200' of the remote pilot and cannot be flown out of the direct natural vision of the pilot (i.e., do not have an automatic flight control system or equipment to control the flight of aircraft by other references, internal or external to the aircraft).
- UAS that weigh less than 250g [or some other weight threshold] (regardless of operator type or operating rule).
- UAS that meet the ASTM F963 toy standard, and subsequently are eligible to be sold in the toy aisle.
- UAS with transmitter output limited to 25 mW [or some other threshold to be determined through empirical testing] and that cannot be flown out of the direct natural vision of the pilot (i.e., do not have an automatic flight control system or equipment to control the flight of aircraft by other references, internal or external to the aircraft).
- UAS that are not designed to have the capability of flying beyond 400' of the remote pilot [or some other distance determined through empirical testing], or for longer than a specified period of time, and are operated within visual line of sight of the remote pilot.
- UAS that are operated over private property with the permission of the property owner and at very low altitudes (e.g., below the height of neighboring obstacles).
- Racing UAS that operate at very low altitudes on closed courses.
- UAS that are operated within 100' of the remote pilot and at very low altitudes (e.g., below the height of neighboring obstacles).
- UAS that are operated under air traffic control and are equipped with the equipment associated with such operations (including ADS-B, transponder, and communication with ATC).
- Where the operation is authorized by the FAA (e.g., for the purposes of law enforcement security or defense, or under an FAA waiver).

The ARC's final recommendations regarding the applicability of remote ID and tracking requirements are included below in section 6.1.

To identify the requirements for meeting the security and public safety needs of the law enforcement, homeland defense, and national security communities for the remote ID and tracking of UAS, WG2 also made findings and conclusions related to the following issues:

- The types of data that should be made available¹⁴ regarding the unmanned aircraft or associated control station,¹⁵ and who should have access to what data and under what circumstances.

¹⁴ WG2 considered requiring that the information be broadcast but was concerned that the term "broadcast" could be limiting regarding the technology used.

¹⁵ In discussing how data could be made available, WG2 originally assumed that information regarding the position of the unmanned aircraft would be transmitted by the unmanned aircraft, and information regarding the location of the control station would be transmitted by the control station. However, so long as the information regarding the aircraft and the control station is accurate and provided in near real-time, WG2 determined that the source of the transmission of the information is immaterial. WG2 concluded that data could be transmitted directly from the aircraft, could be transmitted from the control station, or could be transmitted from other sources.

- Data authentication and retention.

WG2's findings and conclusions about types of data needed and data authentication and retention were presented to and considered by the full ARC. The ARC's recommendations related to those findings and conclusions are discussed below in sections 6.5 and 7.1.

5.3. Feasibility and affordability of available technical solutions, and the ability of those technologies to address the needs of public safety and air traffic control communities

WG3 was tasked with evaluating "the feasibility and affordability of available technical solutions, and determining how well those technologies address the needs of the law enforcement and air traffic control communities." WG3's findings and conclusions were presented to and considered by the full ARC. The ARC's recommendations related to those findings and conclusion are discussed below in section 6.

6. ARC RECOMMENDATIONS

6.1. Applicability of the ID and tracking requirements

The ARC did not reach consensus on an applicability threshold for ID and tracking requirements. Two final options were presented to ARC members. Of those members who supported one of these two options, they were roughly split. The ARC recommends the FAA give due consideration to both of these options.

Option 1:

Except for those members who strongly favor a weight-based threshold for applicability and those members who strongly oppose an exemption for model aircraft operated in compliance with 14 CFR part 101 (*see* discussions above in 5.2.3), the ARC recommends that all UAS be required to comply with remote ID and tracking requirements *except* under the following circumstances:

1. The unmanned aircraft is operated within visual line of sight of the remote pilot and is not designed to have the capability of flying beyond 400' of the remote pilot.¹⁶
2. The unmanned aircraft is operated in compliance with 14 CFR part 101, *unless* the unmanned aircraft:
 - a. Is equipped with advanced flight systems technologies that enable the aircraft to navigate from one point to another without continuous input and direction from the remote pilot.

¹⁶ The ARC is not intending to encompass drone racing at very low altitudes on a closed course that may be authorized by operation, by location, or some other mechanism.

- b. Is equipped with a real-time downlinked remote sensor that provides the remote pilot the capability of navigating the aircraft beyond visual line of sight of the remote pilot.
- 3. The UAS is operated under ATC and contains the equipment associated with such operations (including ADS-B, transponder, and communication with ATC).
- 4. The UAS operation is exempt from ID and tracking requirements by the FAA (e.g., for the purposes of law enforcement, security or defense, or under an FAA waiver).

Option 2:

Except for those members who strongly favor a weight-based threshold for applicability (*see* discussion above in 5.2.3), the ARC recommends UAS with either of the following characteristics must comply with remote ID and tracking requirements:

- 1. Ability of the aircraft to navigate between more than one point without direct and active control of the pilot.
- 2. Range from control station greater than 400' *and* real-time remotely viewable sensor.

The ARC further recommends that UAS operating under the following circumstances be *exempt* from the remote ID and tracking requirement:

- The UAS is operated under ATC and contains the equipment associated with such operations (including ADS-B, transponder, and communication with ATC).
- The UAS operation is exempt from ID and tracking requirements by the FAA (e.g., for the purposes of law enforcement, security or defense, or under an FAA waiver).

Regardless of which option FAA chooses for applicability, the ARC recommends the FAA include a waiver mechanism in the remote ID and tracking rule, to allow individual operations or classes of UAS to deviate from the requirements of the rule if operations are conducted under the terms of a certificate of waiver.

The ARC also recommends the FAA apply the remote ID and tracking requirements to the remote pilot, *not* to the manufacturer of the UAS. The ARC further recommends the FAA require manufacturers to label their products to indicate whether they are capable of meeting applicable remote ID and tracking requirements. If a product is labeled as capable of meeting remote ID and tracking requirements, such capabilities must be enabled by default and the manufacturer must not present the user with an option to turn off the ID and tracking.

The ARC also discussed whether unmanned aircraft equipped with advanced flight system technologies that are strictly for safety purposes and that keep the aircraft within visual line of sight

of the remote pilot, such as a “return to home” feature, should be exempt from remote ID and tracking requirements. The ARC recommends the FAA consider whether such an exemption would be appropriate, provided the safety features cannot be readily altered or reprogrammed.

6.2. Direct broadcast and network publishing requirements for remote ID and tracking

Through the working group process (as discussed above in section 5), the ARC identified a set of minimum requirements for remote ID and tracking of UAS. The ARC also identified additional information that would be helpful but not required. In the context of these requirements, the ARC determined that there are two ways of providing remote ID and tracking data. The first is by broadcasting locally and the second is by publishing information to an FAA-approved internet-based database. This section provides an overview of how direct broadcast and network publishing work, followed by a discussion (in section 6.3) of the ARC’s recommendations as to when direct broadcast or network publishing or both would be required.

6.2.1. Direct broadcast (locally)

Direct broadcasting means to transmit data in one direction only with no specific destination or recipient. Data can be received by anyone within broadcast range. A direct broadcast requires no handshaking and does not require bi-directional communication capabilities to work. Although range is limited to the broadcast area, dependability is high as there is no reliance on infrastructure “repeaters.” Broadcast reception area can be increased by either deploying specialized antenna on receivers or increasing the number of receiving stations. This can be useful especially around sensitive areas such as critical infrastructure, airports, defense installations, or remote locations where network coverage may not be available. Receiving stations can also be tied into a larger network to publish received data to an FAA-approved internet-based database. Direct broadcast systems include technologies such as ADS-B, Low Power Direct RF, Unlicensed Integrated C2, and some visual light solutions. Receivers must be capable of decoding the broadcast technology, and compatibility between receivers and transmitters becomes an important factor in cost and deployment.

The direct broadcast capability would enable public safety officials equipped with an appropriate receiver to obtain information transmitted from the vehicle. Transmission and receipt of required UAS information is not network dependent for direct broadcast solutions.

Since public safety officials may not be able to equip with receivers for all possible direct broadcast technologies, the ARC recommends the FAA adopt an industry standard for data transmission, which may need to be created, to ensure UA equipment and public safety receivers are interoperable. This will also help mitigate concerns about proprietary technology licensing and vendor exclusivity.

6.2.2. Network publishing (to an FAA-approved internet-based database)

Publishing means the act of transmitting data to an internet service or federation of services. Clients, whether ATC or public safety officials, can access the data to obtain ID and tracking information for UAS for which such data has been published. Networked Cellular, Satellite, and SW-based Flight Notification w/ Telemetry are among methods by which data can be published, as well as broadcast to a networked ground station. As interoperability is established at the IP and application level,

technologies do not need to be compatible as long as the transmitter hardware can pass data to the internet based service(s) and the client can connect to the internet based service(s).

The FAA should leverage internet-based database infrastructure that exists or that is already under development and that could integrate with the FAA's future UTM roadmap. To accomplish this objective, the FAA could provision remote ID and tracking services using private Third-Party Providers/UAS Service Suppliers (TPP/USS) to provide services specific to UAS operations. Such services would be accomplished through an exchange of information between the operator, the TPP/USS and the FAA, whereby the TPP/USS would be the primary interface to the operator. The TPP/USS would follow business rules provided by the FAA to collect and transmit to the FAA telemetry information.

This model could allow the FAA to leverage existing infrastructure that is under development to allow for a high scale competitive ecosystem of TPP/USS. Much of this infrastructure already exists or is under development by scores of companies participating in NASA UTM development efforts, trials, and the LAANC program. Provisioning services in this manner will allow the FAA to deploy a telemetry Application Programming Interface (API) to allow TPP/USS to transmit telemetry data from operators for publishing to an internet-based database. For rapid deployment, the API can be modeled on the already tested NASA UTM telemetry API which can be added to the existing LAANC Automation Platform. TPP/USS will provide full information regarding operations as required by the FAA (telemetry information, id, etc.) to the FAA in a manner similar to how TPP/USS will interact with the notice and authorization APIs.

TPP/USS could provide remote ID and tracking services on behalf of the FAA. TPP/USS are expected to be private entities. They provide the primary interface to the operator initially via system application software that is likely to include mobile applications and eventually from on board hardware that will publish to the TPP/USS for transmission to the FAA. The TPP/USS could manage (if necessary) communications and messaging with the operator and with the FAA. The TPP/USS could manage and store all the records of telemetry based on SORN (Systems of Records Notices) requirements. The TPP/USS would send telemetry data to the FAA for display to ATC or the appropriate parties. All interfaces to the FAA where a TPP/USS is exchanging information with the FAA will be tested, proven, controlled and securely managed. Services provided by a TPP/USS will be monitored for performance and to collect metrics.

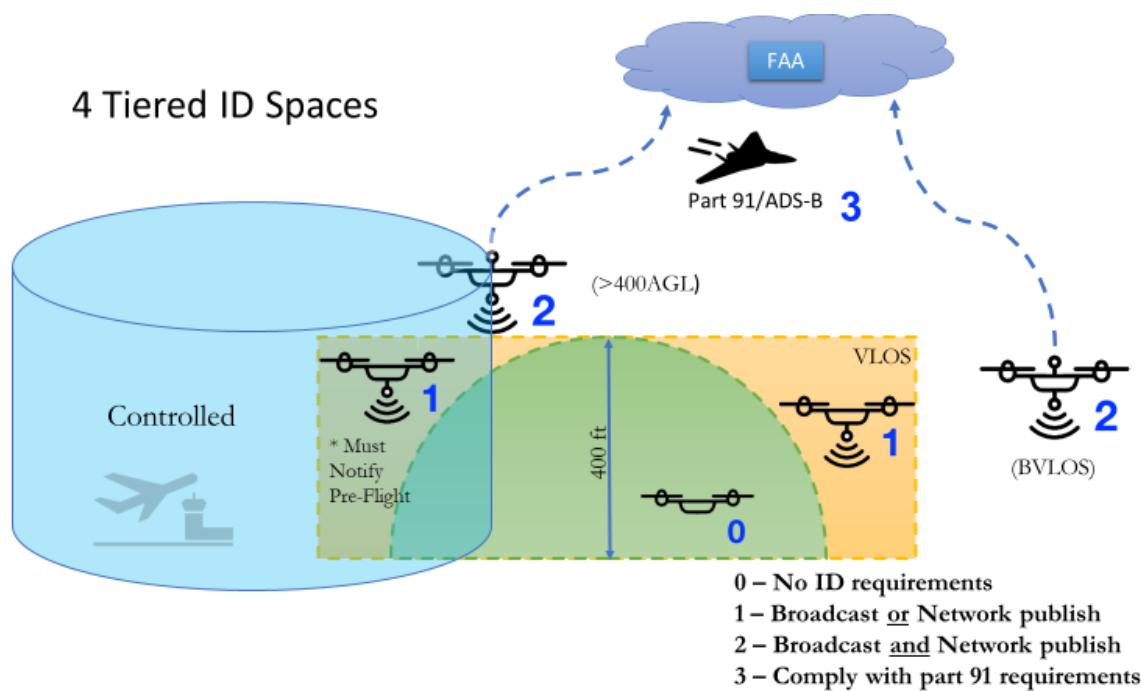
Following the deployment plan outlined above could result in the rapid deployment of internet-based database publishing capability by leveraging technologies that already exist, and aligning industry UTM product development roadmaps with the FAA's desire for a remote ID and tracking requirement and an eventual UTM system. Consumers could benefit from this competitive environment because a vendor or operator can choose to comply with this part of the ID and tracking requirement using one broadcast technology, while a different vendor/operator could choose a different broadcast technology, so long as the technology can publish to an API it will have the possibility of satisfying the internet-based database publishing requirement. This could help mitigate concerns about proprietary technology licensing and vendor exclusivity and enable a broad range of vendors to make and sell equipment.

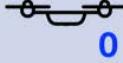
ID and tracking using technology that publishes could help public safety officials improve UAS investigations. As discussed elsewhere in this report, there are privacy considerations that need to be

addressed, and the ARC recommends that information held by TTP/USS be governed by restrictive use conditions imposed on the TPP/USS related to the use and dissemination of any data and information collected.

6.3. Tiered UAS direct broadcast and network publishing requirements for remote ID and tracking

Throughout the discussions of the ARC, members acknowledged a need for tiered, context-appropriate solutions. In order to illustrate how these tiers may be applied to the technologies, explanatory implementations are included in this report. These explanatory implementations reflect the identified needs of public safety officials and acknowledge that, although the minimal compliance is based on UAS capabilities, additional tiers beyond the minimum requirements, e.g. tiers based on operation type rather than capabilities, are acceptable. Public safety officials need to be able to obtain both ID and tracking information while in the field. However, for line of sight operations, public safety concerns do not require publishing of data, though there are benefits to such information being published. The explanatory implementations are intended to address both public safety needs as well as ATC/UTM needs that may arise. The two graphics below summarize what is discussed in this section.



Tier	Requirement	Examples of Qualifying Conditions
	No ID and tracking requirements	<ul style="list-style-type: none"> Pending applicability decision (Section 6.1), operating within VLOS of remote pilot and not designed to be capable of flight beyond 400' of remote pilot. Pending applicability decision (Section 6.1), operating in compliance with 14 CFR part 101 (except as specified). Operating under ATC and contains equipment associated with such operations (ADS-B, transponder, and communication with ATC). Operation exempt from ID and tracking requirements by FAA.
	Broadcast (locally) or Network publish	UAS does not qualify for a Tier 0 exemption and does not meet the conditions for Tier 2 or Tier 3, for example UAS conducting most part 107 operations.
	Broadcast (locally) and Network publish	Conducting waivered operations that deviate from certain part 107 operating rules, and where the FAA determines that Tier 2 ID and tracking are required as a condition of the waiver (e.g., operations BVLOS, operations above part 107 maximum altitudes, operations over unprotected persons).
	Part 91 Requirements (Mode S, ADS-B, etc.)	<ul style="list-style-type: none"> Weight above 55 pounds and operating BVLOS. Operating in IFR conditions. Operating in controlled airspace.

6.3.1. Tier 0 – No ID and tracking requirement

Tier 0 requires no ID or tracking mechanism. Other rules may require registration, markings, or limit flights with certain airspace. This tier is intended to eliminate UAS that are less capable, that pose less of a threat to either safety or airspace, or for which there is less chance for anonymity of the remote pilot.

Tier 0 includes UAS operated under any of the following circumstances:

1. Pending applicability decision (Section 6.1), UAS operated within visual line of sight of the remote pilot and is not designed to have the capability of flying beyond 400' of the remote pilot.¹⁷
2. Pending applicability decision (Section 6.1), unmanned aircraft operated in compliance with 14 CFR part 101, *unless* the unmanned aircraft:
 - a. Are equipped with advanced flight systems technologies that enable the aircraft to navigate from one point to another without continuous input and direction from the remote pilot.
 - b. Are equipped with a real-time downlinked remote sensor that provides the remote pilot the capability of navigating the aircraft beyond visual line of sight of the remote pilot.
3. UAS operated under ATC and contains the equipment associated with such operations (including ADS-B, transponder, and communication with ATC).
4. UAS operation is exempt from ID and tracking requirements by the FAA (e.g., for the purposes of law enforcement, security or defense, or under an FAA waiver).

¹⁷ Again, the ARC is not intending to encompass drone racing at very low altitudes on a closed course that may be authorized by operation, by location, or some other mechanism.

All other UAS will be subject to remote ID and tracking requirements in either Tier 1 or Tier 2, or to part 91 requirements in Tier 3.

6.3.2. Tier 1 – Direct broadcast (locally) *or* Network publish to FAA-approved internet-based database

Tier 1 requires that aircraft must broadcast both ID and tracking information so that any compatible receiver nearby can receive and decode the ID and tracking data. The person receiving the transmitted data (public safety, civilian) must either be within broadcast range of the aircraft or have access to data re-transmitted by a ground station repeater in broadcast range of the aircraft. If a network is available, publishing to an FAA-approved internet-based database satisfies this requirement.

A UAS would fall into Tier 1 if it does not qualify for a Tier 0 exemption and does not meet the conditions for Tier 2 or Tier 3, for example UAS conducting most part 107 operations.

6.3.3. Tier 2 – Direct broadcast (locally) *and* Network publish to FAA-approved internet-based database

Tier 2 requires UAS (aircraft or aircraft + ground station) to broadcast ID and tracking data *and* publish ID and tracking data to an FAA-approved internet-based database. The remote pilot must use the necessary technology for operational conditions. As interoperability is established at the IP and application level, the FAA should specify the performance requirements such as minimum latency and frequency. Local broadcast should always be a requirement as it provides a backup means of ID and tracking if the network is compromised, degraded, or unavailable. This tier is intended to address both public safety needs as well as ATC/UTM needs that may arise.

An example of UAS that may fall in Tier 2 would be UAS that are conducting waivered operations that deviate from certain part 107 operating rules, and where the FAA determines that Tier 2 ID and tracking are required as a condition of the waiver. Such operations could include, but are not limited to:

1. Operations beyond visual line of sight of the remote pilot.
2. Operations above part 107 maximum altitudes.
3. Operations over unprotected persons.

6.3.4. Tier 3 – Flight under part 91 rules

Tier 3 requires that UAS must adhere to the rules of manned aircraft as defined in 14 CFR part 91. This tier is intended for aircraft that are integrated into the manned aircraft airspace. These UAS are likely outside the scope of the public safety concerns identified by the ARC, as most of these UA would not be operating anonymously because UA operators are likely to be in contact with ATC, have likely filed flight plans, or could be integrated into a UTM structure.

An example of UAS that may fall into Tier 3 are those weighing above 55 pounds and operating BVLOS, in IFR conditions, or operating in controlled airspace. Aircraft would be required to adhere to part 91 (including §§91.225 and 91.227) requirements.

6.4. Implementation approach to direct broadcast and network publishing requirements for remote ID and tracking

6.4.1. Pre-Rule

The value and advantages of a remote ID and tracking capability for UAS operating in the NAS are well recognized and generally supported by all stakeholders. Although the direct broadcast and network publishing technologies identified by the ARC may meet the remote ID and tracking requirements, the Agency may need time to resolve other regulatory and technical issues before a final rule is enacted.

For example, UAS remote ID and tracking using direct broadcast technology will rely on the Agency to adopt industry consensus standards to ensure receivers are interoperable across technologies. ID and tracking using network publishing technology may require additional regulatory due-diligence and relies on the Agency to adopt industry performance standards. Over time, the direct broadcast and network publishing solutions will mature to address the remote ID and tracking requirement in real or near-real time.

To help address the concerns of public safety officials before an ID and tracking rule is finalized, the Agency could broaden UAS safety education efforts and continue the UAS detection pathway research with industry.

6.4.2. Before final rule is enacted

Before the final rule is enacted, the Agency could work to scope standards needed to enable direct broadcast and network publishing technologies for implementing the remote ID and tracking requirement on new equipment and existing equipment. The ARC recognizes capabilities and associated standards often develop at different rates and recommends the FAA ensure that standards for ID and tracking technology move forward at a rapid pace. ARC members discussed identifying “carrots” for early adoption and use of ID technologies. The Agency should also work closely with industry on developing the ideal architecture for the PII System.

The ARC discussed whether the Agency should consider an interim system to allow operators to self-declare before the ID and tracking rule is finalized. Some members thought self-declaration could allow the remote pilot/operator (or through a third party) to meet the objectives laid out for the UAS-ID ARC while direct broadcast and network publishing technology matures. Other members thought self-declaration would be a distraction from developing and implementing the solutions to comply with remote ID and tracking requirements, with little benefit.

Also, to encourage early adoption of an ID and tracking rule the FAA could link remote ID and tracking to additional types of operational waivers, exemptions, and other FAA authorizations.

6.4.3. After final rule enacted

After the ID and tracking rule is enacted and standards are in place, all UAS manufactured and sold within the United States that are capable of meeting the threshold for compliance should be labeled if ID and tracking capable. The final rule will enable flight information to be shared through direct broadcast and/or network publishing technologies for Tier 1 and Tier 2 UAS operations.

Compliance with the final ID and tracking requirements is key to maximizing its value. As such, the

FAA should allow a reasonable grace period to carry out retrofit of UAS manufactured and sold within the United States before the final rule. The grace period should end when retrofit options are inexpensive and easy to implement.

6.5. Types of data related to direct broadcast and network publishing requirements for remote ID and tracking

The ARC recommends that the following types of data related to the UA or associated control station must be made available:

- **Unique identifier of the UA**, which should be specific to the UA, continuously available in near-real time, electronically and physically readable, tamper resistant, and easily accessible.
- **Tracking information for the UAS**, including aircraft position and control station location (or take-off location if ground control station location is not available).
- **Identifying information of the UAS owner and remote pilot** (not broadcast or published but available from the PII System).

The ARC also recommends that the following types of data related to the UA or associated control station be optional:

- **Mission type**, which characterizes the flight path of the UA.
- **Route data** – i.e., the pre-programmed navigation or flight plans.
- **Operating status** of the UA, which refers to operational information that may provide some insight into the current operations of the UA.

6.5.1. Unique identifier of the UA

The unique identifier should be: (a) specific to the UA; (b) continuously available in near-real time; (c) both electronically and physically readable; (d) tamper resistant; and (e) easily accessible.

a. Specific to the UA

The unique identifier should be assigned specifically to the UA itself (e.g., CTA standard) and become part of the UA's certificate of registration (if registration is required).¹⁸ Unique identifiers will allow public safety officials to identify the specific UA and, if more information is warranted, subsequently determine the owner. Unique identifiers also protect the privacy of the UAS owner or remote pilot because the unique identifier alone will not contain any PII, such as a name, date of birth, or address. The unique identifier should be broadcast and/or published for all UAS that meet the category threshold compliance. This is in addition to any physical incorporation of the unique identifier or 'license plate' on the aircraft itself.

¹⁸ The ARC recommends that the FAA reconcile the requirements for UAS ID and tracking with the requirements for UAS registration to ensure that information necessary to support the PII System is appropriately available.

b. Continuously available in near-real time

The unique identifier must be continuously (near-real time) available upon commencement to termination of flight. This can provide early notification that a UAS may soon be operating in the area. In cases of large public gatherings, restricted areas, or areas close to airports, this provides stakeholders responsible for public safety an indication that a UAS may become a hazard.

c. Electronically and physically readable

The unique identifier must also be available in both electronic and physical form. The electronic information should be in a standardized form that is easily accessible. The unique identifier must also be physically located on the unmanned aircraft. This will provide owners, remote pilots, and others with access to the unique identifier even when the UA is not powered on. The physical identifier could be an FAA-approved data plate, depending on size of the UA, and it must be affixed for the duration of operation.

d. Tamper resistant

The unique identifier should be assigned to the UA in a way that makes it tamper resistant.

e. Easily accessible

Finally, the unique identifier must be easy to access. This means the information made available regarding the unmanned aircraft and the control station must be receivable through devices, including portable devices that are readily available on the market at the time the ID requirement comes into effect. This also means that unique identifiers physically on the UA must be easily accessible on the aircraft (similar to the registration rule allowing marking of the aircraft inside of a compartment not requiring tools to access).

6.5.2. Tracking information for the UAS

Tracking information is a key piece to enable effective UAS integration into the NAS, as well as to assist with public safety. Tracking is required to support safe separation between aircraft. In manned aircraft, air traffic controllers have the ability to talk with the pilot in command in real time in order to discern their intent. However, there is currently no two-way communication in real time between UAS and ATC or other pilots. Whenever there is an issue or concern with a UAS, the process is to notify public safety officials to initiate actions to locate the UA as well as the remote pilot to enable discussion or intervention to terminate the flight.

Historical tracking information could be a helpful tool in assisting public safety officials. It may be the key to locating the remote pilot. If a UA has already landed and is no longer visible when public safety officials arrive on-scene following an incident, the last known flight track of the UA will provide these first responders with a geographic starting or termination point that will help locate the remote pilot. If the UA has crashed and public safety officials recover the aircraft without finding the remote pilot, they will be able to use the unique identifier located on the UA to identify the registrant and subsequently the remote pilot and would be able to use the tracking information to help determine the cause of the accident or incident.

In addition, tracking information provides definitive answers as to whether the UA entered unauthorized airspace or not. After the fact, historical tracking information could support potential enforcement actions.

Currently, the biggest challenge facing public safety officials when responding to matters regarding UAS activity is their inability to locate the operator of a UAS that is causing concern or risk to the safety of the public or the airspace system. The ARC recommends tracking information include both the position of the unmanned aircraft and the location of the control station, or take-off location if ground control station location is not available, which will often be the location of the remote pilot. Note that operator control station location is considered to be as important as UA location so that public safety officials can identify and speak with the remote pilot in a timely fashion if needed. Information about the position of the UA must include time stamp, altitude, and geographic coordinates. Information about both the position of the UA and the location of the control station, or take-off location if ground control station location is not available, must be available in near-real time from commencement to termination of the flight.

6.5.3. Identifying information of the UAS owner and remote pilot

In establishing a remote ID and tracking system, it is important to protect the privacy of UAS owners and operators. At the same time, given the risks associated with UAS operations, airspace management and public safety authorities must have the ability to identify owners and remote pilots when necessary. For that reason, the ARC recommends that each UA's unique identifier should be linked to limited forms of PII about the UA's owner and remote pilot. That information would include names, dates of birth, addresses, gender, and phone numbers. The ability to readily have PII available is necessary to ensure the public's safety and protect UAS owners from mistaken identity. In essence, having an appropriate amount of data included in the PII will help filter false positives.

Importantly, this information should be available only to authorized users for purposes of official business. The ARC expects that public safety and airspace management personnel would have access to the extent required to perform their functions. Due to the sensitivity of this information, the systems in which it is stored and accessed must be highly secure. The PII System will also need to incorporate authentication measures to ensure that the information is correct.

Identifying information is often of vital importance. In instances when a dangerous situation exists or is developing, contact with the remote pilot can help ensure the protection of the public and impede or defuse a potential catastrophic incident from occurring. For example, if a medical transport helicopter must land near a UA, first responders must have the ability to promptly identify and contact the UAS remote pilot. Likewise, in cases where UAS are operated in an unsafe manner, the ability to quickly determine the operator's motivation and intent and to identify potential witnesses to an incident becomes important for investigative purposes.

The ability to identify the remote pilot in command serves as an additional mechanism for public safety officials to determine if the remote pilot is authorized to operate in the area.

Identity of the owner and/or remote pilot is considered PII, so it is not a candidate for real-time transmission from the UA system. The ARC suggests that only authorized users be able to access this information. The presumption is that the UA unique identifier could be linked to the PII,

perhaps at the time of aircraft registration, and that the FAA will maintain this remote pilot/owner/operator PII database with appropriate security and access control.

6.5.4. Mission type (optional)

Unmanned aircraft are flown for numerous reasons, such as hobby, commercial, sport, security, etc. New uses are being devised daily. With each new use, there is a mission profile that characterizes the flight path of the UA. The UAS operator may wish to voluntarily share the mission type by loading it into the database that public officials could access during their response to an event. This information (along with route data, discussed below) would help public safety officials understand the nature of a UAS operation and assist in anticipating flight behavior. This would enable responders to determine if the UA was operating within the boundaries of this mission profile or not. For example, if a UA is used for pipeline inspection, first responders would expect to see a UA operating along a section of pipeline, and even hovering over a section of pipeline to provide a closer analysis. Mission type focuses more on the type of operation and may or may not include pre-planned navigation points. This information could be included with information in the tracking database, as part of a larger UAS management system and operational approval system (e.g. LAANC or UTM).

6.5.5. Route data (optional)

If possible, authorities would like access to pre-programmed navigation or flight plans. This voluntarily provided information could help with threat discrimination and emergency response. For example, if a UAS was determined to pose a safety hazard and the likely future flightpath or destination was known, authorities could properly position resources for interdiction, coordinate evacuations, or relocate other assets for protection or response.

6.5.6. Operating status (optional)

There is other operational information that may provide some insight into the current operations of the UA, such as battery level. Accessing such data will provide additional clues into understanding the intent of the UA. For example, if a UA flies through a restricted area, and the public official is able to query the UA on its status and determine the UA is in a return-to-home mode, the official can follow the UA to the return home location with the expectation of locating the operator. As this is a dynamic value (and in fact may be indicative of a failure condition in the UA system), this would be of value for transmitting in real time.

6.5.7. Table of data elements, time of data provision, and requirements

The table on the next page describes a potential scheme for data provision, including both the time of data provision and a scheme for which data elements may be required depending on the type of operation. The ARC notes that specific data elements to be provided by the UAS operator may vary depending on the nature of the operation or additional requirements expected by the Agency.

Table 5.

	Time of Data Provision		Type of UAS Operation			
	Real-time In-Flight Provision	Prior to Flight (e.g. via internet)	TIER 0	TIER 1	TIER 2	TIER 3
1. Unique UA Identifier	Yes	n/a	Optional	Required	Required	<i>See part 91</i>
2. UA and GCS Location and Time	Yes	n/a	Optional	Required	Required	<i>See part 91</i>
3. Operator PII	No	Yes	Optional	Required	Required	<i>See part 91</i>
4. Mission Type	Optional	Yes	Optional	Optional	Optional	<i>See part 91</i>
5. Route Data	Optional	Yes	Optional	Optional	Optional	<i>See part 91</i>
6. UA Status	Optional	n/a	Optional	Optional	Optional	<i>See part 91</i>

6.6. Key implementation considerations from ATC and for critical infrastructure and airports

6.6.1. Air Traffic Control

While the UAS-ID ARC was convened primarily to address the needs of public safety officials, the ARC charter recognizes that ATC may play a role in the public safety and national security activities that the ARC addresses. This section describes how this may occur and makes recommendations for how ATC should interoperate and maximize the benefits of ID and tracking equipage.

FAA's ground rules for UAS operations Beyond Visual Line of Sight are that these operations must comply with remote ID and tracking requirements as recommended by the ARC. In addition, FAA has also indicated that UAS operating under Instrument Flight Rules (IFR) on IFR flight plans must comply with the requirements of 14 CFR part 91, including avionics equipage requirements.

The ARC recommends that the FAA identify whether BVLOS operations will routinely occur (i.e. without a waiver) *without* an IFR flight plan, and if so, under what operational conditions (e.g. airspace, altitudes, speeds, etc.)

Furthermore, the FAA has indicated that any solution for ID and tracking should avoid causing congestion or interference on the FAA's Secondary Surveillance Radar (SSR), Airborne Collision Avoidance Systems (ACAS, including TCAS I/II), and Automatic Dependent Surveillance – Broadcast (ADS-B) systems. Specifically, these include airborne transponders transmitting on 1090 MHz, and ADS-B systems transmitting on 1090 MHz and 978 MHz. The concern for congestion on the 1090 MHz frequency is particularly acute, as existing studies suggest that this frequency is nearing capacity limits in certain high density airspace areas (e.g. Los Angeles Basin). The ARC recommends that any proposal for using ADS-B frequencies in the solution for UAS ID and tracking must be analyzed for the impact on the performance of current and future SSR, ACAS, and ADS-B.

6.6.1.1. Airspace Considerations

To facilitate integration with ATC surveillance, UAS operating in Class D airspace and below 2500' AGL in Class E and Class G airspace should comply with the ID and tracking requirements recommended by the ARC (other than those operations identified by the ARC as being below the threshold for compliance.). For UAS operating in Class A, B, or C airspace, and at or above 2500' AGL in Class E and Class G airspace, and if analysis shows that it is appropriate, UAS could be equipped with ADS-B Out capabilities meeting appropriate requirements, so as to facilitate integration with ATC surveillance.

6.6.1.2. Operational Considerations

ATC operations at low altitudes in the vicinity of major airports are often complex and of high intensity. As a result, ATC does not have the capability to monitor or manage all UAS operations, especially smaller UAS operating at low altitudes. In addition, if the volume of UAS operations increases as envisioned by the industry, displaying UAS operations which are not under ATC control would cause significant clutter, which would be distracting to ATC. Therefore, UAS that are not

operating in a mixed environment with manned aviation should not generally be displayed on ATC automation (e.g., D-BRITE, STARS/ARTS, etc.).

However, there is a need for ATC to be aware of any UAS that blunders or otherwise enters airspace of interest to ATC operations, to ensure ATC is able to provide aircraft separation for safety, especially along the approach and departure flight paths near airports. Finally, in the case where public safety official operations may require assistance from ATC, it may be helpful for specifically identified (“designated”) UAS to be displayed.

The ARC recommends the following:

- The UAS ID and tracking system should interoperate with the ATC automation, such that target information from the ID and tracking ground system, including ID and position, can be passed to ATC automation.
 - FAA automation should be able to accept target information from the UAS ID and tracking ground system.
 - The end-to-end latency from UA position report to ATC automation should ideally be low enough to be of use in the tactical ATC environment.
- FAA automation should by default filter out UAS ID and tracking system targets from the ATC display that fall outside of adapted airspace deemed to be of interest to ATC (i.e., away from typical manned aviation flight paths).
 - FAA automation should be able to alert ATC personnel (e.g. Certified Professional Controller or Front-Line Manager) when an unexpected UAS enters airspace of interest to ATC operations.
 - FAA should define standard criteria for identifying airspace that should be adapted as being of interest to ATC operations in this context, and ensure that the UAS ID and tracking ground system has coverage in these areas.
- FAA automation and the UAS ID and tracking system should be able to display designated UAS targets of interest (e.g. by a public safety official, in the UAS ID and tracking system) to ATC personnel.

6.6.2. Airports and Critical Infrastructure

The various proposed technologies would impact critical infrastructure facilities in different ways. Critical infrastructure encompasses the “assets, systems, and networks... so vital to the US that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.”¹⁹ This includes airports and heliports, energy infrastructure, and many other facilities that are part of the national security enterprise, and therefore would benefit from the implementation of UAS ID and tracking. For example, critical infrastructure could require installation of equipment to receive electronic broadcasts or employing networked software-based solutions. Additionally, security and response strategies for facilities may need to be updated. New procedures may include interfacing with public safety officials for UAS threat mitigation. For example, facility managers may need to remotely identify the UAS “license

¹⁹ <https://www.dhs.gov/what-critical-infrastructure>.

plate” and contact public safety officials that have access to the information necessary to inform an appropriate response.

The ARC recommends FAA do the following:

- Incorporate implementation costs of critical infrastructure facilities into rulemaking analysis, including physical (e.g., radio receivers) and digital (e.g., networked software solutions) infrastructure, and any financial burdens associated with planning and capability requirements for critical infrastructure facilities to implement UAS ID and tracking systems and security procedures.
- Identify an approach and timeline to designating approved technologies for airports and critical infrastructure facilities, and address any legal barriers to implementing approved technologies. If a period of optional equipage is defined, the requested approach and timeline should support testing and deployment of systems at facilities during this phase.
- Provide guidance to airports on any impact or interference to safe airport operations, including how UAS ID and tracking may impact definition of UAS Facility Maps, security procedures, and risk assessments of UAS operations.

7. OTHER RECOMMENDATIONS AND CONSIDERATIONS

The ARC’s efforts have focused on the core mission of developing recommendations concerning UAS ID and tracking technologies that meet the needs of public safety officials in timely and cost-effective ways. In the process of this effort, the ARC has identified a number of related issues that also impact implementation of effective UAS ID and tracking solutions. Accordingly, the ARC has identified those issues in this section, and urges the FAA to devote future time and consideration to them as the Agency moves forward with its rulemaking and policy deliberations and actions.

7.1. Access to data related to direct broadcast and network publishing requirements for remote ID and tracking

Access to information made available by the unmanned aircraft and control station should be in accordance with the role and responsibility of the individual(s) seeking the information. The ARC therefore recommends at least three levels of access to the information that is either broadcast or captured and contained in the appropriate database. Those levels of access are: (1) information available to the public; (2) information available to designated public safety and airspace management officials; and (3) information available to the FAA and certain identified Federal, State, and local agencies.

7.1.1. Public access

Certain information should be available to the public at large. Specifically, the ARC recommends that the UA unique identifier should be available to the public. In making this determination, the ARC assumes that the method by which the unique identifier is made available is readily accessible and available to the public at minimal to no cost.

Public access is invaluable. Similar to a license plate on a vehicle, the public-facing unique identifier provides a means for the public, as well as public safety officials, to identify a specific UAS. Such a

system would provide a means by which individuals can report UAS that are operating in a suspicious, dangerous, or unauthorized manner. It would also help to protect UAS owners and remote pilots by reducing the likelihood that compliant operations could be mistaken for non-compliant activities.

If the identifier is composed of alphanumeric characters without visible PII, it can be made public while protecting the privacy of the registrant.

7.1.2. Designated public safety and airspace management officials access

The ARC recommends that access to PII should be limited to public safety officials and similarly regulated public safety entities, including airspace management officials. While the ARC does not specify a method by which this data must be made available, it could be retained in a central database, much like other forms of records accessible to public safety official personnel, and accessed upon appropriate need in a particular case.

Additionally, the ARC believes these categories of authorities also require access to real-time tracking information, at least in the vicinity of their respective area of operations. This information will enhance the ability of public safety authorities to respond to incidents and mitigate risks to safety and security.

7.1.3. Federal, State, and local agency and FAA access

The ARC assumes that FAA will maintain the PII System and permit access to authorized users only for official purposes. For example, the data should be available to other Federal, State, and local agencies, and, after appropriate vetting, other designated personnel who may require access. Agencies may include, but are not necessarily limited to, the National Transportation Safety Board; Federal security agencies; and State, local and tribal law enforcement agencies.

7.1.4. Data authentication and retention

The ARC recommends that all relevant tracking data should be retained for a reasonable period of time to allow public safety officials and other authorized users to have access to information critical to investigations.

The ARC suggests that the FAA review existing manned aircraft data retention standards for guidance, while bearing in mind the unique nature of UAS.

7.1.5. Privacy considerations

The ARC recommends that the United States government be the sole keeper of any PII collected or submitted in connection with new UAS ID and tracking requirements. This recommendation is similar to the ones made by the UAS Registration Task Force ARC in 2015 when recommending a new registration rule for UAS.

Additionally, historical tracking information for UAS, although not necessarily falling within certain definitions of PII, raises serious pilot privacy concerns that must also be addressed through various legal, technical and procedural protections. Owners and operators have legitimate reasons to keep the locations, dates, and times of their UAS flights private even if that data is not directly associated with PII in the same database. Tracking information for UAS indicates very precisely the location of

a specific person or company operating the UAS for a specific personal or business purpose. Aggregate historical tracking information can reveal patterns that compromise business confidentiality or personal privacy. It could indicate that a certain farmer's field is of particular economic interest, for example. Many people use small UAS for personal and private purposes, such as family photography. Because UAS ID and tracking will be a regulatory mandate, rather than a consumer option, and because the ARC has recommended a threshold that captures a broad range of UAS aircraft and operations, this privacy concern is heightened compared to location-enabled technologies in the marketplace that are used voluntarily.

These concerns require the FAA, in consultation with privacy experts and other agencies, to consider whether and how historical tracking information is recorded or maintained in a regional or central database and whether any non-governmental third party should generate, maintain, or have access to any repository of UAS historical tracking information, as well as any safeguards that might be put into place to mitigate these privacy concerns.

Some ARC members note that full treatment of the issue of privacy (including data protection) was not attempted during this ARC. These members believe that the ARC also lacks sufficient time to perform an exhaustive analysis of all the privacy implications of remote ID, tracking, or UTM, and did not specifically engage with privacy experts, from industry or otherwise, during this ARC. These members agree, however, that it is fundamentally important that privacy be fully considered and that appropriate privacy protections are in place before data collection and sharing by any party (either through remote ID and/or UTM) is required for operations. A non-exhaustive list of important privacy considerations include, amongst other issues, any data collection, retention, sharing, use and access. Privacy must be considered with regard to both PII and historical tracking information. The privacy of all individuals (including operators and customers) should be addressed, and privacy should be a consideration during the rulemaking for remote ID and tracking.

7.1.6. Governmental UAS operations

Finally, the ARC recommends the remote ID and tracking system include reasonable accommodations to protect the operational security of certain governmental UAS operations, consistent with accommodations provided to governmental operations in the manned space. For operational security purposes, some UA may have their unique identifier masked. Special procedures need to be defined to support these limited types of operations.

7.2. Interoperability with current & future systems/programs

The ARC also notes that the ID and tracking proposals can complement NASA's development of a small UTM system and the FAA's LAANC system. However, the integration or overlapping elements of the ID and tracking systems with those programs was not within the time or resources of the ARC to explore. As such, the ARC encourages the Agency to leverage those initiatives as they develop the remote ID and tracking system. This is an area where industry support and advice is crucial.

Finally, as we collectively seek to take advantage of the safety benefits of UAS and grow the commercial UAS industry exponentially, compliance is critical for the viability of successful UTM systems. UTM systems in development now will open the airspace in a safe, secure, and responsible way. The more vehicles participating in these UTM systems with UAS ID and tracking, the more successful these efforts will be.

7.3. First Amendment

The ARC recognizes that the use of UAS for news-gathering and other purposes can implicate First Amendment rights and considerations. Although the legal questions associated with these issues was viewed as outside the scope of the assigned work, we encourage the FAA to ensure its final rule is content-neutral and narrowly focused on regulating aviation safety.

7.4. Education

The proposal assumes that a strong cooperative effort will be made by interested stakeholders to educate the UAS industry at large (including operators, users, manufacturers, and others), hobbyists, public safety officials, public agencies, and the public about the final rule, how to comply, and what is expected. Using a mix of traditional and new media, the ARC urges the FAA to partner with industry to communicate its final rule to operators, public safety officials, and the public.

7.5. Pending Federal legislation

The U.S. Congress is considering the FAA Reauthorization Act and other legislation which could impact the work of the UAS-ID ARC as well as the larger regulatory questions on low altitude air traffic management. Although neither potential integration nor overlapping elements of the ID and tracking systems with elements of pending legislation were within the mandate, time, or resources of the ARC to address, we nevertheless encourage government to make resources available for the UAS remote ID and tracking system.

7.6. Pending State/local legislation

Many states and localities are introducing (and passing) legislation which could impact FAA's rule on remote ID and tracking or related topics like registration and enforcement. In such respects, it is noted that the Drone Advisory Committee TG1 is addressing basic issues on the roles of Federal, State, and local authorities that might provide a helpful framework for any similar issues arising with respect to UAS remote ID and tracking.

7.7. Global harmonization

International entities like ICAO can provide important venues for addressing global solutions and standards for UAS. In addition, a number of countries around the world are considering approaches to ID and tracking. We encourage the Agency to adopt remote ID and tracking requirements that promote international standardization.

7.8. Children and minors

The UAS-ID ARC notes that there are laws and requirements that relate to the protection of children and to their registration and use of UAS. Nothing in this report or the ARC's recommendations is intended to propose changes in any of those laws or rules. The ARC urges the FAA to ensure that its future actions ensure the safety, privacy, and protection of children and minors.

7.9. Effect on other laws

The ARC's recommendations assume that UAS operators will separately ensure compliance with evolving applicable Federal, State, and local applicable laws and regulations. As noted above, there are Congressional, State, and local legislative initiatives that could lead to future changes in law.

7.10. Trusted Operator System

To enhance the effectiveness of any comprehensive remote UAS ID and tracking rule beyond a minimum threshold for compliance, the FAA could consider working with security agencies to establish a "Trusted Operator System." Given the strong public benefit of commercial UAS use, it is important to streamline these operations and allow authorized commercial operators to proactively gain the trust of public officials and the general public in order to unleash the enormous potential of the commercial UAS market.

8. CONCLUSION

The stated objectives of the ARC charter were: to identify, categorize and recommend available and emerging technology for the remote identification and tracking of UAS; to identify the requirements for meeting the security and public safety needs of the law enforcement, homeland defense, and national security communities for the remote identification and tracking of UAS; and to evaluate the feasibility and affordability of available technical solutions, and determine how well those technologies address the needs of the law enforcement and air traffic control communities.

The deliberations of the ARC reflected the vast experience of its members, and the final recommendations were agreed upon in a spirit of cooperation and compromise. The focus of the group remained steadfastly on reaching a general consensus and to provide the FAA with a workable solution that meets its safety, security, and policy requirements. The members of the ARC appreciate the opportunity to work closely with the FAA on this endeavor, and remain committed to providing future solutions that will ensure the safe and efficient integration of UAS into the national airspace as well as the protection of our citizens.

9. APPENDICES

Appendix A ARC Membership List

Appendix B Working Group 1 Report

Appendix C Working Group 2 Report

Appendix D Responses and Voting Results

Appendix A ARC Membership List

1. A3 & Aerial by Airbus
2. Academy of Model Aeronautics (AMA)
3. Aerospace Industries Association (AIA)
4. Air Line Pilots Association (ALPA)
5. Airborne Law Enforcement Association (ALEA)
6. Aircraft Owners and Pilots Association (AOPA)
7. AirMap
8. Airspace Systems, Inc.
9. Amazon Prime Air
10. American Association of Airport Executives (AAAE)
11. American Petroleum Institute (API)
12. Analytical Graphics, Inc. (AGI)
13. Ariascend/DUGN
14. Association of Unmanned Vehicle Systems International (AUVSI)
15. ASSURE
16. ASTM International
17. AT&T
18. BNSF Railway
19. California Highway Patrol, Office of Air Operations
20. College Park (MD) Airport
21. Commercial Drone Alliance
22. Consumer Technology Association (CTA)
23. CTIA/Akin Gump
24. DJI Technology
25. DLA Piper
26. Drone Aviator, Inc.
27. Dronsystems Limited
28. Fairfax County Police Department
29. Farris Technology
30. Flight Safety Foundation
31. FlyTransparent/Black River Systems Company
32. Ford Motor Company
33. GE Aviation
34. General Atomics
35. General Aviation Manufacturers Association (GAMA)
36. Globalstar
37. Grand Forks Sheriff's Office
38. Hangar51
39. Helicopter Association International (HAI)
40. Insitu, Inc.
41. Institute of Electrical and Electronics Engineers (IEEE)

- 42. Intel
- 43. International Association of Chiefs of Police (IACP)
- 44. Just Innovation
- 45. Los Angeles World Airports
- 46. Metropolitan Police Department (DC)
- 47. Miami Beach Police Department
- 48. Miami-Dade International Airport
- 49. Montgomery County Police Department
- 50. National Agricultural Aviation Association (NAAA)
- 51. National Association of State Aviation Officials (NASAO)
- 52. National Council on Public Safety
- 53. National Governors Association
- 54. New York Police Department (NYPD)
- 55. News Media Coalition
- 56. Northrop Grumman
- 57. PrecisionHawk
- 58. Professional Helicopter Pilots Association
- 59. Qualcomm
- 60. RelmaTech
- 61. Rockwell Collins
- 62. RTCA
- 63. SAE International
- 64. SkyPod, USA
- 65. Skyward, A Verizon Company
- 66. Texas Department of Public Safety, Aircraft Operations Division
- 67. The Brookings Institute
- 68. The MITRE Corporation
- 69. The Police Foundation
- 70. The Toy Association, Inc.
- 71. T-Mobile USA
- 72. uAvionix
- 73. Verizon
- 74. X

Appendix B Working Group 1 Report

Analysis of Technology Alternatives

UAS ID and Tracking Aviation Rule-Making Committee Working Group 1

28 August 2017

1. Background

The FAA chartered the Unmanned Aircraft Systems (UAS) Identification and Tracking Aviation Rulemaking Committee (UAS-ID) Aviation Rulemaking Committee (ARC) to provide recommendations to the FAA regarding technologies available for the remote identification and tracking of UAS. The ARC consisted of three working groups. Working Group 1 (WG1) was tasked with identifying, categorizing and recommending available and emerging technologies for the remote identification and tracking of UAS. WG1 considered technologies for near term retrofitting of UAS to comply with the identification and tracking requirement, as well as appropriate technologies for integration into UAS over the longer term.

WG1 used data needs identified from Working Group 2 (WG2) as guidance in determining how well various technology alternatives may satisfy the “requirements” for Identification (ID) and Tracking including (a) the unique identifier of the UA, (b) the position of the UA, and (c) the location of the ground control station (if possible).

There are a wide variety of potential operating environments for an ID and Tracking solution. The UAS may be operating along the following dimensions:

- Remote Areas ⇔ Urban
- Outside of Network Coverage ⇔ Overlapping Network Coverage
- Areas with Minimal Buildings and Obstructions ⇔ Urban canyons
- Little Spectrum Usage ⇔ Heavy Spectrum Congestion

Differing technology alternatives may be most appropriate for varying environments. This analysis does not yet address the operating environment nor the appropriateness for various classes of UAS.

2. Definitions

For purposes of this activity, we are working under the following definitions:

- “Compliance Burden” refers to the impact on the owner/operator to comply with the ID and tracking regulation. This includes purchasing the technology, installation, configuration, network provision, reduction in range/ flight duration due to added weight and/or power consumption, establishment and maintenance of subscription, recurring cost, operational tasks specific to individual flights (e.g., charge separate batteries or submit a flight plan), etc.
- “Configuration” is the process by which the owner/operator sets up a device to communicate the appropriate unique ID.

- “Federated Approach” is a framework that allows for interoperability and information sharing among systems from different vendors to deliver a common, seamless service to users.
- “Identity” refers to a data set that can be traced to a unique UAS, its owner and/or operator.
- “Interoperability” is the ability of systems to exchange and make use of information.
- “Original Equipment” refers to solutions that are integrated into the UAS by the OEM at the time of manufacture.
- “Owner/Operator” refers to the person or organization who is responsible for ensuring compliance with the ID and tracking regulation.
- “Provision” is the process of enabling a communications device to participate in a network service.
- “Remote Identification” means discerning identity from a distance.
- “Registration” is the process by which the owner/operator associates himself/herself (including contact information and other PII) and aircraft (e.g., make, model, modifications) with an assigned, unique identifier.
- “Retrofit” is the installation of an ID and tracking solution on an existing UAS. This may include items physically attached to the airframe, connected to the existing subsystems, or software updates.
- “Technical Readiness Level (TRL)” is defined by NASA/DoD as a method of estimating technology maturity of critical technical elements.
- “Technology Alternative” is defined as a broad, non-industry member specific category proposed solution for UAS ID and tracking.
- “Tracking” is the process of following the location of UAS components over time.
- “Unmanned aircraft system (UAS)” means an unmanned aircraft and its associated elements (including communication links and the components that control the UA) that are required for the safe and efficient operation of the small unmanned aircraft in the national airspace system.

3. Technology Alternatives

In early spring, AUVSI solicited ideas from industry on ID and Tracking solutions. A total of 53 white papers proposals were received. At the request of the FAA, MITRE-CAASD analyzed these ideas and presented their findings (without revealing proprietary information) to WG1. WG1 also received briefings on various specific ideas from working group members. Using this information, the working group, complied a set of eight technology alternatives that enveloped all of the ideas submitted. WG1 analyzed the eight technology alternatives against a set of criteria. More detailed descriptions and discussions against the criteria are being developed.

The eight technology alternatives are as follows:

- **Automatic Dependent Surveillance Broadcast (ADS-B):** Two alternatives are discussed related to a rule-compliant version (i.e., adheres to current ADS-B rules/standards) and a lower-power alternative that leverages the message, protocols, and frequency but uses a significantly lower transmit power to address concerns about potentially overwhelming existing ADS-B services.
- **Low-Power Direct RF:** Includes a variety of RF based protocols leveraging unlicensed spectrum to include Bluetooth, Wi-Fi, RFID, and others.

- **Networked Cellular:** Will leverage the existing cellular network to collect ID and tracking information.
- **Satellite:** Leverages existing satellite tracking services.
- **SW-based Flight Notification w/ Telemetry:** Leverages existing and developing UAS services that enable UAS operators to exchange operational information during flight. Depends upon a network connected device coupled with a ground control station that many small UAS operators use today.
- **Unlicensed Integrated C2:** Modulates ID and Tracking packets on existing C2 communication channels.
- **Physical Indicator:** Consist of unique and/or categorical physical markings (e.g., etched numbers, streamers) that will need to be visually observed. Some concepts do not provide remote identification.
- **Visual Light Encoding:** Leverages software controlled LEDs to digitally encode information that can be decoded by a device connected to a visual sensor.

Fundamentally, the eight technology alternatives fall into two broad categories: 1) *direct broadcast solutions* (e.g., ADS-B, Low-Power Direct RF, Unlicensed Integrated C2, and Visual Light Encoding) and 2) *network solutions* (e.g., Networked Cellular, Satellite, and SW-based Flight Notification w/ Telemetry). For *network solutions*, there will be the need for some sort of technology which collects and distributes the ID and tracking data. This may be in the form of a single server/database or a federated database on distributed servers. It is envisioned that consumers of the ID and tracking data (e.g., public safety officials) will have integrated access. *Direct broadcast solutions* are likely to have lower end-end latency between transmission from the UA to display on to a public safety official's device than *network solutions*.

The assumption was made that the FAA would be responsible for maintaining the database which correlates unique electronic ID with owner/operator contact information and other PII. The FAA would be responsible for the procedural and technical access controls to such data and thus was not considered as a comparison point in characterizing the technology alternatives.

4. The Five Criteria

WG1 developed a set of criteria to be used in analyzing technology alternatives. The criteria were developed based upon the working groups expertise and understanding of the desired requirements as communicated by WG2. There was not full consensus on the criteria. Where full consensus did not exist, text is noted with an icon (●) and an alternative view is shared.

a) Ease of Compliance for Owner/Operator ●

An analysis of how easy it will be for the owner/operator to comply. Will the burden (i.e., the detrimental impacts and seamless nature of the process) be minimal? This criterion is analyzed for both retrofits (i.e., installation of an ID and tracking solution on an existing UAS) and for original equipment (i.e., solutions that are integrated into the UAS by the OEM at the time of manufacture), and includes time and effort to install or configure, and size, weight and power (SWaP) impacts to the UAS.

- Many in the working group believe that broad compliance is critically important for an ID and Tracking solution to have value. The assumption is that most owner/operators want to be compliant. The likelihood that they will comply depends upon the relative ease of complying and the perceived costs of complying. Some believe that a more appropriate criterion would have been the “Likelihood of Compliance” which would include the “Ease of Compliance” along with the “Willingness to Comply”. The “Willingness to Comply” is likely impacted by costs that include the following:

Material – Financial cost of equipment or services

Operational – Reduced utility of the UAS (e.g., reduced flight duration or range)

Disclosure of Operationally Sensitive Information – Many owner/operators may have a perceived cost associated with the loss of control of information associated with their flight operations. Even without disclosure of PII, the widespread availability of operational sensitive information could have an impact on an owner/operator’s perceived privacy and our commercial interests. The holding of such information by a third party may be especially concerning to some owner/operators. If broad operational data is available, it may be archived and mined for information that would be detrimental to the owner/operator. Even if access is limited to just public safety enforcement or a few third parties, the perception may be detrimental to the willingness to comply.

Criteria Scale

For Retrofits

High: Involves no to minimal time and effort to install and configuration initially and the weight penalty is less than 10g.

Medium: A separate piece of hardware needs to be installed and configured. The HW would require either integration into aircraft system power or have its own batteries which would require separate recharging. Weight is less than 250g.

Low: Requires either installation that involves physical connections to existing sub-systems, a weight of >250g, or specific operational tasks required for each flight (e.g., participate in a flight notification program).

For Original Equipment

High: Installed by OEM upon purchase and requires minimal additional tasks by the owner/operator to comply with the ID & Tracking regulation other than those associated with registration and minimal configuration (<10 mins).

Medium: Requires complex configuration tasks by the owner/operator upon setup (>10 mins).

Low: Requires specific operational tasks for each flight (e.g., submit flight plan).

Critical Considerations

Requires A 3rd Party (Yes/No): Does establishment of the ID and tracking capabilities require involvement of an intermediary to either provide communications services or otherwise facilitate the delivery of information? ●

- There were some working group members who felt that the establishment of a 3rd party relationship will have a significant impact on both the ease and willingness to comply. Concern was raised that tasks and costs associated with new subscription services would lower the ease of compliance. Depending upon specific business models that emerge there may be little to no specific tasks for the owner/operator to complete.

b) Readiness for Implementation

This criterion helps to evaluate how the technology alternative is for implementation for remote UAS ID and tracking of UAS. This criterion is scored (Yes/No) based on the availability in less than one year for existing UAS, the time for public safety enforcement availability, and if the technology requires significant changes in FAA/FCC policies, integration capability into new OEM products, and the required infrastructure and data management capabilities. NASA/DoD Technology Readiness Levels¹, a commonly used measure of technology maturity, were originally used to inform the rating, but the data allowed for simplification based on industry input.

Critical Considerations

Retrofit/Integrated < 1 yr: In less than a year, products will be available for owner/operators to retrofit, products will be available for the public safety enforcement community, no significant changes in FAA/FCC policies specific to use of this technology are needed, new OEM products will have integrated solutions, and all required infrastructure and data management capabilities will be established.

c) Operational Performance/Security and d) Interoperability

This criterion helps analyze how well the technology is expected to perform in an operational setting. There are several critical considerations.

Performance Against Requirements

Meets Criteria for Direct Broadcast or Networked Database (yes/no) – Each alternative has a **Primary** method of operation that maps into one of the two basic requirements of WG2: 1-Direct Broadcast or 2-Networked Database. Although some solutions could have secondary means of meeting a second requirement, the Primary method is identified and it is noted how the secondary requirements could be achieved, if applicable.

Update Rate ≥ 1Hz (yes/no) – Can provide "transmit to public safety officer display" update of telemetry at least once per second.

Latency <3.5 s (yes/no) – Can provide "transmit to public safety officer display" update of telemetry within 3.5s. Network solutions require "right-sized" server capacity and bandwidth. Direct broadcast solutions are likely to have < 1s latency.

Range: Effective range of the solution. Four broad categories are considered:

- **Radio Range:** Solution works to the radio transmission range of the equipment involved. Varies by power, propagation effects, and communications environment.
- **Network Range:** Communicates if the unmanned aircraft and/or GCS are in an area served by the network.

¹ A commonly used scale that ranks technology maturity from basic research (1) to an operational system (9).

- **Satellite Range:** Communicates if the unmanned aircraft and/or GCS are in an area served by the satellite.
- **Visual Range:** Individual/Receiver must be able to see the unmanned aircraft.
- **Licensed Spectrum (yes/no)** – Spectrum that is likely free from interference from other applications implying a higher quality of service. ●

● There was not full consensus on the operational performance value of technology alternatives that may or may not use licensed spectrum. The discussion revolved around the question of reliability of the RF communications link that would be used to broadcast ID and tracking data to a ground receiver or a server via the network. Today, many small UAS operate under Part 107 using unlicensed spectrum for C2 and there have not been reports of significant issues. There is a concern that in certain areas of high density usage by both UAS operators and other spectrum users, that the reliability of the unlicensed spectrum may be diminished and that there would be performance advantages of using licensed spectrum for ID and Tracking purposes.

Some key points:

1. There is a claim that use of unlicensed spectrum for UAS communications is reliable for the visual line of sight operations (i.e., Part 107 operations) being conducted today.
2. All radio technologies could be impacted by uncontrolled interference and therefore regulatory protection of spectrum is a consideration. In contrast with licensed spectrum rights, devices or systems operating on an unlicensed basis have no regulatory protection against interference from users in the band and therefore there is no assurance of link performance. Ref: FCC 47 C.F.R. § 15.5
3. The level of RF link reliability in the unlicensed spectrum may be impacted when considering levels of interference in populated environments where there is a high density of Wi-Fi networks and other unlicensed spectrum users near the ground based receiver attempting to capture UAS transmitted data.
4. Technology standards are evolving to improve coexistence amongst users of unlicensed spectrum through protocols such as LBT (listen before talk) which mitigates interference impact.
5. The level of impact due to interference will vary and needs to be assessed against the performance requirements for ID and tracking. Interference to an RF communications link manifests in range reduction, lost or delayed data, etc.
6. The operational function of ID and Tracking may be tolerant of a communications environment where messages are occasionally dropped or delayed.

Security

Spoofing Security (yes/no) – A mechanism is in place that would make it more difficult for mischievous/malicious electronic intervention.

Tamper Proof (yes/no) – A mechanism is in place that would make it more difficult for mischievous/malicious physical intervention.

Tracking Verification (yes/no) – A mechanism is in place that could independently correlate location information received in the ID and tracking messages.

Interoperability

This criterion identifies if the technology alternative would enable interoperability, including serving as a data source for Air Traffic or being able to be Federated as a potential source of information for a low-altitude traffic management capability (e.g., UTM).

- **ATC (yes/no):** Could serve as a data source for ATC without significant changes to ATC infrastructure.
- **International (yes/no):** Compatible with solutions that may be employed internationally.
- **Federated (yes/no):** Does the capability support a federated approach where multiple vendors can provide the same service in a manner that is seamless to owner/operators and the public safety enforcement community. Can the solution leverage a data exchange created for LAANC, SWIM, or other low-altitude traffic management capability?

e) Costs

This criterion focuses on the initial and reoccurring costs of the Primary solution of each alternative for the owner/operator, public safety enforcement, and OEMs and/or 3rd parties. The costs are grouped into three categories: Transmitter, Receiver and Development Costs². Individual components are broken out and the bearer(s) of each cost is identified. As there are many factors in the determination of actual amounts, **\$s are used to show relative costs within a row and are not keyed to any dollar figure.** The relative scale used here is from \$ to \$\$\$\$, with each \$ roughly reflecting a doubling (e.g. \$\$ is relatively 2x the cost of \$).

Critical Considerations

- **Transmitter HW** – This represents the cost of hardware to add the transmission capability for the solution. This cost is assumed to be borne by the owner of the UA, the purchaser. This is a per unit cost.
- **Transmitter Data** – For some solutions there may be a cost associated with the transmission of data from the UA. The burden of this cost can be applied to either the OEM or the owner as it may be bundled entirely in the cost of the UA or may be a separate cost. This cost may be one-time or reoccurring. This is a per unit cost.
- **Receiver HW (Non-Internet Device)** – This represents the cost of a receiver that is not a smartphone or other Internet connected device.
- **Receiver Internet Device** – This represents whether an internet device, like a smartphone, is required to be the receiver. Given that only 30% of patrol officers currently have department-issued smartphones³, **Required** indicates that it is required to complete the solution. **Optional** indicates that it can add value to the solution, like the ability to query a database, but is not required to complete the solution.
- **Receiver Internet Data** – This represents whether an Internet Device data plan is required to complete the receiver solution. Optional indicates that it can add value to the solution, like the ability to query a database, but is not required to complete the solution.

² Does not include the cost to setup, maintain, and provide access control for the database which connects owner contact information and other PII with the unique ID.

³ https://www.washingtonpost.com/news/true-crime/wp/2017/08/02/firstnet-broadband-network-to-enable-police-and-fire-responders-to-talk-to-each-other-ready-to-launch/?utm_term=.bd12dfcbe3c6

Note: Regardless of Receiver solution, for public safety officers in the field to directly retrieve owner contact information and other PII, a device connected to the network (e.g., handheld smartphone, laptop in patrol car) will be required⁴.

- **Development Costs** – This is a relative guide to include all costs (per unit, non-recurring HW+SW engineering [NRE], certifications, distribution, etc.) for all pieces necessary for an OEM and 3rd parties, collectively, to complete the solution (transmitters and receivers).

5. Characterization of the Eight Technology Alternatives

The eight technology alternatives were characterized using the five criteria. A summary of that characterization can be found in Table 1. More details associated with each of the characterization of each technology alternative can be found in the Appendix.

⁴ A radio call to a dispatcher may be sufficient.

Table 1. Summary Characterization of the Eight Technology Alternatives

Technology Alternatives: Summary		ADS-B	Low Power Direct RF	Networked Cellular	Satellite	SW-Based Flight Notification w/ Telemetry	Unlicensed Integrated C2	Physical Indicator	Visual Light Encoding
Summary Information	Primary Requirement Met	Direct Broadcast	Direct Broadcast	Networked	Networked	Networked	Direct Broadcast	Direct Broadcast	Direct Broadcast
	Retrofit Transmitter	External device attached to UA	External device attached to UA	External device attached to UA	External device attached to UA	Manual flight planning	Integrated with C2 (may not be possible for all UA)	Physical	Integrated w/lights (may not be possible for all UA)
	Integrated Transmitter	Integrated	Integrated	Integrated	Integrated	Integrated Flight Planning	Integrated with C2	Physical	Integrated
	Mobile Receiver	Device that can decode ADS-B	Device that speaks same transport as transmitter, e.g. Bluetooth	Connected Internet Device	Connected Internet Device	Connected Internet Device	Device that can decode special channel in C2 link	Eyes	Smartphone Camera

Technology Alternatives: Ease of Compliance and Technology Readiness		ADS-B	Low Power Direct RF	Networked Cellular	Satellite	SW-Based Flight Notification w/ Telemetry	Unlicensed Integrated C2	Physical Indicator	Visual Light Encoding
Ease of Compliance for Owner / Operator	Retrofit	Medium	Medium	Medium	Medium	High, if GCS sends telemetry via Internet connected device	High, if device capable	Low - High (varies)	High, if device capable

	Integrated	High	High	Med-High	Med-High	High (same caveat as Retrofit)	High	High	High
	Requires 3rd Party	No	No	Yes	Yes	Yes	No	No	No
Readiness for Implementation	Retrofit in < 1yr	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
	Integrated in < 1yr	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No

Technology Alternatives: Operational Performance, Security and Interoperability	ADS-B	Low Power Direct RF	Networked Cellular	Satellite	SW-Based Flight Notification w/ Telemetry	Unlicensed Integrated C2	Physical Indicator	Visual Light Encoding
Performance Against Requirements	1 - Direct Broadcast	Yes	Yes	No	No	No	Yes	Yes
	2 - Networked Database	No	No	Yes	Yes	Yes	No	No
	Notes	Could be networked from receiver	Could be networked from receiver		Network only needed for receiver	Telemetry requires Internet connected GCS	Could be networked from receiver	Could be networked from receiver
	Update Rate $\geq 1\text{Hz}$	Yes	Yes	Yes	No	Yes	Yes	N/A
	Latency $<3.5\text{s}$	Yes	Yes	Yes	Yes	Yes	N/A	Yes
	Range	Radio Range	Radio Range	Network Range	Network Range	Network Range	Radio Range	Visual Range
	Licensed Spectrum	Yes	No	Yes	Yes	Varies by HW	No	N/A

Security	Spoofing Security	No	Solution dependent	Yes	Yes	No	Yes	No	No
	Tamper Resistance	Yes, Integrated; No, for Retrofit	No	Yes	No	No			
	Tracking Verification	No, except ATC	No	Yes	No	No	No	No	No
Interoperability	ATC	Yes	No	No	No	Yes	No	No	No
	International	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Federated	Yes	No	Yes	Yes	Yes	No	No	No

Technology Alternatives: Costs (Primary Implementation Only)		ADS-B	Low Power Direct RF	Networked Cellular	Satellite	SW-Based Flight Notification w/ Telemetry	Unlicensed Integrated C2	Physical Indicator	Visual Light Encoding
Costs Item	Cost To								
Transmitter HW	Owner	\$\$\$\$ (rule compliant), \$\$ (low power)	\$-\$	\$\$	\$\$	None - \$\$	None	<\$	\$
Transmitter Data	OEM and/or Owner; one-time or recurring; bundled with hardware or separate	None	None	\$-\$	\$-\$	None - \$\$	None	None	None

Receiver HW (Non Internet Device)	Public Safety Officer	\$\$	None (existing device) - \$\$ (standalone)	None	None	None	\$\$\$-\$	None	None
Receiver Internet Device		Optional	Optional	Required	Required	Required	Optional	Optional	Required
Receiver Internet Data		Optional	Optional	Required	Required	Required	Optional	Optional	Optional
Development Costs	OEM and/or 3rd Party	\$-\$	\$-\$	\$-\$	\$-\$	Near Zero - \$	Near 0-\$ (OEM); \$-\$-\$ (receivers)	Near Zero	\$-\$-\$

Detailed Description of the Eight Classes of Technology Alternatives

31 August 2017

A. Technology Alternative: ADS-B

General Description

ADS-B transceivers, widely used in manned aviation today, provide precise ID and location information for manned aircraft using satellite signals for position information and barometric altimeters, offering situational awareness of other manned aircraft in the sky. ADS-B transceivers range in size, weight, power and cost (SWaP-C) depending on performance and airworthiness needs. A number of inexpensive low-SWaP solutions are available that would enable UAS compliance with airspace access requirements and could also meet certain public safety needs for remote ID and tracking. Tracking data is only available if GPS position and barometric altimeter sensors are either integrated with the ADS-B transceiver in a stand-alone product or the transceiver is integrated with existing avionics to receive position information. In a non-networked environment, ID and tracking data generated by an ADS-B transceiver could be directly received on the ground through a receiver coupled to a mobile device. These coupled devices exist today. Radio Line of Sight (RLOS) range varies by broadcast power, but the technology is typically reliable to ranges of 20+ miles. Low SWaP-C and lower than standard power technologies exist that may address FAA/ATC concerns of utilization and congestion related to ADS-B spectrum and potential for display clutter. In addition to having lower SWaP-C, these low power alternatives reduce broadcast range. A low-power alternative will require FAA approval. Although ADS-B technology is commonly used by manned aircraft today, it is used in a more limited fashion by a variety of UAS.

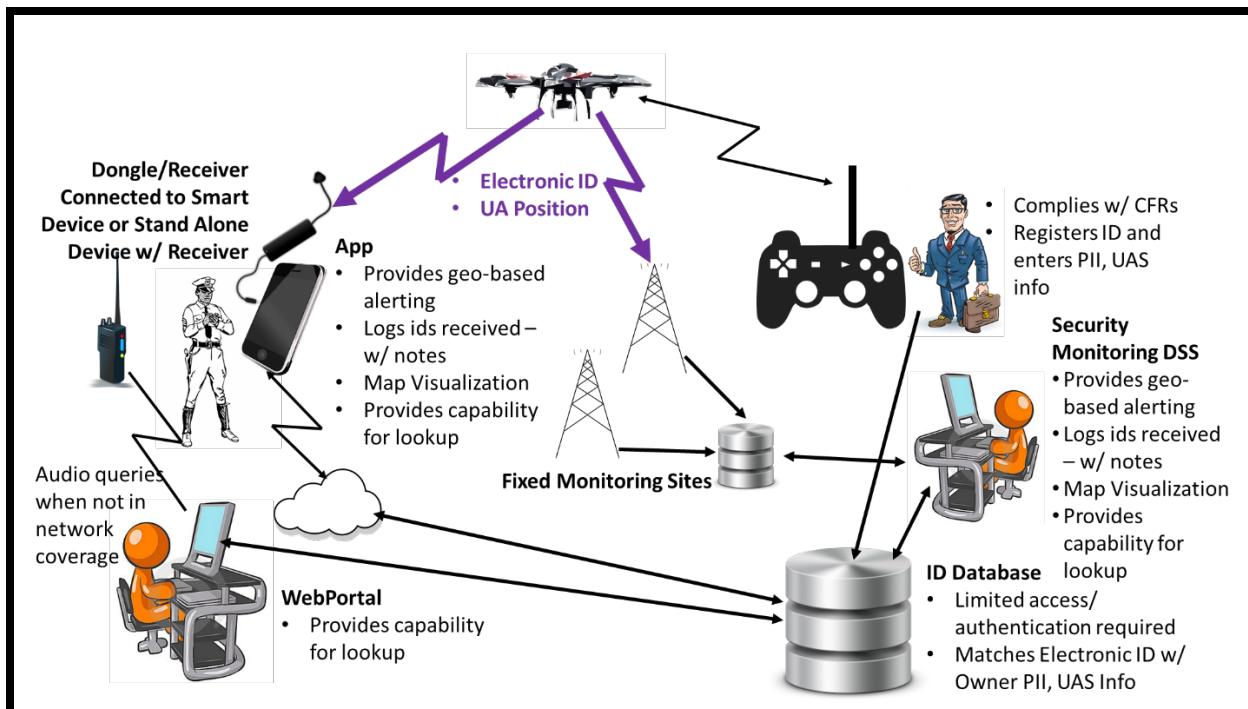


Figure 1. High Level Overview of ADS-B Architecture

ADS-B transceivers can broadcast aircraft position information and offers two potential fields for unique identifiers. The first field is an ICAO address, which is limited worldwide by the number of bits available (~17 million addresses). The second field is called “Call Sign”. Call Sign is used in manned aviation to alternate between a flight ID (UA924) or tail number (N12345), and squawk code. Call Sign consists of 40 bits (UAT/978) and 64 bits (1090) resulting in over 1 trillion uniquely available combinations per frequency. These fields could be leveraged to contain a unique ID which would need to be associated by the UAS owner/operator to the data in the registration database.

Ease of Compliance

- Overall the ease of compliance for retrofit is *medium* because a separate piece of hardware needs to be installed and configured. The hardware would require either integration into UA system power or have its own batteries which would require separate recharging. Weight is less than 100g.
- For UAS that have ADS-B as original equipment the solution will be integrated and has an overall ease of compliance of *high* because there is minimal time and effort to install and configuration initially and the weight penalty is very low.
- There is no required 3rd party involvement in delivering ADS-B services in that it is a peer-to-peer broadcast communications capability. There is a national ground network operated by Harris under contract to the FAA that collects messages from broadcasts in range of their ground-based transceivers. This is unlikely to be a perceived barrier to owners/operators.
- Low SWaP ADS-B rule-compliant solutions ranging with compliant position sources (i.e., GPS position and barometric altitude) from 20g-100g in weight are available now. There are multiple variations of hardware that have differing SWaP that can be appropriate for different UAS sizes and application needs. However, they may not be appropriate for some small to medium UAS depending on physical configuration and spectrum limitations.
- ADS-B solutions can be integrated into OEM autopilot systems as well as “payload” or “retrofit” stick-on solutions. Transmit power is directly related to energy density/battery weight, which affects range, and is mostly dependent upon use case.
- The ICAO limit of ~17M addresses does limit the variations of unique identifiers that are available but it may be possible to use dynamically-generated IDs. Unless additional fields are used such as Call Sign as described above, this does present a challenge of association between the ID and the owner/operator information in the registration database. This would require a minor modification to the convention regarding the use of the Call Sign field, which would provide over 1 trillion unique addresses.
- The UAS owner/operator would need to configure the ADS-B device with the unique ID.

Readiness for Implementation

- ADS-B is an established technology mandated by the FAA for certain manned operations. Multiple options exist for qualification ranging from TSO’ed (Technical Standard Ordered) installed units on commercial aircraft and manufacturer declarations that are tested for conformance to international standards (e.g., experimental and light sport aircraft).
- Technology Readiness Level 9 – Operational now, ADS-B transponders with a variety of SWaP-C characteristics are available on the market today. Most vendors are geared toward manned aircraft applications, but at least two specialize in solutions for UAS.
- The basic underlying technology has a high level of readiness because its manned aviation version is widely deployed and in use. Modifications to existing standards (e.g., lowering

transmit power) would need to be developed for wide-scale deployment for UAS operations to avoid overwhelming the ADS-B transmissions in use today. This is a concern for both the FAA and the FCC, and some vendors have proposed high TRL solutions to mitigate these concerns.

Operational Performance/Security

- ADS-B technology is based upon internationally-defined protocols used for Air Traffic Control (“ATC”) purposes – operational performance is considered highly reliable. Compliant ADS-B equipment must achieve certification for installation on type certificated aircraft, or declare “meets the performance of 14 CFR 91.227” which defines the performance requirements for ADS-B Out equipment.
- ADS-B is an unencrypted protocol and therefore hacking and spoof-ability is a concern.
- Both the FAA and the FCC are concerned about overuse of ADS-B spectrum. In order to use the technology at large scale, approving already developed solutions at low-power (0.01W-1W) would be needed which would reduce the effective broadcast range to 1-10 miles. This would significantly bring down SWaP and per unit costs to tens of dollars vs. hundreds or thousands.
- The reduced range would also partly address ATC concerns over display saturation.
- ADS-B technology will provide a unique identifier but it must be integrated with GPS and barometric-altimeter sensors to provide tracking data. ADS-B technology would provide broad geographic coverage, in various operational conditions in terms of functional locations (without internet connectivity), but is not tamper resistant and is spoofable. Its range is the radio transmission distance, which is typically tens to hundreds of miles as installed in manned aviation, which presents a range distance benefit, but also is a detriment in terms of saturating the bandwidth in a wide area. Low power solutions, if approved, could provide densities up to 14,000 sUAS within an 30 mile radius as modeled and reported by MITRE corporation in a published report titled “[ADS-B Surveillance System Performance with Small UAS at Low Altitudes](#)”.
- ADS-B technology does not offer any means to broadcast launch location or the position of the ground control station (GCS) unless a separate transmitter were to be placed at the GCS, but this is likely undesirable from an ATC perspective because of the limited spectrum available for ADS-B use.
- Public safety and the general public would require a receiver connected to a display device to directly receive information. A network connection thus would not be required for receipt of ID and tracking data. No launch location or GCS information would be available.
- For unmanned aircraft in range of an ADS-networked receiver on the ground, a network option would exist. Historical tracking would only be available for those aircraft in range of an ADS-B networked ground receiver.
- ADS-B uses licensed / protected aviation spectrum.
- ADS-B UAT transmits a ID and Tracking message once a second. ADS-B 1090 is at a slightly higher rate (several times a second). The latency is limited to on-board processing in the avionics and is minimal (<1sec). For manned aircraft, standards require visual display of ADS-B position information received from other aircraft within a few seconds.

Cost

- OEM costs in the \$1s to \$10s per unit are available now (TRL 9) as proposed by one vendor once there is approval of low-power solutions.

- Current rule compliant solutions range from \$1000-\$4000 per unit for ADS-B out transceiver installation for civil aviation applications. Low power retrofits are likely to cost <\$50 per unit and would include integration with GPS.
- With respect to ground-based mobile applications (e.g., public safety) receivers for ADS-B, costs depend upon implementation. Mobile pocket-sized receivers are <\$200 in single units which are intended to be combined with a display device. Networkable fixed installation receivers range from \$10s to \$1000s per unit.
- Crowdsourcing websites such as flightradar24.com and flightaware.com aggregate hobbyist and professional networks to provide agency access for free, in locations where the Internet can be reached by the agency official and the tracked aircraft is within range of a networked ADS-B receiver on the ground.
- Existing rule-compliant technology presents moderate and high development costs and per-unit costs to OEMs and Operators because this technology requires the integration (or retrofit) of new hardware into the UAS. Unless the UAS has a GPS that can be utilized, integration would require installation of a GPS component to enable tracking. This would be required for most retrofits for example. An advantage is that there would be no infrastructure cost, and agencies would simply buy a relatively affordable receiver, which are commonly available, as a one-time cost. Thus, in general almost all the cost of this technology is borne by the OEMs and owners/operators.
- The FAA is already funding Harris to maintain a network of ground-based transceiver (GBTs) to collect data. Coverage is limited and designed around manned aircraft operational needs. Low-altitude aircraft using low-power ADS-B are unlikely to be in range of existing GBTs for the duration of the entire flight.

Interoperability

- ADS-B is an international open standard for ATC. Universal Access Transceivers (UAT) for ADS-B, while an international standard, is only really used in the United States, although the UK CAA recently announced a UAT trial.⁵
- There are concerns from FAA and FCC that unless there are changes to the transmit power standards, the density of UAS traffic may saturate ADS-B bands impacting existing air traffic operations.
- There are also concerns that large numbers of small UAS concentrated in a limited geographic area in uncontrolled airspace (i.e., Class G) could overwhelm ATC displays of air traffic unless appropriately filtered.
- It may be feasible to incorporate use of ADS-B technology as part of a federated UTM-like service to provide situational awareness of all [manned and] unmanned aircraft.
- ADS-B also has utility for a detect and avoid capability.

Appropriateness for Different Operational Categories

- The benefits of ADS-B are most realized where UAS operations have a high likelihood of interacting with other traditional air traffic (e.g., in Class E, C, D, and B airspace) independent of its benefit as an ID system. Where encounters with manned aviation are of very low probability

⁵ <https://wwwcaa.co.uk/News/ADS-B-can-help-reduce-airspace-infringements-and-mid-air-collisions-says-CAA/>

(e.g., due to procedural separation for UAS operations at low altitude) its utility as an ID system only may not outweigh some of the potential drawbacks. If ADS-B is being leveraged for operational integration (e.g., detect and avoid), it may also serve as an ID and tracking source for security purposes.

- This technology is appropriate for nearly all operational categories, but may be more burdensome than warranted for some or all Part 101 (model/recreational uses) and some Part 107 (small UAS) operations.

Appropriateness for Different UAS

- Rule-compliant ADS-B is most appropriate in large commercial and medium-sized unmanned aircraft that may have a high likelihood of interacting with other traditional air traffic (e.g., in Class E, C, D, and B airspace). It seems less appropriate for small, UAS at low altitude, consumer, hand-size, budget, racing, and “tiny” unmanned aircraft unless also part of a detect and avoid solution. However, if UAS are utilizing ADS-B as a component of detect and avoid solution or as a means of airspace access, ADS-B may satisfy the requirement and intent for remote identification.

B. Technology Alternative: Low-Power Direct RF (Unlicensed)

General Description

Low-power, unlicensed direct radio-frequency technologies describe common communication technologies including standards based technologies such as Wi-Fi, Bluetooth, and RFID. Other custom solutions include RF technology leveraging unlicensed ISM bands or using other bands. Each of these solutions have different characteristics including technology readiness level (TRL) but are all low-power and use unlicensed bands and are treated together in this broad category. Given the broad nature of the technologies under consideration, this technology alternative is difficult to characterize and broad generalizations are included.

Depending upon the specific protocols, the operational environment, and the specific transmit power, a low-power (0.01W-1W) direct RF unlicensed transmitter could provide communications line-of-sight (LOS) ranges from 0.5-1.5 miles. One RF technology leveraging unlicensed ISM bands has a tested a range of 10 miles. Options for OEM install in chipset format exist at very low SWaP (less than 5 grams), as well as retrofit options which include an integrated GPS at less than 50 grams.

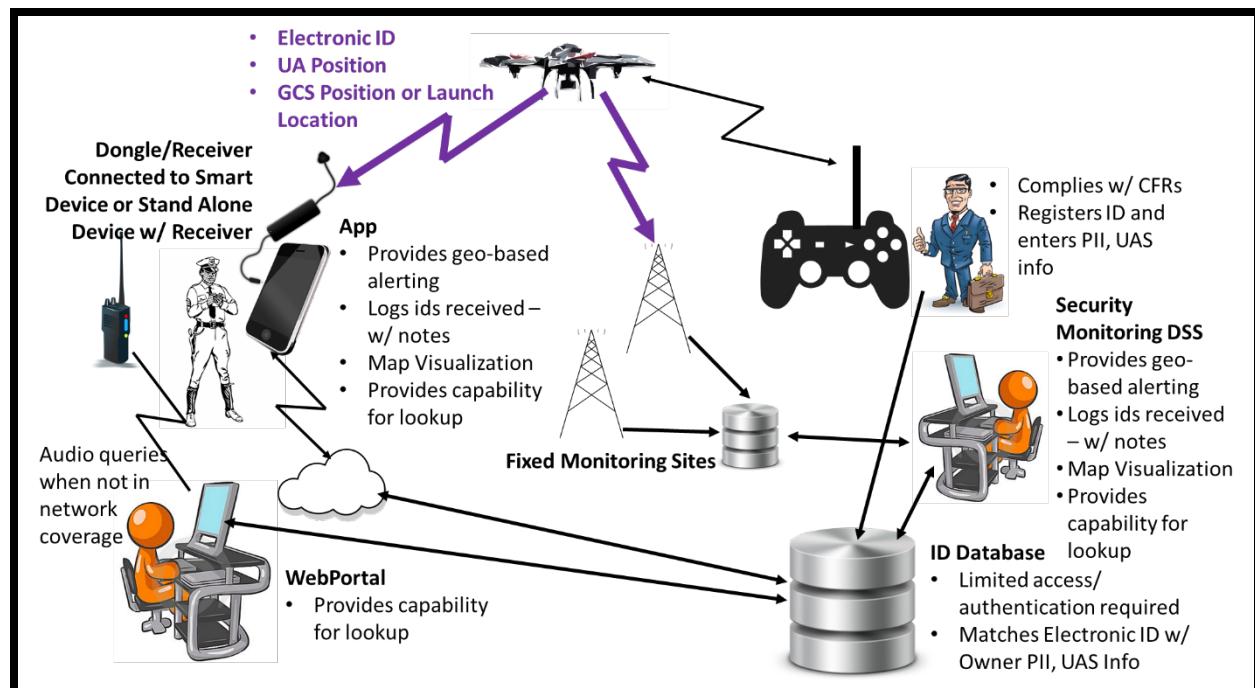


Figure 2. High-Level Overview of Low-Power RF Architecture

The concept is that the aircraft will directly broadcast a unique electronic ID and tracking information that would be able to be received by anyone within radio-line-of-sight equipped with an appropriate receiver. Receivers (e.g., those used by Public safety) would need to have network connection in order to look-up information that isn't transmitted (e.g., owner identification and contact information). If the solution uses common technologies like Wi-Fi, Bluetooth, or RFID, the public may be able to capture transmitted information using a smartphone without the need to purchase any additional receiver hardware. For transmissions using unique protocols, a specialized receiver could be coupled to a smartphone for display of received information.

One other solution that uses Wi-Fi involves UAS connecting to Wi-Fi access points (Wi-Fi via AP) on the ground to provide ID and other information. Broadcast distance will vary greatly based on network congestion, line of sight, and the need for a handshake. The need for bi-directional communication does impact the performance of this technology and generally reduces the effective link range.

Fixed, networkable receivers can provide persistent surveillance and accessibility through a web portal or app.

Options for broadcast of Ground Control Station (GCS) location include: 1) a separate transmitter placed on the GCS either as an OEM installation or as a retrofit; 2) Pre-flight user configuration of GCS location into airborne device; 3) continued broadcast of launch location with each transmission (as an alternative to GCS location); 4) OEM could include GCS location communication in an integrated solution.

Ease of Compliance

- Overall the ease of compliance for retrofit is *medium* because a separate piece of hardware needs to be installed and configured. The HW would require either integration into aircraft system power or have its own batteries which would require separate recharging. Weight is between 5 and 250g.
- For UAS that have an RF-based ID and tracking capability as original equipment the solution will be integrated and has an overall ease of compliance of *high* because there is minimal time and effort to install and configure initially and the weight penalty is very low.
- There is no required 3rd party involvement in delivering RF-based electronic ID and tracking capability in that it is a peer-to-peer broadcast communications capability.
- Low Size, Weight, and Power (SWaP) ID retrofit solutions are available on the market or easily developed using existing standards such as Wi-Fi, Bluetooth, or RFID. A new standard that describes the specifics of the ID and tracking message set will likely be needed. For example, configurable Bluetooth beacons are readily available on the market and can be simply stuck onto a UAS. Retrofits with integrated GPS position and barometric altitude can be developed within one year.
- There are multiple variations of hardware that have differing SWaP that can be appropriate for different UAS size and application needs.
- Solutions are available for integration into OEM autopilot/C2 systems as well as “payload” or “retrofit” stick-on solutions. Transmit power is directly related to energy density/battery weight, which affects range, and is mostly dependent upon use case.
- The UAS owner/operator may need to configure the device with the unique ID depending on hardware configuration, and the potential to enter the wrong code does exist. If the ID is embedded in the hardware, then the owner/operator would not need to enter the unique ID into the device. This could take the form of either a MAC address (if the Wi-Fi protocol is leveraged) or other hardware address. The specifics will need to be addressed in an ID and tracking standard.
- Operation would be automatic if the solutions are integrated into the UAS hardware as part of OEM original equipment.
- If implemented as a retrofit, the user would have some additional burdens to include purchase, installation, and configuration of the transmitter. There may be some per-flight tasks as well

including entering GCS location, ensuring batteries are charged (if not integrated with power), and that the unit is turned on.

- If a ground Access Point (AP) network is used to extend range, subscriptions may be needed from the ground Wi-Fi AP network providers. If access points are leveraged to increase range of coverage, there would be a 3rd party involved.

Readiness for Implementation

- Depending upon specific communications technology employed for the most part the technology is a high state of readiness with TRLs at 6-9. A message standard will need to be defined and demonstrated to be effective.
- Solutions using Bluetooth, Wi-Fi, or RFID to transmit a unique ID are at TRL 9. Only the message standard will need to be defined and the transmitters integrated with GPS. An integrated OEM solution is at TRL 7-8.
- Another approach leverages existing low-SWAP ADS-B hardware to work in alternate frequency, power, and communications data protocol/data fields customized to remote ID. The communications capability and the integration are done, TRL 9. Given that it is a software defined radio, just a new communication standard including RF band needs to be specified and the system appropriately configured. Overall this specific approach is at a TRL 7.
- Another proposed solution uses unlicensed TV whitespace spectrum. This solution would require a standard frequency and protocol to be established.
- There is a potential to leverage Wi-Fi via networked Access Points (AP) to extend range and create network alternatives. The underlying Wi-Fi technology has been proven in many devices. In order to be able to use this technology as a solution for remote ID and tracking of UAS, mesh networks would need to be built. The networks generally do not exist today.
- Message and communications standards already exist for data transmitted for identification and in some cases tracking purposes for other applications.

Operational Performance/Security

- At a base level, all technologies in this narrative can provide a unique electronic ID and tracking information if integrated with position source information. Solutions can be integrated by OEMs in original equipment or available as standalone retrofits. Retrofits could have their own independent position information and would not necessarily require full integration with the UAS. Retrofits are unlikely to be able to provide GCS location unless the retrofit has a way of receiving data directly from the UAS (i.e., fully integrated not just physically installed). Continued transmission of launch location would be an alternative.
- This approach will provide ID and tracking information directly to a public safety official equipped with the appropriate receiver. A single message set standard and a common communications protocol would reduce the complexity of public safety official receiver equipment. In all likelihood, they would require a receiver that could be coupled with a smart device for display of target information. Network connectivity would be required for retrieval of owner/operator identity, contract information, and other PII.
- ID/Tracking information will only be available to individuals with receivers in radio line-of-sight of the transmitting UA. This would limit exposure of information regarding UAS operations to those most directly affected. This helps to address some of the privacy concerns raised by UAS owners/operators about the ability for competitors to monitor activity broadly and the potential for a mega database of operational activity to be captured and data-mined.

- For Wi-Fi via AP, ID and tracking information (if GPS is on-board the UAS) can make its way to cloud and remote observers, as long as the UAS is in the coverage of the ground Wi-Fi AP network. Bi-directional communication requirements of a non-ID only solution increases complexity, reduces range, and increases potential for errors. In areas where there are many Wi-Fi APs from ground and/or UA, it could take more time for the receiver to scan all Wi-Fi channels and connect to potential APs to retrieve the right ID and tracking information of the target UAS. Usage of an AP network would enable a repository for historical tracking information.
- To access ID and tracking information, the general public would need their own receivers; either a separate receiver or potentially leverage existing smart devices. depending upon specific communications protocols that are implemented.
- These technologies would provide local geographic coverage, in various operational conditions, in terms of functional locations (without internet connectivity) and would meet “good enough” level of verifiability if integrated into the UAS itself.
- Because it is a local broadcast, there is no readily established historical tracking repository. Networks of ground receivers can be established linked to a data repository but that would require infrastructure investment. This could be accomplished in a limited geographic region or broadly, depending upon operational needs.
- Transmission range varies on the communications protocol employed, the transmit power, and the operational environment (i.e., interference from other transmissions in the unlicensed spectrum) but is likely to be 100 yards (Bluetooth) to 10+ miles (specialized RF). Bluetooth and Wi-Fi have a shorter range compared to other unlicensed band technologies as they were developed for short range use. While these technologies may not be appropriate where a high degree of certainty is required or there is high frequency congestion, they are adequate to address lower risk/less complex operations. Active battery-powered RFID tags have been developed with read ranges ranging from a few meters to kilometers.
- There is no mechanism to verify tracking information which is communicated unless an AP network is leveraged.
- Although not done today, proposed solutions include pairing the direct low-power RF with TLS/SSL certificates or encrypted IDs for verifiability and “good enough” trust factor. Accompanying certificates could be verified, but only when Internet access is available. This is at a low TRL.
- Unlicensed spectrum has no guarantees from interference and is susceptible to diminished performance if the network is congested from other uses. While a potential operational risk of the required bandwidth for an id and tracking packet is rather small reducing the probability of interference and since updates are continuous, an occasional dropped packet is not likely to have significant operational impact. A potential mitigation would be to increase the refresh rate to account for dropped packets.

Cost

- Hardware costs in the \$1s to \$10s per unit are available now for OEM integrate-able modules or chipsets.
- Retrofit solutions are largely market dependent, but units at ~\$20 including integrated GPS are possible.
- With respect to ground-based mobile applications (e.g., public safety) and receivers, costs depend upon implementation. Most all mobile devices have Wi-Fi and Bluetooth built-in

resulting in almost zero cost for agencies with public safety officials who are equipped with smart devices. For some solutions, mobile receivers including some that have directional antennas to increase detection range are available at a range of prices with some for less than \$200 per unit and others less than \$1,000 per unit. At the low-end, these receivers would need to be coupled to a smart device for display. Networkable fixed installation receivers range from \$10s to \$1000s per unit. Depending on the technology used, covering an area the size of the National Capitol Region could require 20+ fixed installations (for Bluetooth or Wi-Fi) or only 4-5 (for dedicated RF frequency).

- Wi-Fi via AP requires access points on the ground which would require extensive buildout of infrastructure. There would be significant cost to deploy ground Wi-Fi AP networks or expand existing outdoor Wi-Fi AP networks that can cover broad geographical areas.

Interoperability

- Solutions using Bluetooth, Wi-Fi, and RFID would require no changes to existing technical standards (IEEE, SIG, SAE) for the radio waveform. A message standard will be required.
- These solutions could create compatibility problems or interference with the UAS or external systems if they are deployed as add-on devices. Many UAS use control systems in the 5.8GHz and 2.4GHz spectrum and any add on device would need to be tested to ensure that they do not interfere with C2 systems of the UAS. OEMs will need to perform integration testing to determine whether there is concern for interference with existing aircraft transmissions and electronics.
- Solutions using other low-power, unlicensed RF spectrum would require new standards to be developed to define frequency and protocol in order to make competing products compatible with one another. Neither a standards body or creation timeline has been agreed to for development of the technical standard. Solutions in this category would have a lower TRL than what is referenced above. This has a short-term disadvantage in bringing solutions to market, but longer term advantages of less spectrum saturation and interference.
- These technologies could be included as part of a federated UTM-like service only if networked to the Internet.

Appropriateness for Different Operational Categories

- These technologies may not be appropriate for all operations. Depending upon the specific communications waveform and power and the intended operating altitude, there may be insufficient broadcast range for identification of aircraft operating under Part 91, 135, or 121. However, this technology could be supplemented with other technology solutions (e.g. ADS-B) especially for operations in controlled airspace.

Appropriateness for Different UAS

- Given the form factor, weight, power requirements, and price, most of these technologies may be appropriate as the sole identification method for the prosumer/consumer and below classes except for racing and extremely small UAS (e.g., palm size).

C. Technology Alternative: Networked Cellular Communications

General Description

Cellular devices are widely used for voice and data communication. Cellular chips are small, mass produced, low power, and embedded in phones and many devices. The cellular networks cover close to the entire domestic US population today. However, cellular coverage (3G and LTE) may not be reliably available in all areas where identification of UAS may be desired (e.g., wildfires in remote locations). All the major wireless carriers and semi-conductor companies (AT&T, Verizon, T-Mobile, Qualcomm, Intel, Nokia, Ericsson, etc.) are developing technologies for, and testing the cellular networks and associated technologies for, supporting UAS C2 communications functions to include telemetry and tracking information.

For cellular-capable UAS, objectives associated with ID and tracking for security purposes can be addressed by the systems already under testing and evaluation. Cellular communications can provide secure two-way communications, transmitting ID and tracking information from either (1) the UA or the (2) Ground Control Station (GCS). This would require that consumers of the ID and tracking information also be connected to a network infrastructure that would provide access to the ID and tracking information. This requires the establishment of a network-based server/processor that would serve as a data repository and source of public safety agency look-up and/or push of data to public safety officials.

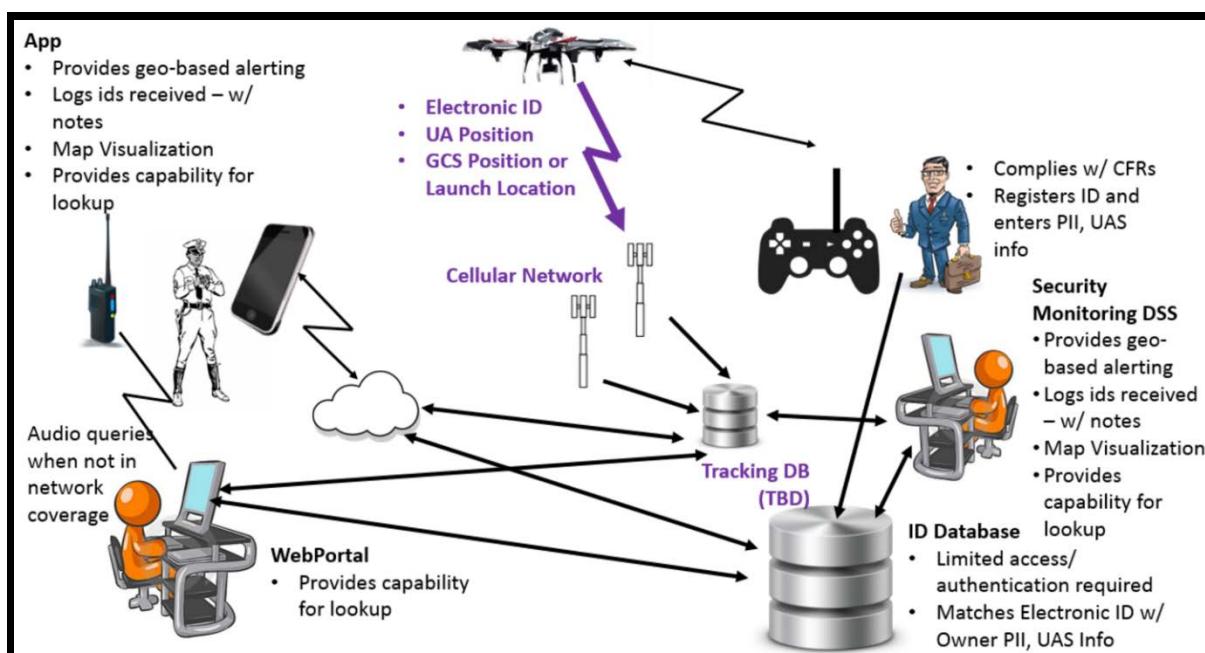


Figure 3: Networked cellular high-level architecture.

In the future, there will be cellular technology that will also work in a “non-networked” mode to provide a direct mechanism for ID and tracking. This broadcast cellular solution is not depicted in Figure 3. A broadcast cellular solution has been standardized through 3GPP, called Cellular Vehicle to Everything (C-V2X). This technology is expected to be embedded in LTE chips within 18-24 months and will provide coverage and direct broadcast communications both in network and out of

network coverage. C-V2X enables direct communications between two devices, without the network, and it provides a high-performance radio for UAS, affording a connection that supports high vehicle speed, at a range of a few hundred yards and low latency. The standard for the technology is finished as part of 3GPP Rel-14 and trials are expected to begin by the end of 2017 or early 2018. This technology will operate simultaneously with LTE operations, including using the cellular networks for C2, and will be integrated into LTE chipsets without the need for a separate chip. Law enforcement personal desiring direct receipt of ID and tracking information, will require a device with the C-V2X technology.

Physical configuration and power consumption are minimal for most UAS except for the very lightest (e.g., racers). For most UAs, the largest power consumer is the method of propulsion, typically electric motors. Power use by the modem would be very low compared to the power required for electric motor and on-board control and cameras. Cellular communications solutions can leverage existing unique International Mobile Equipment Identity numbers (“IMEI”), part of the cellular technology, as unique identifiers for UAS. Existing SIM technology also can be used for independent verification. Like mobile phones, SIM card technology easily identifies, and can independently verify the identity of the owner.

Cellular technology could enable the broadcast of the location of a control station either through embedding or retrofitting the GCS with a cellular chip, typically integrated with GNSS receiver in the same chipset, leveraging cellphones that may be used as part of the GCS, or a cellular-connected UA re-transmitting the information of the GCS.

Ease of Compliance

- Ease of compliance for retrofit solutions is *medium*. Most of the currently deployed UAS would require a retrofit solution for information from the UA rather than from the GCS. Many of today’s GCS are capable of linking a mobile device with cellular access.
- Ease of compliance for Original Equipment Manufacturer (“OEM”) is *medium-high* (*note: Especially in remote areas, owner/operators need to check for network connectivity for entire flight path prior to each flight.*) Cellular solutions can be integrated into OEM autopilot/C2 systems for some classes of UAS; included as a separate ID and tracking system; or retrofit as a stick-on solution. As with any retrofit solution, a retrofit may require the owner/operator to charge a separate battery. Depending upon OEM designs, cellular modules may be able to be integrated with the aircraft’s on-board power supply.
- Depending upon the specifics of the business models which arise, there may be some additional configuration steps for the owner/operator associated with establishing and maintaining a subscription with a cellular provider. This may be more likely for retrofits. For UAS with cellular as part of original equipment, this may be embedded with other registration/configuration steps implemented by the OEM.
- Some owner/operators may have concerns about sensitive operational information being maintained in a 3rd party repository which has broad operational coverage.

Readiness for Implementation

- Technology Readiness Level 9 (Networked) – airborne LTE modems are already available and being tested. They are available for retrofitting on UAS that are already in commerce. Moving forward, LTE chipsets, SIM technology and the use of SSL/TLS certificates can be easily

incorporated in UAS manufacturing for most UAS except for the lightest aircraft where weight/power may be an issue (e.g., racers). A new standard that describes the specifics of the ID and tracking information set will likely be needed. No new technical communication standards are required.

- Technology Readiness Level 6-7 (Broadcast) – The C-V2X broadcast cellular solution has been standardized through 3GPP. Operational trials are expected to begin by the end of 2017 or early 2018.
- The basic underlying technology has a high level of readiness because use of cellular technology is widespread among the general public and public safety organizations. As noted above, since no one cellular carrier covers the entire nation, airborne “roaming” will be required across network capabilities just as it is required today for terrestrial cell phone service. Public safety officials can use internet connected devices they may already have to obtain UAS ID and tracking information.
- Unique IMEI numbers, which are already used in the cellular networks, can be used as part of the unique UAS identifier
- 5G technologies will afford low latency high bandwidth solutions when available.

Operational Performance/Security

- Currently this solution requires network connectivity to provide ID and tracking of UAS.
- As the UAS ID and tracking information is hosted on a server, public safety officials could use any internet connected device to access this information in locations where internet access is available. For locations without internet connectivity, a radio call to a dispatcher with internet connectivity would likely suffice.
- Cellular networks can also provide location information for the UAS. LTE solutions used by smartphones today meet E-911 location requirements, so tracking data such as current position, speed and heading of the UA will be available. GNSS receivers are integrated in most LTE chipsets. An integrated GNSS receiver will reduce the cost and power consumption while improving the availability and accuracy of position fixing using network assistance including cell signal triangulation. Thus, there is a means to independently confirm location information.
- Depending on the database structure and requirements, there is potential to enable a repository for historical tracking of UAS.
- The general public could have ready access to ID and tracking information, perhaps through a lookup capability that will need tight controls.
- Cellular networks will provide redundancy for remote ID and tracking. Modern cellular networks (everything since CDMA) “breathe;” that is, there is overlap between cells/sectors, so if there is an issue in one cell/sector then the overlapping cells/sectors within range will adjust to ensure that a device—or UAS—is still connected to the network and transmitting needed information.
- Cellular networks offer authentication and security. Cellular networks are hard to tamper with and two-way authentication is required.
- Cellular networks rely on licensed spectrum.
- Public safety agencies need to be able to access the internet via a smart device, patrol car laptop, or via a radio call to dispatch. New laws or policies may be needed to address owner/operator privacy and the circumstances under which public safety officials will be entitled to this information.

- Cellular networks plus SSL/TLS certificates can provide extra validation of UAS location. SSL/TLS certificates can be managed (activated, renewed, rescinded & reinstated) using secure cellular communications.

Cost

- Reoccurring costs for cellular network technology are highly dependent on the carrier business model and relationships with OEM (especially for original equipment options). A network subscription fee and/or activation fee for owners/operators and for public safety officials may or may not be charged by the carriers. Some data costs could be transparent to the end user depending upon OEM/carrier business models.
- Costs for this technology are expected to run less than \$50 per module with low data rate modems approaching \$10 per radio for retrofits.
- Integration of a new transmitter into existing UAS radios and power systems may be, in some instances, a substantial development cost for OEMs, over and above the per-unit cost for the modem itself.
- There is an associated cost for any solution that uses SSL certifications.
- With respect to ground-based mobile devices to be used by the public or public safety officials for remote ID and tracking, the receivers can be any internet-connected device. Each public safety agency likely has a policy regarding whether personal devices may be used for official business or are provided by the agency for official use. Access controls for the general public will likely be required to avoid broad public access.⁶
- Some costs may exist for data lookup in networked situations. Agencies could also incur network access fees. All of these costs depend upon specific business models which have not yet fully been defined.
- Given the built-out nature of cellular networks today, there would be no infrastructure costs for this solution other than establishment of an id and tracking data repository. For retrofits, equipment and installation costs would likely be borne by the owner/operator. For original equipment installations, almost all the cost of this technology would be borne by the OEMs. Depending upon the business model, data costs could be borne by the OEM as well.

Interoperability

- Cellular network technology uses global standards for SIM, LTE, and 5G technology.
- Use of cellular communications for remote identification and tracking of UAS can be combined with, and will not preclude use of, non-networked communication technologies or alternative-networked technologies, which may be complementary.
- Cellular technology is being explored as part of a federated UTM-like service to provide situational awareness of all [manned and] unmanned aircraft.
- OEMs will need to perform integration testing to determine whether there is concern for interference with existing UA transmissions and electronics.

⁶ In order to use C-V2X technology in the future, new devices capable of receiving C-V2X data may likely be required.

Appropriateness for Different Operational Categories

- This technology is appropriate for nearly all operational categories in a networked environment and eventually in a non-networked environment given its flexibility, but may be burdensome for some Part 101 (model/recreational uses) and some Part 107 (small UAS) operations if the drones are small and/or inexpensive.

Appropriateness for Different UAS

- This technology is appropriate for most operational categories in networked environments with current technology and non-networked environments once C-V2X is operational.
- This technology may not be appropriate for some Part 101 (model/recreational uses) and some Part 107 (small UAS) operations if the drones are very small and/or inexpensive.

D. Technology Alternative: Satellite Based UAS Communications

General Description

Satellite based Receiver/Transmitter devices are in wide use across the world for communication. These Rx/Tx chip sets are small, lightweight, mass produced, fairly low power, and embedded in many simplex and duplex products from industrial to recreational. Major satellite constellations, including geostationary and low Earth orbiting constellations, currently cover 100% of the North American continent, including areas beyond terrestrial cellular and Wi-Fi systems being proposed for UAS ID and tracking.

To accomplish remote ID and tracking of UAS, the UA would be equipped with a satellite transmitter which would send ID and tracking messages to the satellite and collected by the service provider in a tracking database. Consumers of this data (e.g., public safety agencies) would simply query this database. See Figure 4. Satellite based tracking could be the prime means of ID and tracking or could serve as a secondary method (e.g., as an alternative for areas without cellular coverage).

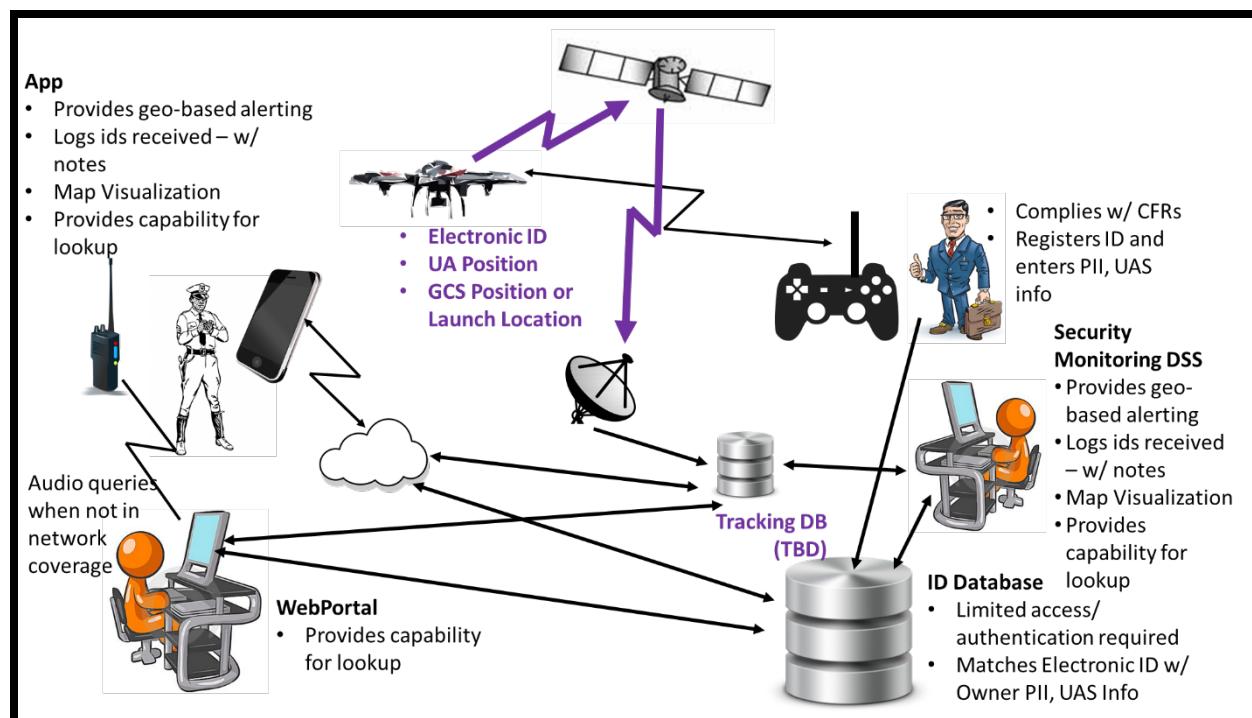


Figure 4. Satellite high-level architecture

Low size, weight and power (SWaP) satellite solutions are technically feasible, are already being tested, and are available commercially. Such solutions are the same or similar to existing satellite applications, including fixed asset management, mobile asset tracking, recreational tracking, and many other services. SWaP challenges may be significant for smaller UAS. For many UAS, power use by the satellite modem (550 milliamps) would be insignificant compared to the power required for electric motor and on-board control and cameras. Satellite solutions can leverage existing unique Electronic Serial Numbers (ESN) or International Mobile Equipment Identity (IMEI) as unique identifiers for UAS. Satellite solutions can provide location information for the UAS using the

satellite's integrated GPS receivers, altimeters, and accelerometers. This in turn may provide tracking data such as current position, altitude, speed, and heading of UAS.

Ease of Compliance

- Overall the ease of compliance for retrofit is *medium* because a separate piece of hardware needs to be installed and configured. The HW would require either integration into aircraft system power or have its own batteries which would require separate recharging/replacement. Weight is less than 250g including battery power. The retrofit satellite solution would be slightly larger than the size of a postage stamp with a built-in small chip antenna or patch antenna can be a stick-on retrofit.
- For UAS that have satellite as original equipment the solution will be integrated and has an overall ease of compliance of *medium-high* (*note: In urban areas, owner/operators need to check for clear sky view for entire flight path prior to each flight.*) because there may be some additional configuration steps.
- Depending upon the specifics of the business models which arise, there may be some additional configuration steps for the owner/operator associated with establishing and maintaining a subscription with a satellite provider. This may be more likely for retrofits. For UAS with satellite as part of original equipment, this may be embedded with other registration/configuration steps implemented by the OEM.
- Some owner/operators may have concerns about sensitive operational information being maintained in a 3rd party repository which has broad operational coverage.

Readiness for Implementation

- Technology Readiness Level 9 - small, lightweight integrated satellite-communication chipsets as well as stand-alone tracking units suitable for light UAS are already on the market.
- Satellite solutions providing complete coverage of the continental US and beyond are in-place, operational and provide commercial service.
- Satellite solutions can take advantage of existing networks without additional implementation and maintenance costs.

Operational Performance/Security

- Satellite networks provide coverage wherever the UAS can see the sky, both within US borders and internationally. This solution does not require ground based infrastructure for connection to the UAS but does require network connectivity and a third-party database.
- Satellite solutions can support many individual tracking messages simultaneously, adding small amount of latency to the system. Satellite based tracking systems currently process hundreds of millions of messages per month using very little system capacity.
- Satellite networks, particularly the multi-satellite low Earth orbit constellations, are inherently redundant.
- Satellite networks rely on licensed spectrum.
- All tracking and identification information carried on satellite networks is encrypted and resistant to tampering and spoofing. Satellite technology does not require the use of local access points to transmit ID and tracking data.
- Public safety officials and the general public would require an internet connected device or the means to communicate to an internet connected device to directly receive information.

Historical tracking and launch location may be available for aircraft that are connected to the satellite network. New laws or policies may be needed to address owner/operator privacy and the circumstances under which public safety officials will be entitled to this information.

- Satellite solutions do not provide tracking verification.
- Satellite solutions are unlikely to be able to support update rates of once per second.

Cost

- OEM Hardware costs for this technology are expected to run less than \$25 per unit. Consumer cost is expected to be about \$25 per unit for retrofit of aircraft.
- Public safety officials and general public can use any internet enabled device to access the ID and tracking data.
- A monthly subscription of less than \$10 per unit can be expected depending upon specifics of the business model. Reoccurring costs for satellite network technology are highly dependent on the business model and relationships with OEM (especially for original equipment options). A network subscription fee and/or activation fee for owners/operators and for public may or may not be charged by the satellite provider.
- A server solution to hold the ID and tracking data can be maintained indefinitely by the satellite service provider.
- Satellite networks are already built and integrated worldwide, and cover virtually 100% of the world's population today.
- Given the built-out nature of satellite networks today, there will be little to no infrastructure costs for this solution. Satellite based id and tracking solutions exist for other domains with existing data repository and access controls.
- For retrofits, equipment and installation costs would likely be borne by the owner/operator. For original equipment installations, almost all the cost of this technology would be borne by the OEMs. Depending upon the business model, reoccurring per unit costs could be borne by the OEM or by the owner/operator.

Interoperability

- Satellite solutions currently do not have ATC interoperability.
- As a network solution, integration with ATC and UTM is feasible.
- Testing may be required to ensure non-interference of satellite transmitters with other electronics on board the aircraft.

Appropriateness for Different Operational Categories

- This technology is appropriate for nearly all operational categories in both networked and beyond terrestrial network environments.
- This technology may be burdensome for some Part 101 operations (e.g., model aircraft, racing) and some Part 107 operations if the drones are small and/or inexpensive.

Appropriateness for Different UAS

- This technology is appropriate for nearly all operational categories in both networked and beyond terrestrial network environments.

- This technology may be burdensome for some Part 101 operations (e.g., model aircraft, racing) and some Part 107 operations if the drones are small and/or inexpensive.

E. Technology Alternative: Software-Based Flight Notification with Telemetry

General Description

Many operators today are already planning their missions before they fly using various software applications to take advantage of the automation now available in UAS. These applications cover all four phases of flights: discovering where to fly and the requirements; planning for gaining access to airspace and optimizing the mission; flying the flight (either manually or semi-automatically); and using the collected data to learn about the mission at hand.

For the most part, these capabilities are enabled through a smart device with applications that are downloaded by recreational and professional owners/operators. In many cases these applications are free. Smart devices either serve as the GCS or are directly coupled to the GCS during flight operations. These devices are often linked to the internet during operations to both receive and share operationally relevant information. Owners/operators use these capabilities for operational situation awareness, asset tracking, pilot activity logging, inventory management, battery tracking, flight logging, mission planning, record keeping, validation, and execution of the flight.

These existing and evolving capabilities can be leveraged to enable the UAS to provide in near real-time ID and tracking information via a federated service provider network.

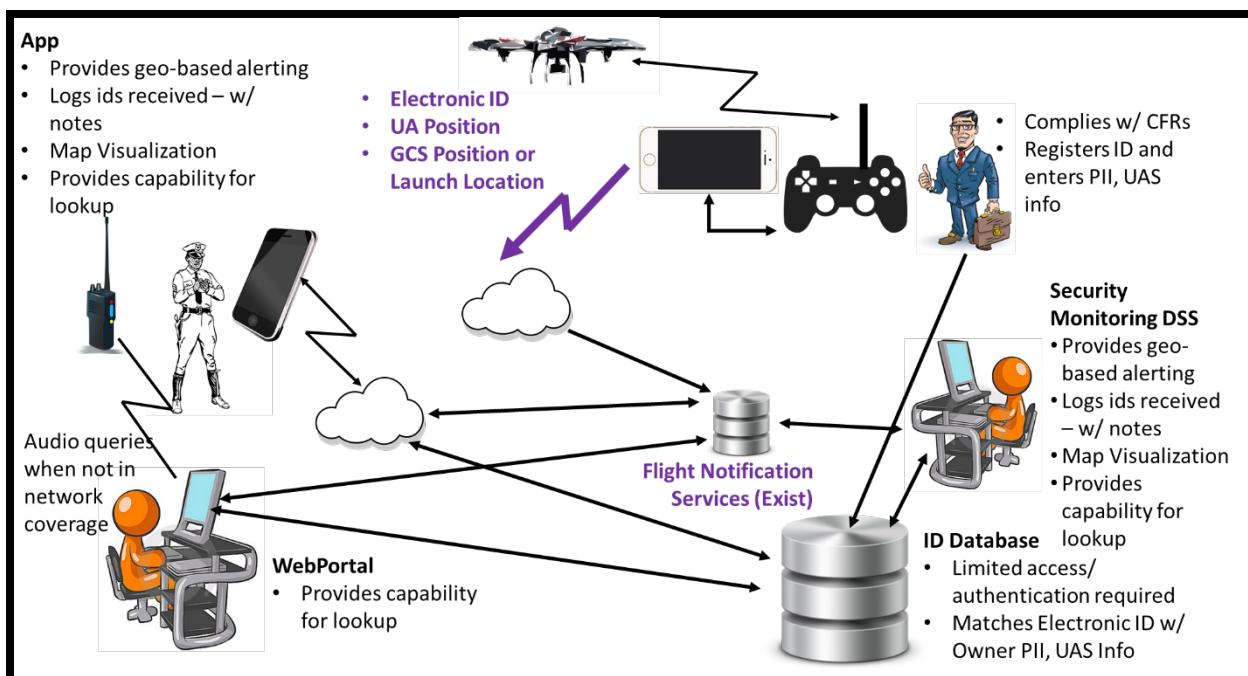


Figure 5. High Level Overview of SW-based Notification with Telemetry Architecture

Under the FAA's Low Altitude Authorization and Notification Capability (LAANC) these capabilities will be leveraged to provide the FAA with situational awareness of sUAS activity in the surface area of controlled airspace. During mission planning, the UAS operator selects the location and approximate working area for their drone (e.g., a circular area, corridor route, or a polygon) including altitude, duration, and type of aircraft. See Figure 6 for an example. Prior to flight this

information is shared to enable authorities to clearly identify compliant operations. Some UAS can share telemetry information in near real-time during the flight stage of the mission. This enables conformance checking for both the operator and authorities to ensure the flight stays in its area of operation. Currently, there are several vendors providing such services. These capabilities continue to evolve.

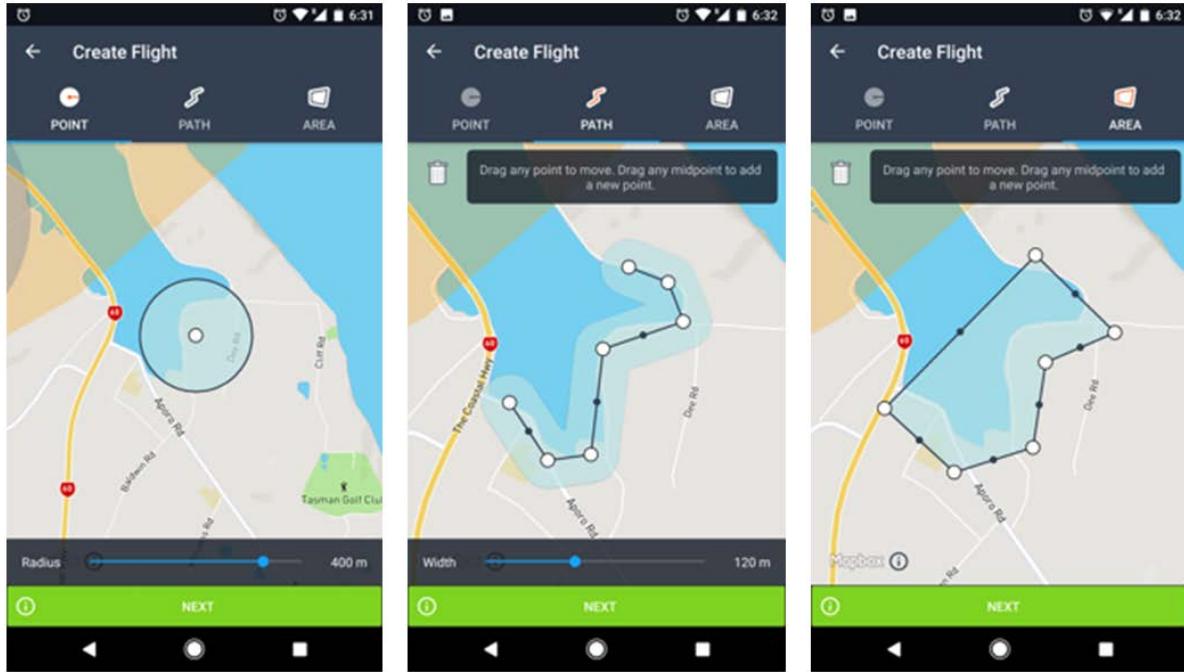


Figure 6. Examples of Mission Planning Input Screens

Software based mission planning (requesting authorization or filing notice) is planned as part of the LAANC demonstrations for flights in proximity to airports and the surface area of controlled airspace. Elsewhere these same systems could enable owners/operators to share their intended flight operation with other stakeholders and if so enabled and connected to the internet during flight near real-time telemetry information could be included.

A major benefit of software based flight notification is that it allows an owner/operator to share their intent prior to flight. For example, an owner/operator may share their intent to fly over a pipeline, their intended flight with their remote ID number can be compared to broadcast remote ID such that appropriately credentialed individuals can know that a flight over that pipeline is not only broadcasting remote ID but is also flying consistent with a shared flight notification. In other areas, policymakers may choose to place conditions on flights (for example requiring advanced notice prior to operating adjacent to critical infrastructure), software based flight notification allows for the easy satisfaction of those advanced notice requirements, and when married up with broadcasted forms of remote ID allows for stakeholders to understand not only identity but intent. This may beyond the scope of the ARC.

Both broadcast and network forms of ID and tracking information can be shown on a shared interface with shared flight notifications. Public safety officers and agencies with credentialed access will be able to view only the flight notifications filed within their geographic areas of responsibility.

Authorities can access that information from a smart phone or tablet (if they desire mobile access and have a smart phone or tablet), for agencies lacking such technology, a designated person or persons (at dispatch for example) could have access to flight plans filed within the geographic area of responsibility and patrol officers could radio to that individual for information about filed flight plans as necessary. Such an approach can also minimize response times and trouble calls allowing officials to quickly dismiss citizen complaints about purely lawful UAS operations, focusing their attention on suspicious or unlawful uses.

Ease of Compliance

- For owners/operators already using a SW-based mission planning capability connected to the internet, this is especially easy to comply with in that no significant changes are required. For those already using a SW-based mission planning capability connected to the internet, ease of compliance for retrofit is thus *high* (*note: The owner/operator must make sure that they have internet connectivity and that the compliant SW is operational for each flight.*) For near real-time telemetry, internet connectivity for the smart device would be required.
- For those not already participating, they may be required to establish an account and start operating with a smart device coupled to the GCS. Owners/Operators may have motivation since they could receive a benefit from such a capability when LAANC comes on-line. LAANC would enable compliance with existing FAA regulations that require individuals to file a notice or receive authorization when flying in proximity to airports. Thus, using a SW-based mission capability with notification should satisfy that requirement. For near real-time telemetry, internet connectivity for the smart device would be required.
- For UAS that will have software-based flight notification with telemetry as original equipment the solution will be integrated and has an ease of compliance of *medium-high* (*note: The owner/operator must make sure that they have internet connectivity and that the compliant SW is operational for each flight.*) For forward-fit UAS, OEMs can configure their UAS to require SW-based Mission Planning capabilities. The UAS will need to be coupled with a smart device with internet connectivity (e.g., cellular connection).
- Owners/Operators will be required to perform mission planning tasks for each flight and new subscriptions and radio communications capabilities may be required.
- A 3rd party or parties will have access to mission planning and potentially flight telemetry information which may be a concern of some owner/operators.
- For telemetry information (i.e., tracking), the UA or GCS will need to be regularly communicating with a 3rd party flight following capability and thus connected to the internet.
- Depending upon specifics, a separate broadcast ID and tracking capability may also be required.

Readiness for Implementation

- The technology to create UAS flight plans exists today, although there is no present requirement that operators file flight notifications (just as there is no present requirement to broadcast remote ID). Many of the services described above are available on the market. TRL 9. The interface to LAANC is being tested and is expected to be operational within a few months.
- Multiple applications on the market support mission planning for a variety of UAS. These vendors have established the necessary database infrastructure for storing and sharing information. Permission-based retrieval capabilities for the public safety community would need to be added.

- There is presently a requirement for operators to file notice at certain airports or request authorization to fly in controlled airspace, that mostly manual process is transitioning to a software and app based process through LAANC.
- The major limitation of software based flight planning is that it requires a device capable of connecting to the internet, in most cases this is satisfied with a smartphone.
- On average at least 100,000 daily UAS flights presently take place using devices that are connected to the internet for flight planning purposes.

Operational Performance/Security

- ID and tracking information will be available for public safety officials with network connectivity either directly through a smart device (portable or in the patrol cars) or via a radio call to a dispatcher with appropriate access. Tracking information will only be available for those UAS that have a smart device coupled to the GCS that is also connected to the internet.
- A historical repository of planned flights and actual flight telemetry would be available for access by the public safety community and potentially by the general public.
- To address sensitivities associated with 3rd party access to broad sets of flight trajectory data, there will need to be some degree of access control for the general public.
- There is no specific verification of track or telemetry data.
- The identity of individuals filing flight plans can be verified by authenticating user accounts against official forms of identification (driver's license or passport), authenticating validity of a telephone number, and authenticating the validity of a credit card. LAANC providers are entrusted to engage in such verification as part of their own business models.
- Flight notification information and telemetry data can be encrypted using TLS/SSL certificates, if needed.
- The capability is only effective if the owner/operator has internet connectivity.
- The range covered is as broad as internet connectivity.

Cost

- Cost is essentially zero to the UAS owners/operators who use mission planning software today.
- Cost is low to UAS manufacturers who need to program their software to allow flight intent and telemetry data to be communicated.
- Cost is low to public safety agencies who merely need to have credentialed access to the flight plans filed within their geographic areas of responsibility. If they don't already have a smart device (portable or in the patrol cars) they may require the purchase of such a device along with a data service plan. There would be zero cost to access the information via a radio call to a dispatcher with appropriate access.

Interoperability

- The standards for sharing these flights are being solidified by the FAA in their LAANC project, the NASA UTM project, the Global UTM Alliance (GUTMA), and have had multiple demonstrations of the capability. This would enable a high degree of interoperability to ATC.
- There is minimal potential for interface with on-board UAS capabilities and/or other services.

Appropriateness for Different Operational Categories

- This technology is appropriate for all UAS categories operating under 14 CFR Part 107 including those that may be operating beyond line of sight. Groups of small UAS used for racing could be identified under a single mission plan.

Appropriateness for Different UAS

- Any mission planning system for any drone can share the information they use to create a flight plan. Since there is no on-board capability even the smallest aircraft may be able to participate.

F. Technology Alternative: Integrated C2

General Description

The majority of small UAS flying in the national airspace today use an unlicensed radio frequency (RF) band for command and control (C2) purposes. For many models there is an opportunity to add an identification mechanism to the C2 radio link through a design change and/or a software update. Once the ID mechanism is included (i.e., a separate ID/tracking message packet multiplexed with C2 information), the C2 link effectively becomes the remote ID mechanism, and anyone within RF range of the UA with an appropriate receiver can receive the remote ID and tracking data of the UAS. This solution would have a zero size, weight, power, and cost (SWaP-C) impact for the UAS operator who uses models from OEM(s) that can implement this approach. The ID and tracking capability would be automatically active whenever the UAS is powered on and would allow access to any information available onboard the UA or its ground control station depending upon individual model capabilities.

Appropriate receivers currently exist although many are subject to proprietary protocols that would have to be made available to others for manufacturers to make the appropriate receivers available to public safety officials and other fixed-site installations (such as airports, prisons, or critical infrastructure). The receiver technology is mature, and it will take less than a year for non-OEM products to appear on the market place for public safety officials assuming the protocol would be opened through a performance standard. A common standard could be adopted for all OEMs to comply with or proprietary approaches from multiple OEMs could be accommodated. A common approach for message format would result in lower public safety official costs for receivers but would likely add to the cost of implementation for OEMs to develop the appropriate design changes/firmware updates. Receiver costs will vary depending upon the range of waveforms supported.

Including the ID mechanism in the manufacturer-supplied C2 link could be done through a firmware update to the communication protocol for most existing UAS models. Because the ID would be an integral part of the UAS firmware, the solution is tamper-resistant and could be made difficult to spoof if the ID is linked specifically to a hardware ID like a manufacturer serial number. Tracking data would be available if the UAS includes GPS and therefore could potentially include information on the take-off point and/or ground control station location. In a non-networked environment, ID and tracking data would be available to anyone with a receiver within radio line-of-sight (RLOS) of the UAS. RLOS will vary with the type of C2 link, but will in general be at least visual line-of-sight (VLOS); if someone can see a potentially problematic UA in your location, he or she can electronically ID it. The ID signal will generally pass through some physical barriers, such as trees and some walls. Likewise, if the technical capability and flight range of the UA is greater, the RLOS distance will be greater. The ID could potentially be broadcast from the UA and/or the GCS. This solution does not add any additional impact to spectrum use.

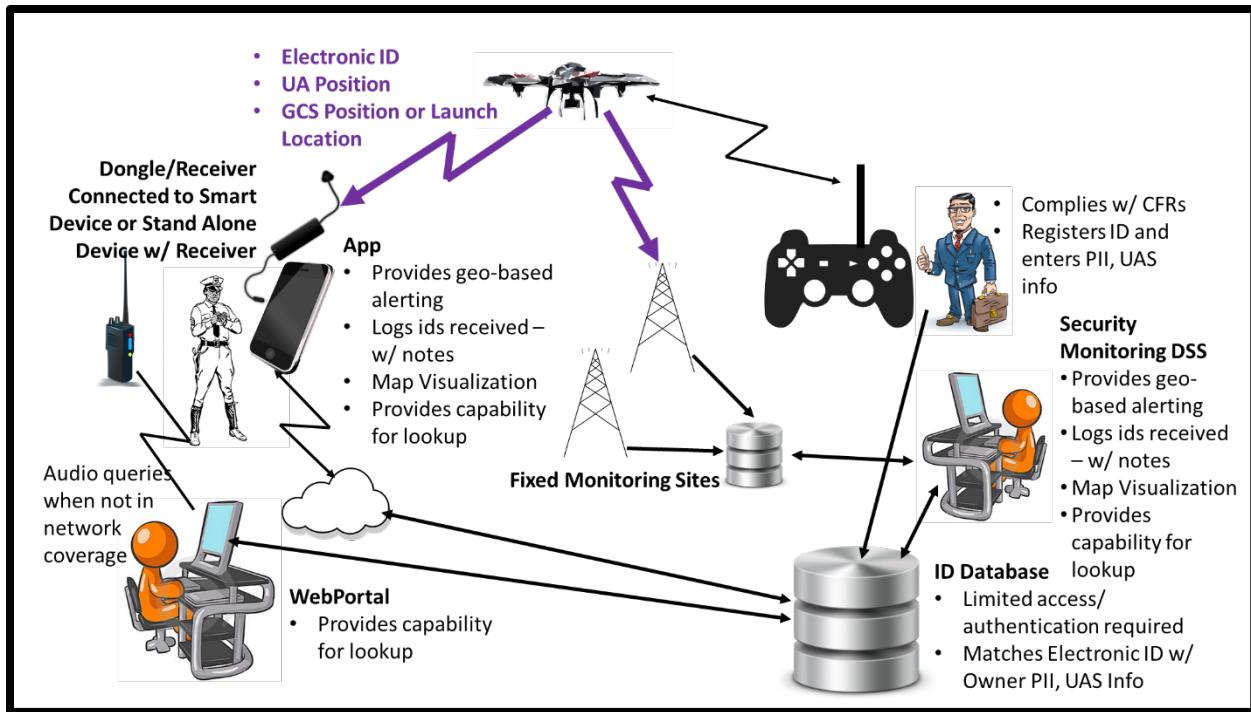


Figure 7. Integrated C2 High-Level Architecture

Ease of Compliance

- Ease of Compliance for retrofit is *high*. Retrofit would require the owner/operator to update their UAS with a manufacturer-supplied firmware update, delivered electronically, instantly and free of charge, if supported by the manufacturer. There would be no need for a hardware update or change.
- Ease of Compliance for original equipment is *high*. Manufacturers would include an ID feature in new firmware releases and new products; thus, new products would automatically include the ID feature. New products may typically be expected to take less than one year from start of development to offering on the market.
- SWaP-C is essentially zero for the owner/operator who use UAS models from OEM(s) that can/would implement this technology, across a broad range of the kinds of UA sought to be included in a remote ID requirement.
- The unique ID transmitted could include the manufacturer assigned serial number, making the ID information harder to spoof as well as verifiable on the back-end owner/operator database.
- The UAS owner/operator would likely need to configure their UAS with the unique ID (such as a registration number), and the potential to enter the wrong identifier does exist.
- This solution would allow the ID and tracking information transmitted to potentially include any information available to the UAS, such as remaining battery life, return-to-home point, and user-defined fields like mobile telephone contact information.
- Once configured, there is no on-going action required of the UAS owner/operator to comply. Thus, compliance is automatic to UAS operation.

Readiness for Implementation

- Technology Readiness Level for identification and tracking is *high (Level 9 – Operational now)*, for UAS retrofit, fixed site receivers, and for mobile receivers. This technology has been deployed by a major UAS manufacturer overseas.
- The basic underlying technology has a high level of readiness because all capable UAS use some sort of C2 which of necessity includes both transmission and reception of information. However, since different manufacturers use different underlying communication technology, there is a need to develop an industry standard for the communication technology and protocols. The standardization organization and timeline of this effort have yet to be determined. Ideally, standards would be developed to define what information is sent, and in what format. The Consumer Technology Association (CTA) already has a published standard defining UAS serial numbers, including a definition of an electronic format. An “open” format for common protocols among OEMs could be developed and released for common use. It will likely take 12-18 months to define the standard open protocol, for OEMs to have the appropriate updates available, and for manufacturers to have products with receivers for the public safety community.

Operational Performance/Security

- ID and tracking data, if available through separate GPS on the UAS, would be available in the absence of internet access.
- This solution could potentially transmit all data requested by WG2 in real-time. Data sent would depend on the equipage of the UAS (e.g., if the UAS does not have GPS, position information will not be included). Data could be sent continuously.
- Data would be available to any appropriate receiver within RLOS (public safety officials or general public). Actual range will depend on the C2 technology but should be similar to the C2 link range. Link range would typically be hundreds of feet for the smallest devices, up to a few miles for the prosumer and commercial devices, so the range of the ID broadcast corresponds to the capability, performance of the UA and spectrum band including the interference level from other sources in the unlicensed band.
- Location of the ground control station (GCS) could be provided in a number of ways depending on the UAS equipage. For example, if the UA has GPS, the solution can report the recorded take-off point as a proxy for GCS location; if the GCS includes a GPS, this location can be reported directly. This would depend on specific OEM implementations.
- Some C2 protocols are proprietary. Making appropriate receivers available would require the manufacturers to either provide their proprietary protocols for anyone to use in making a receiver; or the manufacturer would have to make such receivers available on the market.
- This solution uses unlicensed spectrum, which is susceptible to congestion and interference. As the number of UAS grows and other uses of unlicensed spectrum increase, this may create problems for UAS operators in some areas. Operators can't fly if they can't control their aircraft. Unlicensed spectrum means there is no quality of service guarantee and messages ID/tracking messages may be missed. All RF transmissions (in licensed or unlicensed bands) can potentially be tampered with, hacked, jammed, and spoofed.
- This solution is effectively tamper resistant as the ID and tracking function would be integrated by the manufacturer into the C2 link. Basically, the C2 link does not work if the ID and tracking function is not working. Spoofability could be reduced by adding a manufacturer serial number to the packet that could be checked against the unique ID on the back end.

- Since the front-end ID and tracking functionality will be implemented by the OEM, the data may be treated with high trust. The technology is as resilient/robust/reliable as the C2 link, which is integral to flight of the UA, and therefore very high.
- ID/Tracking information will only be available to individuals with receivers in RLOS of the transmitting UA. This would limit exposure of information regarding UAS operations to those most directly affected. This helps to address some of the privacy concerns raised by UAS owners/operators about the ability for competitors to monitor activity broadly and the potential for a mega database of operational activity to be captured and data-mined.
- Because it is a local broadcast, there is no readily established historical tracking repository. Networks of ground receivers can be established linked to a data repository but that would require infrastructure investment. This could be accomplished in a limited geographic region or broadly, depending upon operational needs.
- This technology would provide broad geographic coverage, in various operational conditions, in terms of functional locations (without Internet connectivity) and would meet “good enough” level of verifiability. ID data could be read by the public-at-large by anyone who has access to a receiver or by using a new standard leveraging a common protocol used by popular devices once an ID/tracking standard is available.
- Without a network of ground receivers, there would be no historical repository of ID and tracking information.

Cost

- Cost is essentially zero to the UAS owners/operators who use UAS models that can implement this approach.
- Cost is low to UAS manufacturers and to radio controller manufacturers (some R&D investment to develop and deploy the ID and tracking protocols in their firmware).
- Assuming ID/tracking signals could be standardized, it is expected that public safety officials and general public receiver will be a dongle or other device attached to an existing mobile device (e.g., a smartphone) with network connectivity. Given the similarity to other such receivers, this is likely to cost less than a \$50 per unit. If there will be various alternative implementations, cost for security agency receivers able to receive proprietary signals from multiple OEM models are likely to cost more, roughly \$100-400 per unit for a basic receiver to approximately \$1000-2000 per unit for a more capable fixed-site receiver.
- This solution does not require a network or larger infrastructure and associated costs for public safety agencies to directly receive unique electronic ID and tracking information. Public safety officials will require a connectivity to retrieve reference information such as PII, owner/operator identification, etc.
- Some costs may exist for data lookup in networked situations. Agencies could also incur network access fees though most agencies already pay for the cellphone plans of employees.

Interoperability

- This method does not directly integrate with current air traffic control technology.
- This method could be compatible with all existing unlicensed C2 links and would not create any additional compatibility problems or interference with the UAS or external systems, assuming the proprietary technology will be standardized in the future and adopted by all major UAS vendors.

- This method could be adopted internationally, as it is independent of any particular technology or infrastructure specific to one country or region or a manufacturer once standardized, and is able to leverage a federated approach.
- Reception of ID and tracking from UAS made by different manufacturers could require the use of different physical receivers. However, software-defined radios are now common and relatively inexpensive that could be developed to support different solutions by different manufacturers. One or more standard protocols could be developed in the future, to achieve wide compatibility of systems. Once the appropriate standards are defined and available, products will be available in less than a year.
- For additional cost, receivers could be created with a network interface that would allow agencies, localities or other groups to combine received ID data, or forward it into a larger system. For example, UAS service suppliers (USS) could aggregate ID data obtained through direct broadcast with data obtained through other networked methods.

Appropriateness for Different Operational Categories

- This technology is appropriate for all operational categories where the UAS is using an unlicensed C2 link. If enabled by default, this allows for compliance by UAS that may be used in multiple operational categories at various times (such as Part 101 and Part 107 operations.) All types of operations would be included because the solution is inherent in the C2 technology.

Appropriateness for Different UAS

- The technology is appropriate for a wide range of UAS using a digital C2 link in an unlicensed band. This would include industrial and heavy commercial UAS, general commercial, prosumer/consumer and budget consumer UAS. This technology may not be appropriate for UAS using an analog C2 link or simplified C2 radio equipment, such as FPV racers, fixed wing/rotary model aircraft, and many toy-type UAS. Upon implementation of software upgrades and common protocols, it is anticipated that this technology would include over 90% of the existing global UAS that are above the threshold for inclusion in a remote ID requirement. An add-on hardware transmitting module using the same ID protocol could be developed to capture the remaining UAS (such as “homebuilt” models).

G. Technology Alternative: Physical Indicator

General Description

Physical indicators include tags, streamers, stickers, or numbers attached to the UAS. While these solutions can comply with low SWaP-C requirements, there are severe limitations to their effectiveness in remote identification and tracking of UAS. Physical indicators are currently being used on UAS in certain situations, such as in flight over people by news networks. In this case, the UA will have a clearly marked and identifiable streamer pre-arranged with public safety officials. Public safety agencies are aware of this specific UA as well as the location of the operator. This solution is effective for sparse, low altitude flight when appropriate authorities are notified in advance and are aware of the operator's intent. However, this alternative does not provide remote ID and tracking information. Placing a sticker or FAA registration number on the UAS will not provide remote ID and tracking, as it would be nearly impossible to read a registration number on a UAS that is more than a few feet away. There is also no way to provide tracking information from the UA to a ground controller or public safety official. The public safety officer would still need to access a database to correlate the registration ID with the owner/operator information.

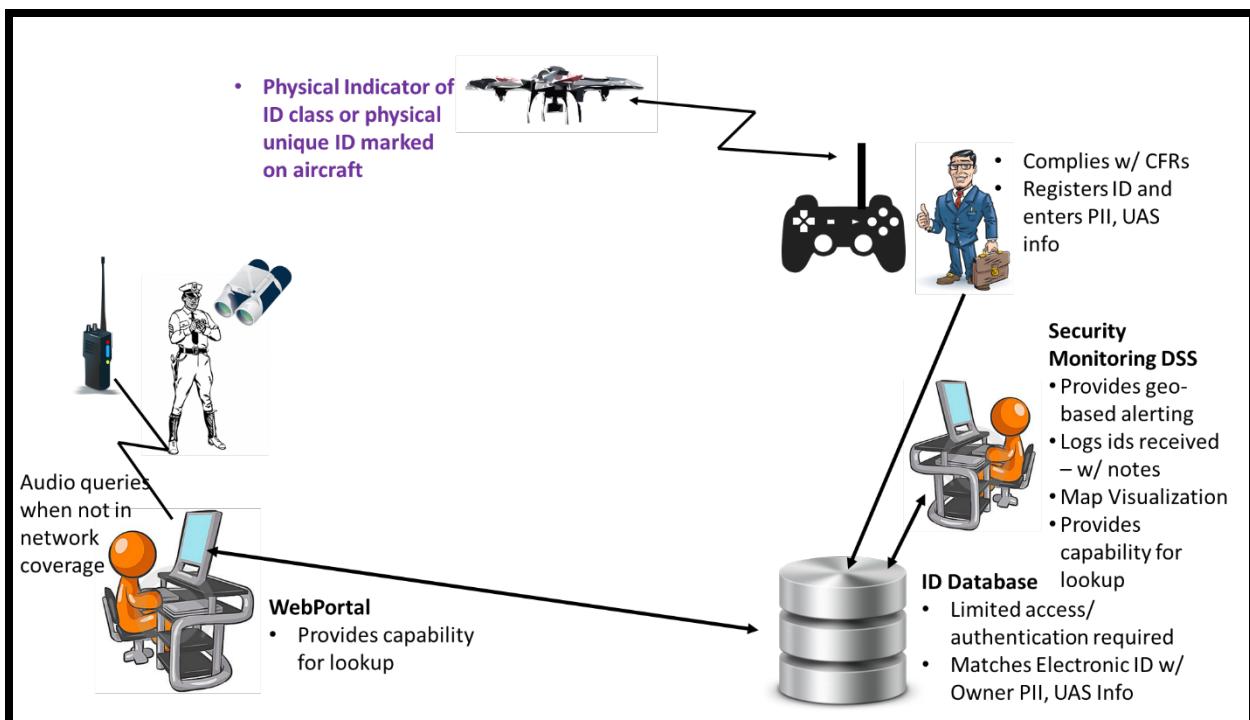


Figure 8. Physical markings high level architecture

Ease of Compliance

- Ease of Compliance varies from *low-high* for both retrofit and OEM aircraft as it varies greatly on the specific implementation. Physical indicators can be integrated onto any UAS platform. Integration would be as simple as placing a sticker or number onto the UAS once the registration number is obtained.

- A streamer, sticker, or number attached to the UAS is a low SWaP-C solution for both retrofit and OEM aircraft. A small plastic streamer or sticker has a negligible weight and consumes no power from the UAS. The size of the indicator could be adjusted based on the size of the UAS, but would not solve the problem of remote ID or provide tracking ability.
- The possibility of writing/printing the wrong FAA registration code on the UAS does exist, but the code or sticker would not be visible while the UA is in flight that is more than a few feet in the air.
- Non-compliant operators could print a false number or fly a random streamer from the UA, giving the appearance that it is compliant.

Readiness for Implementation

- Readiness for Implementation is *high*. Physical indicators are an established “technology” with a TRL of 9. Placing stickers or numbers on items to identify them has been used in many ways (license plates, tail numbers, name tags, etc.).
- This solution could be implemented by anyone with a marker, sticker, or streamer.
- News networks have used this solution, but in very controlled situations where public safety officials are well informed.

Operational Performance/Security

- Physical indicators would have poor operational performance and security. As mentioned earlier, a number, sticker, or streamer would be difficult to see at almost any distance and may require public safety officials to use manual equipment such as binoculars to ID a UAS in flight.
- Physical indicators provide only the registration number and still requires a networked lookup to verify information. This lookup will not likely be available to the general public.
- There would also be no way to track the UA in flight because no ID or tracking information is being transmitted from the UAS to a person on the ground.
- Concerns over security exist. As mentioned earlier, an operator can easily attach a false sticker, number, or streamer to the UAS and appear to be compliant with the rule.

Cost

- Regardless of the specific type of indicator, the cost will be very low (if any) for this solution. The FAA would need to determine if they will distribute a streamer, sticker, or number to the operator of the UAS, or if the operator would apply their own indicator.
- No cost to public safety agencies or UAS manufacturers.
- There are no recurring costs for this alternative.
- A database of registration numbers and owner/operator information needs to exist for lookup.

Interoperability

- A physical indicator could be universally accepted, as it does not interfere with any networks or public safety agencies. Rules for specific colors of streamers and stickers or registration numbers would need to be made for international flight (e.g. an FAA-registered UAS flying in another country).
- It would not be feasible to incorporate the use of physical indicators in a federated system because the UAS would not be able to be remotely ID or tracked.

- Provides no interoperability with ATC services or a UTM capability.

Appropriateness for Different Operational Categories

- This solution would not be independently appropriate for any of the operational categories as it does not meet the requirements for remote ID and tracking of UAS.
- This solution would be appropriate for all operational categories of UAS as a supplemental solution.

Appropriateness for Different UAS

- This solution can be used on any UAS, from heavy commercial UAS to “tiny” UAS. Streamers may be more appropriate for medium to large UAS due to the small increase in drag that the streamer would cause. A sticker or number placed on the UAS would be appropriate for any size UAS.

H. Technology Alternative: Visual Light Encoding

General Description

Bright anti-collision lights on the UA may be used to send a signal via blinks encoded with the device's registration number, location, and any other basic telemetry if the UAS provides telemetry and enables light modulation. A software update to the flight controller would enable the vehicle to transmit the signal through a unique baud rate of the UA lighting. An app running on a regular smartphone can parse the signal and decode the information being transmitted allowing for both public agencies and general public to identify the UAS. This technology alternative is appropriate for very short operational range, less than 50 ft. during day-time operations, increased range may occur during nighttime or other low light operations or if the receiver is equipped with telephoto lens technology. No additional hardware accessories are required as the lighting is currently onboard the UA. There are no SWaP constraints for the UA or cost to the owner/operator.

Visual light encoding is a direct broadcast technology which works without a network connection. As with many of the technology alternatives, when paired with an internet connected device this alternative offers the ability to lookup the transmitted information against a database.

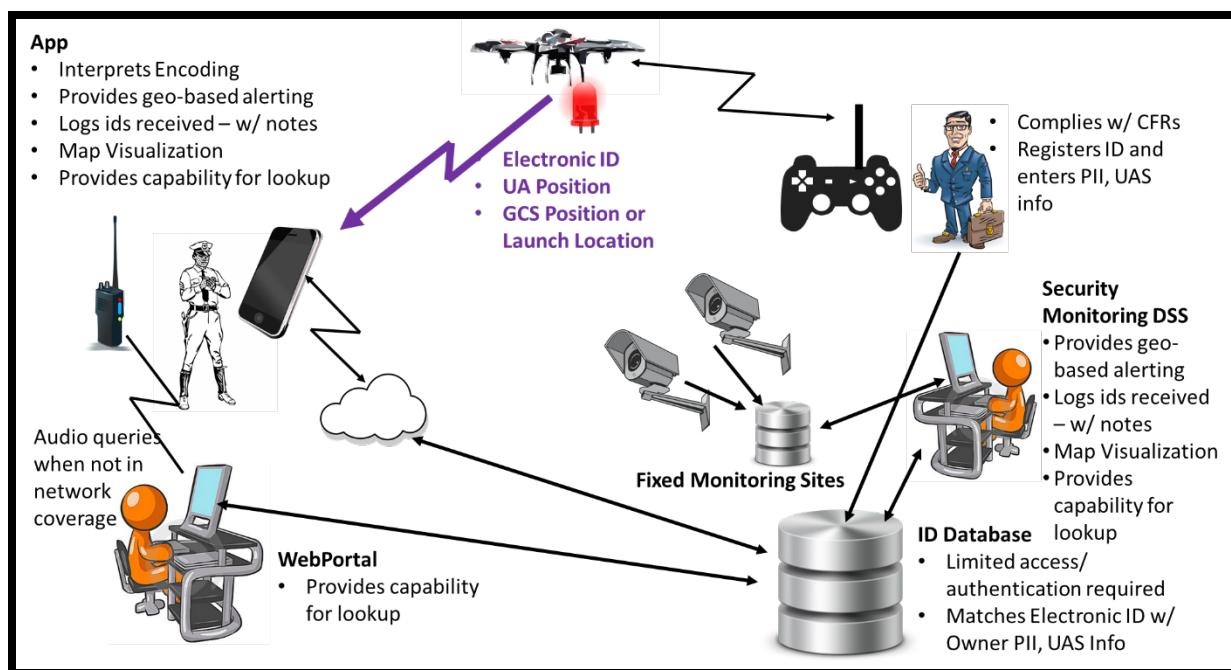


Figure 9. Visual Light Encoding high-level architecture

Ease of Compliance

- For this technology alternative to be deployed on the UA the lights must be software controlled and must be of sufficient intensity for the sensor. For those thus equipped, the ease of compliance for retrofit is *high* because the owner/operator would not be required to take any significant action. Not all UAS have software controlled lighting and those that don't will not be able to employ this alternative.

- For UAS that have visual light encoding as original equipment the solution will be integrated and has an overall ease of compliance of *high* because it is assumed the lights can be modified to send the signal on the aircraft if it is equipped with visual light encoding.
- Low SWaP solutions; modulating the baud rate of the on-board lighting should come with no additional hardware or size, weight, or power requirements.
- Open-source software solution; easily distributable.
- Data broadcast includes position information, unique identifier, and any other telemetry required by standards if the UAS has the correct equipage to provide telemetry. Standards for this message will need to be developed.
- One-time configuration required, may be executed by UAS owner/operator for unique identifier. Owner/operator execution presents the possibility of user error in setup.
- Automatic to UAS operation if integrated into UAS hardware; no subscription required.

Readiness for Implementation

- Underlying technology has been well researched and applied in field, though not in UAS specific applications.
- Specific application of proposed solution is currently at TRL 4. Can be extended to TRL 7-9 with additional research dedicated to enhancing computer vision and machine learning algorithms for the mobile app receiver.

Operational Performance/Security

- Visual light encoding currently has a maximum day-time operational range of 50 ft. using an un-augmented smart device electro-optic sensor (i.e., camera).
- Transmits identification without dependence on other components; requires pairing with an onboard GPS or telemetry system for tracking.
- Low range, low geographic coverage. Works better during night ops and low light conditions.
- Non-spoofable for OEM devices since transmission sequence is encoded in firmware by manufacturer. Spoofing or error is possible when setup is performed by owner/operator.
- Could be bypassed by covering lights.
- If a unique identifier is provided after purchase, then solution relies on the UAS having the functionality to enter a unique identifier and the owner/operator keying the correct identifier into the device.
- Technology still works if there are multiple UAS in the area.

Cost

- Ignoring the cost of initial R&D to develop a robust solution, cost of acquiring, distributing, and replicating solution is near zero for manufacturers, operators and public safety officials. Dedicated cameras with narrow field of view, telephoto lenses etc. would have additional costs if required.
- Assumes public safety officials are provided with a standard smartphone.

Interoperability

- Visual light encoding is based on open source software that is universally available.

- Will work across OEM devices, hobby projects, and home-built UAS if equipped with software modulated lights.
- Communication relies on standard ASCII character encoding.

Appropriateness for Different Operational Categories

- Appropriate for short-range basic operations.
- Proposed on the assumption that a UAS is a greater threat to security and privacy when it is in proximity of a third-party.

Appropriateness for Different UAS

- Technology is complementary to other broadcast and networked solutions.
- Appropriate for consumer, hand-size, budget, racing, and “tiny” UA conducting basic ops.
- Not appropriate for industrial, military and high-performance UA conducting expanded ops.

Appendix C Working Group 2 Report

ID and Tracking ARC: Working Group Two

Requirements Recommendations

August 11, 2017

I. Introduction

Unmanned Aircraft Systems (UAS) may represent one of the greatest opportunities and challenges aviation has presented to society. UAS have already attracted millions of new aviators through aerial photography, drone racing and other recreational activities, while countless commercial remote pilots are finding new applications for these aircraft on a regular basis. From infrastructure inspections, surveying and agricultural applications to providing widespread broadband access and advanced search and rescue capabilities, UAS are beginning to reshape the way we think of our traditionally two-dimensional world.

In the near future, aerial package delivery will be common place and we will begin looking toward unmanned air cargo operations and fusing aviation into transportation planning for Smart Cities through urban air mobility platforms. However, while the enabling technology for this transformational portrait is all but inevitable, the required enabling regulatory policy is forced to examine the risks UAS pose.

Those risks are real and growing. In the hands of an irresponsible remote pilot or a nefarious actor, UAS could provide an ideal platform for illegal surveillance, delivery of contraband to prison inmates, and dropping explosives or other dangerous payloads.

UAS also pose a serious collision risk with a manned aircraft. As with many new technologies, a regulatory foundation for safety and security is essential to garner the public acceptance required for the industry to reach its full potential. A key component of this safety and security foundation is enforcement.

The public trust for any regulated activity revolves around accountability. There is general acceptance of an activity when the public is both confident that adequate rules are in place to maintain an acceptable level of safety and security, and that there is accountability and enforcement for those who operate outside of those rules.

In manned aviation, the FAA has been able to achieve this balance over numerous decades with a comprehensive set of federal aviation regulations and adequate mechanisms for enforcement. However, the nature and number of UAS entering the NAS have begun to unsettle this balance and threatens to diminish the public trust and acceptance of this new technology. Unlike manned aviation, anonymous operation of very small and technically capable unmanned aircraft (UA) is becoming increasingly inexpensive and widely available to the public.

To achieve safety and security through accountability there must be a readily available means for public safety¹ officials to remotely identify, authenticate and track UAS. This UAS ID and Tracking Aviation Rulemaking Committee (ARC) has assembled a broad and diverse group of stakeholders, representing various segments of the aviation industry; UAS manufacturers, owners and remote pilots; and public safety entities to identify the information required by public safety officials and the technical means to meet those needs. The following recommendations are offered as a step toward enhanced safety and security policy, which will allow the growing unmanned and automated aviation industry to accelerate toward full integration into the NAS.

II. Background

Working Group 2 (WG 2) was tasked with determining essential requirements related to the identification of unmanned aircraft systems (UAS). WG 2 considered: (1) the safety and security of the National Airspace System (NAS); (2) protection of the public; (3) accountability of UAS manufacturers and consumers; (4) ease of use for UAS remote pilots, manufacturers, owners and public safety officials; (5) privacy concerns; (6) ease for specific stakeholders (media, government agencies, etc.) to enter airspace otherwise off-limits to UAS; (7) service to the public; and (8) protection of critical infrastructure. The recommendations proposed by WG2 also considered the need to identify specific requirements while also attempting to account for technology advancements in the future regarding UAS equipment, payload capacity, size, speed, and capabilities. This document will not only articulate the requirements by public safety and other stakeholders to identify and track UAS, but also provide the rationale WG 2 used to arrive at those conclusions.

WG 2 discussed the need to identify and track UAS. The focus of WG 2 was public safety official needs; however, it was understood that like any public safety need, considerations of the numerous stakeholders served by public safety officials were paramount.

In exploring the requirements that would be necessary for public safety and other designated officials to adequately identify and track UAS in order to ensure safety and promote accountability, WG 2 held robust discussions and explored dozens of potential scenarios and use cases. Through this process, we were able to determine that there are two general categories of UAS ID and tracking needs. The classifications are incident investigation and active monitoring of heightened awareness areas.

The incident investigation category involves all scenarios where an individual wishes to inquire about the identity and purpose of a sighted UA. In this category, there would be types of information available depending on the authorization level of the individual making the inquiry. For example, a member of the public who witnesses a UA over their

¹ Law enforcement, command and control personnel, and incident management and first responders

home can utilize the designated identity technology to determine the unique identifier of that particular aircraft. Depending on the behavior and information provided, that individual could then contact public safety officials, who would be able to respond and retrieve additional information to determine whether enforcement or some form of compliance action such as education is warranted.

The second category addresses the need to have dynamic and active awareness of UAS near heightened awareness areas. These areas could include: airports, heliports, prisons, military installations, nuclear facilities, large stadiums and other critical infrastructure locations, where a UAS could potentially pose an imminent threat to public safety and security. Stakeholders representing some of these locations expressed the need to have a system in place that would allow certain entities to be alerted when a UAS enters designated airspace near these heightened awareness areas. This would facilitate immediate identification, authentication, communication, and mitigation in areas where timely response is critical.

To achieve the goals of both categories, the working group determined that all UAS meeting the threshold requirements of the report (see section IV for threshold requirements) would need to be tracked, whether passively or actively, from commencement to termination of each operation. Information regarding the position of the aircraft, the location of the ground control station, and/or identity of the remote pilot² will help maintain a safe and secure environment for the general public and public safety officials.

III. Definitions

The Working Group relied on existing statutory and regulatory definitions as its foundation. Therefore, for purposes of its discussions and this report, WG 2 used the following terms:

Authenticate means the unique identifier reasonably confirms the identity of the UAS.

Control station means an interface used by the remote pilot to control the flight path of the small unmanned aircraft.³

Public unmanned aircraft system means an unmanned aircraft system that meets the qualifications and conditions required for operation of a public aircraft (as defined in section 40102 of title 49, United States Code).⁴

Remote Pilot means the person who manipulates the flight controls of the UAS.⁵

²The working group recognized that, in the future, unmanned aircraft may be controlled directly by computers without human intervention. However, for purposes of this discussion, the working group assumes that remote pilots are necessary to control unmanned aircraft.

³14 CFR 107.3.

⁴Section 331(4) of the FAA Modernization and Reform Act of 2012, Public Law 112-95. 126 Stat. 72.

Remote Pilot in Command means a certificated airman that has the final authority and responsibility for the operation and safety of a UAS operation.⁶

Unmanned aircraft (UA) means an aircraft operated without the possibility of direct human intervention from within or on the aircraft.⁷

Unmanned aircraft system (UAS) means an unmanned aircraft and associated elements (including communication links and the components that control the unmanned aircraft) that are required for the pilot in command to operate safely and efficiently in the national airspace system.⁸

Based on these definitions, WG 2 then sought to define the terms “Identify” and “Tracking” to better articulate the requirements necessary to address these two concepts.

Identify: The ability to establish the identity of a specific UAS and its associated owner and remote pilot.

Tracking: The ability to discover, identify, and know the dynamic position of a UAS in near-real time.

IV. Unmanned Aircraft that Must Comply

Working Group Two recommends that UAS with any of the following characteristics must comply with UAS ID and tracking requirements:

1. Ability of an aircraft to navigate between more than one point without direct and active control of the pilot.
2. Range from control station greater than 400', *and* real-time remotely viewable camera.

Note 1: WG 2 discussed additional requirements as a means to define the thresholds. However, the final requirements were based upon capabilities of the UAS vice other factors such as the operational use of the UA. WG 2 also discussed whether the onus to provide ID and track data fell with the manufacturer or the operator. The general consensus is capabilities built into the UAS will offer greater opportunity for compliance versus voluntary information provided by the operator.

Note 2: WG 2 also discussed the idea of creating a separate threshold for toys. The working group recognized the second criteria would encompass many toys. WG 2

⁵ See 14 CFR 107.12.

⁶ Operation and Certification of Small Unmanned Aircraft Systems, June 28, 2016, 81 FR 42064, 42087.

⁷ *ID.*

⁸ Section 331(9) of the FAA Modernization and Reform Act of 2012, Public Law 112-95. 126 Stat. 72.

discussed exempting UAS that meet the ASTM F963 toy standard, and subsequently are eligible to be sold in the toy aisle, from the ID and tracking requirements above. There was no consensus of whether these toys should be exempt. Radio controllers are getting better, toys are flying farther, and capabilities of toy UAS are getting more advanced.

WG 2 recognizes the benefit of acknowledging that toys are different from the highly capable military systems and the desire to distinguish toys from the low end of commercial UA manufacturers. However, there was no consensus on how to separate toy UAS from the total UAS population, given that even small UAS can be used maliciously, whether to invade private areas or deliver harmful substances.

V. Impacts to Safety and Security from Unmanned Aircraft:

While the majority of UAS will be operated in compliance with operational regulations, non-compliant or unauthorized UAS operations must be adequately addressed to ensure the safety and security of the NAS, critical infrastructure, and people on the ground.

At the core of the concern regarding UAS operations is accountability. With manned aircraft there is a pilot who is easily identifiable, and often in two-way communication with air traffic control. The intent of the flight is known. However, with UAS operations, identifying the pilot to determine intent may be more problematic especially if the pilot is operating beyond line of sight, or if the UAS is operating in an autonomous mode. The anonymity of the remote pilot is the central concern. In addition, the manned aircraft is normally equipped with a transponder which is transmitting a unique flight code allowing air traffic to track the aircraft electronically. At present the primary method for LE and public safety officials to track a UA in flight is visually. A unique identifier that is available electronically would support both identification and tracking.

The key considerations for WG 2 in determining the requirements necessary for identifying and tracking a UAS were:

1. Public safety: Assist responding public safety officials in identifying the owner and operator of UAS being used to harass others or rogue UAS over crowds, during large athletic events, or at disaster or crash scenes where other manned aircraft are responding.
2. Aviation safety: Avoid conflict with manned aircraft and safely integrate UAS into the NAS by providing the UA the ability to operate BLOS and autonomous with a UTM architecture.
3. National security: Support security for critical infrastructure, such as nuclear power plants or military sites where there has been evidence of UA attempting to perform persistent surveillance. Similarly, there is evidence of UA being used autonomously, or flown beyond visual line of sight to fly drugs across the southern border, or to deliver contraband inside prisons.

The working group considered other factors such as weight, inertia, speed, payload, and waivers (R&D, experimental, etc.) as potential discriminators to define thresholds requiring ID and tracking. However, as previously stated, the final requirements were based upon capabilities of the UAS vice other factors such as the operational use of the UA. General consensus is that capabilities built into the UAS that support ID and tracking will offer greater opportunity for compliance versus voluntary action or information provided by the operator.

VI. Types of Data Requested from Each Unmanned Aircraft

This report first describes the types of data that are to be made available⁹,¹⁰ regarding the unmanned aircraft or associated control station, and then describes who has access to what data under what circumstances.

The following types of data must be made available:

1. The unique identifier of the UA.
2. Tracking information for the UAS, including aircraft position and control station location.
3. Identifying information of the UAS owner and remote pilot.¹¹
4. Mission type (voluntary).
5. Pre-planned navigation data. (voluntary)
6. Operating status¹² of the UA (voluntary).

Below is an explanation of each type of data.

1. Unique identifier of the UA

The requirements of the unique identifier are that it is specific to the UA, continuously made available in near-real time, both electronically and physically readable, tamper-resistant, and easily accessible.

⁹ The working group considered requiring that the information be broadcast but was concerned that the term “broadcast” could be limiting regarding the technology used.

¹⁰ In discussing how data could be made available, the working group originally assumed that information regarding the position of the unmanned aircraft would be transmitted by the unmanned aircraft, and information regarding the location of the control station would be transmitted by the control station. However, so long as the information regarding the aircraft and the control station is accurate and provided in near real-time, the working group determined that the source of the transmission of the information is immaterial. The working group concluded that data could be transmitted directly from the aircraft, could be transmitted from the control station, or could be transmitted from other sources.

¹¹ The working group notes that it uses the term remote pilot to reference both the remote pilot in command who has ultimate operational responsibility, as well as any remote pilot manipulating the controls of the UAS. The phrase “remote pilot” in this context references both persons in all situations.

¹² Operating status of the UA may include such information as the mode the UA is currently operating (e.g., return home) or whether it has lost link with the ground controller. Information included in the operating status may vary depending on the type of operation the UA is performing.

The **first** requirement is for the identifying information to be unique to the UA itself (e.g., CTA standard). The unique identifier should be assigned specifically to the UA and become part of the UA's certificate of registration (if registration is required). Unique identifiers will allow public safety officials to identify the specific UA and, if more information is warranted, subsequently determine the owner. Unique identifiers also protect the privacy of the UAS owner or remote pilot because the unique identifier alone will not contain any personal identifying information, such as a name, date of birth, or address.

Unique identifiers also provide a means by which to facilitate airspace access. For example, in areas subject to UAS flight restrictions, such forest fires, access could be granted on a targeted basis to specific operators authorized to fly in those conditions, (e.g., government agencies, media, etc.). The unique identifier would therefore assist UAS remote pilots by allowing them access to otherwise restricted areas, while also providing assurance to ground personnel that the UAS has permission to operate in the area.

The **second** requirement is for the unique identifier to be continuously (near-real time) available upon commencement to termination of flight. This can provide early notification that a UAS may soon be operating in the area. In cases of large public gatherings, restricted areas, or proximity to airports, this provides stakeholders responsible for public safety an indication that a UAS may become a hazard.

The **third** requirement is for the unique identifier to be available in both electronic and physical form. The electronic information should be in a standardized form that is easily accessible, such as over Wi-Fi, or other inexpensive technologies. In addition to making the unique identifier available electronically, the unique identifier must also be physically located on the unmanned aircraft.¹³ This would provide owners, remote pilots, and others with access to the unique identifier even when the UA is not powered on. The physical identifier could be an FAA approved data plate, dependent on size of the UA, but needs to be affixed for the duration of operation. The unique identifier should be assigned to the UA in a way that makes it tamper resistant.

The **fourth** requirement is that the unique identifier must be easy to access. This means the information made available regarding the unmanned aircraft and the control station must be receivable through currently available devices or low cost, portable equipment. For example, smart phones or a similar hand held device can search for Wi-Fi/RF signals in range of the device. If a UAS is broadcasting its unique identifier over Wi-Fi/RF, any device that can search and receive the signals will be able to discern the unique identifier. This also means that unique identifiers on the UA must be easily accessible on the aircraft.

¹³ 14 CFR 48.205.

2. Tracking information for the UAS

Tracking information is a key piece to enable effective UAS integration into the National Airspace System. Tracking is required to support safe separation between aircraft. In manned aircraft, air traffic controllers have the ability to talk with the pilot in command in real time in order to discern their intent. However, there is currently no two-way communication in real time between UAS and air traffic or other pilots. Whenever there is an issue or concern with a UAS, the process is to notify public safety officials to initiate actions to locate the UA as well as the remote pilot to enable discussion or intervention to terminate the flight.

Historical tracking information is a necessity. It may be the key to locating the remote pilot. If a UA has already landed and is no longer visible when public safety officials arrive on-scene following an incident, the last known flight track of the UA will provide these first responders with a geographic starting or termination point that will help locate the remote pilot. If the UA has crashed and public safety officials recover the aircraft without finding the remote pilot, they will be able to use the unique identifier located on the UA to identify the registrant and subsequently the pilot and would be able to use the tracking information to help determine the cause of the accident or incident.

In addition, tracking information provides definitive answers as to whether the UA entered unauthorized airspace or not. After the fact, historical flight tracking could support potential enforcement actions. Also, tracking information could support counter-UAS systems, should those systems become widely available and lawful to use.

WG 2 recommends tracking information include *both* the position of the unmanned aircraft *and* the location of the control station, which will often be the location of the remote pilot. Information about the position of the UA must include time stamp, altitude, and geographic coordinates. Information about both the position of the UA and the location of the control station must be available in near-real time from commencement to termination of the flight. Currently, the biggest challenge facing public safety officials when responding to matters regarding UAS activity is their inability to locate the operator of a UAS that is causing concern or risk to the safety of the public or the airspace system. Having tracking information from the UA and the control station will allow public safety officials to link a specific UA to a specific control station and will enable them to conduct investigations and pursue enforcements when necessary.

Flight tracking information will allow people on the ground to identify qualifying UA. But electronic identification standards are not enough. Qualifying UA must also be sufficiently visible to the naked eye. Working Group Two recommends that FAA consider requiring high-visibility features (lighting, paint, etc.) on UA that meet the threshold category.

3. Identifying information of the UAS owner and remote pilot

In establishing a remote ID and tracking system, it is important to protect the privacy of UAS owners and operators. At the same time, given the risks associated with UAS operations, airspace management and public safety authorities must have the ability to identify owners and remote pilots when necessary. For that reason, Working Group Two recommends that each UA's unique identifier should be linked to limited forms of personally identifiable information (PII) about the unmanned aircraft's owner and remote pilot. That information would include names, dates of birth, addresses, gender, and phone numbers. The ability to readily have PII available is necessary to ensure the public's safety and protect UAS owners from mistaken identity. In essence, having an appropriate amount of data included in the PII will help filter false positives.

Importantly, this information should be available only to authorized users for purposes of official business. WG2 expects that public safety and airspace management personnel would have access to the extent required to perform their functions. Due to the sensitivity of this information, the systems in which it is stored and accessed must be highly secure. The system will also need to incorporate authentication measures to ensure that the information is correct.

Identifying information is often of vital importance. In instances when a dangerous situation exists or is developing, contact with the remote pilot can help ensure the protection of the public and impede or defuse a potential catastrophic incident from occurring. For example, if a medical transport helicopter must land near a UA, first responders must have the ability to promptly identify and contact the UAS remote pilot. Likewise, in cases where UAS are operated in an unsafe manner, the ability to quickly determine the operator's motivation, intent and or identify potential witnesses to an incident becomes important for investigative purposes.

The ability to identify the remote pilot in command serves as an additional mechanism for public safety officials to determine if the pilot is authorized to operate in the area.

4. Mission type (voluntary)

Unmanned aircraft are flown for numerous reasons such as hobby, commercial, sport, security, etc. New uses are being devised daily. With each new use, there is a mission profile which would characterize the flight path of the UA. The UAS operator may wish to voluntarily share the mission type by loading it into the data base that public officials could access during their response to an event, so that the responders would be able to determine if the UA was operating within the boundaries of this mission profile or not. For example, if a UA is used for pipeline inspection, first responders would expect to see a UA operating along a section of pipeline, and even hovering over a section of pipeline to provide a closer analysis. Mission type focuses more on the type of operation and may or may not include pre-planned navigation points.

5. Pre-planned navigation data (voluntary)

If possible, authorities would like access to pre-programmed navigation or flight plans. This voluntarily provided information could help with threat discrimination and emergency response. For example, if a UAS was determined to pose a safety hazard and the likely future flightpath or destination was known, authorities could properly position resources for interdiction, coordinate evacuations or relocate other assets for protection or response.

6. Operating status (voluntary)

There are many other tidbits of information currently relayed between the UA and the controller which may provide some insight into the current operations of the UA. Many of these bits of information could be referred to as the telemetry data. Telemetry data may include the current flight status of the UA, position of the UA, battery level, and so on.

Accessing the telemetry data will provide additional clues into understanding the intent of the UA. For example, if a UA flies through a restricted area, and the public official is able to query the UA on its status and determines the UA is in a return home mode, the official can follow the UA to the return home location with the expectation of locating the operator.

VII. Access to Data

Access to information made available by the unmanned aircraft and control station should be in accordance with the role and responsibility of the individual(s) seeking the information. The working group determined there should be at least three levels of access to the information either broadcast or captured and contained in the appropriate database; that is information available to the (1) public, (2) designated public safety and airspace management officials and (3) FAA and certain identified Federal, State, and local agencies.

A. Public Access

Certain information should be available to the public at large. Specifically, the working group determined that the unmanned aircraft unique identifier should be available to the public. In making this determination, WG 2 assumes that the method by which the unique identifier is made available is readily accessible and available to the public at minimal to no cost.

Public access is invaluable. Similar to a license plate on a vehicle, the public-facing unique identifier provides a means for the public, as well as public safety officials, to identify a specific UAS. Such a system would provide a means by which individuals can report UAS that are operating in a suspicious, dangerous, or unauthorized manner. It would also help to protect UAS owners and remote pilots by reducing the likelihood that compliant operations could be mistaken for non-compliant activities.

If the identifier is composed of alphanumeric characters without visible personally identifiable information (PII), it can be made public while protecting the privacy of the registrant.

B. Designated Public Safety Officials

The working group determined that access to the PII information should be limited to law enforcement and similarly regulated public safety entities, including airspace management officials. While the working group did not specify a method by which this data must be made available, it could be retained in a central database, much like other forms of records accessible to law enforcement personnel, and accessed upon appropriate need in a particular case.

Additionally, WG 2 believes these categories of authorized also require access to tracking information, at least in the vicinity of their respective area of operations. This information will enhance the ability of public safety authorities to respond to incidents and mitigate risks to safety and security.

C. Federal, State, and local agency and FAA Access

The working group assumes that FAA will maintain the records and permit access to authorized users only for official purposes. For example, the data should be available to other Federal, State, and local agencies, and, after appropriate vetting, other designated personnel who may require access. Agencies may include, but are not necessarily limited to, the National Transportation Safety Board; Federal security agencies; and State, local and tribal law enforcement agencies.

VIII. Data authentication and retention

It was also determined that all relevant tracking data should be retained for a reasonable period of time to allow public safety and other authorized users to have access to information critical to investigations.

WG 2 suggested that this requirement could closely mirror applicable data retention standards in manned aviation.

IX. Other Considerations

Finally, WG 2 recommends the remote ID and tracking system include reasonable accommodations to protect the operational security of certain governmental UAS operations, consistent with accommodations provided to governmental operations in the manned space. For operational security purposes, some UA may have their unique identifier masked. Special procedures need to be defined to support these limited types of operations.

X. Appendix – Use Cases

The use cases included in this appendix are provided to add context to the discussions surrounding law enforcement needs regarding the identification and tracking of UAS. These use cases are not all-encompassing; instead, they are intended to illustrate some of the most pressing issues faced by public safety personnel.

Local sheriff responds to a call about a UAS in a firefighting zone interfering with manned aircraft attempting to drop retardant in a very rural area with no cellular coverage.

Currently, law enforcement officials have little information to adequately respond to this type of call because the average flight time for consumer UAS is short and the UAS is generally no longer in flight by the time a law enforcement officer can report to the scene. Because the fire command post has no access to information about the UAS, they are unable to provide any actionable details for law enforcement to follow up on. If the UAS were broadcasting a unique identifier, the first responders could provide that information to the law enforcement officer. The law enforcement officer can contact the operator to prevent interruption of firefighting efforts. Because there is no cellular coverage in the area, the unique identifier may need to be broadcast or attainable through redundant means.

A UA is illegally flying over a large crowded event like a parade or marathon.

Public safety officials can quickly mitigate any real or perceived threat in situations like this by quickly identifying the presence of an unknown UAS and tracking it to the control station so that the operator can terminate the flight. If the situation escalates, law enforcement can take necessary action by using the unique identifier to promptly access information about the registered owner and can use the tracking data to monitor the flight path which may enable them to take necessary action to preclude an incident. If the situation results in recommended criminal or civil action, the ID and Tracking information can be used to establish evidence.

Government agencies respond to a UA flying over the US Capitol Building.

UAS are prohibited from flying in the FRZ. Capitol Police should be able to quickly track the UAS to its control station or starting point so that the operator can terminate the flight. The ID and Tracking information will be used for evidence if further action is warranted.

A collision on an interstate highway results in multiple injuries. There are reports of two UA of unknown origin in the immediate vicinity that will be a danger to the air ambulance helicopter when it arrives. In addition, news media have asked to fly their UA to capture video of the accident.

There have been several documented cases where an air ambulance helicopter has had to terminate or delay operations due to the presence of unknown UA flying in the vicinity. In these cases, patient care could be delayed or reduced resulting in additional medical

issues or death. This situation is made more complex because first responders are focused on the task at hand and do not have the resources to scan the area for UAS and attempt to find the operators. That strategy is also ineffective because UAS have a small footprint and may be difficult to spot or track with the eye, so it would be difficult to determine with a high degree of confidence if the area is clear. Similarly, air rescue helicopters conducting hoist or other external load operations have been delayed and canceled because of the presence of UA. This results in rescues being delayed and adds risk to victims and rescuers.

This situation can be managed or mitigated in the future if the ground or flight personnel had access to ID and Tracking information for each UAS in the area. Using the ID information, the first responders can be made immediately aware of the number of UAS in the area. From there they can attempt to locate or contact the operators with the readily available information so that they can terminate the flight or move to a location away from the helicopter. Short of that, the tracking information can be used to determine the position and proximity of the UAS flights to the helicopter's flight path so that the pilot may attempt to navigate to the scene safely. Additionally, the first responders may be able to create a transgression zone so that they can receive active alerts when UAS enter a certain area. In this case, the news UASs would likely be able to enter the zone while the unknown UASs would not.

Appendix D Responses and Voting Results

Voting Member:	Mark Aitken
Company Name:	AUVSI
Date Received:	10/2/17
Response:	I concur with the final report as written with the following exceptions:

AUVSI's Comments about the Recommendations by the FAA's UAS Identification and Tracking Aviation Rulemaking Committee

Date: September 30, 2017

Re: Section 6.1 – Applicability of ID and Tracking Requirement

AUVSI concurs with the FAA's UAS Identification and Tracking Aviation Rulemaking Committee's (ARC) final recommendation report, except for Section 6.1. As a member of the ARC, AUVSI's position is that all UAS operators – whether flying for civil, commercial or recreational purposes – must comply with remote ID and tracking requirements, with no exceptions. We also urged the ARC to apply the weight-based threshold that was established under the original UAS registration requirement to remote identification. Linking these two requirements is paramount for interoperability and increasing compliance among users.

We are disappointed that the ARC's recommendations do not reflect this approach to better address concerns by federal security agencies. Establishing remote ID standards for all UAS operators and requiring they register with the FAA will help enhance the safety and security of the national airspace. But, with the ARC recommending that some operators be exempt from these standards, future regulations that are needed to enable the UAS industry's growth may be stalled.

AUVSI looks forward to working with the FAA to address these concerns, which are shared by other ARC stakeholders that raised similar issues with the final report, including the Commercial Drone Alliance, General Aviation Manufacturers Association, and Aerospace Industries Association.

Voting Member:	Jack Barker
Company Name:	Farris Technology
Date Received:	10/5/17
Response:	I concur with the final report as written

Voting Member:	Jon Beatty
Company Name:	Flight Safety Foundation
Date Received:	10/2/17
Response:	I concur with the final report as written with the following exceptions:
<p>The Flight Safety Foundation (FSF) commends the ARC for its comprehensive report and recommendations. FSF concurs with the final report as written with the following exceptions:</p> <p>The final report should recommend Option 1 for applicability of the tracking/ID requirements—i.e., applicability to all UAS with certain exceptions. Applicability Option 2—applying the tracking/ID requirements to only those UAS that have certain capabilities (i.e., point-to-point without pilot control; 400 ft.+ range)—insufficiently addresses safety and security when considering the mobility of UAS systems. For example, a small UAS could be operated in the vicinity of an airport without having to comply with the tracking/ID requirements. For this same reason, FSF recommends removing exceptions 1 (within VLOS and no further than 400 feet from the remote pilot) and 2 (model aircraft) from Option 1.</p> <p>The final report recommends that information held by third-party providers (TPP)/UAS service suppliers (USS) be governed by restrictive use conditions imposed on the TPP/USS related to the use and dissemination of any data and information collected. Page 35. The recommendations also indicate that “all relevant tracking data” will be accessible to “authorized users” and that the FAA should address privacy with regards to historical tracking information. Pages 47-48. FSF considers that the availability of certain flight information, such as historical tracking information, to be critical for the industry to assess safety hazards and to respond to prevent such hazards. FSF submits that restrictions on the dissemination and use of such information should allow for the accessibility and use of such information when the purpose is to improve aviation safety. FSF recommends that the final report promote the availability and use of tracking information for safety purposes.</p>	

Voting Member:	Greg Belaus
Company Name:	AT&T
Date Received:	10/2/17
Response:	I concur with the final report as written

Voting Member:	Ted Branch
Company Name:	Drone Aviator, Inc.
Date Received:	10/2/17
Response:	I concur with the final report as written

Voting Member:	Sean Cassidy
Company Name:	Amazon Prime Air
Date Received:	10/2/17
Response:	I concur with the final report as written with the following exceptions:

A significant number of ARC members felt that 1) a weight-based threshold should have been included as a threshold criteria, and 2) those operating under 14 CFR part 101 should not be excluded from future ID and tracking requirements. Since a significant number of members felt strongly enough about one or both of the aforementioned items to warrant mention of those concerns as a note of dissent in the preamble to the options, my belief is the recommendations as currently worded do not accurately capture the sentiments of the ARC absent an additional choice. I believe section 6.1, pages 31-32 of the final recommendations report should have been modified to capture a third option- one that does not exempt operations conducted under CFR Part 101 from ID and tracking **and** includes operations flown outdoors with vehicles weighing over 250 grams.

Voting Member:	Diana Marina Cooper
Company Name:	PrecisionHawk
Date Received:	10/2/17
Response:	I concur with the final report as written

Voting Member:	Gabriel Cox
Company Name:	Intel Corporation
Date Received:	10/2/17
Response:	I concur with the final report as written

Voting Member:	Mark DeAngelo
Company Name:	SAE International
Date Received:	10/2/17
Response:	I concur with the final report as written

Voting Member:	Bud Devillers
Company Name:	GlobalStar
Date Received:	10/2/17
Response:	I concur with the final report as written

Voting Member:	Lisa Ellman
Company Name:	Commercial Drone Alliance
Date Received:	10/2/17
Response:	I non-concur with the final report as written:

DISSENT TO SECTION 6.1 OF THE COMMERCIAL DRONE ALLIANCE, THE GENERAL AVIATION MANUFACTURERS ASSOCIATION, THE AEROSPACE INDUSTRIES ASSOCIATION, THE NATIONAL AGRICULTURAL AVIATION ASSOCIATION, X, GE, uAVIONIX, FORD MOTOR COMPANY, AIRMAP, AND GENERAL ATOMICS

The Commercial Drone Alliance (“the Alliance”)¹, the General Aviation Manufacturers Association (“GAMA”)², the Aerospace Industries Association (“AIA”)³, the National Agricultural Aviation Association (“NAAA”)⁴, X, GE, uAvionix, Ford Motor Company, AirMap, and General Atomics respectfully submit this **Dissent** from the recommendations and discussion of the UAS ID and Tracking Aviation Rulemaking Committee (“ARC”) in Section 6.1 (“Applicability of the ID and tracking requirements”) of the ARC’s Final Report (“Report”), dated September 30, 2017.

These organizations appreciate the extensive efforts of the ARC, but strongly disagree on the critical point of who and what UAS should have to comply with ID and Tracking requirements.

Specifically, these organizations **dissent** from the Report because:

(1) it recommends that the FAA consider an Option 1 that expressly exempts model aircraft from UAS ID and Tracking;

¹ The **Commercial Drone Alliance** is an independent 501c6 non-profit organization led by key members of the commercial drone industry. The Alliance seeks to advance commercial drone technology and policy. The Alliance actively participated as a member of the ARC in the Plenary sessions, Working Group (“WG”) 3, and the Final Report’s writing committee. It has provided verbal comments during these meetings and written comments throughout the process.

² The **General Aviation Manufacturers Association** exists to foster and advance the general welfare, safety, interests and activities of the global business and general aviation industry. This includes promoting a better understanding of general aviation manufacturing, maintenance, repair, and overhaul and the important role these industry segments play in economic growth and opportunity, and in serving the critical transportation needs of communities, companies and individuals worldwide.

³ The **Aerospace Industries Association** (AIA), founded in 1919, represents more than 340 major aerospace and defense companies and their suppliers, embodying every high-technology manufacturing segment of the U.S. aerospace and defense industry including commercial aviation and avionics, manned and unmanned aircraft systems, space technologies and satellite communications.

⁴ The **National Agricultural Aviation Association** works to support the agricultural aviation industry which is made up of small businesses and pilots that use aircraft to aid farmers in producing a safe, affordable and abundant supply of food, fiber and biofuel, in addition to protecting forestry and controlling health-threatening pests.

- (2)** it recommends that the FAA also consider an Option 2 with a narrow capabilities-based threshold that effectively exempts a large segment of model aircraft/UAS from UAS ID and Tracking; and
- (3)** it did not include a recommendation for a risk-based weight threshold for UAS ID and Tracking.

The Alliance, GAMA, AIA, NAAA, X, GE, uAvionix, Ford Motor Company, AirMap, and General Atomics are strongly supportive of the goals of the UAS ID and Tracking ARC, and, to that end, each actively participated in the ARC and its working groups. Indeed, these organizations consider UAS ID and Tracking to be a critical prerequisite for unleashing the enormous potential of the commercial UAS marketplace. UAS ID and Tracking is necessary now to expand UAS operations which essentially remain grounded until the law enforcement and national security communities are comfortable with their ability to identify and track UA. Just as a high degree of UAS owner/operator compliance is necessary for any UAS ID and Tracking regulation to be successful, it is likewise imperative that any such regulations encompass all but the smallest and most unsophisticated UAS in order to be effective. Any common-sense threshold must also focus primarily on risk rather than operator intent. However, a model aircraft exemption (Option 1), a narrow capabilities-based threshold for ID and Tracking compliance (Option 2), and the lack of a weight-based threshold fly in the face of these principles, and will have adverse implications for the safety and efficiency of the National Airspace System (“NAS”), public safety, and the efficacy of future UAS Traffic Management (“UTM”) systems. Our organizations note that other ARC members, including the Air Line Pilots Association and Association of Unmanned Vehicle Systems International, have stated similar concerns separately.

(1) Model Aircraft Should Not Be Exempt from ID and Tracking (Option 1). The ARC Report recommends that the FAA consider exempting a large segment of the UAS community from complying with future ID and Tracking regulations by carving-out unmanned aircraft “operated in compliance with 14 CFR part 101, unless the unmanned aircraft is equipped [with certain technology]”. [ARC Report, Section 6.1, pages 31-32.] ***The Alliance, GAMA, AIA, NAAA, X, GE, uAvionix, Ford Motor Company, AirMap, and General Atomics firmly oppose any such carve-out for model aircraft and hobbyists.***

This exemption is a loophole that swallows the rule. It would permit a huge segment of the UAS community to avoid participating in the UAS ID and Tracking system and complying with the corresponding ID and Tracking regulations. For example, the Academy of Model Aeronautics (“AMA” or “modelers”) reportedly represents more than 195,000 modelers worldwide.⁵ The FAA Aerospace Forecast (fiscal years 2017-2037) estimates that there were approximately 1.1 million units of distinctly hobbyist sUAS or model aircraft in 2016, with significant growth projected in the next few years to 2.75 million (low), 3.55

⁵

<http://www.modelaircraft.org/aboutama/whatisama.aspx>

million (base case) or 4.47 million (high case) such units in 2021.⁶ By contrast, that same Forecast estimates that the non-hobbyist (commercial) fleet is smaller, with approximately 42,000 units in 2016, with growth projected in the next few years to 238,000 (low), 422,000 (base case) or 1.61 million (high case) such units in 2021.⁷ Moreover, this exemption provides many operators having no intent to comply fully with Part 101 with cover for not following ID and Tracking regulations. If, as envisioned by Option 1 in Section 6.1, such a huge segment of the UAS community is not subject to the ID and Tracking regulations, there will be direct, adverse implications for the safety and efficiency of the NAS, public safety, and the efficacy of future UTM systems.

Moreover, the carve-out for model aircraft operated under Part 101 (and in compliance with Section 336) is also flawed in that public safety officials will not be able to discern whether a particular UAS flying nearby is compliant with the regulations in accordance with the carve-out or operating nefariously by not providing positive ID and Tracking. The public safety official simply will not know the operator's intent and will not be able to determine if enforcement activity is appropriate. Inability to positively ID and track UAS large enough to interfere with manned flight and public safety operations, as well as harm non-participants through direct kinetic impact, limits public safety officials in their ability to enforce safe UAS statutes and regulations.

In addition, as a matter of process, this carve-out for model aircraft and hobbyists was a relatively last-minute addition to the ARC Report. The focus of debate on the applicability of UAS ID and Tracking had been on the approach that WG2 developed, which did not include an express carve-out for model aircraft. [See ARC Report, Section 5.2.3, page 29.] As a result, this carve-out did not receive proper broad discussion by the ARC.

(2) The Narrow Capabilities-Based Threshold Is Not Sufficiently Inclusive (Option 2). The ARC Report also recommends that the FAA consider carving out a large segment of the UAS community from having to comply with future ID and Tracking regulations by using a narrow capabilities-based threshold. Specifically, under this Option, only UAS with (i) the ability to navigate between more than one point without direct and active control of the pilot, or (ii) a range from the control station greater than 400' and a real-time remotely viewable sensor will have to comply under the ARC's recommendation. [ARC Report, Section 6.1, pages 31-32.] ***The Alliance, GAMA, AIA, NAAA, X, GE, uAvionix, Ford Motor Company, AirMap, and General Atomics firmly oppose any such narrow capabilities-based approach which effectively amounts to a model aircraft/hobbyist exemption and excludes a huge segment of UAS from compliance with future ID and Tracking regulations.***

As with the flawed Option 1 (discussed above), this narrow capabilities-based approach is essentially a loophole that swallows the rule. The AMA represents nearly

⁶

FAA Aerospace Forecast (2017-2037), at 30-31.

⁷

FAA Aerospace Forecast (2017-2037), at 32.

200,000 members, and the FAA Aerospace Forecast (fiscal years 2017-2037) estimates that there will be 2.75 million – 4.47 million units of distinctly hobbyist sUAS or model aircraft in 2021. The ARC’s recommendation would permit a huge segment of the UAS community to avoid participating in the UAS ID and Tracking system and complying with the corresponding ID and Tracking regulations, thereby having direct, adverse implications for the safety and efficiency of the NAS, public safety, and the efficacy of future UTM systems.

Moreover, this narrow capabilities-based threshold is flawed in that public safety officials will not be able to discern whether a particular UAS flying nearby has autonomous capabilities or sensors and thus is compliant in not providing ID and Tracking, or whether it is a nefarious operator warranting further investigation. The public safety official simply will not know the vehicle’s capabilities and will not be able to determine if enforcement activity is appropriate. Inability to positively ID and track a huge segment of UAS that could interfere with manned flight and public safety operations, as well as harm non-participants through direct kinetic impact, limits public safety officials in their ability to enforce safe UAS statutes and regulations.

(3) There Should Be A Weight-Based Threshold For UAS ID And Tracking. The Alliance, GAMA, AIA, NAAA, X, GE, uAvionix, Ford Motor Company, AirMap, and General Atomics strongly advocated for a weight-based threshold: As a general rule, any UAS or model aircraft weighing 250 grams or more must comply with the ID and Tracking regulations.

Yet, although the ARC Report recommends that the FAA consider two fundamentally flawed thresholds for compliance with any UAS ID and Tracking requirements (Options 1 and 2 in Section 6.1), it did not recommend that the FAA consider a weight-based threshold. This omission is glaring because there are several principal arguments in favor of such a weight-based approach.

First, it is **simple, adaptable, and enforceable**, each of which promotes compliance, which in turn promotes the safety and efficiency of the NAS, thereby enabling sustained growth and innovation to succeed without compromising the safety of the world’s leading aviation system.

Second, it is **familiar** insofar as other UAS-related ARCs have found merit in using a weight-based applicability threshold. For example, the UAS Registration Task Force ARC concluded that a weight-based approach was appropriate because it was easy to understand and apply and would therefore encourage compliance, and the Micro UAS ARC later adopted the same weight-based threshold for exclusion from performance-based standards for operations over people.

Third, it is **comprehensive**, properly encompassing the majority of UAS except for very small and unsophisticated UAS, thereby supporting robust UTM systems. In order to take advantage of the safety benefits of UAS and grow the commercial UAS industry

exponentially, a basic level of compliance is critical for the viability of successful UTM systems. The more vehicles participating in these UTM systems with UAS ID and Tracking, the more successful UTM efforts will be.

Fourth, it is an applicability threshold which is **future-proofed** to accommodate technological developments without need to constantly revisit the threshold levels.

Fifth, it would **close the massive gaps** in UAS ID and Tracking inherent in the model aircraft carve-outs and capabilities-based applicability threshold in the ARC's recommendation in Section 6.1.

A basic weight threshold is the easiest and most logical way to ensure that UAS ID and Tracking requirements bear some reasonable relationship to the aviation, public safety, and security risks presented, and its simplicity will help promote compliance. Adopting this approach would also properly focus on risk of operation rather than operator intent and would streamline implementation.

The Alliance, GAMA, AIA, NAAA, X, GE, uAvionix, Ford Motor Company, AirMap, and General Atomics understand that certain local law enforcement members of the ARC were of the view that some UA weighing less than 250 grams with certain technological enhancements (i.e., autonomous navigation; equipped with real-time downlinked remote sensor enabling beyond visual line of sight operations) may nonetheless present possible security/safety issues. We appreciate the input of law enforcement and support additional separate and independent thresholds such as these whereby, if necessary, UA weighing less than 250 grams would also be required to comply with the ID and Tracking regulations.

In sum, it is our considered view that the exemptions for a massive segment of the UAS industry from UAS ID and Tracking requirements (whether through an express model aircraft carve-out or an overly narrow capabilities-based threshold) and the lack of a weight-based threshold for such compliance greatly undermine the value, benefits, and utility of UAS ID and Tracking, not to mention jeopardize the safety of the airspace and comprehensiveness of any future UTM.

The Alliance, GAMA, AIA, NAAA, X, GE, uAvionix, Ford Motor Company, AirMap, and General Atomics therefore dissent from (i) the ARC's recommendations that the FAA consider expressly exempting model aircraft or a narrow capabilities-based threshold that effectively exempts a large segment of model aircraft/UAS from UAS ID and Tracking; and (ii) the ARC's failure to include a recommendation for a risk-based weight threshold for UAS ID and Tracking.

Voting Member:	Matt Fanelli
Company Name:	Skyward, A Verizon Company
Date Received:	10/2/17
Response:	I concur with the final report as written

Voting Member:	Steven Feldman
Company Name:	Miami Beach Police Department
Date Received:	10/4/17
Response:	I concur with the final report as written with the following exceptions: Although it is not pertinent in my jurisdictional area, I sympathize with the comments made by my fellow law enforcement officer from the Grand Forks County Sheriff's Department where he states: Executive Summary Page 4 and 6.3 Pages 35-37: Discussion of sUAS Tiers; Permitting sUAS in Tier 1 to "direct broadcast OR network publish" creates a situation in which a sUAS using only "network publish" would be undetectable in a network deprived environment. Consequently, law enforcement and the public would be unable to obtain an ID from these sUAS. Tier 1 should be required to "direct broadcast" with the addition of "network publish" being optional.

Voting Member:	Alan Frazier
Company Name:	Grand Forks County Sheriff's Department
Date Received:	10/2/17
Response:	I concur with the final report as written with the following exceptions: Executive Summary Page 4 and 6.3 Pages 35-37: Discussion of sUAS Tiers; Permitting sUAS in Tier 1 to "direct broadcast OR network publish" creates a situation in which a sUAS using only "network publish" would be undetectable in a network deprived environment. Consequently, law enforcement and the public would be unable to obtain an ID from these sUAS. Tier 1 sUAS should be required to "direct broadcast" with the addition of "network publish" being optional.

Voting Member:	Pat Gannon
Company Name:	Los Angeles World Airport
Date Received:	10/2/17
Response:	I concur with the final report as written

Voting Member:	Todd Graetz
Company Name:	BNSF Railway
Date Received:	10/1/17
Response:	I concur with the final report as written

Voting Member:	Paul Guckian
Company Name:	QualComm Technologies
Date Received:	10/2/17
Response:	I concur with the final report as written

Voting Member:	Philip Hall
Company Name:	RelmaTech Ltd
Date Received:	10/1/17
Response:	I concur with the final report as written with the following exceptions:
Page 32, Section 6.1, Option 2(2) – I strongly believe that the “Range from control station greater than 400’ <i>and</i> real-time remotely viewable sensor” provision would provide a loop-hole that would allow a UAS of any size/weight/range/capability, but <u>not fitted</u> with a real-time remotely viewable sensor, to be operated at ranges greater than 400’ from the remote control station without ID and tracking. It is my understanding that we reached consensus across the ARC that 400’ was the maximum range that Law Enforcement Officers on the scene could confidently locate the operator of a UAS without relying on ID and tracking capabilities, and irrespective of the size/weight/capability of the UAS.	

Voting Member:	Richard Hanson
Company Name:	Academy of Model Aeronautics
Date Received:	10/2/17
Response:	I concur with the final report as written with the following exceptions:
<p>Section 6.1: AMA strongly suggests that the FAA consider Option 2 as its course of action as this was the consensus recommendation of WG2 and which also approached consensus by the entire ARC at the last plenary session. Option 1 was presented as an alternative to WG2's recommendation towards the end of the last plenary session where the majority of the members were either not present due to the Interdrone conference held concurrently in Las Vegas or who had left the plenary session early to make their end of the week travel arrangements. Option 1 was never fully vetted by the entire ARC in open plenary.</p> <p>AMA is also very concerned that its submission in regards to Part 101 (P.L. 112-95 Sec 336) that was requested and included in the draft version of the report dated 9/24/2017, was subsequently removed by the writing committee and does not in any way appear in the final report.</p> <p>The ARC spent considerable time discussing the need to include or exclude operations under Part 101 from the ID & Tracking requirements. Several members of the ARC have mischaracterized Sec 336 as being a loophole that somehow gives the hobbyist/recreational flyer a means of operating outside the requirements of ID & Tracking. And, the comments submitted by several members indicate there is general and pervasive misunderstanding of the congressional intent in regards to P.L. 112-95, Sec 336.</p> <p>As the final report is mute on this subject, AMA is including its submission on Part 101 here as part of its concurrence position:</p> <p>14 CFR Part 101, Subpart E (P.L. 112-95, Sec 336)</p> <p>Unmanned aircraft operating under 14 CFR Part 101 must "operate in accordance with a community-based set of safety guidelines and within the programming of a nationwide community-based organization," and "must be flown strictly for hobby or recreational use." Such aircraft are defined as <i>Model Aircraft</i> and are by law limited to operations "within visual line of sight of the person operating the aircraft."</p> <p>Community-based organizations as defined by Congress are membership based associations that provide their members a comprehensive set of safety guidelines that underscores safe aeromodeling operations within the national airspace and the protection and safety of the general public on the ground. Such organizations act as a liaison to government agencies and are represented in this ARC.</p>	

Community-based organizations such as the Academy of Model Aeronautics have a long-standing history of safe operations, and maintain an interactive safety program that assures safe aeromodeling operations, compliance by its members to its safety guidelines, and responsible model aircraft operations at safe and appropriate locations.

Recommendation for adoption by the CBO community (AMA)

Pending the manner and means by which FAA enacts the requirements of UAS ID & Tracking, it is AMA's position that all model aircraft equipped with advanced flight systems technologies that enable the aircraft to navigate from one point to another without continuous input and direction from the pilot meet all federally mandated UAS ID & Tracking requirements.

Exception: Model aircraft that are equipped with advanced flight systems technologies strictly for safety purposes and that keep the aircraft within visual line of sight of the operator, such as a "return to home" feature, are exempt from the requirements of ID & Tracking provided these features cannot be readily altered or reprogrammed.

All model aircraft that are equipped with a real-time downlinked remote sensor that provides the pilot the capability of navigating the aircraft beyond visual line of sight must similarly meet all federally mandated UAS ID & Tracking requirements.

Note: Unmanned aircraft equipped with a real-time downlinked remote sensor and operated beyond the visual line of sight of the operator are not allowed under Part 101, are not allowed under Part 107 without waiver and as such are prohibited under current regulation and statute.

Voting Member:	Mark Hatfield
Company Name:	Miami-Dade International Airport
Date Received:	10/5/17
Response:	I concur with the final report as written

Voting Member:	Jens Hennig
Company Name:	GAMA
Date Received:	10/3/17
Response:	I concur with the final report as written with the following exceptions:

Requested to include exceptions submitted from the Commercial Drone Alliance

DISSENT TO SECTION 6.1 OF THE COMMERCIAL DRONE ALLIANCE, THE GENERAL AVIATION MANUFACTURERS ASSOCIATION, THE AEROSPACE INDUSTRIES ASSOCIATION, THE NATIONAL AGRICULTURAL AVIATION ASSOCIATION, X, GE, uAVIONIX, FORD MOTOR COMPANY, AIRMAP, AND GENERAL ATOMICS

The Commercial Drone Alliance (“the Alliance”)⁸, the General Aviation Manufacturers Association (“GAMA”)⁹, the Aerospace Industries Association (“AIA”)¹⁰, the National Agricultural Aviation Association (“NAAA”)¹¹, X, GE, uAvionix, Ford Motor Company, AirMap, and General Atomics respectfully submit this **Dissent** from the recommendations and discussion of the UAS ID and Tracking Aviation Rulemaking Committee (“ARC”) in Section 6.1 (“Applicability of the ID and tracking requirements”) of the ARC’s Final Report (“Report”), dated September 30, 2017.

These organizations appreciate the extensive efforts of the ARC, but strongly disagree on the critical point of who and what UAS should have to comply with ID and Tracking requirements.

Specifically, these organizations **dissent** from the Report because:

⁸ The **Commercial Drone Alliance** is an independent 501c6 non-profit organization led by key members of the commercial drone industry. The Alliance seeks to advance commercial drone technology and policy. The Alliance actively participated as a member of the ARC in the Plenary sessions, Working Group (“WG”) 3, and the Final Report’s writing committee. It has provided verbal comments during these meetings and written comments throughout the process.

⁹ The **General Aviation Manufacturers Association** exists to foster and advance the general welfare, safety, interests and activities of the global business and general aviation industry. This includes promoting a better understanding of general aviation manufacturing, maintenance, repair, and overhaul and the important role these industry segments play in economic growth and opportunity, and in serving the critical transportation needs of communities, companies and individuals worldwide.

¹⁰ The **Aerospace Industries Association** (AIA), founded in 1919, represents more than 340 major aerospace and defense companies and their suppliers, embodying every high-technology manufacturing segment of the U.S. aerospace and defense industry including commercial aviation and avionics, manned and unmanned aircraft systems, space technologies and satellite communications.

¹¹ The **National Agricultural Aviation Association** works to support the agricultural aviation industry which is made up of small businesses and pilots that use aircraft to aid farmers in producing a safe, affordable and abundant supply of food, fiber and biofuel, in addition to protecting forestry and controlling health-threatening pests.

- (1)** it recommends that the FAA consider an Option 1 that expressly exempts model aircraft from UAS ID and Tracking;
- (2)** it recommends that the FAA also consider an Option 2 with a narrow capabilities-based threshold that effectively exempts a large segment of model aircraft/UAS from UAS ID and Tracking; and
- (3)** it did not include a recommendation for a risk-based weight threshold for UAS ID and Tracking.

The Alliance, GAMA, AIA, NAAA, X, GE, uAvionix, Ford Motor Company, AirMap, and General Atomics are strongly supportive of the goals of the UAS ID and Tracking ARC, and, to that end, each actively participated in the ARC and its working groups. Indeed, these organizations consider UAS ID and Tracking to be a critical prerequisite for unleashing the enormous potential of the commercial UAS marketplace. UAS ID and Tracking is necessary now to expand UAS operations which essentially remain grounded until the law enforcement and national security communities are comfortable with their ability to identify and track UA. Just as a high degree of UAS owner/operator compliance is necessary for any UAS ID and Tracking regulation to be successful, it is likewise imperative that any such regulations encompass all but the smallest and most unsophisticated UAS in order to be effective. Any common-sense threshold must also focus primarily on risk rather than operator intent. However, a model aircraft exemption (Option 1), a narrow capabilities-based threshold for ID and Tracking compliance (Option 2), and the lack of a weight-based threshold fly in the face of these principles, and will have adverse implications for the safety and efficiency of the National Airspace System (“NAS”), public safety, and the efficacy of future UAS Traffic Management (“UTM”) systems. Our organizations note that other ARC members, including the Air Line Pilots Association and Association of Unmanned Vehicle Systems International, have stated similar concerns separately.

(4) Model Aircraft Should Not Be Exempt from ID and Tracking (Option 1). The ARC Report recommends that the FAA consider exempting a large segment of the UAS community from complying with future ID and Tracking regulations by carving-out unmanned aircraft “operated in compliance with 14 CFR part 101, unless the unmanned aircraft is equipped [with certain technology]”. [ARC Report, Section 6.1, pages 31-32.] ***The Alliance, GAMA, AIA, NAAA, X, GE, uAvionix, Ford Motor Company, AirMap, and General Atomics firmly oppose any such carve-out for model aircraft and hobbyists.***

This exemption is a loophole that swallows the rule. It would permit a huge segment of the UAS community to avoid participating in the UAS ID and Tracking system and complying with the corresponding ID and Tracking regulations. For example, the Academy of Model Aeronautics (“AMA” or “modelers”) reportedly represents more than 195,000 modelers worldwide.¹² The FAA Aerospace Forecast (fiscal years 2017-2037) estimates that there were approximately 1.1 million units of distinctly hobbyist sUAS or model aircraft in

¹²

<http://www.modelaircraft.org/aboutama/whatisama.aspx>

2016, with significant growth projected in the next few years to 2.75 million (low), 3.55 million (base case) or 4.47 million (high case) such units in 2021.¹³ By contrast, that same Forecast estimates that the non-hobbyist (commercial) fleet is smaller, with approximately 42,000 units in 2016, with growth projected in the next few years to 238,000 (low), 422,000 (base case) or 1.61 million (high case) such units in 2021.¹⁴ Moreover, this exemption provides many operators having no intent to comply fully with Part 101 with cover for not following ID and Tracking regulations. If, as envisioned by Option 1 in Section 6.1, such a huge segment of the UAS community is not subject to the ID and Tracking regulations, there will be direct, adverse implications for the safety and efficiency of the NAS, public safety, and the efficacy of future UTM systems.

Moreover, the carve-out for model aircraft operated under Part 101 (and in compliance with Section 336) is also flawed in that public safety officials will not be able to discern whether a particular UAS flying nearby is compliant with the regulations in accordance with the carve-out or operating nefariously by not providing positive ID and Tracking. The public safety official simply will not know the operator's intent and will not be able to determine if enforcement activity is appropriate. Inability to positively ID and track UAS large enough to interfere with manned flight and public safety operations, as well as harm non-participants through direct kinetic impact, limits public safety officials in their ability to enforce safe UAS statutes and regulations.

In addition, as a matter of process, this carve-out for model aircraft and hobbyists was a relatively last-minute addition to the ARC Report. The focus of debate on the applicability of UAS ID and Tracking had been on the approach that WG2 developed, which did not include an express carve-out for model aircraft. [See ARC Report, Section 5.2.3, page 29.] As a result, this carve-out did not receive proper broad discussion by the ARC.

(5) The Narrow Capabilities-Based Threshold Is Not Sufficiently Inclusive (Option 2) The ARC Report also recommends that the FAA consider carving out a large segment of the UAS community from having to comply with future ID and Tracking regulations by using a narrow capabilities-based threshold. Specifically, under this Option, only UAS with (i) the ability to navigate between more than one point without direct and active control of the pilot, or (ii) a range from the control station greater than 400' and a real-time remotely viewable sensor will have to comply under the ARC's recommendation. [ARC Report, Section 6.1, pages 31-32.] *The Alliance, GAMA, AIA, NAAA, X, GE, uAvionix, Ford Motor Company, AirMap, and General Atomics firmly oppose any such narrow capabilities-based approach which effectively amounts to a model aircraft/hobbyist exemption and excludes a huge segment of UAS from compliance with future ID and Tracking regulations.*

¹³

FAA Aerospace Forecast (2017-2037), at 30-31.

¹⁴

FAA Aerospace Forecast (2017-2037), at 32.

As with the flawed Option 1 (discussed above), this narrow capabilities-based approach is essentially a loophole that swallows the rule. The AMA represents nearly 200,000 members, and the FAA Aerospace Forecast (fiscal years 2017-2037) estimates that there will be 2.75 million – 4.47 million units of distinctly hobbyist sUAS or model aircraft in 2021. The ARC’s recommendation would permit a huge segment of the UAS community to avoid participating in the UAS ID and Tracking system and complying with the corresponding ID and Tracking regulations, thereby having direct, adverse implications for the safety and efficiency of the NAS, public safety, and the efficacy of future UTM systems.

Moreover, this narrow capabilities-based threshold is flawed in that public safety officials will not be able to discern whether a particular UAS flying nearby has autonomous capabilities or sensors and thus is compliant in not providing ID and Tracking, or whether it is a nefarious operator warranting further investigation. The public safety official simply will not know the vehicle’s capabilities and will not be able to determine if enforcement activity is appropriate. Inability to positively ID and track a huge segment of UAS that could interfere with manned flight and public safety operations, as well as harm non-participants through direct kinetic impact, limits public safety officials in their ability to enforce safe UAS statutes and regulations.

(6) There Should Be A Weight-Based Threshold For UAS ID And Tracking. The Alliance, GAMA, AIA, NAAA, X, GE, uAvionix, Ford Motor Company, AirMap, and General Atomics strongly advocated for a weight-based threshold: As a general rule, any UAS or model aircraft weighing 250 grams or more must comply with the ID and Tracking regulations.

Yet, although the ARC Report recommends that the FAA consider two fundamentally flawed thresholds for compliance with any UAS ID and Tracking requirements (Options 1 and 2 in Section 6.1), it did not recommend that the FAA consider a weight-based threshold. This omission is glaring because there are several principal arguments in favor of such a weight-based approach.

First, it is **simple, adaptable, and enforceable**, each of which promotes compliance, which in turn promotes the safety and efficiency of the NAS, thereby enabling sustained growth and innovation to succeed without compromising the safety of the world’s leading aviation system.

Second, it is **familiar** insofar as other UAS-related ARCs have found merit in using a weight-based applicability threshold. For example, the UAS Registration Task Force ARC concluded that a weight-based approach was appropriate because it was easy to understand and apply and would therefore encourage compliance, and the Micro UAS ARC later adopted the same weight-based threshold for exclusion from performance-based standards for operations over people.

Third, it is **comprehensive**, properly encompassing the majority of UAS except for very small and unsophisticated UAS, thereby supporting robust UTM systems. In order to take advantage of the safety benefits of UAS and grow the commercial UAS industry exponentially, a basic level of compliance is critical for the viability of successful UTM systems. The more vehicles participating in these UTM systems with UAS ID and Tracking, the more successful UTM efforts will be.

Fourth, it is an applicability threshold which is **future-proofed** to accommodate technological developments without need to constantly revisit the threshold levels.

Fifth, it would **close the massive gaps** in UAS ID and Tracking inherent in the model aircraft carve-outs and capabilities-based applicability threshold in the ARC's recommendation in Section 6.1.

A basic weight threshold is the easiest and most logical way to ensure that UAS ID and Tracking requirements bear some reasonable relationship to the aviation, public safety, and security risks presented, and its simplicity will help promote compliance. Adopting this approach would also properly focus on risk of operation rather than operator intent and would streamline implementation.

The Alliance, GAMA, AIA, NAAA, X, GE, uAvionix, Ford Motor Company, AirMap, and General Atomics understand that certain local law enforcement members of the ARC were of the view that some UA weighing less than 250 grams with certain technological enhancements (i.e., autonomous navigation; equipped with real-time downlinked remote sensor enabling beyond visual line of sight operations) may nonetheless present possible security/safety issues. We appreciate the input of law enforcement and support additional separate and independent thresholds such as these whereby, if necessary, UA weighing less than 250 grams would also be required to comply with the ID and Tracking regulations.

In sum, it is our considered view that the exemptions for a massive segment of the UAS industry from UAS ID and Tracking requirements (whether through an express model aircraft carve-out or an overly narrow capabilities-based threshold) and the lack of a weight-based threshold for such compliance greatly undermine the value, benefits, and utility of UAS ID and Tracking, not to mention jeopardize the safety of the airspace and comprehensiveness of any future UTM.

The Alliance, GAMA, AIA, NAAA, X, GE, uAvionix, Ford Motor Company, AirMap, and General Atomics therefore dissent from (i) the ARC's recommendations that the FAA consider expressly exempting model aircraft or a narrow capabilities-based threshold that effectively exempts a large segment of model aircraft/UAS from UAS ID and Tracking; and (ii) the ARC's failure to include a recommendation for a risk-based weight threshold for UAS ID and Tracking.

Voting Member:	Robert Hughes
Company Name:	Northrop Grumman
Date Received:	10/4/17
Response:	I concur with the final report as written

Voting Member:	Andrew Jetton
Company Name:	Rockwell Collins
Date Received:	10/2/17
Response:	I concur with the final report as written with the following exceptions: Section 6.1, pages 31-32, on the critical issue of who and what UAS should be required to comply with ID and Tracking requirements. Section 6.1 proposes two alternative threshold applicability criteria. We believe both Option 1 and Option 2 are too broad to fully address the security concerns of federal, state and local law enforcement, and the federal homeland defense and national security agencies. These security concerns were at the core of the FAA's Charter given to the UAS-ID ARC. We share the concerns raised by the Dissent to Section 6.1 of the Commercial Drone Alliance, the General Aviation Manufacturers Association, the Aerospace Industries Association, the National Agricultural Aviation Association, X, GE, uAvionix, Ford Motor Company, AirMap, and General Atomics. We also share in the concerns regarding Section 6.1 addressed in separate comments submitted by: The Association of Unmanned Vehicle Systems International; and the Air Line Pilots Association Rockwell Collins encourages the FAA to expeditiously propose a UAS ID and Tracking requirement that is based on risk-based methodology, and that promotes the full value, benefits and utility of commercial UAS technology without jeopardizing the safety of the airspace.

Voting Member:	Doug Johnson
Company Name:	CTA
Date Received:	10/2/17
Response:	I concur with the final report as written with the following exceptions: CTA would urge FAA to pursue Option 2 in Section 6.1 on page 32, especially given that this option reflects the considered views of the law enforcement, homeland security and national security communities as represented in the ARC's Working Group 2.

Voting Member:	Fabrice Kunzi
Company Name:	General Atomics
Date Received:	10/2/17
Response:	I non-concur with the final report as written: GA-ASI does not concur with Section 6.6, which builds on false underlying assumptions and contains concepts that are not developed to an extent that would give the community confidence that they will be positively received by the Air Traffic Control community. One example is the recommendation to exempt UAS with "advanced flight system technologies" (p. 3), another is the recommendation to use data provided by the LD and tracking system for tactical ATC (p.5). From the perspective of the larger aviation community, it is paramount to have a high level of maturity and integrity in systems that are used to provide separation services. As such we do not concur with the recommendations that go beyond positively linking an operator to an aircraft, which appears to be the primary need from the law enforcement community. Additionally, GA-ASI non-concurs with Section 6.1 and has decided to endorse the position stated in, "DISSENT TO SECTION 6.1 OF THE COMMERCIAL DRONE ALLIANCE, THE GENERAL AVIATION MANUFACTURERS ASSOCIATION, THE AEROSPACE INDUSTRIES ASSOCIATION, THE NATIONAL AGRICULTURAL AVIATION ASSOCIATION, X, GE, uAVIONIX, FORD MOTOR COMPANY, AND AIRMAP" (Recognizing that this was the title at the time and may change based on other signatories.) As a pioneer of UAS technology, GA-ASI is committed to the safe and efficient integration of UAS into the National Airspace System (NAS) and the productive transition from military to civilian and commercial applications. GA-ASI continuously encourages the UAS industry to adapt existing aviation standards and aim for a high level of safety in UAS operations

Voting Member:	Philip Kenul
Company Name:	ASTM International
Date Received:	10/1/17
Response:	I concur with the final report as written with the following exceptions: P31. 6.1. Applicability of the ID and tracking requirements Simply put, I don't believe we should kick the can down the road on this very important point and too many exemptions will leave the final regulation as relatively ineffective for the stated purpose.

Voting Member:	Shawn Kimmel
Company Name:	IEEE
Date Received:	10/5/17
Response:	I concur with the final report as written with the following exceptions: Section 6.1, remove exceptions for model aircraft, and based on aircraft weight or capabilities: I feel that all UAS operators – whether flying for civil, commercial or recreational purposes – must comply with remote ID and tracking requirements, unless and until proven to be low risk and to not reduce the efficacy of the remote ID and tracking solution. The current exceptions have a very realistic potential to reduce the efficacy of the implemented solution, leaving a gap in the needs of the public, law enforcement, and critical infrastructure owner/operators. In particular, blanket exceptions for model aircraft could undermine the efficacy of remote ID and tracking solutions, and I do not feel this exception reflects the sentiments of the majority of ARC members during discussions. Exceptions based on a risk assessment may hold merit as a means to exempt certain aircraft, e.g., based on weight, capabilities, or operator training, but this would require a more rigorous risk assessment than has been conducted under the ARC. Exceptions I find acceptable include explicit FAA (including ATC) approved exceptions, e.g., based on use of ADS-B or for law enforcement purposes.

Voting Member:	Chris Kucera
Company Name:	Analytical Graphics, Inc.
Date Received:	10/2/17
Response:	I concur with the final report as written

Voting Member:	Andrew R. Lacher
Company Name:	The MITRE Corporation
Date Received:	10/2/17
Response:	I concur with the final report as written

Voting Member:	Justin Manley
Company Name:	Just Innovation
Date Received:	10/3/17
Response:	I concur with the final report as written

Voting Member:	Chris Martino
Company Name:	Helicopter Association International
Date Received:	10/1/17
Response:	I concur with the final report as written

Voting Member:	Travis Mason
Company Name:	A3 & Aerial by Airbus
Date Received:	10/2/17
Response:	I concur with the final report as written

Voting Member:	Paul McDuffee
Company Name:	Insitu, Inc.
Date Received:	10/2/17
Response:	I non-concur with the final report as written: This report leaves way too much for the FAA to decide. Do not concur with burdening the operator with sole responsibility for remote ID and tracking. Requirements imposed on ATC to support ID and tracking are vague and potentially distracting to ATC mandated role to separate air traffic. Multiple other objections too numerous to list here. This report leaves way too much to interpretation and will result in even more distraction to overall integration efforts.

Voting Member:	Gregory S. McNeal
Company Name:	AirMap
Date Received:	10/2/17
Response:	I concur with the final report as written with the following exceptions:

Page 31, Section 6.1

- 1) We join the letter of The Commercial Drone Alliance, et.al.
- 2) We further urge the FAA, as part of its considerations regarding applicability, to consider how the technology outlined on Pages 22-26 of the Appendix regarding technology alternatives, specifically "E. Technology Alternative: Software-Based Flight Notification with Telemetry" can allow for the rapid adoption of Remote ID and Tracking for nearly all classes of UAS. Software based telemetry is a feature present in the SDKs of leading UAS manufacturers. UAS not capable of sharing telemetry can safely share flight location information and flight plans and notices using software apps presently available on the marketplace as well as emerging software for use with LAANC. In both instances, the FAA need only define an API for the receipt of telemetry and/or flight notices, and this service can be provided in a scalable way by TPP/USSs. Compliance can be achieved with a high ease of compliance, a high readiness for implementation, and essentially zero cost to UAS Owners/Operators.

Many operators today are already planning their missions before they fly using various software applications to take advantage of the automation now available in UAS. Traditional model aircraft operators can similarly use software based tools to make their flights known to appropriate persons (what many ARC participants referred to as "self-declaration"). For the most part, the capabilities describe in Section E., are enabled through a smart device with applications that are downloaded by recreational and professional owners/operators. In many cases these applications are free. Smart devices either serve as the GCS or are directly coupled to the GCS during flight operations. These devices are often linked to the internet during operations to both receive and share operationally relevant information like TFRs, inbound manned traffic alerts, nearby first responder activity, and other important real time updates. Operators regularly fly with these tools and we expect that these operators would continue to stay connected to send Remote ID and Tracking information because it makes their operations safer, just like receiving real time TFRs makes their operations safer (in fact, a study conducted by one of our software partners indicates greater than 92% connectivity for flights across more than 10,000 operators in a 30-day period). The FAA should be encouraging more flights with connectivity, as it leads to safer operations (through receipt of real time TFRs and other alerts) and fits within a UTM roadmap. While owners/operators use these capabilities for operational situation awareness, other benefits include asset tracking, pilot activity logging, inventory management, battery tracking, flight logging, mission

planning, record keeping, validation, and execution of the flight. These existing and evolving capabilities can be leveraged to enable the UAS to provide in near real-time ID and tracking information (oftentimes with less than 3 seconds of latency end to end) via a federated service provider network.

Importantly many operators presently send their telemetry to the cloud through software that is enabled by default from UAS manufacturers or through third party apps paired with smartphones. For example, a leading app provider using the SDK of a leading drone manufacturer advertises the ability of their software to provide flight records based on real time telemetry. In this software's implementation the telemetry is sent automatically as part of flying the drone. Similarly, the apps from leading OEMs are capable of sharing real time telemetry information automatically with merely a software update. In fact, some manufacturers have even provided a feature where flight logs were sent to a manufacturer's servers by default, proving ease of implementation.

Software based real time telemetry does not require any new hardware and importantly does not require any steps on the part of the operator. All that is necessary is that a software update is made to the existing flight control apps used by major manufacturers or any of their hundreds of developer apps that they allow to fly their drones. An FAA rule that mandates transmission of real time telemetry sent to stakeholders (i.e. mandating a software update) through a defined API at the FAA or with a TPP/USS will allow for the FAA to achieve substantial near term compliance using existing technology, existing software, and existing smart phones. It is not a 100% solution (none of the solutions are) but it is a substantial near term solution that the FAA should strongly consider.

From an interoperability perspective, both broadcast and network forms of Remote ID (which includes software based flight notices and telemetry) can be shown on a shared interface (as described in Section 6.2.2). Law enforcement and security agencies with credentialed access will be able to view only the flight notices or telemetry information within their geographic areas of responsibility. Authorities can access that information from a smart phone or tablet (if they desire mobile access and have a smart phone or tablet), for agencies lacking such technology, a designated person or persons (at dispatch for example) could have access to flight notices and telemetry within the geographic area of responsibility and patrol officers could radio to that person at dispatch for information about nearby flights as necessary. Such an approach can also minimize response times and trouble calls allowing officials to quickly dismiss citizen complaints about purely lawful UAS operations, focusing their attention on suspicious or unlawful uses.

Page 47, Section 7.1.5.

1) The sentence beginning "The ARC recommends that the United States government..." should read:

"The ARC recommends that the United States government be the sole keeper of any PII collected or submitted in connection with new UAS ID and tracking requirements, unless the FAA chooses to rely on a TPP/USS governed by restrictive use conditions imposed on the TPP/USS related to the use and dissemination of any data and information collected." This reflects the consensus in Section 6.2.2.

2) The line: "This recommendation is similar to the ones made by the UAS Registration Task Force ARC in 2015 when recommending a new registration rule for UAS" should be stricken as the similarities are tenuous at best. This ARC is about ID and tracking; those are capabilities which were not robustly discussed at the Registration Task Force. As this report notes, privacy was not fully discussed in this ARC and privacy experts were not consulted.

Voting Member:	David Miller
Company Name:	American Petroleum Institute (API)
Date Received:	10/2/17
Response:	I concur with the final report as written

Voting Member:	Rebecca Mond
Company Name:	The Toy Association, Inc.
Date Received:	10/2/17
Response:	I non-concur with the final report as written:
<p>We felt that the threshold language was changed at the last minute and ARC members did not have time to truly evaluate it or come to a consensus. Now, it seems as though what <i>should</i> have been a dissenting opinion is being presented as a consensus option. The Toy Association cannot concur with a report that presents a threshold option that would no longer exclude most toys as we do not feel toys or toy operators should be included in these requirements. We therefore dissent with the entire report given how this modification impacts the report's applicability for our industry</p>	

Voting Member:	Andrew Moore
Company Name:	National Agricultural Aviation Association
Date Received:	10/2/17
Response:	I concur with the final report as written with the following exceptions: Section 6.1, page 31, Section 6.1, pages 31-32." We dissent from these provisions because: (1) it recommends that the FAA consider an Option A that expressly exempts model aircraft from UAS ID and Tracking; (2) it recommends that the FAA also consider an Option B with a narrow capabilities-based threshold that effectively exempts a large segment of model aircraft/UAS from UAS ID and Tracking; and (3) it did not include a recommendation for a risk-based weight threshold for UAS ID and Tracking.

Voting Member:	Sean Patrick Murphy
Company Name:	T-Mobile USA
Date Received:	10/5/17
Response:	I concur with the final report as written

Voting Member:	Bill Nabors
Company Name:	Texas Department of Public Safety, Aircraft Operations Division
Date Received:	10/4/17
Response:	I concur with the final report as written

Voting Member:	George Novak
Company Name:	AIA
Date Received:	10/2/17
Response:	I concur with the final report as written with the following exceptions: As noted in the dissent filed by the Commercial Drone Alliance, and signed by AIA, we have serious reservations regarding the ultimate success of this initiative with such a significant population of aircraft that would be exempt from identification requirements.

Voting Member:	Vas Patterson
Company Name:	ALPA
Date Received:	10/2/17
Response:	I concur with the final report as written with the following exceptions:

ALPA Dissent on the UAS ID Tracking ARC Final Report

The Air Line Pilots Association, International, representing the safety interests of over 57,000 pilots flying for 33 air carriers in the US and Canada, concurs with the UAS Identification and Tracking Aviation Rulemaking Committee Final Report, with the following exception: ALPA provides a dissenting view specifically on the recommendations that establish the compliance or exemption for remote ID and tracking, as described in Section 6.1 of the report.

Text for Inclusion in the Final Report Main Body

Section 5.2.3, p. 29 End of paragraph that begins “The ARC’s discussions concerning the WG2 threshold...”: Insert the following sentence: “Other ARC members were concerned that the Working Group 2 proposal left a potentially dangerous loophole for a substantial-sized UAS (not specifically model aircraft) to be flown without remote ID and tracking under VLOS at an unspecified distance from the operator. Finally, other ARC members also expressed the view that exemptions should be based more generally only on capabilities or characteristics, rather than type of operations (e.g. Part 101 vs. Part 107 vs. Certificate of Authorization).”

Section 6.1, p. 32, after the last bullet stating “The UAS operation is exempt from ID and tracking requirement by the FAA...”: Insert the following sentence: “Some ARC members hold dissenting views of how the threshold criteria for remote ID and tracking compliance are defined under both options. Those members noted that, under the first option, some operators of UAS with certain capabilities and characteristics would be required to participate, while others with the same make and model of UAS would not be required to participate. Under the second option, a UAS of any size could be operated without ID and tracking at any horizontal distance, as long as it did not have either ability to navigate between more than one point without direct and active control of the pilot, or a real-time remotely viewable sensor. From a safety and security perspective, those members could see no valid reason to exempt either operation.”

Section 6.3.1, p.36, end of the first paragraph: Insert the following sentence: “Some ARC members hold dissenting views of how Tier 0 exemptions to ID and tracking are defined.”

ALPA Dissenting View on Exemptions to ID and Tracking Requirement (for Inclusion in Appendix D)

ALPA recommends that remote ID and tracking requirements should apply to all UAS, with exemptions provided from these requirements. We recommend that the primary capability-based exemption should be for UAS meeting the following:

“Unmanned aircraft operated within visual line of sight of the remote pilot and not designed to have the capability of flying beyond 400’ of the remote pilot.”

Other exemptions for “UAS under ATC”, and “UAS authorized by FAA” (items 3 and 4 in both options) should also be retained as-is.

UAS Exemptions Should Be Based on UAS Capabilities or Characteristics

With regard to Option 1, any exemption to ID and tracking requirements should be defined on the basis of UAS capability or characteristics (e.g. weight), and should not be dependent on the type of operation. We base this assertion on the fact that it will be very difficult for public safety officials to determine whether or not a particular UAS operation is in compliance with ID and tracking requirements, and thus whether the UAS is an anomalous operation, if those requirements depend on the type of operation. ALPA notes that the Commercial Drone Alliance and other ARC members have stated similar concerns in separate dissents.

Ultimately, we believe that an exemption scheme based only on UAS capability or characteristics will be simpler to implement and easier to apply in the real world, and accomplish the objective of ensuring public safety officials have consistent and immediate access to knowing who and where the pilot of a UAS is located, to intervene in unsafe or unauthorized flights. In addition, this would prevent any operators with no intent to comply with all provisions of 14 CFR Part 101, from claiming operation under Part 101 as a cover for not following ID and tracking regulations.

As an example scenario, consider a public safety official that observes two of the same make and model of UAS flying in an area where UAS are temporarily not authorized; for example, the site of a major highway accident where helicopter medical evacuation is needed, and therefore the airspace needs to be clear of other aircraft. Under Option 1 in the main ARC report, one of these UAS may be transmitting ID and tracking information, and one may not, with both being compliant with regulations. While the public safety official could take steps to determine the location of the participating UA’s pilot and intervene in the operation, it will be substantially more difficult if not impossible for the official to determine the identity and location of the pilot of the non-participating UAS, thus impeding his or her ability to ensure public and aviation safety. Yet, with the given exemption, the non-participating pilot could legally be operating as Part 101 subpart E.

This is clearly a loophole in the objectives of the ARC, which is to recommend ID and tracking technologies and equipage to increase the ability for public safety officials to intervene to

ensure safety and security. In addition, a public safety official in this situation would generally have no means to identify the operating framework under which each of the vehicles is operating, so he or she would be unable even to determine whether an identification and tracking regulation is being broken.

By making the requirement entirely based on the capabilities or characteristics of the UAS, then all operations for a particular make and model of UAS would be subject to the same requirement for ID and tracking, regardless of who is operating the UAS and the type of operation. This would in turn make it much easier for public safety officials to accomplish their public safety mission.

UAS Exemptions Must Not Create Loopholes for Potentially Hazardous UAS Operations Without ID/Tracking

ALPA notes that as defined in Option 2, the thresholds for compliance with ID and tracking allow for a UAS of any size to be operated without a maximum distance from the operator, without ID and tracking, as long as it is not equipped with the ability to navigate between more than one point without direct and active control of the pilot, or is not equipped with a real-time remotely viewable sensor.

Therefore, it is entirely allowable under this scheme for a substantial (e.g. up to 55 lbs.) UAS to be flown within visual line of sight laterally from the remote pilot, without ID and tracking. We note that a larger UAS can be tracked at a longer distance visually, increasing the effective range of visual line of sight operations.

Such a large UAS would present a potentially catastrophic hazard to any manned aircraft into whose path it may blunder, even unintentionally. This would have potential impact even in rural areas, where an UAS blunder could affect passenger airliners arriving and departing from non-towered airports, as well as air ambulance, law enforcement, or agricultural aircraft that normally operate at low altitudes.

Finally, a recent study by Virginia Tech indicates that a UAS that is larger but still under 55 lbs. presents a significant risk of bodily harm to people in case a person is struck in a loss of control event or other mishap¹⁵; therefore, in our opinion this provides yet another reason for participation in remote ID and tracking for larger UAS.

¹ <https://link.springer.com/article/10.1007/s10439-017-1921-6>

Voting Member:	Laura Ponto
Company Name:	X
Date Received:	10/2/17
Response:	I non-concur with the final report as written:

**DISSENT
OF X**

X¹ respectfully submits this Dissent from the Final Report (dated September 30, 2017) of the unmanned aircraft systems (UAS) ID and Tracking Aviation Rulemaking Committee (“ARC) for the following reasons:

1. *Performance-Based Standards Are Critical.*

Section 6.3 of the ARC Report provides a discussion about tiered, context-appropriate technology solutions for UAS ID and tracking. The diagram and chart on pages 35-36, as well as the discussion in Section 6.3.3, assert that Tier 2 operations (e.g., expanded operations) should require the UAS to broadcast **and** publish ID and tracking data. The ARC Report further states in Section 6.3.3 that “[l]ocal broadcast should always be a requirement as it provides a backup means of ID and tracking if the network is compromised, degraded, or unavailable.” X dissents from this position.

It is fundamentally important that any regulations governing UAS ID and tracking be performance-based (as the FAA has repeatedly indicated they would be) and that no specific technology be required. In order to leverage the full range of technical solutions ~~available~~, any technology that meets the to-be-determined performance-based standards should be sufficient. However, the ARC Report’s “broadcast **and** network” concept and statement that local broadcast should always be required for Tier 2 operations effectively requires a specific technological solution.

2. *Broad Exemptions Will Prevent the U.S. From Realizing the Full Value of Remote ID and UTM solutions.*

X dissents from the ARC Report’s recommendation in Section 6.1 that the FAA consider exempting all model aircraft operating under Part 101 and Section 336 from complying with any UAS ID and tracking requirements. X also dissents from the ARC Report’s recommendation in Section 6.1 that the FAA consider exempting all UAS that do not meet a narrow capabilities-based threshold. X supports, joins, and incorporates by reference the discussion on this point in the Dissent provided by the Commercial Drone Alliance.

3. A Weight-Based Threshold for Application of UAS ID and Tracking Regulations Should Be Applied.

X dissents from the ARC's rejection of a weight-based threshold for application of any UAS ID and tracking requirements. X supports, joins, and incorporates by reference the discussion on this point in the Dissent provided by the Commercial Drone Alliance.

¹ X is an Alphabet company and a voting member of the ARC. X participated in Working Groups 1, 2, and 3, as well as in the Plenary sessions, and provided comments during the ARC process.

Voting Member:	Bruce Preiss
Company Name:	FlyTransparent/Black River Systems Company
Date Received:	10/5/17
Response:	I concur with the final report as written

Voting Member:	Christian Ramsey
Company Name:	uAvionix
Date Received:	10/2/17
Response:	I concur with the final report as written with the following exceptions:

Requested to include exceptions submitted by the Commercial Drone Alliance:

DISSENT TO SECTION 6.1 OF THE COMMERCIAL DRONE ALLIANCE, THE GENERAL AVIATION MANUFACTURERS ASSOCIATION, THE AEROSPACE INDUSTRIES ASSOCIATION, THE NATIONAL AGRICULTURAL AVIATION ASSOCIATION, X, GE, uAVIONIX, FORD MOTOR COMPANY, AIRMAP, AND GENERAL ATOMICS

The Commercial Drone Alliance (“the Alliance”)¹⁶, the General Aviation Manufacturers Association (“GAMA”)¹⁷, the Aerospace Industries Association (“AIA”)¹⁸, the National Agricultural Aviation Association (“NAAA”)¹⁹, X, GE, uAvionix, Ford Motor Company, AirMap, and General Atomics respectfully submit this **Dissent** from the recommendations and discussion of the UAS ID and Tracking Aviation Rulemaking Committee (“ARC”) in Section 6.1 (“Applicability of the ID and tracking requirements”) of the ARC’s Final Report (“Report”), dated September 30, 2017. These organizations appreciate the extensive efforts of the ARC, but strongly disagree on the critical point of who and what UAS should have to comply with ID and Tracking requirements.

Specifically, these organizations **dissent** from the Report because:

(1) it recommends that the FAA consider an Option 1 that expressly exempts model aircraft from UAS ID and Tracking;

¹⁶ The **Commercial Drone Alliance** is an independent 501c6 non-profit organization led by key members of the commercial drone industry. The Alliance seeks to advance commercial drone technology and policy. The Alliance actively participated as a member of the ARC in the Plenary sessions, Working Group (“WG”) 3, and the Final Report’s writing committee. It has provided verbal comments during these meetings and written comments throughout the process.

¹⁷ The **General Aviation Manufacturers Association** exists to foster and advance the general welfare, safety, interests and activities of the global business and general aviation industry. This includes promoting a better understanding of general aviation manufacturing, maintenance, repair, and overhaul and the important role these industry segments play in economic growth and opportunity, and in serving the critical transportation needs of communities, companies and individuals worldwide.

¹⁸ The **Aerospace Industries Association** (AIA), founded in 1919, represents more than 340 major aerospace and defense companies and their suppliers, embodying every high-technology manufacturing segment of the U.S. aerospace and defense industry including commercial aviation and avionics, manned and unmanned aircraft systems, space technologies and satellite communications.

¹⁹ The **National Agricultural Aviation Association** works to support the agricultural aviation industry which is made up of small businesses and pilots that use aircraft to aid farmers in producing a safe, affordable and abundant supply of food, fiber and biofuel, in addition to protecting forestry and controlling health-threatening pests.

(2) it recommends that the FAA also consider an Option 2 with a narrow capabilities-based threshold that effectively exempts a large segment of model aircraft/UAS from UAS ID and Tracking; and

(3) it did not include a recommendation for a risk-based weight threshold for UAS ID and Tracking.

The Alliance, GAMA, AIA, NAAA, X, GE, uAvionix, Ford Motor Company, AirMap, and General Atomics are strongly supportive of the goals of the UAS ID and Tracking ARC, and, to that end, each actively participated in the ARC and its working groups. Indeed, these organizations consider UAS ID and Tracking to be a critical prerequisite for unleashing the enormous potential of the commercial UAS marketplace. UAS ID and Tracking is necessary now to expand UAS operations which essentially remain grounded until the law enforcement and national security communities are comfortable with their ability to identify and track UA. Just as a high degree of UAS owner/operator compliance is necessary for any UAS ID and Tracking regulation to be successful, it is likewise imperative that any such regulations encompass all but the smallest and most unsophisticated UAS in order to be effective. Any common-sense threshold must also focus primarily on risk rather than operator intent. However, a model aircraft exemption (Option 1), a narrow capabilities-based threshold for ID and Tracking compliance (Option 2), and the lack of a weight-based threshold fly in the face of these principles, and will have adverse implications for the safety and efficiency of the National Airspace System (“NAS”), public safety, and the efficacy of future UAS Traffic Management (“UTM”) systems. Our organizations note that other ARC members, including the Air Line Pilots Association and Association of Unmanned Vehicle Systems International, have stated similar concerns separately.

(7) Model Aircraft Should Not Be Exempt from ID and Tracking (Option 1). The ARC Report recommends that the FAA consider exempting a large segment of the UAS community from complying with future ID and Tracking regulations by carving-out unmanned aircraft “operated in compliance with 14 CFR part 101, unless the unmanned aircraft is equipped [with certain technology]”. [ARC Report, Section 6.1, pages 31-32.] ***The Alliance, GAMA, AIA, NAAA, X, GE, uAvionix, Ford Motor Company, AirMap, and General Atomics firmly oppose any such carve-out for model aircraft and hobbyists.***

This exemption is a loophole that swallows the rule. It would permit a huge segment of the UAS community to avoid participating in the UAS ID and Tracking system and complying with the corresponding ID and Tracking regulations. For example, the Academy of Model Aeronautics (“AMA” or “modelers”) reportedly represents more than 195,000 modelers worldwide.²⁰ The FAA Aerospace Forecast (fiscal years 2017-2037) estimates that there were approximately 1.1 million units of distinctly hobbyist sUAS or model aircraft in 2016, with significant growth projected in the next few years to 2.75 million (low), 3.55

²⁰

<http://www.modelaircraft.org/aboutama/whatisama.aspx>

million (base case) or 4.47 million (high case) such units in 2021.²¹ By contrast, that same Forecast estimates that the non-hobbyist (commercial) fleet is smaller, with approximately 42,000 units in 2016, with growth projected in the next few years to 238,000 (low), 422,000 (base case) or 1.61 million (high case) such units in 2021.²² Moreover, this exemption provides many operators having no intent to comply fully with Part 101 with cover for not following ID and Tracking regulations. If, as envisioned by Option 1 in Section 6.1, such a huge segment of the UAS community is not subject to the ID and Tracking regulations, there will be direct, adverse implications for the safety and efficiency of the NAS, public safety, and the efficacy of future UTM systems.

Moreover, the carve-out for model aircraft operated under Part 101 (and in compliance with Section 336) is also flawed in that public safety officials will not be able to discern whether a particular UAS flying nearby is compliant with the regulations in accordance with the carve-out or operating nefariously by not providing positive ID and Tracking. The public safety official simply will not know the operator's intent and will not be able to determine if enforcement activity is appropriate. Inability to positively ID and track UAS large enough to interfere with manned flight and public safety operations, as well as harm non-participants through direct kinetic impact, limits public safety officials in their ability to enforce safe UAS statutes and regulations.

In addition, as a matter of process, this carve-out for model aircraft and hobbyists was a relatively last-minute addition to the ARC Report. The focus of debate on the applicability of UAS ID and Tracking had been on the approach that WG2 developed, which did not include an express carve-out for model aircraft. [See ARC Report, Section 5.2.3, page 29.] As a result, this carve-out did not receive proper broad discussion by the ARC.

(8) The Narrow Capabilities-Based Threshold Is Not Sufficiently Inclusive (Option 2). The ARC Report also recommends that the FAA consider carving out a large segment of the UAS community from having to comply with future ID and Tracking regulations by using a narrow capabilities-based threshold. Specifically, under this Option, only UAS with (i) the ability to navigate between more than one point without direct and active control of the pilot, or (ii) a range from the control station greater than 400' and a real-time remotely viewable sensor will have to comply under the ARC's recommendation. [ARC Report, Section 6.1, pages 31-32.] ***The Alliance, GAMA, AIA, NAAA, X, GE, uAvionix, Ford Motor Company, AirMap, and General Atomics firmly oppose any such narrow capabilities-based approach which effectively amounts to a model aircraft/hobbyist exemption and excludes a huge segment of UAS from compliance with future ID and Tracking regulations.***

As with the flawed Option 1 (discussed above), this narrow capabilities-based approach is essentially a loophole that swallows the rule. The AMA represents nearly

²¹

FAA Aerospace Forecast (2017-2037), at 30-31.

²²

FAA Aerospace Forecast (2017-2037), at 32.

200,000 members, and the FAA Aerospace Forecast (fiscal years 2017-2037) estimates that there will be 2.75 million – 4.47 million units of distinctly hobbyist sUAS or model aircraft in 2021. The ARC's recommendation would permit a huge segment of the UAS community to avoid participating in the UAS ID and Tracking system and complying with the corresponding ID and Tracking regulations, thereby having direct, adverse implications for the safety and efficiency of the NAS, public safety, and the efficacy of future UTM systems.

Moreover, this narrow capabilities-based threshold is flawed in that public safety officials will not be able to discern whether a particular UAS flying nearby has autonomous capabilities or sensors and thus is compliant in not providing ID and Tracking, or whether it is a nefarious operator warranting further investigation. The public safety official simply will not know the vehicle's capabilities and will not be able to determine if enforcement activity is appropriate. Inability to positively ID and track a huge segment of UAS that could interfere with manned flight and public safety operations, as well as harm non-participants through direct kinetic impact, limits public safety officials in their ability to enforce safe UAS statutes and regulations.

(9) There Should Be A Weight-Based Threshold For UAS ID And Tracking. The Alliance, GAMA, AIA, NAAA, X, GE, uAvionix, Ford Motor Company, AirMap, and General Atomics strongly advocated for a weight-based threshold: As a general rule, any UAS or model aircraft weighing 250 grams or more must comply with the ID and Tracking regulations.

Yet, although the ARC Report recommends that the FAA consider two fundamentally flawed thresholds for compliance with any UAS ID and Tracking requirements (Options 1 and 2 in Section 6.1), it did not recommend that the FAA consider a weight-based threshold. This omission is glaring because there are several principal arguments in favor of such a weight-based approach.

First, it is **simple, adaptable, and enforceable**, each of which promotes compliance, which in turn promotes the safety and efficiency of the NAS, thereby enabling sustained growth and innovation to succeed without compromising the safety of the world's leading aviation system.

Second, it is **familiar** insofar as other UAS-related ARCs have found merit in using a weight-based applicability threshold. For example, the UAS Registration Task Force ARC concluded that a weight-based approach was appropriate because it was easy to understand and apply and would therefore encourage compliance, and the Micro UAS ARC later adopted the same weight-based threshold for exclusion from performance-based standards for operations over people.

Third, it is **comprehensive**, properly encompassing the majority of UAS except for very small and unsophisticated UAS, thereby supporting robust UTM systems. In order to take advantage of the safety benefits of UAS and grow the commercial UAS industry

exponentially, a basic level of compliance is critical for the viability of successful UTM systems. The more vehicles participating in these UTM systems with UAS ID and Tracking, the more successful UTM efforts will be.

Fourth, it is an applicability threshold which is **future-proofed** to accommodate technological developments without need to constantly revisit the threshold levels.

Fifth, it would **close the massive gaps** in UAS ID and Tracking inherent in the model aircraft carve-outs and capabilities-based applicability threshold in the ARC's recommendation in Section 6.1.

A basic weight threshold is the easiest and most logical way to ensure that UAS ID and Tracking requirements bear some reasonable relationship to the aviation, public safety, and security risks presented, and its simplicity will help promote compliance. Adopting this approach would also properly focus on risk of operation rather than operator intent and would streamline implementation.

The Alliance, GAMA, AIA, NAAA, X, GE, uAvionix, Ford Motor Company, AirMap, and General Atomics understand that certain local law enforcement members of the ARC were of the view that some UA weighing less than 250 grams with certain technological enhancements (i.e., autonomous navigation; equipped with real-time downlinked remote sensor enabling beyond visual line of sight operations) may nonetheless present possible security/safety issues. We appreciate the input of law enforcement and support additional separate and independent thresholds such as these whereby, if necessary, UA weighing less than 250 grams would also be required to comply with the ID and Tracking regulations.

In sum, it is our considered view that the exemptions for a massive segment of the UAS industry from UAS ID and Tracking requirements (whether through an express model aircraft carve-out or an overly narrow capabilities-based threshold) and the lack of a weight-based threshold for such compliance greatly undermine the value, benefits, and utility of UAS ID and Tracking, not to mention jeopardize the safety of the airspace and comprehensiveness of any future UTM.

The Alliance, GAMA, AIA, NAAA, X, GE, uAvionix, Ford Motor Company, AirMap, and General Atomics therefore dissent from (i) the ARC's recommendations that the FAA consider expressly exempting model aircraft or a narrow capabilities-based threshold that effectively exempts a large segment of model aircraft/UAS from UAS ID and Tracking; and (ii) the ARC's failure to include a recommendation for a risk-based weight threshold for UAS ID and Tracking.

Voting Member:	Jennifer Richter
Company Name:	CTIA / Akin Gump
Date Received:	10/1/17
Response:	I concur with the final report as written

Voting Member:	Steven Rush
Company Name:	PHPA
Date Received:	9/30/17
Response:	I concur with the final report as written

Voting Member:	Brendan Schulman
Company Name:	DGI Technology
Date Received:	10/2/17
Response:	I concur with the final report as written with the following exceptions:

DJI concurs with the final report as written with the following exception relating to section 6.1 (pages 31-33):

DJI concurs with the ARC report, and respectfully offers this comment about the threshold requirement described in Section 6.1 and as to which the ARC did not reach consensus. The threshold issue is fundamental, because it determines which UAS may need to be equipped with technologies to enable compliance, and which UAS operators will be saddled with the burdens and costs of compliance.

This ARC, as directed by its charter, has focused almost exclusively on the needs and desires of the law enforcement, homeland defense, and national security communities. These communities worked diligently in Working Group 2 (WG2) to describe which UAS they needed to be remotely identified and tracked. That capability-based determination was presented to the ARC, is described in section 5.2.3, and is incorporated in section 6.1 as “Option 2.” This determination was not balanced with the interests of other stakeholders, such as UAS owners and operators, and does not provide for reasonable exemptions for UAS that pose little, if any, safety or security concerns and for which an ID requirement’s costs and burdens may outweigh its benefits. For example, the report contains no low-weight exemption, no short-flight-time exemption, no “my own backyard” exemption, no ASTM-standard toy exemption, no “selfie drone” exemption, no low-radio-power exemption, no exemption for flight within close proximity to the pilot, no express exemption for low-altitude racing drones,²³ no exemption for drones that cannot carry even a light payload, and so on. Despite much discussion on these and other very-low-risk UAS, the focus of the ARC has remained squarely on the needs articulated by WG2.

WG2 was clear about those needs: ID and tracking is only required for UAS that either (i) have the ability to navigate between more than one point without direct and active control of the pilot, or (ii) have a real-time remotely viewable sensor with a control range of 400 feet or more. This option, set out as Option 2 in section 6.1, is the only option that fulfills the directive in our charter to “[i]dentify the requirements for meeting the security and public safety needs of the law enforcement, homeland defense, and national security communities for the remote identification and tracking of UAS.” We respectfully suggest the FAA afford greater consideration to the WG2/Option 2 determination based on UAS capability, and in the rulemaking process that is to come, undertake to balance those needs and desires with the interests of UAS owner, pilot, and operator stakeholders.

²³ Footnote 16 on page 31 and footnote 17 on page 36, concerning the ARC’s intent relating to racing drones, was intended by the ARC to also appear in Option 2. The omission appears to be a transcription error.

The issue of model aircraft operated pursuant to 14 CFR part 101, awkwardly woven into Option 1, is an implementation issue, not a threshold issue. FAA can, today, implement Remote ID and tracking among community-based organizations by working with them to incorporate such requirements into their safety guidelines. Alternatively, if necessary, and in coordination with the community based organizations, the statute concerning model aircraft could be amended to provide for ID and tracking of UAS that pose a sufficient safety or security risk to warrant such a requirement, in light of technologies that were not envisioned or in popular use in 2012. DJI is supportive of ID and tracking solutions for technologies that raise serious safety and security concerns, but does not support burdening with ID and tracking requirements the types of basic-capability UAS that have been operated safely for decades without raising such concerns.

Voting Member:	Daniel Schwarzbach
Company Name:	ALEA
Date Received:	10/5/17
Response:	I concur with the final report as written with the following exceptions: My exception is with Section 6.1, pages 31-32, and mirrors that of Andrew Jetton of Rockwell Collins, including the concerns raised by the Commercial Drone Alliance, GAMA, AIA, NAAA, AAAE, AUVSI, ALPA and others.

Voting Member:	Al Secen
Company Name:	RTCA
Date Received:	10/4/17
Response:	I concur with the final report as written

Voting Member:	Mike Sedam
Company Name:	California Highway Patrol, Office of Air Operations
Date Received:	10/2/17
Response:	I concur with the final report as written

Voting Member:	Michael Senkowski
Company Name:	DLA Piper
Date Received:	10/2/17
Response:	I concur with the final report as written

Voting Member:	John Shea
Company Name:	NASAO
Date Received:	10/2/17
Response:	I concur with the final report as written

Voting Member:	Adi Singh
Company Name:	Ford Motor Company
Date Received:	10/3/17
Response:	I non-concur with the final report as written:

DISSENT TO SECTION 6.1 OF THE COMMERCIAL DRONE ALLIANCE, THE GENERAL AVIATION MANUFACTURERS ASSOCIATION, THE AEROSPACE INDUSTRIES ASSOCIATION, THE NATIONAL AGRICULTURAL AVIATION ASSOCIATION, X, GE, uAVIONIX, FORD MOTOR COMPANY, AIRMAP, AND GENERAL ATOMICS

The Commercial Drone Alliance (“the Alliance”)²⁴, the General Aviation Manufacturers Association (“GAMA”)²⁵, the Aerospace Industries Association (“AIA”)²⁶, the National

Agricultural Aviation Association (“NAAA”)²⁷, X, GE, uAvionix, Ford Motor Company, AirMap, and General Atomics respectfully submit this **Dissent** from the recommendations and discussion of the UAS ID and Tracking Aviation Rulemaking Committee (“ARC”) in Section 6.1 (“Applicability of the ID and tracking requirements”) of the ARC’s Final Report (“Report”), dated September 30, 2017.

These organizations appreciate the extensive efforts of the ARC, but strongly disagree on the critical point of who and what UAS should have to comply with ID and Tracking requirements.

Specifically, these organizations **dissent** from the Report because:

(1) it recommends that the FAA consider an Option 1 that expressly exempts model aircraft from UAS ID and Tracking;

²⁴ The **Commercial Drone Alliance** is an independent 501c6 non-profit organization led by key members of the commercial drone industry. The Alliance seeks to advance commercial drone technology and policy. The Alliance actively participated as a member of the ARC in the Plenary sessions, Working Group (“WG”) 3, and the Final Report’s writing committee. It has provided verbal comments during these meetings and written comments throughout the process.

²⁵ The **General Aviation Manufacturers Association** exists to foster and advance the general welfare, safety, interests and activities of the global business and general aviation industry. This includes promoting a better understanding of general aviation manufacturing, maintenance, repair, and overhaul and the important role these industry segments play in economic growth and opportunity, and in serving the critical transportation needs of communities, companies and individuals worldwide.

²⁶ The **Aerospace Industries Association** (AIA), founded in 1919, represents more than 340 major aerospace and defense companies and their suppliers, embodying every high-technology manufacturing segment of the U.S. aerospace and defense industry including commercial aviation and avionics, manned and unmanned aircraft systems, space technologies and satellite communications.

²⁷ The **National Agricultural Aviation Association** works to support the agricultural aviation industry which is made up of small businesses and pilots that use aircraft to aid farmers in producing a safe, affordable and abundant supply of food, fiber and biofuel, in addition to protecting forestry and controlling health-threatening pests.

(2) it recommends that the FAA also consider an Option 2 with a narrow capabilities-based threshold that effectively exempts a large segment of model aircraft/UAS from UAS ID and Tracking; and

(3) it did not include a recommendation for a risk-based weight threshold for UAS ID and Tracking.

The Alliance, GAMA, AIA, NAAA, X, GE, uAvionix, Ford Motor Company, AirMap, and General Atomics are strongly supportive of the goals of the UAS ID and Tracking ARC, and, to that end, each actively participated in the ARC and its working groups. Indeed, these organizations consider UAS ID and Tracking to be a critical prerequisite for unleashing the enormous potential of the commercial UAS marketplace. UAS ID and Tracking is necessary now to expand UAS operations which essentially remain grounded until the law enforcement and national security communities are comfortable with their ability to identify and track UA. Just as a high degree of UAS owner/operator compliance is necessary for any UAS ID and Tracking regulation to be successful, it is likewise imperative that any such regulations encompass all but the smallest and most unsophisticated UAS in order to be effective. Any common-sense threshold must also focus primarily on risk rather than operator intent. However, a model aircraft exemption (Option 1), a narrow capabilities-based threshold for ID and Tracking compliance (Option 2), and the lack of a weight-based threshold fly in the face of these principles, and will have adverse implications for the safety and efficiency of the National Airspace System (“NAS”), public safety, and the efficacy of future UAS Traffic Management (“UTM”) systems. Our organizations note that other ARC members, including the Air Line Pilots Association and Association of Unmanned Vehicle Systems International, have stated similar concerns separately.

(10) Model Aircraft Should Not Be Exempt from ID and Tracking (Option 1). The ARC Report recommends that the FAA consider exempting a large segment of the UAS community from complying with future ID and Tracking regulations by carving-out unmanned aircraft “operated in compliance with 14 CFR part 101, unless the unmanned aircraft is equipped [with certain technology]”. [ARC Report, Section 6.1, pages 31-32.] ***The Alliance, GAMA, AIA, NAAA, X, GE, uAvionix, Ford Motor Company, AirMap, and General Atomics firmly oppose any such carve-out for model aircraft and hobbyists.***

This exemption is a loophole that swallows the rule. It would permit a huge segment of the UAS community to avoid participating in the UAS ID and Tracking system and complying with the corresponding ID and Tracking regulations. For example, the Academy of Model Aeronautics (“AMA” or “modelers”) reportedly represents more than 195,000 modelers worldwide.²⁸ The FAA Aerospace Forecast (fiscal years 2017-2037) estimates that there were approximately 1.1 million units of distinctly hobbyist sUAS or model aircraft in 2016, with significant growth projected in the next few years to 2.75 million (low), 3.55

²⁸

<http://www.modelaircraft.org/aboutama/whatisama.aspx>

million (base case) or 4.47 million (high case) such units in 2021.²⁹ By contrast, that same Forecast estimates that the non-hobbyist (commercial) fleet is smaller, with approximately 42,000 units in 2016, with growth projected in the next few years to 238,000 (low), 422,000 (base case) or 1.61 million (high case) such units in 2021.³⁰ Moreover, this exemption provides many operators having no intent to comply fully with Part 101 with cover for not following ID and Tracking regulations. If, as envisioned by Option 1 in Section 6.1, such a huge segment of the UAS community is not subject to the ID and Tracking regulations, there will be direct, adverse implications for the safety and efficiency of the NAS, public safety, and the efficacy of future UTM systems.

Moreover, the carve-out for model aircraft operated under Part 101 (and in compliance with Section 336) is also flawed in that public safety officials will not be able to discern whether a particular UAS flying nearby is compliant with the regulations in accordance with the carve-out or operating nefariously by not providing positive ID and Tracking. The public safety official simply will not know the operator's intent and will not be able to determine if enforcement activity is appropriate. Inability to positively ID and track UAS large enough to interfere with manned flight and public safety operations, as well as harm non-participants through direct kinetic impact, limits public safety officials in their ability to enforce safe UAS statutes and regulations.

In addition, as a matter of process, this carve-out for model aircraft and hobbyists was a relatively last-minute addition to the ARC Report. The focus of debate on the applicability of UAS ID and Tracking had been on the approach that WG2 developed, which did not include an express carve-out for model aircraft. [See ARC Report, Section 5.2.3, page 29.] As a result, this carve-out did not receive proper broad discussion by the ARC.

(11) The Narrow Capabilities-Based Threshold Is Not Sufficiently Inclusive (Option 2). The ARC Report also recommends that the FAA consider carving out a large segment of the UAS community from having to comply with future ID and Tracking regulations by using a narrow capabilities-based threshold. Specifically, under this Option, only UAS with (i) the ability to navigate between more than one point without direct and active control of the pilot, or (ii) a range from the control station greater than 400' and a real-time remotely viewable sensor will have to comply under the ARC's recommendation. [ARC Report, Section 6.1, pages 31-32.] ***The Alliance, GAMA, AIA, NAAA, X, GE, uAvionix, Ford Motor Company, AirMap, and General Atomics firmly oppose any such narrow capabilities-based approach which effectively amounts to a model aircraft/hobbyist exemption and excludes a huge segment of UAS from compliance with future ID and Tracking regulations.***

As with the flawed Option 1 (discussed above), this narrow capabilities-based approach is essentially a loophole that swallows the rule. The AMA represents nearly

²⁹

FAA Aerospace Forecast (2017-2037), at 30-31.

³⁰

FAA Aerospace Forecast (2017-2037), at 32.

200,000 members, and the FAA Aerospace Forecast (fiscal years 2017-2037) estimates that there will be 2.75 million – 4.47 million units of distinctly hobbyist sUAS or model aircraft in 2021. The ARC's recommendation would permit a huge segment of the UAS community to avoid participating in the UAS ID and Tracking system and complying with the corresponding ID and Tracking regulations, thereby having direct, adverse implications for the safety and efficiency of the NAS, public safety, and the efficacy of future UTM systems.

Moreover, this narrow capabilities-based threshold is flawed in that public safety officials will not be able to discern whether a particular UAS flying nearby has autonomous capabilities or sensors and thus is compliant in not providing ID and Tracking, or whether it is a nefarious operator warranting further investigation. The public safety official simply will not know the vehicle's capabilities and will not be able to determine if enforcement activity is appropriate. Inability to positively ID and track a huge segment of UAS that could interfere with manned flight and public safety operations, as well as harm non-participants through direct kinetic impact, limits public safety officials in their ability to enforce safe UAS statutes and regulations.

(12) There Should Be A Weight-Based Threshold For UAS ID And Tracking. The Alliance, GAMA, AIA, NAAA, X, GE, uAvionix, Ford Motor Company, AirMap, and General Atomics strongly advocated for a weight-based threshold: As a general rule, any UAS or model aircraft weighing 250 grams or more must comply with the ID and Tracking regulations.

Yet, although the ARC Report recommends that the FAA consider two fundamentally flawed thresholds for compliance with any UAS ID and Tracking requirements (Options 1 and 2 in Section 6.1), it did not recommend that the FAA consider a weight-based threshold. This omission is glaring because there are several principal arguments in favor of such a weight-based approach.

First, it is **simple, adaptable**, and **enforceable**, each of which promotes compliance, which in turn promotes the safety and efficiency of the NAS, thereby enabling sustained growth and innovation to succeed without compromising the safety of the world's leading aviation system.

Second, it is **familiar** insofar as other UAS-related ARCs have found merit in using a weight-based applicability threshold. For example, the UAS Registration Task Force ARC concluded that a weight-based approach was appropriate because it was easy to understand and apply and would therefore encourage compliance, and the Micro UAS ARC later adopted the same weight-based threshold for exclusion from performance-based standards for operations over people.

Third, it is **comprehensive**, properly encompassing the majority of UAS except for very small and unsophisticated UAS, thereby supporting robust UTM systems. In order to take advantage of the safety benefits of UAS and grow the commercial UAS industry

exponentially, a basic level of compliance is critical for the viability of successful UTM systems. The more vehicles participating in these UTM systems with UAS ID and Tracking, the more successful UTM efforts will be.

Fourth, it is an applicability threshold which is **future-proofed** to accommodate technological developments without need to constantly revisit the threshold levels.

Fifth, it would **close the massive gaps** in UAS ID and Tracking inherent in the model aircraft carve-outs and capabilities-based applicability threshold in the ARC's recommendation in Section 6.1.

A basic weight threshold is the easiest and most logical way to ensure that UAS ID and Tracking requirements bear some reasonable relationship to the aviation, public safety, and security risks presented, and its simplicity will help promote compliance. Adopting this approach would also properly focus on risk of operation rather than operator intent and would streamline implementation.

The Alliance, GAMA, AIA, NAAA, X, GE, uAvionix, Ford Motor Company, AirMap, and General Atomics understand that certain local law enforcement members of the ARC were of the view that some UA weighing less than 250 grams with certain technological enhancements (i.e., autonomous navigation; equipped with real-time downlinked remote sensor enabling beyond visual line of sight operations) may nonetheless present possible security/safety issues. We appreciate the input of law enforcement and support additional separate and independent thresholds such as these whereby, if necessary, UA weighing less than 250 grams would also be required to comply with the ID and Tracking regulations.

In sum, it is our considered view that the exemptions for a massive segment of the UAS industry from UAS ID and Tracking requirements (whether through an express model aircraft carve-out or an overly narrow capabilities-based threshold) and the lack of a weight-based threshold for such compliance greatly undermine the value, benefits, and utility of UAS ID and Tracking, not to mention jeopardize the safety of the airspace and comprehensiveness of any future UTM.

The Alliance, GAMA, AIA, NAAA, X, GE, uAvionix, Ford Motor Company, AirMap, and General Atomics therefore dissent from (i) the ARC's recommendations that the FAA consider expressly exempting model aircraft or a narrow capabilities-based threshold that effectively exempts a large segment of model aircraft/UAS from UAS ID and Tracking; and (ii) the ARC's failure to include a recommendation for a risk-based weight threshold for UAS ID and Tracking.

Voting Member:	Kyle Snyder
Company Name:	ASSURE
Date Received:	10/2/17
Response:	I concur with the final report as written

Voting Member:	Ken Stewart
Company Name:	GE
Date Received:	10/2/17
Response:	I non-concur with the final report as written:

GE Dissent

GE appreciates the opportunity to have actively participated in the UAS ID and Tracking Aviation Rulemaking Committee (ARC). However, GE respectfully submits this Dissent from the recommendations and discussions of the ARC in section 6.1 (“Applicability of the ID and tracking requirements”) of the ARC’s Final Report, dated September 30, 2017.

GE signed a dissent to Section 6.1 with the Commercial Drone Alliance and several other organizations, and incorporates the arguments therein by reference here.

In summary, we dissent from the report based on our belief that the recommendations do not adequately promote a safe National Airspace System (NAS) based on the following:

1. The recommendation did not include a weight based threshold for applicability of ID and Tracking, which limits the ability of public safety to quickly determine compliance.
2. The recommendation contains two options for applicability, both of which allow significant numbers of UAVs to avoid participating:
 - a. Option A, which expressly excludes model aircraft from UAS ID and Tracking.
 - b. Option B, which potentially excludes many noncommercial and hobbyist UAS from UAS ID and Tracking.

GE is strongly supportive of the goals of the UAS ID and Tracking ARC, and actively participated in ARC Working Group 2. GE believes that the safe operation of drones in the NAS requires an effective, enforceable, and affordable positive ID and Tracking policy and technology approach. Creating loopholes that effectively omit a large number of UAS from the applicability of Remote ID and Tracking is not in the best interest of public safety, and compromises the safety of the world’s leading aviation system.

Weight Based Threshold

1. There needs to be a weight based threshold for UAS ID and Tracking.

GE strongly supports weight being added to the applicability of remote ID and tracking requirements. We believe that weight of 250 grams is a fundamental element that is indicative of a UAS’s capabilities as to whether it can be associated with its operator directly or requires remote ID and tracking. This weight threshold would effectively omit toys from the requirement as that category of UAS and operators that could easily be identified without the need for remote ID. Furthermore, GE believes that the lack of a weight threshold creates a real safety concern for both manned aircraft and public safety. Weight simplifies compliance

as it encompasses the majority of UAS except those too small and technologically limited. A weight based threshold is the easiest, most practical and comprehensive way to ensure that UAS ID and Tracking requirements are applied to ensure public safety and security as well as safely integrating UAS operations in the NAS.

Capabilities Based Approach

2. Options for Applicability

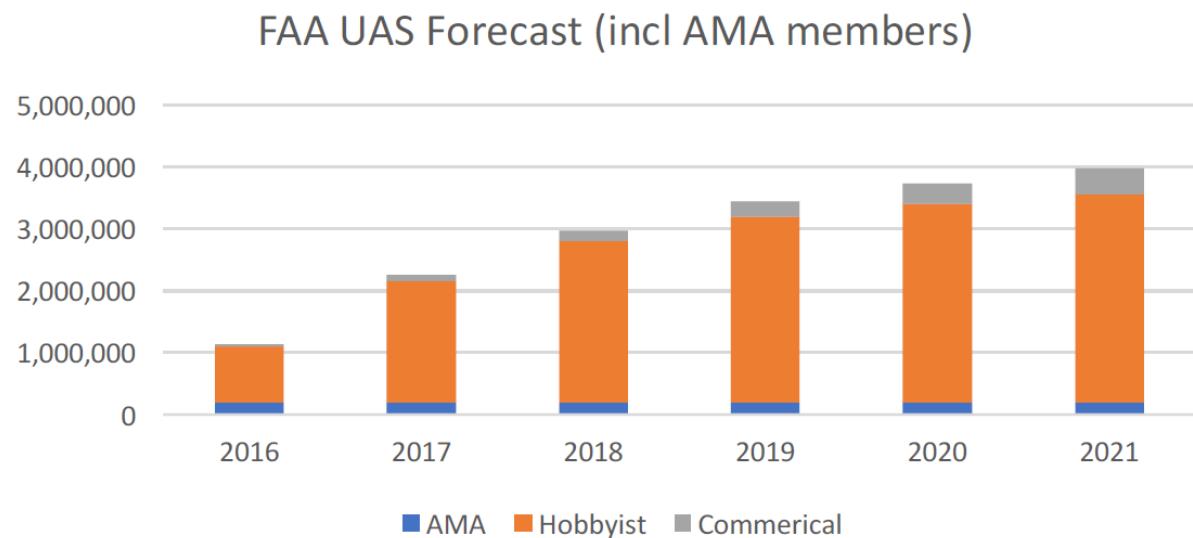
- a. Model Aircraft should not be exempt from the applicability of ID and Tracking.

Model aircraft should not be excluded or exempted from the applicability of ID and Tracking. This would exclude a large number of UAS. AMA represents 195,000 modelers worldwide; hobbyist UAS estimates exceed 1.1 million in 2016 (inclusive of modelers). Excluding hobbyist and modelers from the Positive ID and Tracking requirements would significantly impair law enforcement's and other agency's abilities to identify the UAS as compliant, rather than forcing officials to assume whether it is rogue or non-compliant. Lastly, there is additional benefit by providing protection to their members in the event the UAS is lost or stolen.

- b. The recommended capabilities-based threshold is not sufficient.

The ARC report recommends that the FAA consider carving out a large segment of the UAS community from having to comply with ID and tracking by narrowly focusing on two specific capabilities: (1) the ability to navigate between more than one point without direct and active control of the pilot, or (2) a range from the control station greater than 400' and a real-time remotely viewable sensor. Capability "1" represents a large and increasing percentage of UAVs (88% to 96%) not required to have positive ID and Tracking. The actual numbers may be higher, as the membership from AMA reflects their global members as US numbers are not available. Capability "2", the range requirement, will also provide a path to future exclusion from positive ID and Tracking rules as enabling technology is increasing rapidly.

1 <http://www.modelaircraft.org/aboutama/whatisama.aspx>



Figures from FAA Aerospace forecast (fiscal years 2017-2037) & AMA Website

Option B still retains the same flaws in Option A but to a greater extent as the membership of AMA no longer applies.

Summary

GE believes that the ARC recommendations do not allow for UAV growth consistent with safety in the NAS. Limited enforceability due to lack of a weight restriction and from substantial exclusions would leave law enforcement and other agencies without the policy and technology needed to effectively ensure public safety.

Voting Member:	Kenji Sugahara
Company Name:	AriAscend/DUGN
Date Received:	10/2/17
Response:	I concur with the final report as written

Voting Member:	Chuck Tobin
Company Name:	Ballard Spahr
Date Received:	10/1/17
Response:	I non-concur with the final report as written:

**Dissent of the News Media Coalition
To ARC Recommendations and Final Report
To FAA Administrator Michael Huerta**

September 30, 2017

**Submitted on Behalf of the
News Media Coalition Consisting of:**

Advance Publications, Inc.
 American Broadcasting Companies, Inc.
 American Society of Media Photographers
 The Associated Press
 Capitol Broadcasting Co.
 Gannett Co., Inc.
 Getty Images (US), Inc.
 Gray Television, Inc.
 Media Law Resource Center
 MPA – the Association of Magazine Media
 The National Press Club
 National Press Photographers Association
 NBCUniversal Media, LLC
 News Media Alliance
 The New York Times Company
 Radio Television Digital News Association
 Reporters Committee for Freedom of the Press
 The E.W. Scripps Company
 Sinclair Broadcast Group, Inc.
 TEGNA, Inc.
 WP Company LLC

The News Media Coalition, a collective of 21 of the country's leading broadcast, print and digital news organizations and professional associations, is grateful to the Federal Aviation Administration for the opportunity to have participated in the FAA's Advisory Rulemaking Committee (ARC) regarding the remote identification and tracking of unmanned aircraft systems (UAS) or drones.

As the FAA is aware, the News Media Coalition has actively participated in all aspects of rulemaking, policy, and consensus-building as the FAA, Department of Commerce, Federal Trade Commission, and Congress have worked to implement the mandate of the 2012 FAA Modernization and Reform Act to safely integrate unmanned aerial vehicles into the National Airspace. We have appreciated the collegial discussions in the ARC and other multi-stakeholder forums as we have worked together on behalf of the public's interest in safety, security, and protecting the freedoms guaranteed by the United States Constitution.

The ARC Charter, issued on May 4, 2017, charged the UAS Identification and Tracking ARC to make recommendations to the Administrator "for how remote identification may be implemented." The Charter also identified among the ARC objectives to "consider and evaluate the need to provide information" about individual UAS operations and operators to security and public safety officials "that could assist in threat discrimination and determination of hostile intent."

The Charter thus provided the ARC with wide-ranging authority to consider safety and security concerns, available technologies, and implementation challenges, including civil liberties issues. The News Media Coalition was included as a member of the ARC to ensure that the ARC would weigh implementation issue related to the First Amendment freedoms of journalists alongside other concerns. Unfortunately, the discussion at the ARC meetings on the important First Amendment considerations have been extremely limited, and the ARC's Recommendations and Final Report (Report) to the Administrator contains insufficient consideration of the constitutional guarantees for journalists to gather, and the public to receive, news and information in the public interest.

The News Media Coalition therefore respectfully dissents from the Report. We ask that in preparing to formalize a regulation for the remote identification and tracking of UAS, the Administrator and the FAA take the following issues into account, and that any notice of proposed rulemaking address these concerns.

The Proposed Regulation Should Articulate a Legal Standard for Law Enforcement and Security Officials Accessing UAS Database Information

The Report recommends that public safety officials be provided with access to information about a UAS and its operator "in accordance with the role and responsibility of the individual(s) seeking the information." (Report 7.1). The News Media Coalition supports the concept that the FAA should restrict access to any database of information that could identify a journalist operating a drone to gather news, the news organization involved in the newsgathering, or the flight history of that operation or any previous operations conducted with the drone. The News Media Coalition also has no objection to the recommendation of a visible unique identifier, akin to a license plate, that would contain alphanumeric characters without personal identifying information. (Report 7.1.1).

But the Report contains no guidance whatsoever for public safety officials to make a threshold determination of whether to even seek further information about a drone or its operator. Indeed, the Report would provide officials with unbridled discretion before accessing a database containing personal identifying information (PII) or historical tracking information about the operation. Report sections 5.1.2.3, 5.2.1, 6.5.1.2, 6.5.1.3 and 7.1.1 contain specific scenarios in which the FAA contemplates public safety officials may wish access to that type of information. While some of these sections reference access to the information “for official purposes only” and urge “that privacy be fully considered and that appropriate privacy protections are in place before data collection and sharing,” they do not even begin to address the constitutional considerations that should have informed the ARC’s charge to “consider and evaluate the need to provide information[.]” (ARC Charter) (emphasis supplied).

The News Media Coalition believes that a member of the public or an official spotting a drone in flight and notifying the government, without a suspicion or actual violation of any law or

regulation, is insufficient grounds for public safety officials to query a database and review PII on the drone operator or its flight history. A pilot-in-command operating a drone, in airspace where a drone is permitted to fly and in a manner that reasonably would not arouse legitimate safety concerns, should be permitted to continue the operation without further government involvement or inquiry. Once an official determines that the operation is lawful, and in the absence of an articulable safety concern, the official should proceed no further.

The regulatory scheme included in this recommendation is different than license plate on a vehicle – it is more akin to the information included on your driver’s license. A license plate on a vehicle can be seen from the naked eye, and courts have therefore held that an operator has no legitimate right to privacy to your license plate. However, in this case the recommendation is that a UAS must broadcast its identification and history of operations beyond line of sight. Allowing a public safety officer access to the PII associated with the drone and the history of the drone operation without cause is more similar to allowing them to ask an individual to produce their license and search their phone’s location history without cause.

To ensure that public safety officials act only under appropriate circumstances, and to protect the lawful rights of journalists, and other drone operators, any proposed rule should recommend the inclusion of a standard to guide officials who consider whether to access the database. Law enforcement officials already are familiar with the “probable cause” and “reasonable suspicion” standards, under which the law strikes the balance between public safety and individual freedoms. Indeed, current law and regulation already contain numerous examples that limit access to information about journalists’ activities to instances where law enforcement is able to satisfy legal standards:

- The Privacy Protection Act, 42 U.S.C. § 2000aa, which governs the issuance of search warrants to journalists, provides that “it shall be unlawful for a government officer” to

search or seize a journalist's work product unless "there is probable cause to believe that the person possessing such materials has committed or is committing the criminal offense to which the materials relate..." .

- Similarly, the United States Attorney General's policy regarding obtaining information from, or records of, journalists, 28 CFR § 50.10, applies in all instances except where the government has "reasonable grounds to believe that the individual or entity is", for example, "a member or affiliate of a terrorism organization." Moreover, before authorizing a subpoena in a criminal matter, the Attorney General himself must articulate, among other requirements, "reasonable grounds to believe, based on public information, or information from non-media sources, that a crime has occurred[.]"

The News Media Coalition urges that any proposed rule contain either a "probable cause" or "reasonable suspicion" standard before a public safety officer accesses information beyond the visible unique identifier. This would both provide officials in advance with guidance on when interrogation of a drone or an operator is appropriate, and it would ensure that if required after the fact, officials could articulate, in clear and specific terms, the conduct or characteristic of the drone operation that justified accessing the additional information.

The Proposed Regulation Should Require the FAA to Maintain a Record, Subject to the Freedom of Information Act,
Listing All Instances Where Public Safety Officials Access the Database

The Report notes that for public safety officials, "the core of the concern regarding UAS operations is accountability." (Report 5.2.2). Accountability of the government, especially where it concerns accessing the PII of its citizens and tracking their movements, is at the core of the First Amendment. Public confidence in its government is best fostered through transparency. The Report provides for no oversight or accountability whatsoever for officials' decisions to interrogate a drone or its operator.

Given the First Amendment, Fourth Amendment, and general privacy implications inherent in accessing information about drone operators and operations – and especially information about the independent operations of journalists – the FAA should serve transparency by establishing and maintaining a central record of all instances where a public safety official accesses the database. That record should contain, at a minimum, the date of access, the agency and officer accessing the information, the probable cause or reasonable suspicion for accessing the information, and the agency's determination as to the validity of a threat.

The News Media Coalition understands that because of the exigencies in responding to a perceived threat, in many instances this information cannot be logged simultaneously with the event. Any proposed rule therefore should provide that, within a reasonable time period following the conclusion of a public safety official's response to an inquiry about a UAS, the

official must complete the information in the FAA's central record. The proposed rule also should provide that the central record is subject to the federal Freedom of Information Act, 5 U.S.C. § 552.

The Proposed Regulation Should Not Impose Requirements on News Organizations' Policies for the Retention of Newsgathering Materials

The control of journalists' newsgathering materials, such as notes and photographs – absent a subpoena or a warrant, and an opportunity to challenge it in court – ordinarily is left in the hands of the news media.¹ Indeed, when the President directed the National Telecommunications and Infrastructure Administration to convene a group to develop voluntary UAS privacy “best practices”, the multi-stakeholders in attendance agreed to carve journalists out altogether from the requirements to retain information.²

The Report recommends that any proposed rule require operators retain “all relevant tracking data” “for a reasonable period of time to allow public safety and other authorized users to have access to information critical to investigations.” (Report 7.1.4). A requirement imposing on journalists an obligation to preserve newsgathering materials, absent a subpoena or court order

¹ See, e.g., 28 C.F.R. § 50.10, the Department of Justice’s policy regarding obtaining information or records from the news media.

² https://www.ntia.doc.gov/files/ntia/publications/uas_privacy_best_practices_6-21-16.pdf).

and an opportunity for a court challenge, would run afoul of the First Amendment and directly threaten the autonomy of the free and independent press.

Any proposed rule, to the extent it imposes requirements for the retention of information that would track an operation, therefore should expressly exempt journalists’ newsgathering materials.

The Proposed Regulation Should Not Require Journalists Operating in Class G Airspace to File Flight Plans

The Report provides for the optional providing of “route data,” further defined as “prep-programmed navigation or flight plans.” (Report 6.5.1.5). The News Media Coalition agrees and underscores that mandatory filing of flight plans, by journalists operating under Part 107, would raise legal and practical concerns and would constitute prohibited routine surveillance of journalists.

Under our legal system, the First Amendment autonomy for journalism takes precedence absent a government safety interest of the highest order. A system that requires all journalists using drones to file flight plans would, by definition, constitute the perpetual surveillance of journalists' activities without a specific threat to safety. Such a system would be unconstitutional.

Additionally, given the nature of breaking news and the assignment system in newsrooms in general, journalists often must react to newsworthy developments with little prior notice. It is therefore impractical, and overly burdensome to ordinary news operations, for journalists to be required to routinely file flight plans for operations under Part 107 in Class G airspace before beginning a UAS operation.

We further note that, in manned aviation, a flight plan is only required in certain circumstances where the FAA has determined that it is necessary to maintain safe operations. Similarly, the transition to Automatic Dependent Surveillance-Broadcast (ADS-B) for manned aircraft only requires its use in controlled airspace. Manned aircraft operating in Class G and other non-controlled airspace are not ordinarily required to file a flight plan in advance or to communicate flight details, direction or altitude. It is illogical for the FAA to place an unmanned aircraft under 55 pounds operating under 100 mph under a more rigorous requirement to file flight plans than larger, faster-moving manned aircraft.

Any proposed regulation therefore should not require that journalists conduct operations in Class G airspace, pursuant to Part 107, to file a flight plan.

**The Report Appropriately Recognizes that a Proposed Regulation
Must be Content Neutral and Narrowly Tailored**

The News Media Coalition acknowledges and appreciates the inclusion in the Report of a section titled "First Amendment" in which the ARC acknowledges "the use of UAS for news-gathering and other purposes can implicate First Amendment rights and considerations [,]" and that a proposed rule must be "content-neutral and narrowly focused on regulating aviation safety". (Report 7.3).

As this language notes, content-neutrality and narrow tailoring are legally required whenever the government regulates in a manner that would implicate the First Amendment interests of journalists and the public. This language, however, is the only portion of the Report that reflects the ARC's consideration of these interests. As this Dissent notes, other indispensable First Amendment issues must also be addressed in the rulemaking process.

* * *

The News Media Coalition thanks all members of the ARC for the congenial and collaborative exchange of ideas during the ARC's work over the past few months. We look forward to this proposed rulemaking, and we sincerely hope that it will incorporate the significant First Amendment issues we have raised.

Respectfully submitted by the News Media Coalition, consisting of:

Advance Publications, Inc.

American Broadcasting Companies, Inc.

American Society of Media Photographers

The Associated Press

Capitol Broadcasting Co.

Gannett Co., Inc.

Getty Images (US), Inc.

Gray Television, Inc.

Media Law Resource Center

MPA – the Association of Magazine Media

The National Press Club

National Press Photographers Association

NBCUniversal Media, LLC

News Media Alliance

The New York Times Company

Radio Television Digital News Association

Reporters Committee for Freedom of the Press

The E.W. Scripps Company

Sinclair Broadcast Group, Inc.

TEGNA, Inc.

WP Company LLC

Represented by: Charles D. Tobin, Ballard Spahr LLP
Joel E. Roberson, Holland & Knight LLP

Voting Member:	Justin Towles
Company Name:	AAAE
Date Received:	10/2/17
Response:	I concur with the final report as written with the following exceptions:
<p>We take exception with Section 6.1, specifically Option 1 for the threshold category. This language and overall concept was not thoroughly vetted through Working Group 2 and runs contrary to some of the key needs articulated by that group. Furthermore, this language was submitted late in the ARC process and was only discussed at and subsequent to the last plenary meeting, where a number of key stakeholders were not present. The lack of thorough discussion of this issue, we believe, may have led to confusion among the members of the ARC regarding the concept.</p> <p>Option 1 creates an operational-based equipage requirement that will likely lead to manufacturers deciding to not equip their aircraft with the ID or tracking capabilities due to large numbers of Part 101 customers being exempt. This will significantly deteriorate overall compliance. The way the report is presented assigns equal weight to two principals that were not equally debated and discussed. There was consensus coming out of Working Group 2 about option 2, while I'm not aware of any true consensus for option 1. We feel that if the ARC had the time to hold one additional plenary or an additional call on the topic we may have been able to gain consensus. Unfortunately, as written, we simply cannot concur with this portion of the report.</p>	

Voting Member:	Melissa Tye
Company Name:	Verizon
Date Received:	10/2/17
Response:	I concur with the final report as written

Voting Member:	Tyler Valiquette
Company Name:	Airspace Systems, Inc.
Date Received:	10/2/17
Response:	I concur with the final report as written

Voting Member:	Michael Wall
Company Name:	Fairfax County Police Department
Date Received:	10/5/17
Response:	I concur with the final report as written

Voting Member:	John J. Zelenka
Company Name:	Sky Pod USA
Date Received:	10/2/17
Response:	I concur with the final report as written

FAA UAS ID & Tracking ARC Voting Member Declaration - ARC Recommendations Final Report

	Last Name	First Name	Organization	Concur with Report as Written	Concur with Report as Written with Exceptions	Non-Concur with Final Report	No Response
1	Aitken	Mark	AUVSI		X		
2	Barker	Jack	Farris Technology	X			
3	Beatty	Jon	Flight Safety Foundation		X		
4	Belaus	Greg	AT&T	X			
5	Bishop	Ron	Hangar51				X
6	Branch	Ted	Drone Aviator, Inc.	X			
7	Cassidy	Sean	Amazon Prime Air		X		
8	Coon	Jim	AOPA				X
9	Cooper	Diana	PrecisionHawk	X			
10	Cox	Gabriel	Intel	X			
11	Daniel	Edwin	Montgomery County Police Department				X
12	DeAngelo	Mark	SAE International	X			
13	Devillers	Bud	Globalstar	X			
14	Ellman	Lisa	Commercial Drone Alliance			X	
15	Fanelli	Matt	Skyward, A Verizon Company	X			
16	Feldman	Steven	Miami Beach Police Department		X		
17	Frazier	Alan	Grand Forks Sheriff's Office		X		
18	Gannon	Pat	Los Angeles World Airports	X			
19	Gonzalez	Ralph	New York Police Department (NYPD)				X
20	Graetz	Todd	BNSF Railway	X			
21	Guckian	Paul	Qualcomm	X			
22	Hall	Philip	RelmaTech		X		
23	Hanson	Rich	AMA		X		
24	Harrington	Dan	Metropolitan Police Department (DC)				X
25	Hatfield	Mark	Miami-Dade International Airport	X			
26	Hennig	Jens	GAMA		X		
27	Hughes	Robert	Northrop Grumman	X			
28	Jetton	Andrew	Rockwell Collins		X		
29	Johnson	Doug	CTA		X		
30	Kenul	Philip	ASTM International		X		
31	Kimmel	Shawn	IEEE		X		
32	Kucera	Chris	Analytical Graphics, Inc.	X			

33	Kunzi	Fabrice	General Atomics			X	
34	Lacher	Andy	The MITRE Corporation	X			
35	Manley	Justin	Just Innovation	X			
36	Martino	Chris	HAI	X			
37	Mason	Travis	A3 & Aerial by Airbus	X			
38	McDuffee	Paul	Insitu, Inc.			X	
39	McLeod	Jeff	National Governors Association				X
40	McNeal	Greg	AirMap		X		
41	Miller	David	American Petroleum Institute (API)	X			
42	Mond	Rebecca	The Toy Association, Inc.			X	
43	Moore	Andrew	NAAA		X		
44	Murphy	Sean Patrick	T-Mobile USA	X			
45	Nabors	Bill	Texas Department of Public Safety, Aircraft Operations Division	X			
46	Novak	George	AIA		X		
47	Patterson	Vas	ALPA		X		
48	Ponto	Laura	X			X	
49	Preiss	Bruce	FlyTransparent/Black River Systems Company	X			
50	Ramsey	Christian	uAvionix		X		
51	Reyes	Eddie	The Police Foundation				X
52	Richter	Jennifer	CTIA/Akin Gump	X			
53	Roby	Don	IACP				X
54	Rush	Steven	PHPA	X			
55	Schulman	Brendan	DJI Technology		X		
56	Schwarzbach	Daniel	ALEA		X		
57	Secen	Al	RTCA	X			
58	Sedam	Mike	California Highway Patrol, Office of Air Operations	X			
59	Senkowski	Michael	DLA Piper	X			
60	Shea	John	NASAO	X			
61	Shomko	Dennis	Dronsystems Limited				X
62	Singh	Adi	Ford Motor Company			X	
63	Snyder	Kyle	ASSURE	X			
64	Sommer	Lee	College Park (MD) Airport				X
65	Stewart	Ken	GE Aviation			X	
66	Sugahara	Kenji	Ariascend/DUGN	X			
67	Tobin	Chuck	News Media Coalition (Ballard Spahr LLP)			X	
68	Towles	Justin	AAAE		X		
69	Tye	Melissa	Verizon	X			

70	Valiquette	Tyler	Airspace Systems, Inc.	X			
71	Wall	Michael	Fairfax County Police Department	X			
72	Werner	Charles	National Council on Public Safety				X
73	West	Darrell	The Brookings Institute				X
74	Zelenka	John	SkyPod, USA	X			
			TOTALS:	34	20	8	12