

Association of Corporate Counsel National Capital Region

Hot Topics in New Technologies

Akin Gump
STRAUSS HAUER & FELD LLP

September 29, 2021

Jennifer L. Richter
Partner
Akin Gump Strauss Hauer & Feld
jrichter@akingump.com
+1 202.887.4524

Avonne Bell
Director, Connected Life
CTIA
abell@ctia.org
+1 202.736.3246

© 2021 Akin Gump Strauss Hauer & Feld

ACC Association of
Corporate Counsel
— NATIONAL CAPITAL REGION —

Overview

Small Unmanned Aircraft Systems (UAS)

- Market Forecasts
- Use Cases
- UAS Integration Timeline
- Compliance Requirements

Connected Life

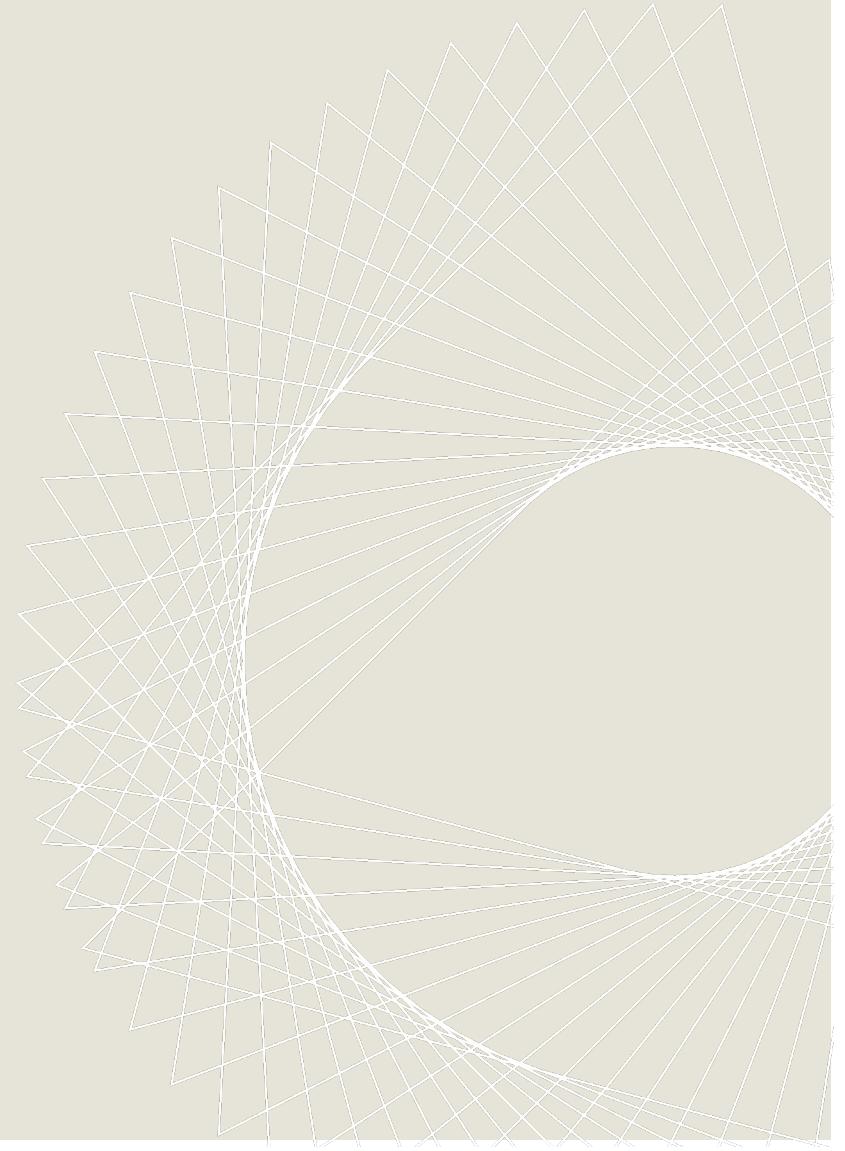
- Mobile Wireless Connectivity, AI, & IoT

Protecting Your Assets

UAS Traffic Management

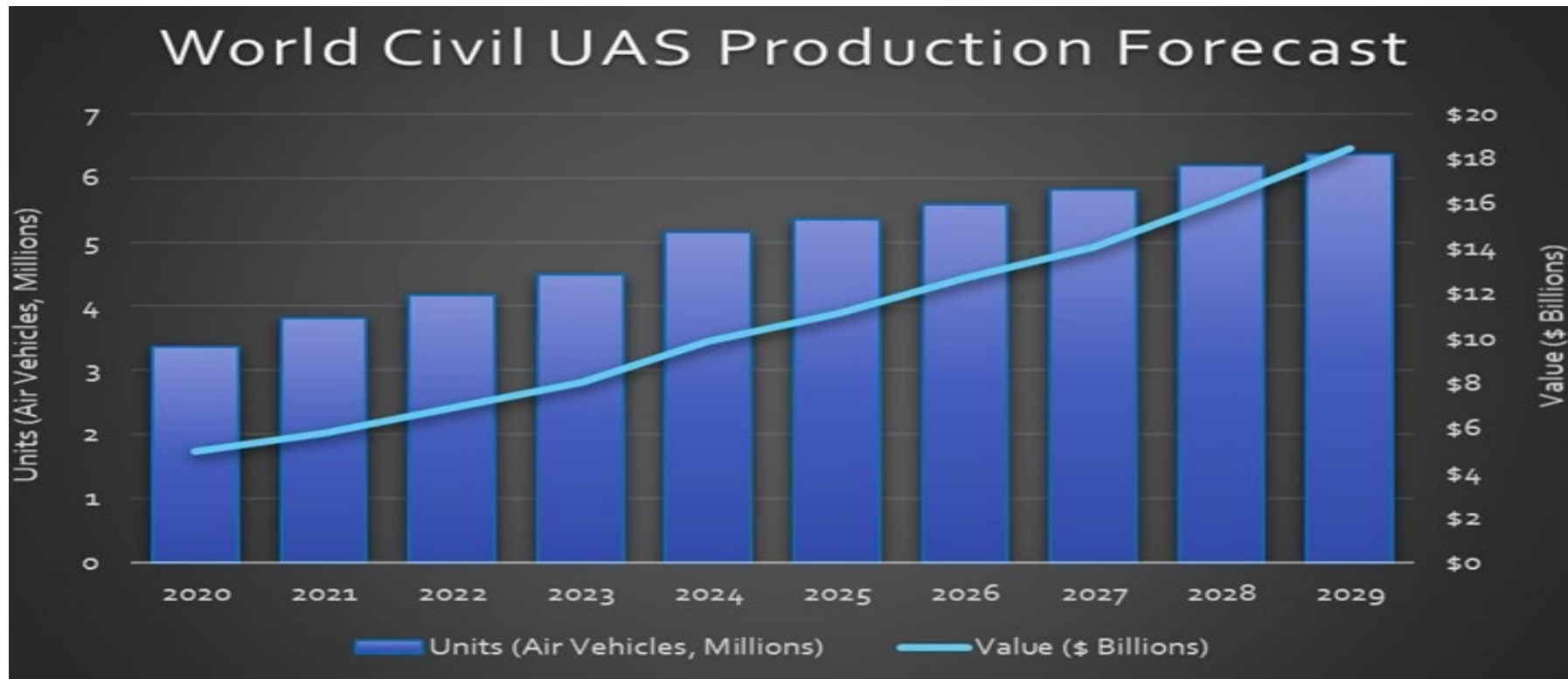
Advanced Air Mobility (AAM)

Market Forecasts



Market Forecasts – The Economics

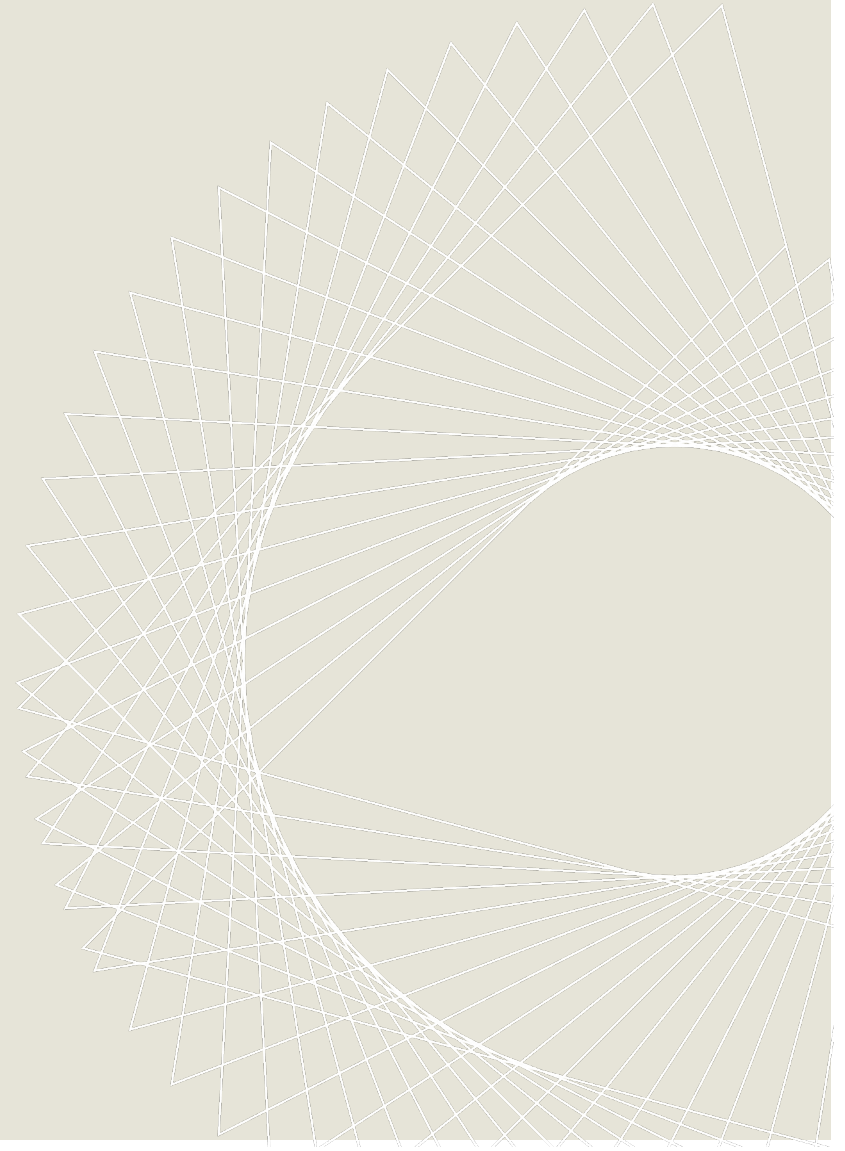
Teal Group's forecast projects that non-military UAS production and use will total \$108 billion in the next decade, soaring from \$5 billion worldwide in 2020 to \$18.4 billion in 2029. Their study includes annual forecasts of commercial, consumer and civil government systems.



The forecast notes that commercial use will drive the market as consumer use slows. Corporations are moving from proof of concept to deployment of fleets of drones, driving the commercial market.

There is a more than a 21 percent compound annual growth rate for commercial UAS production over the 10-year forecast. The civil market is attracting leading tech companies and driving faster development of systems and business applications.

Use Cases



Use Cases – Where Won't Drones Have Application?

Oil Industry

- “The energy industry has turned to robots and drones to cut costs and improve safety in some of the world’s tougher working environments.”
- “Big oil producers ...are racing to create the [oilfields of the future, where smart devices replace workers](#). They have the potential to cut costs, save lives, and reduce the scope for human error.”

Electrical Utility Industry

- “When hurricane Harvey hit Texas last August, drone operators became an integral part of the recovery response, flying missions to [inspect critical infrastructure](#), assess damage and map flooded areas.”
- “Just like with any first responders, properly trained drone operators need to be able to deploy as soon as possible after a storm hits. The quicker they can respond, the quicker they can remediate, which is why pre-positioning is so critical...”

Telecommunications

- “AT&T has deployed its helicopter Flying COW (Cell on Wings) to [temporarily provide data, voice and text services](#) to Puerto Rico in the aftermath of Hurricane Maria.”
- “The [Flying COW](#) hovers 200 to 400 feet above the ground and offers wireless connectivity in an up to 40-square-mile area, a distance that AT&T says is farther than other temporary cell sites.”

Health Care

- “[E]arly public acceptance of drone delivery networks in urban areas will revolve around hospitals. And once drones can safely and reliably [carry blood and medical supplies](#), that will pave the way to other kinds of drone deliveries.”
- “Beyond blood and medical supply deliveries, drones could transform another key component of healthcare — lab tests. Timely test results help doctors diagnose infections and reduce guesswork in prescribing medications. Some of those decisions have life-or-death implications.”

Package Delivery

- “In the future, Amazon drones may be able to tell you to get out of the way — and listen to your response — when delivering a package.”
- “The concept is in line with other Amazon products that are being developed with voice-controlled digital assistant, Alexa. It’s possible that human customer service agents may also use the technology to communicate remotely with people and animals on the ground, the patent says.”

Use Cases – Where Won't Drones Have Application?

Construction

- “[C]onstruction drone usage has skyrocketed by 239 percent year over year, compared to 198 percent in mining and 172 percent in agriculture, according to a May report on commercial drone trends by DroneDeploy, which provides mapping solutions for drone users.”
- “Drones have taken over the role of cumbersome and expensive planes that previously handled [on-site aerial photography](#). While the devices can be outfitted to handle more advanced jobs like mapping and thermal heat imaging...the majority of drone work is to take aerial site photographs.”

Newsgathering

- “Faster mobile bandwidth will allow us to get richer content from our journalists faster and will hopefully allow us to deploy this technology more widely for [breaking news events](#).”
- “Drones have democratized aerial imagery, as it no longer costs thousands of dollars to rent a helicopter or a plane to make images from above.”

Real Estate

- “The Cleveland Fed said one commercial real-estate builder invested in drones to [conduct land surveys](#) because of an engineering shortage.”
- “Firms are also updating their current technologies or adopting new ones to boost production and keeping labor costs down.”

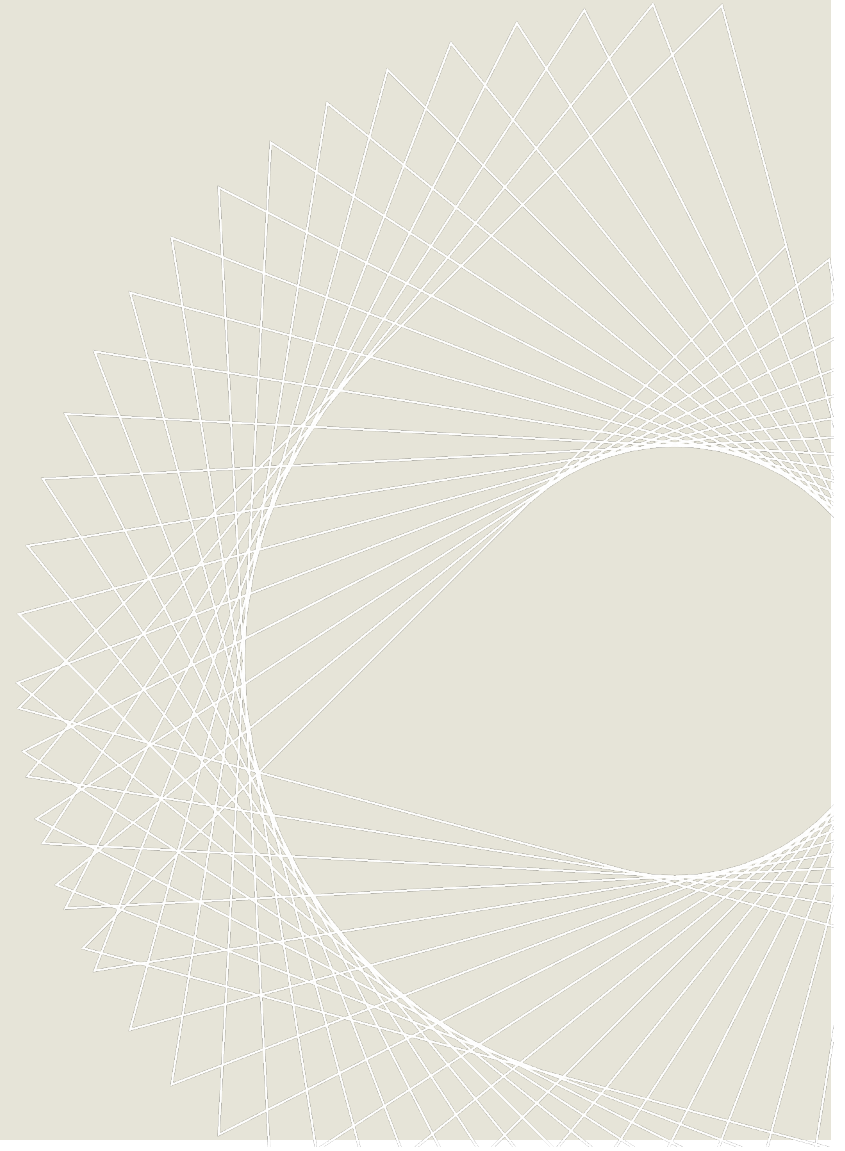
Insurance

- “The ability of drones to capture massive amounts of data quickly and efficiently is beneficial in all aspects of the insurance transaction.”
- “Claims adjusters can use the flying technology to automatically generate loss reports without placing human workers in potentially dangerous scenarios. There are also opportunities for underwriters to use drones to generate a richer understanding of [a current state of an area or item](#), and therefore provide more accurate coverage and pricing solutions.”

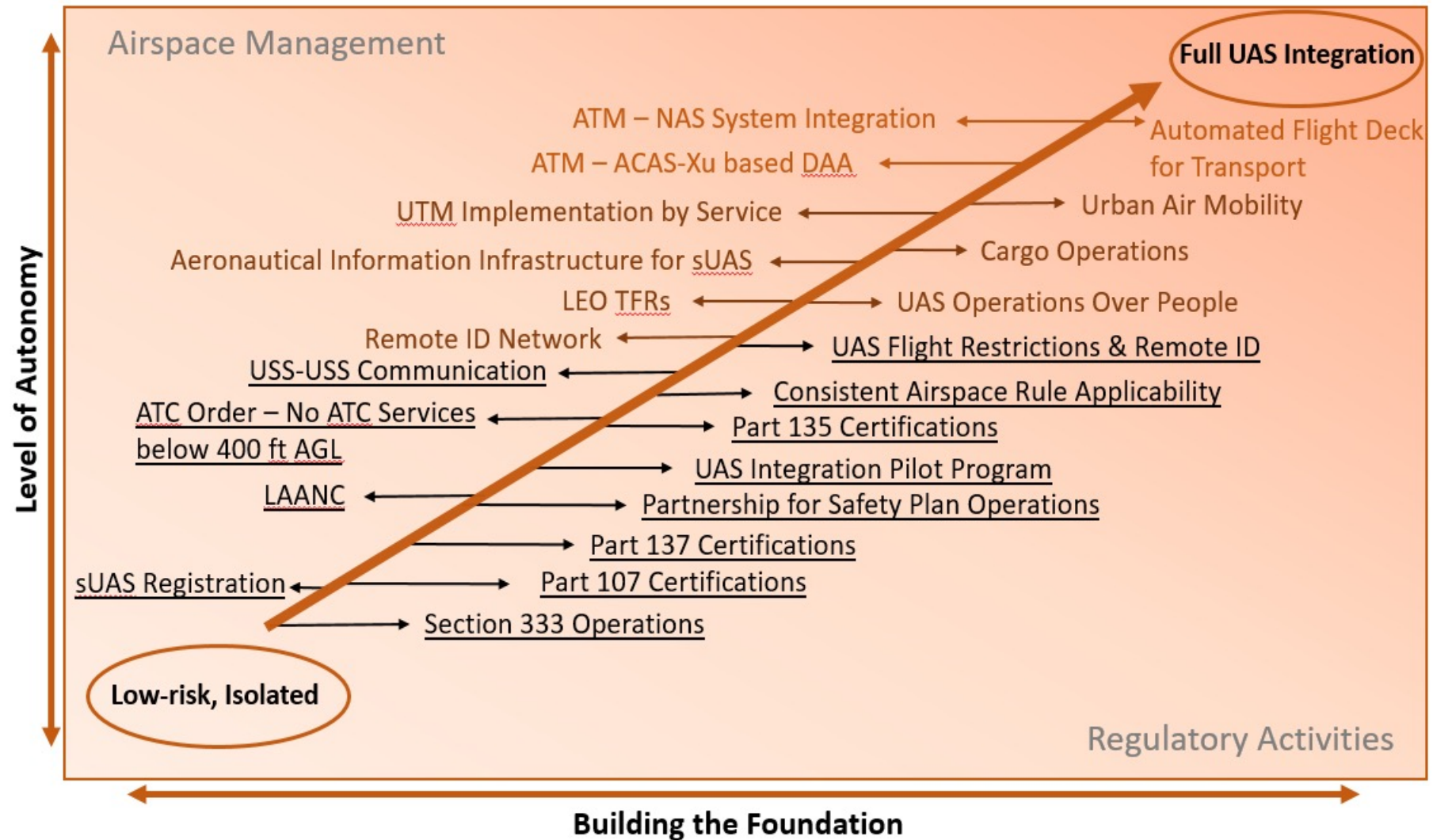
Farming

- “[R]esearchers are working on other ‘[agribots](#),’ such as drones that can pollinate flowers instead of bees, and smart sprayers that can calculate exactly how much pesticide should be spewed onto grapevines to prevent disease.”
- “[Agribots] could impact the future of food safety and security: As more crops move from fields into greenhouses, whether because of climate change or other reasons, pollinating can be a challenge.”

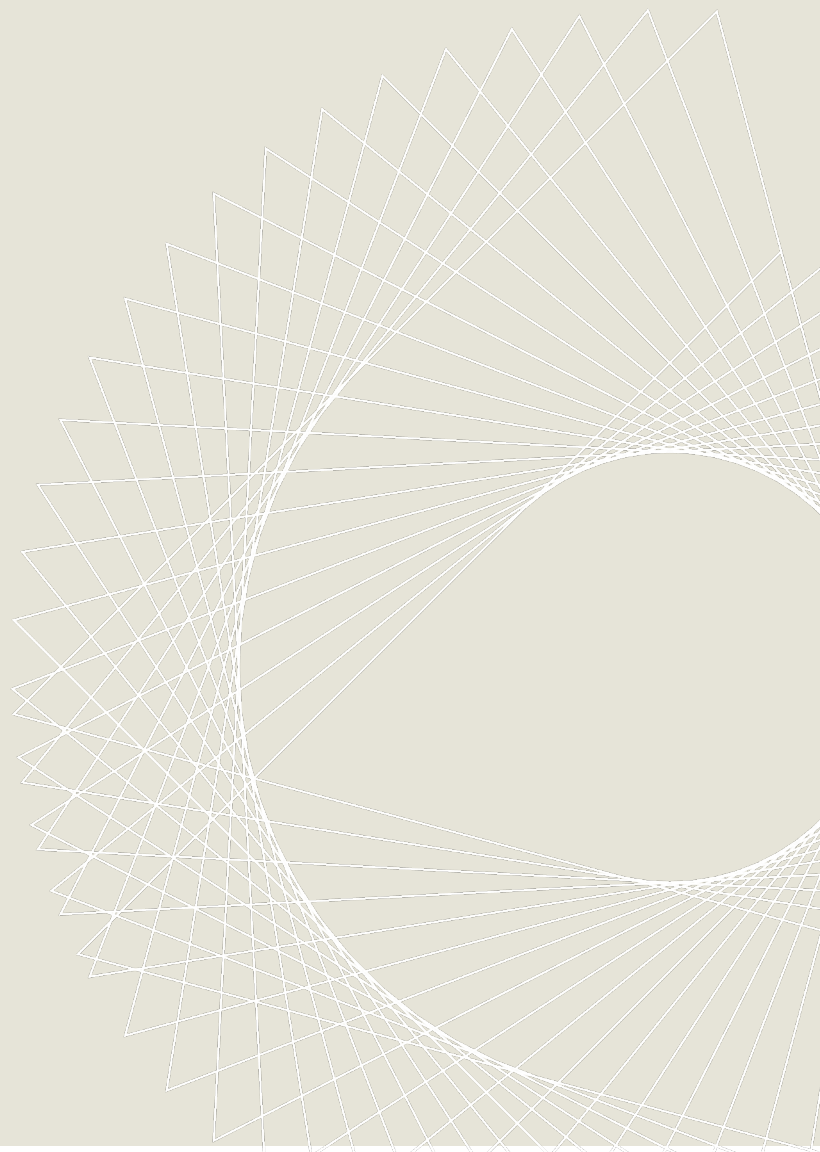
UAS Integration Timeline



UAS Integration Strategy - 2020



Compliance Requirements



FAA Compliance – The Basics

Recreational Operations		Small UAS Operations (Part 107)	Public COA Operations
Pilot Requirements	<ul style="list-style-type: none"> No FAA pilot requirements 	<ul style="list-style-type: none"> Must have Remote Pilot Airman Certification Must be 16 years or older Must undergo TSA security screening 	<ul style="list-style-type: none"> Self-certification of crew and equipment
Aircraft Requirements	<ul style="list-style-type: none"> Must be registered if over 0.55 pounds 	<ul style="list-style-type: none"> Must be less than 55 pounds Must be registered if over 0.55 pounds Must undergo pre-flight checklist 	<ul style="list-style-type: none"> Must verify Public Aircraft Operator eligibility and be issued a Certificate of Waiver or Authorization (COA) or MOA
Location Requirements	<ul style="list-style-type: none"> Must notify all airports and air traffic control (if applicable) within five miles of proposed area of operations 	<ul style="list-style-type: none"> Class G airspace without ATC permission Class B, C, D, and E require ATC permission 	<ul style="list-style-type: none"> Detailed in COA and/or MOA
Operating Rules	<ul style="list-style-type: none"> Must ALWAYS yield right of way to manned aircraft Must keep aircraft in visual line-of-sight Must follow community-based safety guidelines 	<ul style="list-style-type: none"> Must keep aircraft in visual line-of-sight* Must fly under 400 feet* Must fly only during daylight hours* Must fly at or below 100 mph* Must yield right of way to manned aircraft* Must NOT fly over people* Must NOT fly from a moving vehicle* 	<ul style="list-style-type: none"> Detailed in COA and/or MOA
Applications	<ul style="list-style-type: none"> Education or recreational flying only 	<ul style="list-style-type: none"> Flying for commercial/business use Flying recreationally Public operators choosing to operate as Part 107 operator 	<ul style="list-style-type: none"> Federal Agencies State and Local Entities

*These requirements are subject to waiver

FAA Resources

- Waivers: Drone Zone
- Authorizations: Low-Altitude Authorization and Notification Capability (LAANC)
 - Private-sector partners

FAA Compliance

Pilot Requirements

- UAS operations must be executed by a remote pilot that holds a Remote Pilot Airman Certificate granted by the Federal Aviation Administration (FAA).
- Ensure that your pilots are trained in specific, safe operations of UAS around your particular kinds of assets (e.g., understand line sway).
- Develop your own safety manual.
- It would be wise to have all remote pilots working for your company provide their supervisor with a copy of their Remote Pilot Airman Certificate.
- Your remote pilots also should have a copy of their certificate with them while operating a UAS.
- Ensure that you have obligated each of our pilots to keep their certificates current, and certify at regular intervals that they will comply with any of your operating rules and policies, as well as applicable federal rules and regulations.
- There is a 1:1 rule in effect right now – each remote pilot can only command a single UAS at a time.

FAA Compliance

Aircraft Requirements

- Be aware of advisories from our federal government, Immigration and Customs Enforcement (ICE), Army, Department of Homeland Security (DHS) related to purchasing and using foreign manufactured UAS.
- Ensure the drone you are using is appropriate for operations around your particular assets – not recreational, not made of material that will conduct energy if that is an issue for you, contains the right sensors for strategic asset allocation (SAA) / dynamic asset allocation (DAA) and geofencing, has the right cameras, has secure and reliable comms link.
- The aircraft itself, the UAS, must be registered in accordance with FAA rules. Make sure to assign this responsibility and keep copies of the UAS registrations for your organization.
- Under the Small UAS rule, your UAS cannot exceed 55 lbs (25 kgs) including payload (anything you attach to it). You can apply for waiver.
- Develop a preflight inspection checklist.
- Develop a maintenance schedule for your UAS, in accordance with manufacturer recommendations. Keep your maintenance records.

FAA Compliance

Operating Rules

- Develop your own safe operations manual for your particular UAS operations.
- Have a written or verbal flight plan for each mission that considers nearby land features, buildings, infrastructure, topography, weather patterns, location of airports, hospitals, schools and special events. There are software programs that can help.
- There are no federal privacy laws related to UAS, but there are state privacy laws. Consider privacy issues of third parties that could be impacted by your operation.
- Conduct a pre-flight inspection. The remote pilot should record the pre-flight inspection in hard copy or online. There are various services available.
- Empower your remote pilot to abandon operations if there is any concern about safe operations.
- Under current FAA rules and, without waivers, maintain visual line-of-sight at all times and employ a visual observer where possible to assist.
- Avoid operations over people unless those people are participating in the flight plan.

FAA Compliance

Operating Rules (cont.)

- UAS must yield the right-of-way to other aircraft.
- Operations must stay within Class G airspace – well away from airports.
- If operations must move into other controlled airspace – Class B, C, D, for example – the remote pilot must request and receive permission from air traffic control (ATC).
- Operations should steer clear of heliports.
- No careless or reckless operations.
- No carriage of hazardous materials.
- Remember that if UAS operations result in serious injury, loss of consciousness or property damage of at least \$500, the remote pilot must make an official report to the FAA.

FAA Compliance

Operational Waivers

- The FAA will entertain waivers of the Part 107 rules after filing the appropriate applications.
- Waivers are available for:
 - Daylight operation (§ 107.29) – to enable nighttime operations
 - Visual line of sight aircraft operation (§ 107.31) – to enable beyond visual line of sight (BVLOS)
 - Visual observer (§ 107.33)
 - Operation of multiple small unmanned aircraft systems (§ 107.35)
 - Operation over people (§ 107.39)
 - Operation in certain airspace (§ 107.41)
 - Operating limitations for small unmanned aircraft (§ 107.51)
 - Operation from a moving vehicle or aircraft (§ 107.25)
 - Yielding the right of way (§ 107.37(a))

Corporate Compliance – Privacy and Data Security

- There are no federal privacy laws related to UAS operations, but privacy has been a big focus in Washington, D.C. and some states have considered privacy regulations related to drones.
- The California Consumer Privacy Act (CCPA), signed into law in 2018, provides a number of private rights related to privacy and the collection of personal information, including a right to “opt-out” of sale of their personal information, the right to demand deletion of their personal information, etc. The CCPA also requires a number of disclosures to be made regarding personal information that is collected, used or sold and creates a private right of action for data breaches.
- The CCPA defines both “personal information” and “collection” of such information exceedingly broadly. For example, “**personal information**” is defined as “information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household,” including but not limited to “audio, electronic, visual, thermal, olfactory, or similar information.” Similarly, “**collection**” is defined as “buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means...either actively or passively, or by observing the consumer’s behavior.” With such broad definitions, the provisions of the CCPA could be applied to data captured many different ways, including by drones.
- Also consider the **new California Internet of Things (IoT) Law**, signed September 28, 2018, requiring IoT vendors and manufacturers to ensure that IoT devices (which can include drones) have security features in place that protect information collected, contained or transmitted by the device. Note that the law goes beyond protecting personal data and is meant to protect any data collected, contained or transmitted by the device, including data collected by drones.

Privacy and Data Security (Continued)

- There is a “Voluntary Best Practices for UAS Privacy, Transparency, and Accountability” Guide that was put together by a multi stakeholder group convened by the National Telecommunications and Information Administration (NTIA) in May 2016. https://www.ntia.doc.gov/files/ntia/publications/uas_privacy_best_practices_6-21-16.pdf
 - Under the “best practices,” flight plans and operations should avoid collecting and storing “covered data” when possible. “Covered data” means information collected by a UAS that identifies a particular person.
 - Develop procedures for securing “covered data” or other data collected by a UAS that could infringe on a privacy interest of a third party.
 - Try to avoid UAS operations over third-party private property in order to control for privacy issues.
 - Involve your IT department early and apply the same data protection policies to UAS-collected data as other data.
 - Same is true for your cybersecurity policies – the same policies should apply to your drone operations.

Corporate Compliance

Outside Contractors

- If your company uses outside contractors for your drone operations, develop the right agreement for their services.
- Make sure your agreement requires your contractor to comply with any of your operating rules, your cybersecurity and data protection policies, all FAA regulations...
- Make sure it is clear that you own any data collected by the contractor, they will transfer all data to you, they will not keep any of your data
- Require use of the right types of drones by your contractor; if you are concerned about cybersecurity, limit the ability of the contractor to use foreign-manufactured drones and/or require them to ensure any data links are turned off so that your mission critical information is not compromised.
- You also should ensure that your contractor indemnifies you and holds you harmless from any liability for personal/property damage caused by the contractor's UAS operations.
- Ensure that your contractor has adequate insurance to protect against liability, and provides you with a certificate of insurance specifying you as an additional insured.

Risks From Drones

Insurance Issues

- There are a number of Owner/Operator liability risks associated with using drones:
 - UAS colliding with operator
 - UAS colliding with person
 - UAS colliding with structure, thereby damaging the structure and/or causing personal injury
 - UAS colliding with another UAS
 - UAS colliding with a manned aircraft
 - UAS coming close to a manned aircraft requiring evasive action by the manned aircraft operator, which in turn results in personal injury or property damage
 - UAS being hacked/taken over and used negligently, or for criminal purposes, by third party
 - UAS not operated in compliance with federal law and any applicable state or local law.

Risks From Drones

Insurance Requirements?

- There are presently no insurance requirements for UAS from the Department of Transportation (DOT)/FAA. The best analog is the provision governing air taxi operators (non-scheduled) – 14 CFR Part 205.
- DOT insurance requirements depend on the size of aircraft being used and the nature of operations (i.e., carrying passengers).
 - \$75,000 for any one person (not on the aircraft) in any one occurrence
 - \$300,000 per involved aircraft for each occurrence
 - \$100,000 for each occurrence resulting in damage to or loss of property.
- Although the federal government doesn't require insurance today for drones, some cities and states are considering these requirements. A proposed bill in the city of New York would require an unmanned aerial vehicle (UAV) operator to carry insurance and the failure to meet this requirement could result in a civil penalty and seizure of the UAV.
- As drone use becomes more common, the requirement for appropriate levels of insurance should be expected.

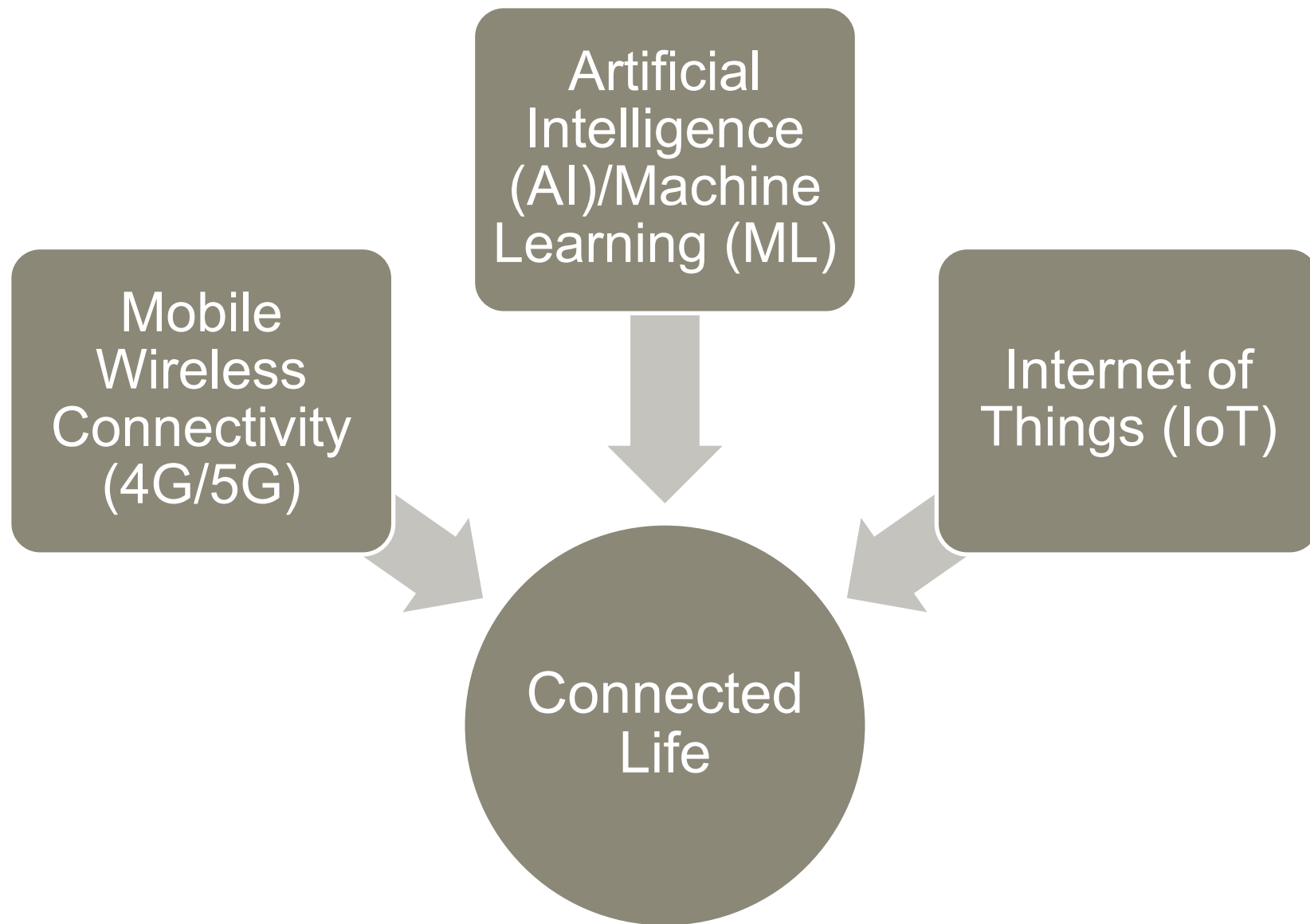
Risks From Drones

Insurance Requirements? (cont.)

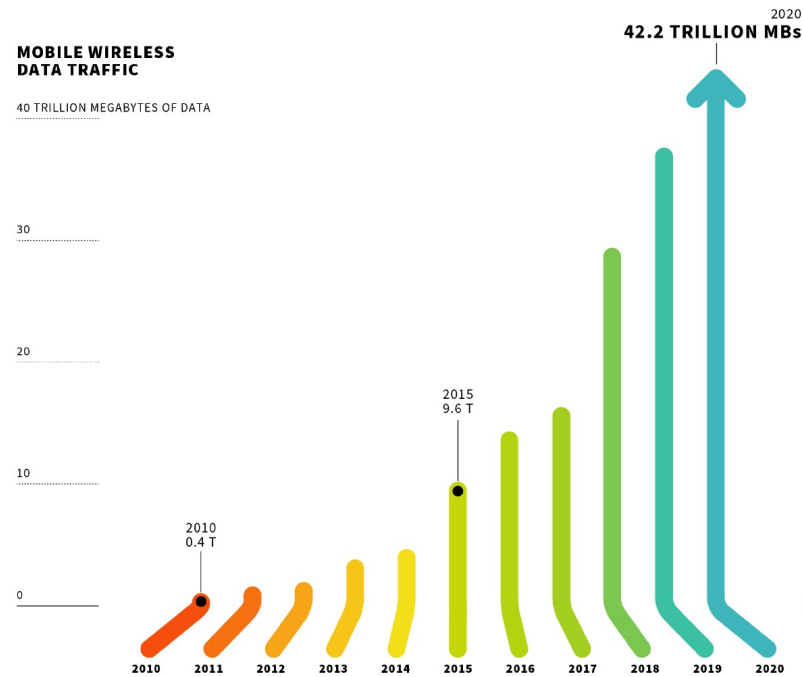
- UAS Aviation insurance falls into two basic categories;
 - Legal Liability together with Physical Damage (otherwise known as hull) for the owner/operator.
 - Product Liability for the service provider.
- Liability insurance is the minimum.
 - This covers the cost to repair property you may damage and injury to persons. Additional coverage may include personal injury (invasion of privacy), non-owned (if you crash someone else's drone), war perils including malicious damage, medical expenses and premises liability.
 - Coverage also is available against physical damage to the UAS system. This covers the cost to repair, or the total loss of either the platform, payload or ground equipment.

IoT, Connected Life, Wireless and 5G

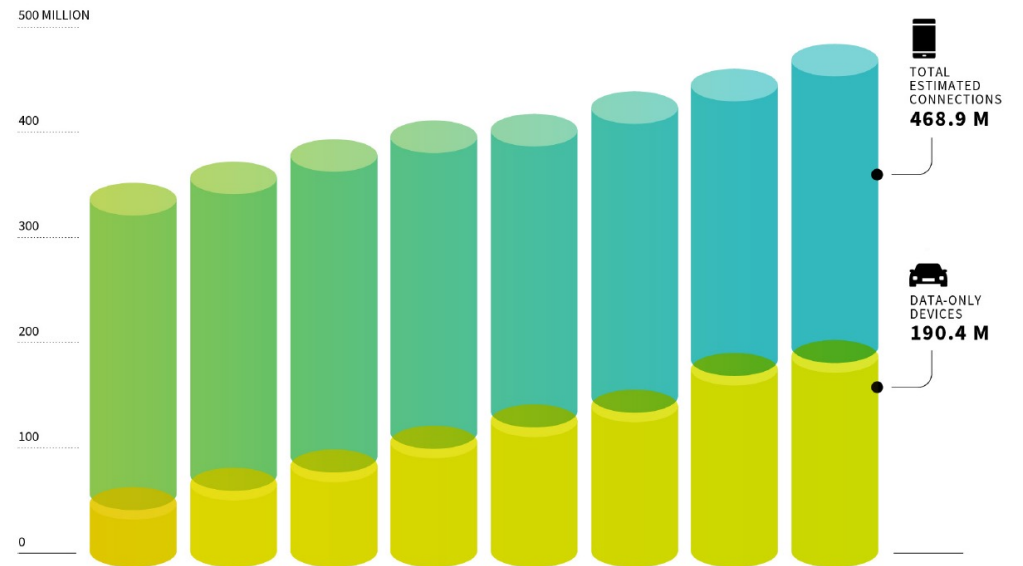
Elements of Connected Life



Growth of U.S. Use of Mobile Wireless Connectivity

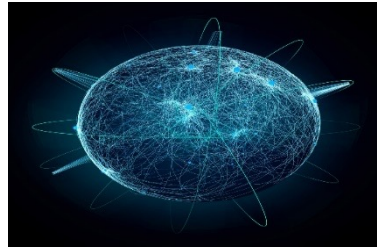


NUMBER OF WIRELESS CONNECTIONS



Source: CTIA 2021 Annual Survey

Mobile Wireless Connectivity (4G/5G)



- 4G provides reliable, secure, high-speed connections, 31x faster than the prior decade.
- 4G enables use of increasingly data-intensive applications.
- 5G is expected to radically disrupt most vertical industry sectors (e.g., transportation, medical, agriculture, commercial/business operations).
- 5G provides ultra-high-speeds, ultra-low latency and multi-device connectivity.
- 5G's edge computing technology enables near-instant communication, computing and processing to provide real-time data.
- Wireless connectivity of today as well as tomorrow can provide the features to power connected life.

Artificial Intelligence/Machine Learning

- Artificial intelligence (AI) and machine learning (ML) use algorithms to automate and optimize certain operations and functions.
- AI/ML in conjunction with 5G help to advance connected technology functions and advance IoT capabilities.
- Outside of IoT it can be used to automate functions like hiring, employee management in identifying patterns, practices.

Corporate Internet of Things Uses

- Smart building/office
- Smart cities
- Connected and automated vehicles
- Connected Health
- Connected Education
- Agriculture/Farming
- Industrial IoT manufacturing

Connected Life Legal Considerations

Cybersecurity

- First half of 2021 saw 1.5 billion attacks on smart devices, up from 639 million during the previous half year, which is more than twice the volume – Kaspersky.
- IoT devices, from smart home accessories to smart offices, have become an essential part of our everyday lives, and they are increasingly a target for cyber attacks.

Government/Regulatory Activity

- IoT Cybersecurity Improvement Act (2020)
- NIST IoT Security Standards publications
- Executive Order on Improving the Nation's Cybersecurity (2021)

Artificial Intelligence (AI) Risk

- Concerns about Trust, Bias and Reliability

Government/Regulatory Activity

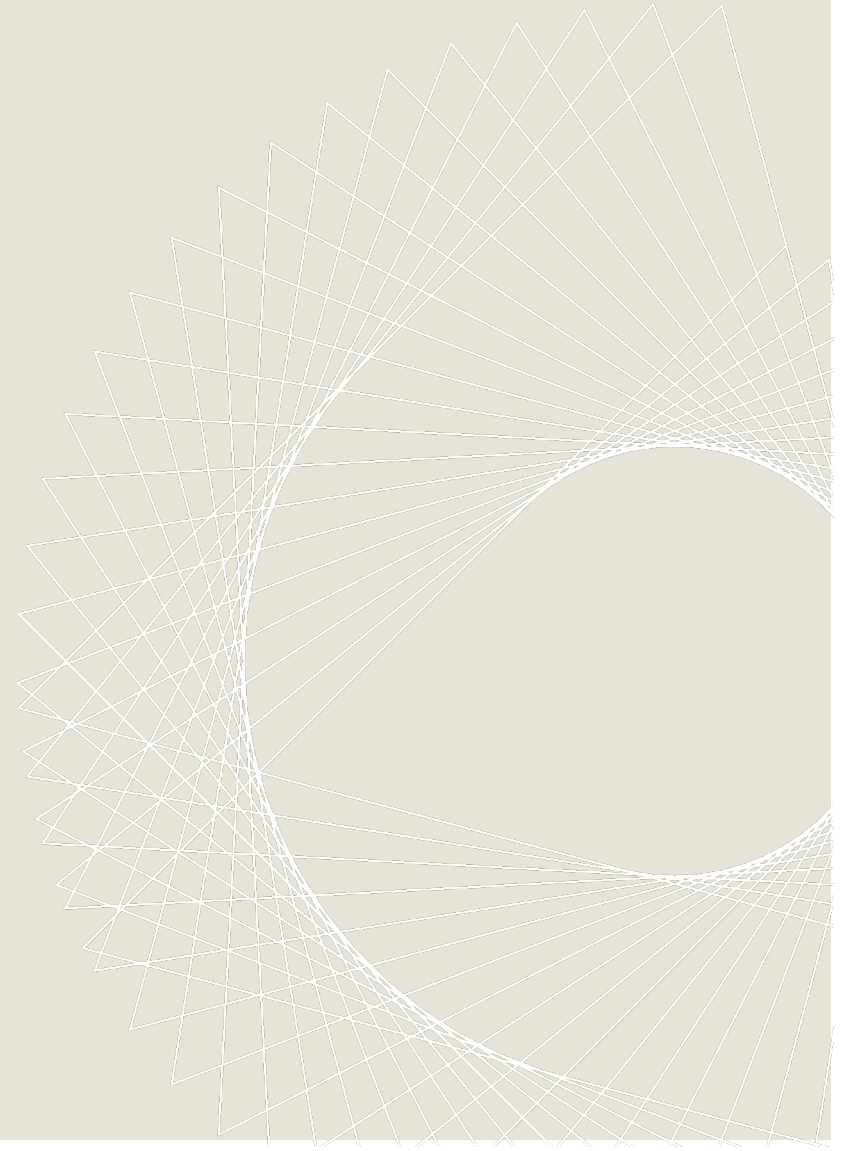
- Executive Order on Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government (2020)
- Department of Treasury RFC on Financial Institutions' Use of AI (2021)
- Federal Trade Commission Guidelines (2021)
- NIST Artificial Intelligence Risk Management Framework RFC (2021)

Risks From Drones

Why Are We Concerned About Cybersecurity and UAS?

- Inherent Qualities of UAS Can Lead to Security Concerns:
 - UAS can fly in unpredictable patterns, they have a low acoustic signature, they can be modified to avoid geo-fencing restrictions.
 - UAS offer a unique level of anonymity, plausible deniability, no required Remote ID and tracking today, there are no controls at the point of sale, they can be easily assembled at home and built with off the shelf parts, registration is voluntary.
- Types of Threats from UAS:
 - They could be weaponized (domestically, a man was charged in a plot to bomb the Pentagon using a model airplane).
 - They could be used for illicit activity (delivering drugs).
 - They can be used in a negligent manner, either ignorantly (White House event) or willfully.
- What do we need to protect from careless, clueless and criminal uses of UAS?
 - Critical infrastructure, power plants, military bases, public gathering places (stadiums, amusement parks).
- What can you do today to protect against drones over your property/operations? Very little.
 - Post “no fly zones,” use attack dog drones, cannot jam, cannot take a drone down.

Protecting Your Assets



Protecting Your Assets – Relying on Property Rights

Supreme Court Case – U.S. v. Causby

The FAA has authority over the “navigable airspace,” but private land owners have control over the airspace that is within the usable and immediate reaches of their land. See United States v. Causby, 328 U.S. 256 (1946).

Navigable Airspace: The FAA has the authority to define and regulate “navigable airspace.” See 49 U.S.C. §§ 40103(a); 40103(b)(1).

- FAA regulations define “navigable airspace” as “airspace at and above the minimum flight altitudes prescribed by [the FAA], including airspace needed for safe takeoff and landing.” 14 C.F.R. § 1.11.
- In general, the navigable airspace begins at 500 – 1,000 feet above the surface. See, 14 C.F.R. § 91.119(b)(c)(d). Below the navigable airspace is, presumably, the area in which a landowner has rights to the airspace.
- However, drones are “aircraft” that can take off and land virtually anywhere, raising the question of where the “navigable” airspace begins. Closer to the ground? FAA is taking an aggressive stance regarding their jurisdiction of all airspace.

Avigation Easements Recognized by the Supreme Court: In 1946, the Supreme Court established the concept of avigation easements, *i.e.*, the property rights of a private landowner to permit aircraft to fly above the landowner’s property.

- At issue in the *Causby* case was whether a chicken farmer’s property was taken, within the meaning of the Fifth Amendment, as a result of frequent and regular flights of army and navy aircraft over the farmer’s land. The glide path for certain military planes passed over the farmer’s property at 83 feet, which was 67 feet above the house and 18 feet above the highest tree.

Protecting Your Assets – Relying on Property Rights

Supreme Court Case – U.S. v. Causby

Avigation Easements Recognized by the Supreme Court:

- The Supreme Court articulated the following in the *Causby* case:
 - Although “navigable air space” is in the public domain, a landowner (1) has “exclusive control of the immediate reaches of the enveloping atmosphere” and (2) “owns at least as much of the space above the ground as he can occupy or use in connection with the land.”
 - Flights over private land by a government entity constitute a “taking” if the flights “are so low and so frequent as to be a direct and immediate interference with the enjoyment and use of the land.”
- The *Causby* case did not answer several important questions:
 - To what height is airspace within the “immediate reaches” of the landowner so as to constitute the landowner’s property?
 - In what circumstances will aircraft flight “direct[ly] and immediate[ly]” interfere with a landowner’s “enjoyment and use” of land?

After Causby: Since *Causby*, a number of courts have recognized the concept of avigation easements. The courts have not yet discussed avigation easements as applied to drones, but we anticipate this will happen.

Protecting Your Assets – Using Tort Law

Right of Action for Trespass?

- The Uniform Law Commission has a Drafting Committee on Tort Law Relating to Drones. They have been working on a uniform law addressing tort liability and defenses uniquely associated with the use of aerial drones, although this work has stalled.
- Issues under consideration include:
 - acquisition of private information of another by improper means,
 - disclosure or use of private information obtained by improper means without consent,
 - trespass by drone,
 - nuisance by drone,
 - self-help and defense of others,
 - and tort action by any party, including a drone owner operator damaged by tortious behavior which includes the use of an unmanned vehicle.

Protecting Your Assets – Using Section 2209

P.L. 114-190

- What can it apply to?
 - Fixed site facility vs. critical infrastructure

SEC. 2209. APPLICATIONS FOR DESIGNATION.

(a) APPLICATIONS FOR DESIGNATION.—Not later than 180 days after the date of enactment of this Act, the Secretary of Transportation shall establish a process to allow applicants to petition the Administrator of the Federal Aviation Administration to prohibit or restrict the operation of an unmanned aircraft in close proximity to a fixed site facility.

(b) REVIEW PROCESS.—

(1) APPLICATION PROCEDURES.—

(A) IN GENERAL.—The Administrator shall establish the procedures for the application for designation under subsection (a).

(B) REQUIREMENTS.—The procedures shall allow operators or proprietors of fixed site facilities to apply for designation individually or collectively.

(C) CONSIDERATIONS.—Only the following may be considered fixed site facilities:

- (i) Critical infrastructure, such as energy production, transmission, and distribution facilities and equipment.
- (ii) Oil refineries and chemical facilities.
- (iii) Amusement parks.
- (iv) Other locations that warrant such restrictions.

(2) DETERMINATION.

(A) IN GENERAL.—The Secretary shall provide for a determination under the review process established under subsection (a) not later than 90 days after the date of application, unless the applicant is provided with written notice describing the reason for the delay.

(B) AFFIRMATIVE DESIGNATIONS.—An affirmative designation shall outline—

- (i) the boundaries for unmanned aircraft operation near the fixed site facility; and
- (ii) such other limitations that the Administrator determines may be appropriate.

(C) CONSIDERATIONS.—In making a determination whether to grant or deny an application for a designation, the Administrator may consider—

- (i) aviation safety;
- (ii) protection of persons and property on the ground;

(iii) national security; or

(iv) homeland security.

(D) OPPORTUNITY FOR RESUBMISSION.—If an application is denied, and the applicant can reasonably address the reason for the denial, the Administrator may allow the applicant to reapply for designation.

(c) PUBLIC INFORMATION.—Designations under subsection (a) shall be published by the Federal Aviation Administration on a publicly accessible website.

(d) SAVINGS CLAUSE.—Nothing in this section may be construed as prohibiting the Administrator from authorizing operation of an aircraft, including an unmanned aircraft system, over, under, or within a specified distance from that fixed site facility designated under subsection (b).

Protecting Your Assets – Counter-UAS Considerations

What is Counter UAS?

- Counter-UAS establishes “lines in the sky.”
- Distinguishes between authorized vs. unauthorized UAS.
- Critical Infrastructure both uses and enables UAS, but also must adopt a defensive posture.

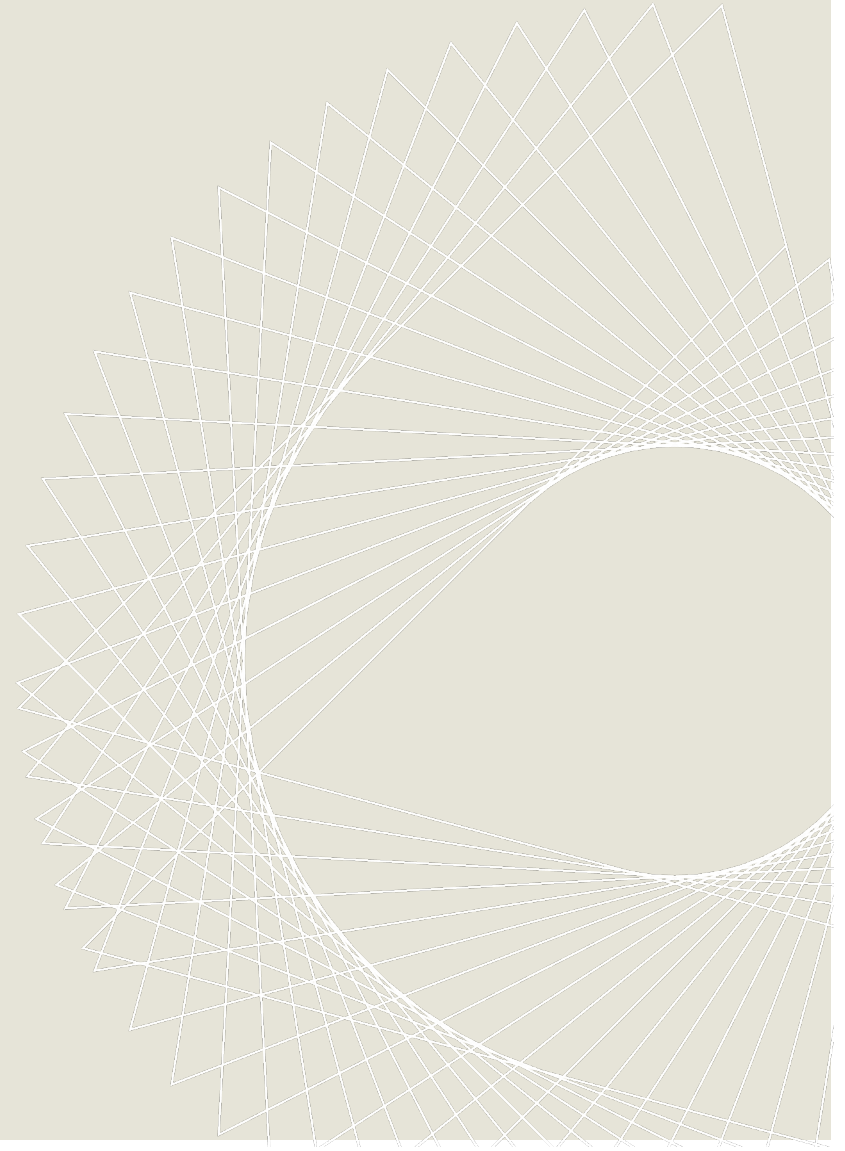
Who has authority to utilize counter UAS technology?

- Title 18 reform is essential
 - Already in place for Department of Defense (DoD), Department of Energy (DOE), Department of Homeland Security (DHS) and the Department of Justice (DOJ).
 - Federal employee at every necessary site? No.
 - Authorizing Critical Infrastructure to implement Counter-UAS also is necessary, but not contemplated.

DHS Critical Infrastructure Partnership Advisory Council (CIPAC) UAS Security Working Group

- Made up of the 16 critical infrastructure sectors recognized by DHS:
 - Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Financial Services, Food and Agriculture, Government Facilities, Healthcare and Public Health, Information Technology, Nuclear Reactors/Materials/Waste, Transportation Systems and Water & Wastewater.
 - Section 2209 uses the term “fixed site facility” vs. critical infrastructure sector used by DHS. Who will be authorized to utilize Counter-UAS?

UAS Traffic Management



UAS TRAFFIC MANAGEMENT COMBINES AVIATION, TECHNOLOGY, CLOUD COMPUTING, IoT and COMMUNICATIONS INFRASTRUCTURE (A SLEEPING GIANT)

Airspace management

- * Existing air traffic control systems are not designed to handle the anticipated traffic.
- * Daily flights for UAS and Advanced Air Mobility (AAM) will be magnitudes greater than the FAA handles.

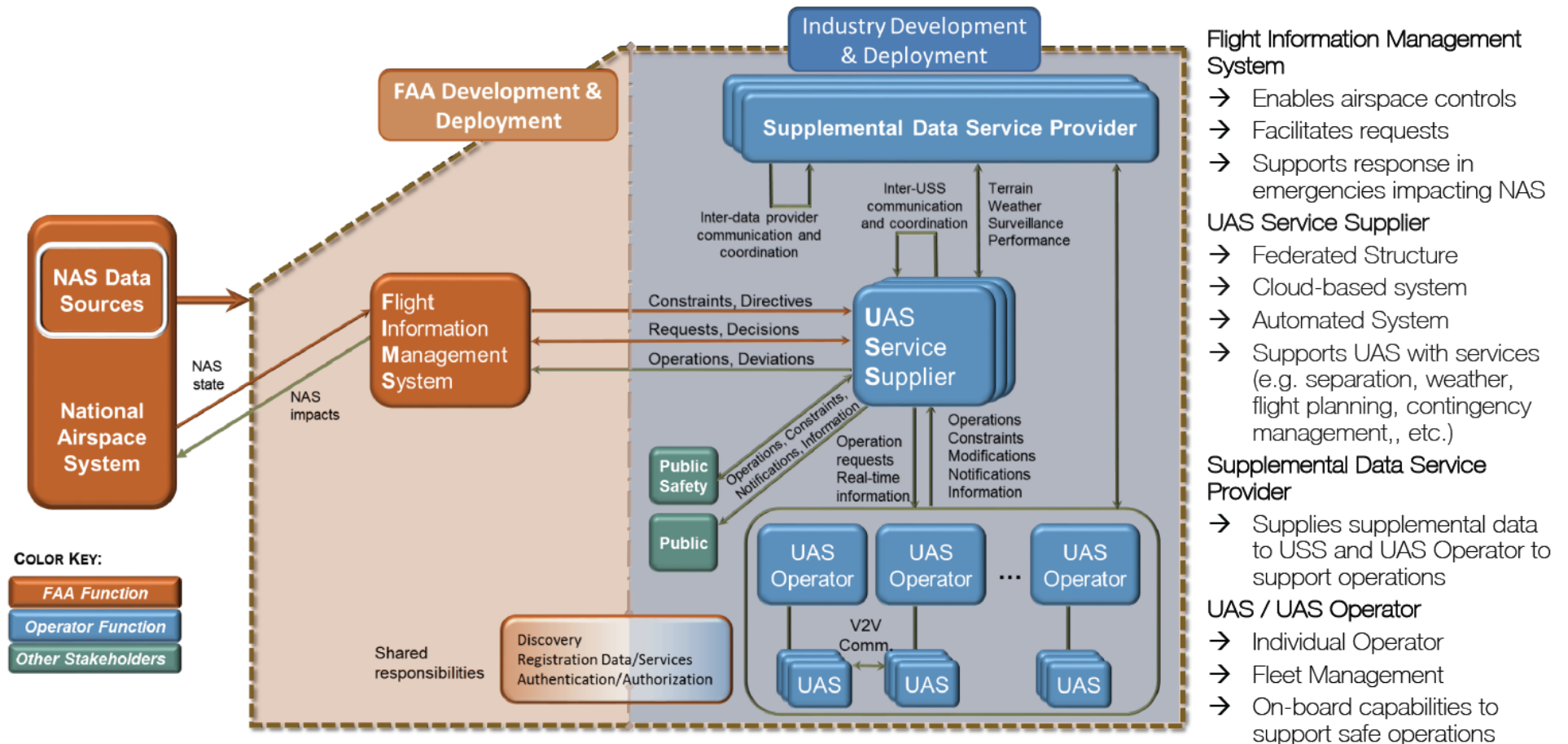
Through a federation of cooperative UTM service suppliers, airspace operations data will be shared for the benefit of all drone operations.

Operations and cloud services

- * Have to build a real time on-demand network for airborne vehicles on a massive scale, operating with precision in real time.
- * We need a communications infrastructure that will support this on demand service for UAS and AAM.
- * We need a safe, scalable network with an automated control layer.

UAS Traffic Management – NASA Architecture

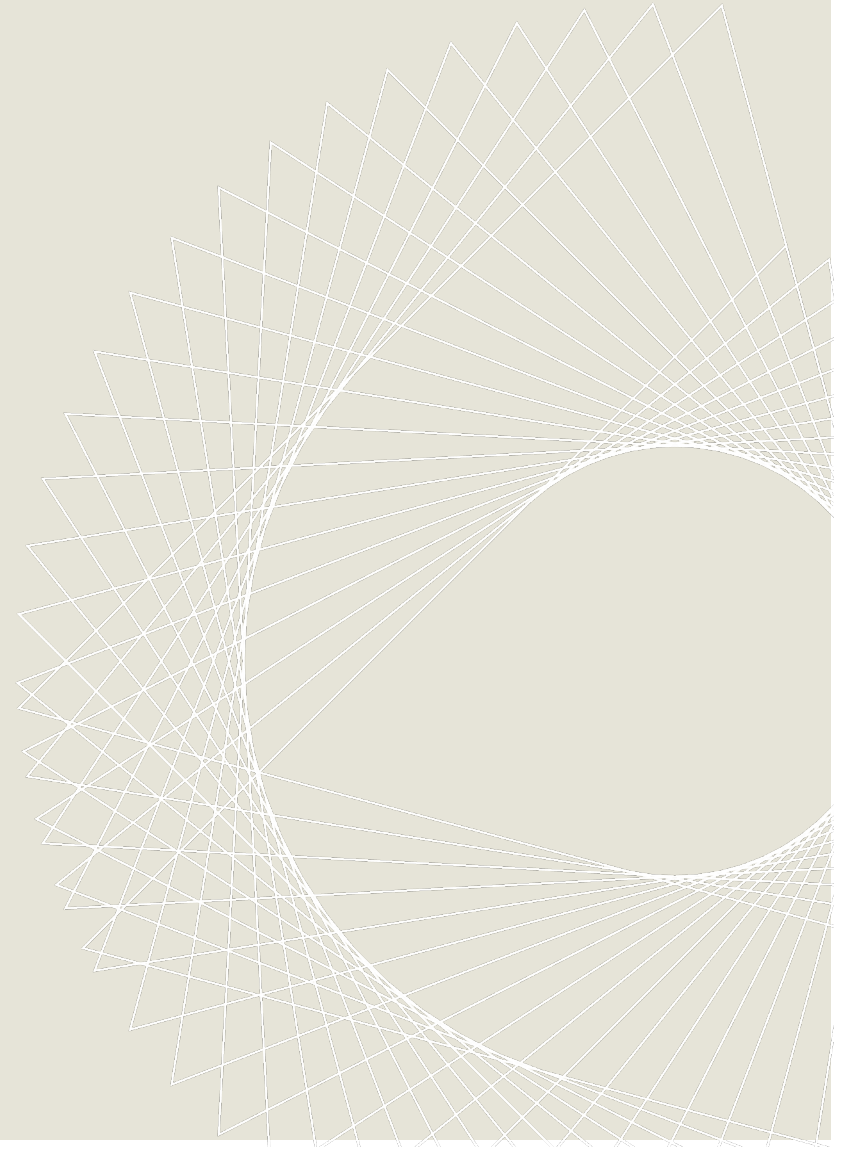
UTM Service-Based Architecture



UAS Traffic Management – In Practice



Advanced Air Mobility Ecosystem



AAM – Part of our Cities of the Future



AAM – Expanding Urban Transportation Options



AAM – Why Do We Need it? Why Is it Possible Now?

Why do we need AAM?

- Huge growth in cities, but cities have not been able to accommodate. Growth is outpacing our infrastructure.
- Not sufficient transportation to the cities. Building new roads and adding lanes is difficult and expensive.
- We live in a world dominated by cars. Trend line is bad. We need to move more people through a fixed and finite amount of space. Using space efficiently is paramount.
- U.S. has 10 of the 25 most congested cities in the world. LA topped the list as the most gridlocked. The average person is spending 2.5 weeks a year sitting in congested traffic
- The situation will get worse because of trends to live in cities
- Cracking the code on urban mobility is necessary. We need fast, safe, efficient movement of people that also is environmentally friendly.

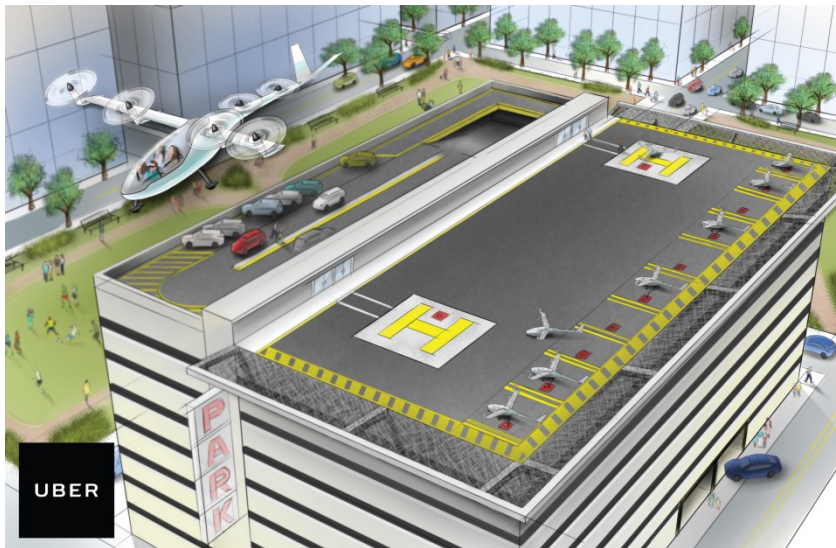
Why is AAM possible now?

- Convergence of many important technologies:
 - Vertical take-off and landing technology (eVTOL) – there are 75 different reference designs for eVTOL aircraft.
 - Autonomy.
 - Distributed electric propulsion – electric engines.
 - Energy storage – developing battery tech that will enable battery powered flight and storage.

Why aren't we using helicopters on a daily basis?

- Can't achieve a scalable business because they are too expensive to operate (vehicle capex, pilots, energy costs, infrastructure costs). Need to make the costs to use aerial ride sharing competitive to cars.

AAM – Skyports



AAM – Stakeholder Opportunities

It's Not Just For Aviation

- City planning
- Cooperation and federalism
 - What are the roles of federal, state and local jurisdictions?
 - Key consideration of the UAS Integration Pilot Program
- Public acceptance and changing norms and habits
- Real Estate and Skyports
- Powering the solutions
 - Battery development and recharging stations
 - Electric vs. hybrid vs. fossil-fuel propulsion
- The vehicle
 - Vertical take-off and landing (VTOL)
 - Single piloted vs. autonomous or self-piloted
 - Appropriate certification
 - Manufacturing challenge – need for rapid scaling – never been done before
 - Supply considerations
 - Composite based?
- Insurance
 - Where does liability reside?

Contacts



Jennifer L. Richter
Partner, Washington, D.C.
202.887.4524
jrichter@akingump.com



Avonne Bell
Director, Connected Life
CTIA
202.736.3246
abell@ctia.com