Date: March 28, 2016

To: Risk Management Committee

From: James Hill, PLAN Risk Manager

Subject: **Unmanned Aerial Systems (UAS) – Pool Coverage Consideration; Drones**

Action Required

No action required. Committee to discuss emerging risk, exposure and pool coverage issues associated with UAS (Drones). Committee will review and discuss approaches to managing risk and explore drone coverage options. Committee to present findings to Executive Committee and PLAN Board of Directors.

Overview

Several public risk management organizations, including CAJPA, PARMA and AGRIP are engaged in discussions regarding the emergence of Unmanned Aerial Systems (UAS), more commonly referred to as "drones". There are potential pool implications and most pools are being compelled to look at coverage considerations, risk management guidelines or best practices and insurance underwriting considerations.

This report will provide some insight and commentary on the emerging risk and look at the following areas:

- Use and application of drones
- Regulatory environment (Federal and Local)
- Ownership and operation
- Inherent risk and exposure
- Coverage perspective
- Policies and best practices

The report is supplemented by a thoughtful and well written paper produced by the Association of Governmental Risk Pools and the National League of Cities; Risk Information Sharing Consortium. The above referenced report and several other recent publications were used as the basis of this staff report. The AGRIP report has been attached as reference.

The Risk Management committee will discuss the emerging risk, exposure and pool coverage issues associated with Unmanned Aerial Systems. The committee's goal is to inform members of current PLAN program coverage restrictions/limitations and to explore approaches to addressing coverage issues.

PLAN Liability and Property programs were designed well in advance of the existing environment and the program did not originally contemplate "drone" operations or activity. There are significant limitations to coverage that should be recognized by PLAN members. The committee to ensure these exposures are fully recognized and appropriate risk management techniques, including insurance options are available to member agencies

Unmanned Aerial Systems (UAS) – Pool Coverage Consideration; Drones (cont.)

Unmanned Aerial Systems (UAS), or, "drones" were developed and first used by the U.S. Military, primarily for surveillance. Drones can come in a variety of shapes and sizes. The key characteristic of a drone is the aircraft portion of the system is "unmanned" and the aircraft is controlled remotely by a person and/or computer.

Drones may include other components or systems used to operate and can carry or include devices to navigate itself, record data (take pictures) or communicate with other systems. For military applications, drones are also designed to carry weaponry giving a clear indication of the weight and size range.

The emergence of drones is no longer a "fad". They have become service mechanisms with a host of applications, including public sector use. In the private sector, over a million drones were sold during the past holiday season!

Use and application of drones

Examples of the use of drones in the public sector include:

- Crime, accident and fire scene investigation and documentation
- Search and rescue operations
- Law enforcement surveillance
- Fire suppression activities
- Tactical uses in hostile situations (law enforcement)
- Inspections in hard to access areas
- Aerial photography and filming

There is also an increase in usage in the private sector which creates additional elements of risk and exposure when contracting projects or activities that involve the use or operation of a drone (surveying, aerial photography, etc.).

Regulatory Environment

The Federal Aviation Administration (FAA) and some local states are regulating the use and application of drones. In addition, some local governments are contemplating regulations including licensure and the prohibition of use in certain situations.

Currently, the FAA regulates all drone usage over 400 feet. Drones may be flown below 400 feet for recreational purposes as long as they are within the "line of sight" of the operator. The FAA oversees government ownership and operation of drones and considers them as "public aircraft operations". Public aircraft operations require a certificate of authorization (COA) from the FAA. Commercial use of drones are similarly regulated and also require a COA.

Ownership and Operation

A public entity can face "drone exposure" by operating its own drone or by using a drone owned and operated by a third party. There are clear benefits for drone usage in mutual aid situations, search and rescue, emergency operations and disaster recovery. Drones are also being used more for inspection and surveillance purposes. The value and benefits of using drones has increased, however, with the increased benefit comes the emergence of a new type of risk and exposure.

Risk and Exposure

Drone usage is new and many of the risk/exposure areas have not yet been explored. There is very little credible underwriting or actuarial information to support meaningful statistical analysis of probability and to determine adequate pricing for the risk/exposure. That said, there are several considerations in terms of evaluating risk to PLAN program members from the use and/or operation of drones.

Unmanned Aerial Systems (UAS) – Pool Coverage Consideration; Drones (cont.)

Loss causation is an important element of the PLAN risk assessment or analysis. The following are some important areas for members to consider when assessing what can cause a loss to happen during drone operation(s) or associated drone activity(s).

- Pilot error (remote pilot)
- Lack of training or familiarity with operating a drone
- Mechanical failure of the drone or failure of its operating system (control system)
- Use, maintenance and storage of any data or information captured by the drone
- Inappropriate use of the drone by an employee
- Unauthorized breach of drone data or information stored by the device or operating system
- Contractual risk associated with contracts related to drone use or operation
- Drone accidents (causing bodily injury or property damage).

When evaluating drone risk from a causation standpoint, it is important to consider the types of claims a member may be exposed to. This aspect of the analysis is extremely important in evaluating coverage considerations for PLAN members and in developing the appropriate coverage, risk transfer or other risk management solution. The following risk scenarios can aid PLAN members in recognizing exposure.

1. Accidents – The crash of a drone could cause bodily injury or property damage (1st and 3rd party).

2. Trespass – The use of a drone could lead to claims of "trespass on private property" (drone crash on private property)

3. Privacy breach and civil rights violation – This is primarily confined law enforcement operations and is a significant exposure due to the complex nature of federal civil rights suits and the impact on claim costs (defense costs).

4. Public Officials Liability (Errors & Omissions) – Claims may arise where the cause of action relates to regulatory issues. While we would not expect our members to operate a drone outside of the scope of any legal authority, plaintiffs may argue otherwise. Where local authorities use land use and zoning power to regulate drone usage, this exposure is further heightened.

5. Cyber Risks - Claims may arise as it relates to an unauthorized breach or release of any privacy related data (personal identifiable information). Also, we must consider "cyber-attacks" which may disable the aircraft causing both bodily injury and property damage.

Coverage Perspective

The PLAN program did not contemplate the emergence of drones when the program was first developed. The current position from a liability perspective is to exclude all aircraft from coverage, including drones, by intent. The PLAN property program has similar exclusions with respect to "aircraft" unless specifically underwritten and authorized. PLAN staff is working closely with coverage counsel and our insurance intermediary to address the issue of coverage. As noted earlier, drone usage is relatively new and the risk/exposure areas are currently being evaluated by PLAN.

PLAN staff has asked coverage counsel to consider expansion of the definition of aircraft within the PLAN Liability MOC to include "drones" and further define what a "drone" is. Alternatively, members may elect to create an "exception" to the Liability MOC aircraft exclusion to afford coverage for "drones" in some manner, including any restrictions and limitations. The challenge then becomes determining the program loss expectancy for this coverage feature and pricing the program's risk/exposure adequately. This may be a daunting task in light of the lack of statistical credibility in both the insurance and pool industry.

Unmanned Aerial Systems (UAS) – Pool Coverage Consideration; Drones (cont.)

Staff has deferred all activity on the contract construction issues until the matter has been vetted by the Risk Management Committee, Executive Committee and Board of Directors. Ken Moy, PLAN General Counsel has been apprised of the situation and is standing by for member recommendations.

At this juncture, the Risk Management committee should explore and discuss the following areas:

1. How are PLAN members using or likely to use drones?

2. What types of coverage would be useful to our members for drone related losses?

3. What type of underwriting information should the pool request from its member agencies?

   Note: A copy of a typical underwriting questionnaire for "drone" risks is attached as a sample.

4. How are pools, commercial insurers and reinsurers treating drone coverage? These questions will be addressed by our insurance intermediaries. Most pools are at the early stages of the discussion.

   Note: A sample of exclusionary language to exclude drones from pool coverage and a sample endorsement to include limited coverage has been attached for committee review/discussion.

Policies and Best Practices

As PLAN considers the risk management and coverage issues associated with the use of drones in our municipal endeavors it is important that PLAN develop effective policies, procedures and best practices. To the extent PLAN members elect to "cover" drones in some manner or fashion, we will need firm policy guidance and close adherence to all agreed upon best practices for the good of all members. Staff will work directly with the Risk Management committee to establish defined best practices to coincide with the implementation of any drone coverage option.

Summary

There are many benefits from the use of Unmanned Aerial Systems (Drones). PLAN can expect growing concern regarding coverage options for exposure related to drone operations or activities. Members need to be very precautious and deliberate in our approach to managing drone risk. To the extent the majority of PLAN members do not achieve a high comfort level with introducing this exposure to the pool, PLAN staff will work with our insurance intermediary to develop "stand-alone" options which contemplate Property, Liability and all other associated risks.

Ace Westchester Specialty Casualty UAV Questionnaire

Intended Use Considered:

- Film & Production: Aerial Photography & Survey
- Construction & Real Estate
- Powerline & Pipeline Patrol
- Municipal Use (all uses of a Municipal Government)
- University & Research

Underwriting Requirements:

a.) Maximum flight speed of 30 miles per hour
b.) UAV less than 55 pounds
c.) Operated below 400 feet above ground level
d.) Operated in daylight conditions and only with sight of operator
e.) Location of use is at least 5 nautical miles from nearest airport
f.) Must exclude Personal & Advertising Injury
g.) Operated within the U.S. and its territories
h.) Liability limits offered up to $25,000,000
i.) Physical damage offered for units valued at $25,000 and higher with 10% deductibles EEL

Please see the below questions for a UAV risk:

1. Make and model name of UAV including size and weight? Manufacture name and Total number of model in question produced by manufacturer.

2. Average flying altitude to include maximum altitude?

3. Area of operation? City, Town, County, State

4. Use of operation: Agriculture, Law Enforcement, Aerial Survey, Weather Research, University program, etc.

5. List any airport(s) within 5 miles of operational area.

6. Does insured want liability only or both liability and hull coverage?

7. Where are UAV's kept during non-operational use?

8. Annual hours expected for use?

9. Please provide pilot record (any pilot ratings and years of experience and where did pilot receive UAV or UAS flight training?)

10. Is UAV fixed wing, rotor wing, or quad rotor? Is the UAV Hand launched or self-take off?

11. Value of UAV? And liability limits insured is seeking?

12. Does UAV come equipped with auto point of take-off return in the event of low battery or lost transmit reception?

13. Are UAV's ever flown in IFR conditions or at night?

14. Was UAV donated, sold, or loaned by Federal Government?

15. Total weight of UAV?

16. Has the applicant ever had a UAV related loss in past 5 years? If so, when and please describe the loss in detail.

I welcome you to forward all UAV submissions to me directly--thanks!

-MC-

Mike Colson | Underwriting Manager

ACE Westchester Specialty Casualty | Aerospace | 1100 Poydras Street, Ste. 2150 | New Orleans, LA 70163

Direct: 504.310.3608 | Fax: 504.310.3610 | Email: michael.colson@acegroup.com

Drone-Related Changes to 2016 MVRMA Liability Coverage Document

Exclusion:

(F) To *Personal Injury* or *Property Damage* or *Public Officials Errors and Omissions Liability* arising out of a covered person's or entity's ownership, maintenance, use or entrustment to others of any *unmanned aircraft*. Use includes operations and loading or unloading. This exclusion applies even if the claims against any covered person or entity allege negligence or other wrongdoing in the supervision, hiring, employment, training or monitoring of others by that insured, if the occurrence which caused the *Personal Injury* or *Property Damage* involved the covered person's or entity's ownership, maintenance, use or entrustment to others of an *unmanned aircraft*.

As used in this exclusion, an *unmanned aircraft* owned, maintained, used or entrusted by a covered person or entity shall include any *unmanned aircraft* owned, maintained, used or entrusted by any third party under any contract, lease, or any other arrangement, between said third party and a covered person or entity on behalf of, or for the benefit of, a covered person or entity.

As used in this exclusion, loading or unloading means the handling of property:

a. After it is moved from the place where it is accepted for movement into or onto an *unmanned aircraft*;

b. While it is in or on an *unmanned aircraft;* or

c. While it is being moved from an *unmanned aircraft* to the place where it is finally delivered; but loading and unloading does not include the movement of property by means of a mechanical device, other than a hand truck, that is not attached to the *unmanned aircraft*.

Definition:

(W) "*Unmanned aircraft*" means an aerial system or device that is not designed, manufactured or modified after manufacture to be controlled by a person from within or on the aerial system or device.

Endorsement No. 12-16

Issued by
Miami Valley Risk Management Association

Effective: 1/1/16 12:01 AM

THIS ENDORSEMENT CHANGES THE COVERAGE DOCUMENT. PLEASE READ IT CAREFULLY.

LIMITED COVERAGE FOR DESIGNATED UNMANNED AIRCRAFT

Schedule

Description of Unmanned Aircraft
Description of Operation(s) or Project(s) Authorized by COA

Exclusion (F) does not apply to *unmanned aircraft* described in the Schedule, but only with respect to the operation(s) or project(s) authorized by, and only while operating within the terms of, a valid Certificate of Waiver or Authorization (COA) granted by the Federal Aviation Administration.

agrip
ASSOCIATION OF GOVERNMENTAL RISK POOLS

NATIONAL LEAGUE of CITIES | RISK INFORMATION SHARING CONSORTIUM

Use and Regulation of Drones by Local Government Entities & Schools: Thoughts for Public Entity Pools

Introduction

The public sector is actively engaged in conversation about use and regulation of, and associated risks related to, drones (more broadly referred to as Unmanned Aerial Systems or UAS). Public entity pools are considering implications of drone use by local governments, schools, and other local public entities, whether that use is direct, by contract with a third party vendor, or through partnership with another public entity.

Input and comments are invited, and materials will be updated as the evolution of this issue continues.

Questions, comments, or other feedback can be directed to:

Claire Reiss, NLC-RISC
creiss@nlcmutual.com
202-626-3165

Ann Gergen, AGRIP
agergen@agrip.org
518-220-0336

Potential pool implications of a members' use or regulation of drones include coverage considerations, risk management guidelines, reinsurance considerations, and more. Commercial insurers are also evaluating these risks and responses, and much can be learned from monitoring commercial insurance market solutions.

Our intent is to provide a starting context and outline issues relative to drones, in particular as they relate to public entities pools and their members. Throughout this document we provide links to known reference materials about drone issues. This is not an exhaustive resource and it does not answer every known question. To the contrary, the intent is to raise questions so pools can independently evaluate their own drone-related needs or concerns, members' likely use of drones, and related questions.

Definitions

There are many names and acronyms for UAS, most commonly referred to as "drones." The key characteristic of a drone is that the aircraft portion of the system is unmanned, although all drones are piloted either by a person or computer. Other commonly used names or designations include:

Remotely Piloted Aircraft System (RPAS)
Unmanned Aerial Vehicle (UAV)
Model Airplane / Model Aircraft

Drones take a wide variety of forms, ranging from small indoor-use children's toys to large and sophisticated equipment. For purposes of this outline, we will use the term drone to refer to all types of unmanned aircraft likely to be operated by local government entities or schools. The most sophisticated drones, such as those used for international military operations, are not expected to be used by pool members.

© 2015 All Rights Reserved

In addition to the drone aircraft itself, drone systems often include associated system components and support equipment – things like a control station, computer software, data links, telemetry, communication systems, navigational tools, etc. The degree to which these system components come into play will vary depending on the level of drone sophistication, the intended use, and whether it is piloted by a person or computer.

Here are some resources to help pools understand the wide spectrum of drones and their common uses:

Trending Now: Domestic Drones – Risk Management Perspective on Domestic Drones, Arthur J. Gallagher & Co., Gallagher Public Sector

Unmanned Aerial Systems/Drones – Regulation, Liability and Insurance Requirements, National Association of Mutual Insurance Companies

Presentation on Drone Risks – March 2015 Governance & Leadership Conference, AGRiP

Pools are encouraged to become familiar with the spectrum of drones. Some pools may choose to classify categories of drones based on degree of perceived risk, and underwrite accordingly for their membership.

Prioritizing Drone Risks

Pools and their member public entities face many high profile liability and risk issues on a daily basis. What makes drone use an issue worth time and attention?

Drone use is more than a fad. Drones are a growing service mechanism with widespread application, including public sector uses. Here are some examples of public sector uses already in place and experiencing growing levels of interest by public entities, including local governments and schools:

- Crime, accident, and fire scene investigation and documentation
- Search and rescue operations
- Law enforcement surveillance
- Fire suppression activities
- Tactical advantage and live imaging in hostile situations
- Monitoring and inspecting infrastructure
- Aerial photography, filming of events
- Property inspections and appraisals

Because the potential use of drones may seem overwhelming and the risks many, it might be tempting to discourage member use of drones by excluding coverage. Given the likely prevalence of drones and anticipated growing use, pools are encouraged to instead help members identify best practices for gradual and thoughtful implementation.

It is also worthwhile to consider the evolving private sector use of drones. Private uses may speak to how public sector drone use will expand. Private uses may also be cause for local governments to consider implementing some degree of drone regulation within their borders. Evolving private sector drone use includes:

- Infrastructure inspection by engineers, construction firms, maintenance companies, etc.
- Commercial aerial photography
- Entertainment, video feeds, filming of events, news media
- Private surveillance and investigation
- Agricultural surveys, inspections, and maintenance

Indeed, drones have advantages both in public and private applications. Drone use can reduce costs, increase efficiencies, reduce dangers or injury to personnel, produce better outcomes, and offer enhanced perspective on projects. As with the evolution of any technology, we probably cannot today appreciate the total spectrum of value (or risk) that will be produced by drone use.

Current Legal Environment for Drone Use by Local Government Entities

While it is likely drones will be used in the future for many purposes we cannot now anticipate, pools must formulate coverage and risk management advice based upon how drones can be used under current law. In no case should local government use of drones, whether direct or contracted, operate outside the scope of legal authority.

The Federal Aviation Administration (FAA) and some states' laws limit how drones can be used by both the public and private sectors. FAA rules are targeted primarily at promoting safe operations and preempt state laws as they relate to the national airspace. Many states, on the other hand, have adopted statutes governing drone use focused to a large extent on privacy issues. Some local governments are attempting to control aspects of drone use within their borders.

Federal regulation

The FAA is responsible for establishing safety standards in the national airspace. Congress has required that the FAA establish regulations to incorporate drones into the national airspace by September 2015, although such regulation is not expected to happen until mid-2016. Current FAA provisions regulate all drone use over 400 feet. Drones may be flown for recreational purposes below 400 feet and within the operator's line of sight. All other uses, including all commercial and governmental uses, require explicit FAA permission, obtained using estabished procedures.

A detailed description of the criteria considered in the COA process is included in the previously noted AGRIP presentation.

A summary of the FAA regulations applicable to public entity drone operation is available, including a link to a helpful decision tree for evaluating whether governmental use of private drones is regulated as public or civil operation.

A summary of the FAA regulations applicable to commercial use is available, as well as an overview prepared by the Association of Unmanned Vehicles Systems International.

The FAA has established an interim policy to provide those who already have a Section 333 exemption with a blanket COA to operate drones meeting certain criteria.

The FAA presently oversees government ownership and operation of drones – including ownership and operation by local governments and schools – as "public aircraft operation." Public aircraft operation requires a certificate of authorization (COA) from the FAA, managed through an online portal.

There is no public entity use of a drone that falls outside a regulatory process. If the drone use takes place above 400 feet, it is regulated by the FAA. Any public entity use under 400 feet would not be classified as "recreational," whether operated directly by the local government agency, a third party contractor, or a volunteer. If a public entity is making any use of a drone, it must comply with FAA regulatory guidelines.

The FAA regulates commercial use of drones as "civil aircraft operation." Civil aircraft operation is regulated through a different process referred to as "Section 333 exemption." In both public and civil aircraft operations, part of the process for granting the COA or Section 333 exemption includes review of intended use.

Civil aircraft restrictions do not apply directly to local government use, but they have implications for local government contracts for drone related services. Local government entities contracting with commercial operators who have a Section 333 exemption can eliminate the need for a public aircraft COA, although uses of leased drones may still be considered public aircraft operation.

This means public entities contracting with vendors who have an existing Section 333 exemption may benefit from expedited approval.

A summary overview and full details of the Notice of Proposed Rulemaking are available.

Notice of proposed rulemaking

On February 15, 2015, the FAA issued a Notice of Proposed Rulemaking ("Notice") that would provide for the routine civil operation of small drones within certain limitations. While the public aircraft operations COA process would continue to exist under the regulations proposed in the Notice, local government entities could bypass that process by conducting their drone operations under the requirements for routine civil operation.

Although the FAA's proposed regulations impose significant requirements and limitations, they would enable public and private entities to develop programs for the routine use of drones.

The new FAA regulations are not expected to be finalized until 2016, after the FAA has considered comments received in response to the Notice. If the regulations are adopted as proposed, drones (including public entity drones) will be able to operate without a special exemption or COA if they meet a list of requirements, including the following:

- Weigh less than 55 pounds
- Remain within the visual sight of the operator or a visual observer
- Not operate over people who are not directly involved in the operation (with some exception for micro drones)
- Operate only during daylight and with weather that allows 3 miles visibility from the control station
- Not exceed 100 mph or go higher than 500 feet
- Comply with requirements for air traffic control permission
- Be inspected by the operator prior to the flight
- Be operated by someone who has passed a test and been vetted by the Transportation Security Administration
- Be registered and have required markings

A new program by the FAA, called Pathfinder Program, will explore with three corporate partners issues related to drone operation outside a pilot's line of sight. The uses explored will be agricultural, train track inspection, and urban.

More information about the Pathfinder Program is available on the FAA website.

An emerging question is the potential use of drones beyond an operator's line of sight. The FAA's Notice requires drones be operated only within the line of sight of the operator or a visual observer. However, many commercial applications would require drones be operated more remotely, using sensing and avoiding technology and possibly navigated by computer. Such use can be expected to raise a host of questions about possible new risks related to technology failure.

Read the full executive order.

What You Need To Know About The Federal Government's Drone Privacy Rules, authored by Dr. Gregory McNeal, is an expert analysis of the executive order.

Executive order

On the same day the FAA issued the Notice, President Obama issued an executive order that federal agencies must require state, local, tribal, and territorial government recipients of federal grant funding for the purchase or use of drones in their operations to have policies and procedures in place to safeguard individuals' privacy, civil rights, and civil liberties.

State regulation

An overview of state legislation to date is available from the National Conference of State Legislatures.

State legislatures are also regulating drones. The National Conference of State Legislatures reports 26 states have adopted legislation that addresses drone related issues. And so far in 2015, 45 states have considered 150 drone related bills.

Of course, half the states do not have laws yet, and most will never have laws that address all possible drone issues. Common state legislation regarding drones, in some cases applicable to public and private drone use, include:

- Defining drone
- Controlling drone use
  - Limit use by law enforcement; require a warrant
    - Exceptions for disasters or emergencies
    - No use for surveillance
  - Prohibit various private uses of drones
    - Voyeurism
    - As a tool for hunting and fishing
    - Interference with hunters and fishers
  - Allow use of drones to counter terrorist attacks
  - Limit retention and disclosure/require destruction of information gathered
  - Prohibit weaponized drones
- Creating a crime of unlawful photography/surveillance
- Providing civil remedies for prohibited use
- Excluding evidence gathered in violation of the law
- Requiring record retention and reporting by drone operator
- Recognizing the value of the drone industry to the state

Some states have passed laws preempting local governments' regulation of drones. The possible conflicts created by multiple tiers of local, state, and federal government authority should be monitored by pools. These conflicts could lead to litigation between governmental authorities over who can regulate drone use, or between a government and aggrieved citizens who either want to operate drones in a manner prohibited by local law, or want to stop drones from operating even though such operation complies with the law. As these situations unfold, pools are likely to be called upon to advise members about local government regulation, resolve coverage questions at the primary and reinsurance levels, and defend public entity members for drone use and/or regulation.

The potential for conflict between federal, state, and local regulation of drones is real – and still unclear. Several resources might help understand related preemption issues:

The FAA's website includes this reference to allowable state and local regulation.

The Brookings Institution also has some analysis of the issue available, as does the *Air & Space Lawyer*, a publication of the American Bar Assocation.

To the extent any state legislation overlaps with federal requirements, there is the potential for conflict. Federal requirements likely preempt states' requirements in civil rights and matters under the jurisdiction of the FAA.

Local regulation

A 2015 compilation of local use restrictions is available from Syracuse University Institute for National Security and Counterterrorism.

Some local government entities are regulating drone use within their borders, although so far relatively few local governments have taken this step. Overall, localities tend to address drone operation in certain geographic locations, use of any drone-collected information as evidence in federal or state court, and equipping drones with anti-personnel devices to target law enforcement or other public safety personnel.

As drone use increases, more local government entities may seek to create licensure requirements, prohibiting use of drones in certain locations under their land use and zoning power, and imposing other restrictions.

Approaches to structuring drone regulation

Presently most government entities are considering adoption of laws and regulations specifically related to drone technology. This approach makes sense from the FAA perspective, because the FAA is tasked with controlling and assuring the safety of the national airspace. But some of the other concerns raised by drone technology and related regulation or laws are not exclusive to drones.

A major concern raised by drone use is the potential for violation of privacy and civil rights. Mounted camera and video technology is one reason drones have so many applications, but imaging technology is in part what concerns privacy and civil rights advocates. Drones are not the only conduit of imaging technology to raise these issues, however. Manned aerial surveillance flights, electronic license plate readers, security cameras at public facilities, street security cameras, and police body/dashboard cameras are all imaging technologies that raise issues of privacy, widespread surveillance, and potential civil rights violations.

To the extent pools advocate at the local, state, or federal level for any drone-related issues, or are asked to comment on drone-specific legislation, it might be helpful to consider technology-neutral solutions, which would focus on the rights to be protected rather than the type of technology involved. The use of a drone, in and of itself, may pose no different or greater risk than recordings made through other means such as security cameras, street cameras, license plate readers, or body cameras. On the other hand, the scope of a drone's perspective is often much larger with granular detail easily accessible, which could give rise to greater public scrutiny of local government use of drones.

Focusing privacy legislation specifically on drones might not consider this larger picture – although in some cases drones may indeed be the true basis of concern. A number of resources offer perspective on the privacy issues raised by drone use, and how to address those issues under the law.

Drone Ownership and Operation Models

A local government entity might buy or lease and operate its own drone, or use a drone owned and operated by a third party.

Operating an owned drone

If a public entity purchases its own drone, it must develop a plan for use, secure an operator whose credentials meet the requirements of the FAA, and obtain a COA. The public entity should also consider whether it will have insurance coverage for any drone accident or incident that results in liability.

From the standpoint of coverage, many of the same considerations apply whether a local government drone is owned and operated directly or through a third party. A pool that does not intend to provide coverage, or wants to sublimit it, must think carefully about language and whether there could be contractual liability coverage, either when the local government provides or receives services under a contract.

Contracting for use of a drone owned and operated by a third party

A local government entity might use a drone owned and operated by someone else. This may be an easier solution if the private entity has equipment, a qualified operator, and a Section 333 exemption encompassing the intended operation. It is important for the local government to be sure its project fits within the owner/operator's Section 333

exemption, or within the FAA's March 15 interim policy that provides those who already have a Section 333 exemption a blanket COA for certain uses.

Volunteers

Public entities should be particularly cautious about accepting services using drones owned and operated by volunteers.

Pools might work with members to ensure local governments and schools understand and manage risks associated with non-professional drone operators, and consider alternatives where possible.

A company that operates drones as part of its business is regulated by the FAA and cannot be considered a recreational user for regulatory purposes when providing services to a public entity, even on a volunteer basis. Thus, professionals must comply with all FAA requirements even if they are not being paid for their services.

An individual drone enthusiast who does not engage in commercial drone operations and is considered to be a recreational user might also volunteer services and drone use to a local government or school. Such circumstances could raise risks for public entities, because the volunteer may be less experienced, less knowledgeable of FAA requirements, may not have the correct exemption/permission, and may not be amenable to allocating liability through a written agreement. Even if a volunteer is amenable to allocating liability, without demonstrated insurance coverage there would be no guarantee of funds to cover losses.

Pools may be of assistance to their members by helping develop contractual language that allocates liability to the party best able to manage the risk. Contracts should require the drone owner/operator to have insurance that provides coverage for drone operations. Other requirements may differ based on the nature of the drone use and which party bears certain responsibilities. For instance, it would makes sense for a third party owning and operating the drone to be responsible for risks of bodily injury and property damage arising from its operation, equipment failure, or misuse of the data collected, while the local government entity would be responsible for privacy violations arising from its design of the mission and its misuse of the data collected. When it comes to mutual aid, pools can play an important role by educating members about likely emerging uses of drones in public safety, associated risks, mutual aid contracting concerns, and the interrelatedness of all three.

Mutual aid

Drones are likely to be used under mutual aid agreements, especially in emergency and disaster situations. Mutual aid agreements may be between public entities in the same state or in neighboring states, and can be formal or informal. Equipment might also be shared state-to-state under the Emergency Management Assistance Compact.

Any mutual aid response including drones and drone operators should be reviewed by the participating entities for observance of all legal requirements related to the operation of drones. It is common in local mutual aid relationships for details of each parties' operational oversight to go unchecked – which could be quite problematic in terms of running afoul of drone regulation.

Provisions for allocation of liability for drone risks under the mutual aid agreement should also be carefully reviewed. Mutual aid partners should address directly how liability will be allocated in the event of an accident or incident involving a drone.

Risks of Drone Use

There are many possible benefits resulting from public entity use of drones. There are also risks, most of which have not yet fully been explored because drone use is so new. We cannot quantify the likelihood or impact of potential risks, but rather provide some starting ideas for further consideration and evaluation by public entity pools.

In exploration of risk areas, probabilities, and possible impacts, it might be helpful to consider likely sources of drone risk:

- Piloting error
- Inadequate training of personnel controlling drones, or overseeing drone use
- Mechanical or technical failure of the drone
- Mechanical or technical failure of associated drone software, hardware, or associated systems
- Maintenance and storage of data and information, including images, captured via drone use
- Inappropriate use of a drone by an employee
- Unauthorized breach of drone technology systems, including data and information storage and control systems
- Contracts related to drone use and operations
- Drone accidents

Thinking further about how these risk sources might translate into claims against public entities and therefore have pooling implications, it might be helpful to consider the following possible risk scenarios.

Accidents. A drone might crash during use, itself sustaining physical damage or causing physical damage to property (city or private) or even personal injury. A drone could also collide with another aircraft, creating the same sorts of risks.

A drone crash or collision could also injure an employee of the public entity operating or overseeing operations of the drone – including the pilot, controller, or others in the general area at the time of the accident.

Trespass. Drone use could entail allegations of trespass on private property, including trespass into the airspace above private property. If a drone needs to be retrieved because of malfunction or crash, and if permission from a landowner is not appropriately granted, there could also be direct trespass concerns.

Privacy breach and civil rights violations. There are risk considerations regarding privacy breach both in law enforcement use of drones and in other public entity use of a more general nature.

If a drone is used by law enforcement, there are risks related to appropriate warrant procedures such as the need for a

When it comes to privacy and civil rights risks, pools are encouraged to take a "technology neutral" approach whenever possible. The use of a drone, in and of itself, may pose no different or greater risk than recordings made through other means such as security cameras, street cameras, license plate readers, or body cameras. On the other hand, the scope of a drone's perspective is often much larger with granular detail easily accessible, which could give rise to greater public scrutiny of local government use of drones

Some resources that offer perspective on the privacy issues raised by drone use include:

Drones and Aerial Surveillance: Considerations for Legislators, Brookings Institution

Electronic Privacy Information Center

American Civil Liberties Union

warrant and the approval of a requested warrant. There may be privacy and civil rights risks related to recordings made by cameras or other devices employed by law enforcement through a drone (or any other means).

Even more generalized use of a drone by a public entity could raise privacy breach concerns – for instance an aerial parks survey conducted by drone could record private activity in the home on an adjoining property. Even if the local government entity does not use such private information in any direct way, the mere recording of information could be cause for privacy concerns.

Public officials liability. Where there is underlying risk to a public entity, there may be risk of public officials liability for an elected body. Of particular concern may be a cause of action somehow involving a drone used in a circumstance where the elected body allowed its use outside federal or state rules and regulations, whether or not it did so knowingly.

Cyber risks. Collection of information and images by drones can provide robust data, stored electronically, to local governments and schools. Such data or images might be subject to the same sorts of cyber attacks or accidental release as are other electronic information sources. In addition, the remote operation of drones could make them subject to direct cyber attack, such as a non-authorized pilot commandeering a drone being operated for a public purpose. This could result in theft or destruction of the drone, itself, but more importantly could lead to liability for the public entity that failed to adequately protect against such cyber-jacking of its (owned or contracted) drone.

One pool's outline of municipal airport contract risks might be of interest to others exploring these concepts – see the League of Minnesota Cities Insurance Trust's resource on topic.

Airport operations liability. Public entity airports may have special considerations when it comes to drones, including direct liability as well as contract liability concerns with airport managers or fixed base operators.

The proposed FAA Notice would permit drone operations near controlled airports with the permission of air traffic control. Consequently, drones may begin to be used at some point at municipally owned airports, or approved by air traffic control at the municipal airport. Such regulations would certainly be an issue to consider for any municipal airport, including how to best allocate drone risks in any contracts with airport managers or fixed base operators.

Regulatory violations. The FAA regulations apply to public entity use of drones, and in some cases there may be penalties for failure to comply. As drone regulation increases and takes firm shape at the federal and state level, other penalties could apply for violation of rules or restrictions.

Land use liability. Local government attempts to regulate when, where, or how drones can be used within their jurisdictions may face push-back from commercial or recreational users, in particular with regards to land use rights for private property.

Failure to supervise or limit use. For any situation where drone use over public property creates a liability concern – for instance by causing damage through a crash or collecting private information – there could be a tort claim against the local unit of government or school for failure to supervise use, failure to protect

against dangers, or failure to apporopriately limit the use of drones in public areas. These claims could be made regardless of whether the local government, itself, operates a drone, allows a drone to be used, or fails to limit drone use over public property.

If your pool hears of a new or differing potential for liability, whether you assess ultimate liability as likely or not, we'd like to hear from you.

Other possibilities. As drone use increases, public entities and pools should expect novel approaches to liability. Might cyber risks associated with drone use also result in public officials liability, if a cyber-jacking incident resulted in harm to another third party and the local government did not take appropriate precautions? How will airplane exclusions and cyber coverage provisions co-mingle in a liability matter that involves drone use? There are many questions that will come to light as drones become more prevalent in the public environment.

Coverage and Underwriting Considerations for Pools

Public entities using drones should have adequate risk transfer and financing in place, but not all public entity pools are currently comfortable providing drone coverage. Pools might ask themselves the following questions to determine whether and how to provide coverage for drone related losses, or what to recommend their member public entities seek in terms of other coverage and risk financing options.

How are member public entities using or likely to use drones?
Include drones in your assessment of members' risk. As drones become more readily available, their use in local government and school operations could emerge in a number of ways, especially in public safety and search and rescue. Members may not realize the importance and coverage implications of drone use, so it is important to ask directly about their current and planned adoption of drones as part of their operations.

What types of coverage are useful for drone related losses?
The manner in which drones are used by public entities differs from many of the commercially focused applications. Currently, the largest emphasis is on search and rescue and law enforcement, neither of which is a focus of the private sector. Also, the private sector has less exposure to civil rights litigation than the public sector. If a private sector organization incorporates drones heavily into its operations, for example using them in order fulfillment, there may be a more significant business interruption/extra expense exposure than is faced by most public entities. Other exposures may be similar in public and private use. General liability and hull coverage affect both public and private sector drone users.

- *General liability (BI, PI & PD).* Drone accidents are relatively common, and can result in bodily injury, property damage and personal injury. This is an important coverage for public entities using drones in any part of their operations. It is even possible a loss could be catastrophic, if the drone collided with a passenger aircraft, for example. Such incidents may be unlikely to happen if the public entity is using a drone within FAA requirements, so a pool electing to provide this coverage may want to consider excluding losses resulting from drone use not in compliance with FAA, state or local requirements. Pools not wanting to provide this coverage

should review aircraft exclusion language to be sure it specifically includes drones, and also check contractual liability language, which could come into play if a public entity hires a third party to operate drones on its behalf.

- *Physical damage to drone/hull coverage.* Some drones may be inexpensive, off-the-shelf items that will not be a significant loss if destroyed or damaged. Other drones are more expensive. Camera equipment and other technology carried by drones could also be a significant loss. Pools providing hull coverage for drones may want to consider sublimiting the coverage, requiring specific information about the equipment, and additional member contribution before offering higher limits.

- *Privacy – general & law enforcement.* This is an important coverage for drone use, especially if it is likely to incorporate use of a camera or other imaging technology. Liability can arise both from an intentional use of the technology that violates an individual's privacy or civil rights, and from images captured unintentionally. Pools considering coverage for privacy and civil rights exposures occuring through the use of drones need to look at law enforcement liability, public officials liability, and other more general liability exposures.

- *Workers' Compensation.* Pools providing workers' compensation coverage will be responsible for claims from members' employees injured during drone operations. On the positive side, drone use may eventually be used to supplement work by employees in hazardous situations, reducing the risk of a work related injury.

- *Cyber.* Most drones are controlled, and their images transmitted, through the operation of computer software. Some drones may rely on computerized navigation and object avoidance systems. Breach of these systems could destroy the drone, cause injuries and property damage, appropriate the drone for an unintended use, and/or steal information and images the drone has gathered. Consequently, cyber coverage is very important to complete protection for drone exposures and pools should consider whether and how they want to extend coverage to cyber hazards including those resulting from drone use.

- *War/terrorism.* War and terrorism exclusions are standard in many insurance policies, but are increasingly problematic in the cyber arena. Data breaches are frequently launched from foreign countries, and the question is whether these breaches are some type of cyber warfare or terrorism, as opposed to criminal acts. The line is becoming increasingly unclear. Pools that want to

  cover their members' drone use need to consider the effect of any war and terrorism exclusions in their coverage documents.

- *Business interruption/extra expense.* Public entities relying heavily on drones may have a related business interruption and extra expense exposure. For the time being, with use just beginning to gain traction in local governments, this may not be a major issue – but it is one pools should watch and consider how their current business interruption and extra expense coverage would apply.

Are aircraft exclusions sufficient to protect pools against drone related losses?
This is an open question. If phrased definitively, with language that incorporates drones into the term "aircraft," drones could effectively be excluded from coverage for general liability and hull exposures. Pools wanting to use an aircraft type exclusion to avoid coverage for any drone exposure should be sure the exclusion applies to all lines of coverage, including public officials and law enforcement liability. For example, if the pool covers breach of privacy in its law enforcement liability coverage document, does an aircraft exclusion eliminate that coverage because the breach of privacy occurs using a drone? If the pool offers cyber coverage, does that include a cyber breach occurring by an attack on a drone or the systems that control it? Specificity is key in determining coverage for drone risks.

What types of expertise does the pool need to write and service drone coverage?
Whenever a pool decides to write coverage for a new risk, the issue arises of whether it needs to add or train staff for the new exposure. To provide drone coverage, it's clear underwriting needs to consider emerging issues, new technology, and untested use by public entities. Loss control and claims staff may also need to become more familiar with these risk areas, so pools are encouraged to look for external resources and build internal resources accordingly.

Pools might consider when the limits offered for drone coverage are high enough that additional underwriting should be performed. Keep in mind that the size and cost of a drone is not the sole determinant of most exposures. Small and inexpensive drones can potentially cause very large losses for bodily injury, personal injury, breach of privacy, and other exposures. Pools may want to consider requiring specific underwriting information at least to confirm their members are operating drones in accordance with FAA and other legal requirements.

What type of underwriting information should the pool request from its members?
Pools may want to consider following the lead of specialized aviation insurers, by collecting detailed information about the number, type and specifications of drone(s) to be used; the base station and transmitter; payload (cameras or other equipment); the operators' names, training, certification, and experience; specific intended uses; how information gathered will be protected and controlled; how its navigation systems are secured; maintenance of logs; and proof of a COA from the FAA for the intended use(s). Obtaining this information should not be difficult, because current FAA rules require a member to present much of it to obtain a COA.

For useful detail on possible underwriting considerations, see *Dawning of the Drones: the Evolving Risk of Unmanned Aerial Systems*, Marsh, June 2015.

How are pools, commercial insurers and reinsurers treating drone coverage?
Drone use is still relatively new and pools, commercial insurers, and reinsurers are analyzing how best to address resulting risks in coverage. Many pools exclude drone use from coverage altogether by excluding damage to aircraft, liability arising from aircraft, and aircraft as a peril. This approach requires a definition of aircraft that is sufficiently broad to encompass unmanned aircraft. Like cyber liability, exclusion may be a short-term strategy as drone use becomes more integrated into public entity operations and risks are better understood.

Commercial GL policies and many pool liability coverages exclude aviation risk, but some are adding exceptions to aircraft exclusions to cover smaller types of unmanned aircraft. An example would be inserting an exception to the aircraft exclusion for "your unmanned remote control helicopter or aircraft up to three feet in wingspan, diameter or length while being used in the course of your

[insert type of industry] business." Some pools have added exceptions to aircraft exclusions for drones that meet certain criteria for speed and size. A good starting place for establishing those criteria would be the FAA Notice, which would require that drones weigh less than 55 pounds and not exceed 100 mph or go higher than 500 feet.

ISO has developed endorsements that are available to its members for the purpose of tailoring ISO CGL and commercial liability umbrella/excess programs to include drone coverage. ISO subscribers can access information about these coverages at http://www.verisk.com/iso/drones.html.

Here are two examples of approaches taken by pools:

- Provide limited hull coverage ($2,500) for no additional premium, and first and third party data breach coverage through a commercial carrier. Exclude BI or PD arising from aircraft except liability assumed under a contract.
- Provide hull coverage for drones valued up to $25,000 as "mobile property." Drones fall outside the policy definition of aircraft because they are not designed for the transport of persons or property. More expensive drones must be reported, separately scheduled, and are subject to additional contribution. Coverage includes third party BI, PD and PI liability, including privacy violations. No special sublimit or deductible or additional premium is imposed, but there is a $3 million annual aggregate on data breach liability.

Pools wanting to provide some level of coverage for drone operations have another potential issue to confront: their reinsurers. Reinsurer reaction may well depend on how well the pool prepares to launch the coverage and information about the ultimate exposure for the reinsurer. Pools should be prepared to discuss with reinsurers, at a minimum, the following information:

- How are drones currently in use by pool members, and what trends are expected?
- What types of coverage will be provided by the pool?
- Will specific uses be identified as covered, or will any use by the member be covered?
- Will there be special sublimits or aggregates?
- Will the pool separately underwrite each risk or will the coverage be granted without specific information?
- Will the pool require an additional contribution for each risk?
- Does the pool support the members with a loss control program directed at drone risks?

We are not aware of any pools that have developed freestanding drone coverage documents – but if your pool has done so, please let us know.

Specialized aviation insurers are offering full suites of coverage designed specifically for drone users, including law enforcement, SWAT teams, emergency responders, fire and rescue, traffic patrol and accident assistance, and others.

Loss Control Considerations for Pools

Regardless of whether or how a public entity pool provides drone coverage, it may be in a strong position to provide member loss control advice and other risk management programs appropriate for evolving use of drones. The focus of such programs may be awareness, compliance, coverage, and policy guidance for those local government or school entities who choose to use a drone for any purpose. Of course, a pool's efforts to help member entities will be guided by its

own familiarity with drone issues. Pools might consider specialized assignments to staff in order to more fully research and understand drone-related risks, or might seek outside expertise.

General awareness. With the growing prevalence of drones in both the private and public sectors, all local government entities and schools should have a general awareness about how drones are likely to be used, whether recreationally or commercially. Elected and appointed officials should know about emerging drone issues and common concerns. Information to raise awareness about drone use should not be limited to ways the public entity, itself, might use drones – rather, awareness efforts should also include how private or commercial drone use could impact residents, businesses, and others within the community.

Compliance. Local government entities and schools should be aware of federal and state requirements regarding drone use, including how those regulations might shift over time and the specific requirements for government use of drones. As federal rules change and state regulations are implemented, and as local governments promulgate regulations of their own, ongoing updates and information sharing will be important.

Coverage. Public entities will benefit from learning about emerging drone use, common issues, and risks – and should be able to consider such uses and risks against available coverage for any specific drone use they might anticipate. Pools are encouraged to share specific information about coverage and limitations, application of coverage in likely scenarios involving drone use, and details about coverage unknowns.

Policies & Practices. As public entities consider increasing use of drones, whether on a direct or contracted basis, they will need to develop associated policies and practices. Pools are in an ideal position to help assure such policies are appropriate, compliant with federal and state laws, and consistent with available coverage. Public entities will benefit from policy guidance, template language, or other resources on:

- Reviewing existing local government operations across all areas to identify functions or activities where drone use might be implemented, and to determine whether revised or additional policies or practice guidelines are necessary.
- Developing policies and practices focused on function, not technology. In other words, developing policies that apply to common risks in use of drones but are not limited to drone technology.
- Considering how long images or information captured by use of drone or other means will be retained, how they will be controlled, and who will have access to them.
- Determining whether such information, images, or utilization logs will be public records.
- Developing appropriate retention schedules and disclosure policies.
- Securing technology systems from breach, including drone controls, software, data links, etc.
- Developing back-up policies and response protocols to be followed in case of security breach.

- Evaluating whether public entities have authority to restrict, enable, or license drone use; and whether a local government can grant privacy in land use to include or exclude drones on certain property.
- Determining appropriate consequences for public entity personnel who violate drone-related policies or required practices.
- Developing appropriate contract language for third-party drone operators and mutual aid operations.

Claims Handling Practices and Related Considerations

Because drone use is new and emerging, there is likely to be a lag until pool claims professionals are faced with their first need to manage a drone-related matter. Developing internal staff expertise now will help adequately prepare the pool for drone-related claim matters, should they arise in the future. A pool might consider whether specialized training on drone-related issues is appropriate for a designated claims specialist, whether all claims staff should receive additional training, or whether useful external resources exist.

In particular, claims staff should be prepared to handle contract-related liability issues involving drone use, which are likely to be more tricky in terms of coverage and member relations. The combination of cyber risks and drone use may also present an area in need of heighted claims staff awareness and specialized expertise.

Finally, it may be a good idea for pools to carefully consider the use of images and information captured via drone use in litigation, including any rules of evidence and the impact of a public entity's storage and retention practices. The collection of information and images via drone could have wide implications for the legal community, on the whole, which would have corresponding impacts on defending member claims.

Pool Use of Drones

It's possible, and probably likely in the long-term, that public entity pools will want to use drone technology in support of their own operations. We've heard of one pool that implemented a drone for inspecting covered properties as part of the regular appraisal process. Other easy-to-imagine pool uses of drones include assessing damages and collecting location information for underwriting purposes. Several commercial insurers have secured FAA approval to test the use of drones in their operations, including evaluating property damage claims, responding to natural disasters, risk assessment, and other risk management functions.

Pools have all of the same risks as any other drone user, and are subject to the same regulatory restrictions and expectations. Depending on the pool's structural status, it could be subject to governmental regulatory standards or commercial standards – and all of the same contractual liability considerations outlined throughout this summary would also apply to a pool's use of a drone.

As a pool seeks to help its members understand and manage drone risks, so too should it evaluate its own possible use of drones and related risks. And, a pool should specifically review and consider its own insurance coverage terms and exclusions to determine whether it has adequate protection in place.

Conclusion

Drones offer public entities of all sizes the opportunity to enhance services, operate more efficiently, and reduce risks to their employees. Pools can expect members, even small ones, to consider and in some cases pursue this opportunity over the next few years. Now is a good time for pools to begin defining their risk appetite in this area, evaluating their coverages, and monitoring their members' drone related activity. NLC-RISC and AGRiP will continue to follow and research drone use issues in the public sector, and will update this resource as additional information becomes available. Pools are encouraged to contact us about any drone related issues not otherwise addressed in this work, and to provide us with new resources to which we can link from this report.