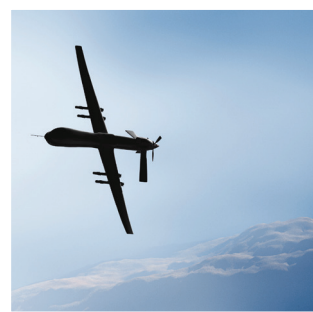
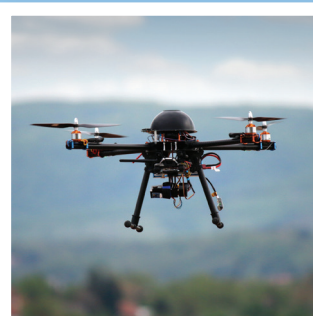




Trending Now: Domestic Drones

Risk Management Perspective on Domestic Drones

Gallagher
Public
Sector



Arthur J. Gallagher & Co.
BUSINESS WITHOUT BARRIERS™

APRIL 2015



The Use and Operation of Drones

The use of drones, also referred to as unmanned aircraft systems (UAS), is becoming increasingly popular and affordable. Drones are small, unmanned, remotely operated aircraft. Drones provide inexpensive options for research, site inspections, search and rescue operations, crime scene investigations and aerial investigations. In addition to the swell in popularity, the drone industry is expected to create over 100,000 jobs in the next 10 years, according to the Association of Unmanned Vehicle Systems International. As a result of technological advances and recent actions from the Federal Aviation Administration (FAA), more and more public agencies and higher education institutions are considering the implementation of drone flight programs.

Local governments, higher education institutions and other public entities may operate drones upon receipt of a certificate of waiver or authorization (COA) from the FAA. The FAA has currently issued 79 COAs to public agencies and other organizations, including city, county and university law enforcement agencies as well as various state colleges and universities. The COA application process can be slow and cumbersome and not every COA application is approved by the FAA. A list of COA holders

is available for review on the FAA website and the website also includes many resources, including guidelines for usage, frequently asked questions, regulations and policies.¹

Commercial use of drones is currently barred unless the FAA issues an exemption, the most common of which is known as a “Section 333 Exemption.” As of March 5, 2015, the FAA has granted 42 Section 333 Exemptions for operations including aerial inspections for insurance purposes (State Farm Mutual Automobile Insurance Company), development of economic platforms for aerial survey, law enforcement, first responders, search and rescue (LowCountryRD, corporation), bridge inspections (Asymmetric Technologies), flare stack inspections (Total Safety U.S.), precision agriculture (Viafield), and closed-set filming (multiple companies).² These commercial use exemptions enable local governments and law enforcement to skip the COA process and contract directly with third parties for the approved drone use.

¹ https://www.faa.gov/uas/public_operations/foia_responses/ (updated as of March 5, 2015)

² https://www.faa.gov/uas/legislative_programs/section_333/333_authorizations/ (last modified March 4, 2015)



Key Issues

Access to and application of the drone technology is only one consideration. Although the advances in drone technology and application are impressive and the use is becoming more commonplace, key considerations for local government and higher education must be addressed, with the potential benefits weighed against potential threats and concerns. Those considerations must include balancing privacy rights and the protection of civil liberties against the collection and use of drone surveillance information. Advocates and civil liberties groups fear that law enforcement agencies may use drones to bypass fundamental Fourth Amendment privacy rights. State legislatures are already reviewing warrant requirements and other considerations, but no uniform approach has yet emerged. Of the 20 states that have passed drone legislation as of the end of 2014, not all of them address privacy issues.³

Information retention and storage practices, either by the local government or its third-party contractor, also raise liability issues. The same technology used in the drone's control, operation and surveillance is constantly collecting data (video footage, audio recordings and other bits of transmitted information). This data may constitute personal identifiable information protected by federal and state consumer privacy statutes. Under Vermont's Security Breach Notice Act, for example, an individual's name and driver's license number constitutes "Personal Information."⁴ Once collected, this data is then stored on servers and hard drives accessible via the entity's computer network and systems. Unauthorized access to the information database would trigger a data breach incident. The City of Memphis police department, for example, had to spend \$30,000 in monitoring fees and provide notices to thousands of individuals after hackers accessed the department's incident report database in 2013.

³ See, e.g., the National Conference of State Legislatures' map of Unmanned Aircraft State Law Landscape, updated through 12/29/2014, www.ncsl.org/research/civil-and-criminal-justice/current-uas-state-law-landscape.aspx

⁴ 9 V.S.A. §2430(5)

How Are Drones Categorized?

The FAA currently classifies the use of drones in the national airspace system (NAS) into three categories: Civil, Public and Model Aircraft.⁵ Each category is subject to separate permitted operation conditions and restrictions.

Civil UAS

Any private sector (non-governmental) operation of a drone for purposes other than recreation or hobby is considered a “Civil” operation.⁶ This category covers all commercial use of drones, including use by private universities and colleges. Pending the approval and implementation of the FAA’s proposed regulations introduced in February, 2015, there are only two methods of authorized Civil UAS flight: via a Section 333 Exemption or a Special Airworthiness Certificate (SAC).⁷ Generally, an SAC is granted in connection with research and development uses by private companies while Section 333 Exemptions are granted for commercial use in defined, low-risk, controlled environments.⁸ Exemptions under Section 333 are limited to the approved company’s specific use under the conditions outlined in the application. Use of a Section 333 Exemption also requires receipt of a COA.⁹

Public UAS

Drones owned and operated by government agencies and organizations, such as state, county, city government agencies or public universities, are considered “Public UAS.” Commonly requested Public UAS operation uses include law enforcement, firefighting, disaster relief, and search and rescue.¹⁰ Public UAS may operate in civil airspace only with the issuance of a COA. Public UAS COA applications are submitted online then evaluated for operational safety.¹¹ Approved COAs typically renew every two years and may include conditions such as limiting operations to daylight hours or other conditions.¹² Normally nonemergency COA applications are reviewed within 60 days, although there are procedures in place to expedite the review of one-time time-sensitive emergency operation requests in as little as a few hours.¹³

Law enforcement organizations have a two-step process before it may operate its UAS.¹⁴ The organization must first receive a COA for training and performance evaluation (indicating proficiency in flying its UAS) then it may receive a jurisdictional COA.¹⁵

Model Aircraft

UAS used as “model aircraft” are small, unmanned aircraft (drones) operated strictly for recreational and hobby purposes. Flights in “furtherance or a business, or incidental to a person’s business” fall outside the scope of recreational or hobby flights.¹⁶ Model aircraft may be operated for recreational and hobby purposes pursuant to the rules and parameters outlined in the FAA Modernization and Reform Act of 2012 and FAA Advisory Circular 91-57 without the requirement for special authorizations or waivers.¹⁷ The safety guidelines generally require that model aircraft weigh less than 55 pounds, operate below 400 feet, remain within the operator’s line of sight, avoid operating over people or stadiums, remain clear of other aircraft, and avoid operating within five miles of an airport without prior control tower approval.¹⁸

5 FAA Fact Sheet – Unmanned Aircraft Systems (UAS), issued February 15, 2015 (http://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=18297)

6 https://www.faa.gov/uas/civil_operations/ (last modified March 4, 2015)

7 https://www.faa.gov/uas/civil_operations/ (last modified March 4, 2015)

8 https://www.faa.gov/uas/civil_operations/ (last modified March 4, 2015)

9 https://www.faa.gov/uas/civil_operations/ (last modified March 4, 2015)

10 FAA Fact Sheet – Unmanned Aircraft Systems (UAS), issued February 15, 2015 (http://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=18297)

11 FAA Fact Sheet – Unmanned Aircraft Systems (UAS), issued February 15, 2015 (http://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=18297)

12 FAA Fact Sheet – Unmanned Aircraft Systems (UAS), issued February 15, 2015 (http://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=18297)

13 FAA Fact Sheet – Unmanned Aircraft Systems (UAS), issued February 15, 2015 (http://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=18297)

14 FAA Fact Sheet – Unmanned Aircraft Systems (UAS), issued February 15, 2015 (http://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=18297)

15 FAA Fact Sheet – Unmanned Aircraft Systems (UAS), issued February 15, 2015 (http://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=18297)

16 FAA Interpretation of the Special Rule for Model Aircraft, 14 CFR Part 91, June 2014

17 https://www.faa.gov/uas/model_aircraft/ (last modified March 4, 2015)

18 https://www.faa.gov/uas/model_aircraft/ (last modified March 4, 2015)

Federal Regulation

The current regulatory landscape for drone use is a patchwork of statutes and rules. The FAA Modernization and Reform Act of 2012, sought to address this by requiring the FAA to fully integrate unmanned aircraft into the NAS by September 30, 2015, and to implement standards for drone operation. In compliance with the act, the FAA has designated six test range sites for use with both manned and unmanned flights. The Act requires a streamlined COA application process for use with Public UAS flights; requires a means of requesting commercial exemptions from the FAA for the operation of small Civil UAS (less than 55 pounds), referred to as “Section 333 Exemptions;” and bars the FAA from regulating model aircraft flights so long as they are operated in accordance with basic safety rules. Designated test sites are required, per FAA policy, to comply with state, local, and federal laws regarding privacy and civil liberties and all operators at the site must provide a written plan for the storage and use of all collected test data.¹⁹

Since June 1, commercial airlines, private pilots and air-traffic controllers have alerted the FAA to **25 episodes in which small drones came within a few seconds or a few feet of crashing into much larger aircraft**, the records show. Many of the close calls occurred during takeoffs and landings at the nation’s busiest airports, presenting a new threat to aviation safety after decades of steady improvement in air travel. — The Washington Post 11/26/14

On February 15, 2015, the FAA released the first draft of their long-awaited proposed small drone regulations, entitled “Operation and Certification of Small Unmanned Aircraft Systems” (Proposed Rules).²⁰ The Proposed Rules, as first published, provide that drone operators must be over the age of 17 and must obtain a license prior to commencing flight operations. Small drones (under 55 pounds) may only be flown under 500 feet above ground level during daylight hours at airspeeds not to exceed 100 mph. The operator or their visual observer must maintain a visual line of sight on the drones at all times during operation. Safety and privacy considerations include a prohibition against operating drones over bystanders (defined as anyone not directly involved in the drone’s operation).²¹

Privacy protections, with respect to surveillance data collection and its storage, are noticeably absent in large part from the Act and the Proposed Rules. To fill this gap, the White House issued a presidential memorandum on February 15, 2015, directing federal agencies to evaluate, monitor, and report their policies for protecting private information gathered via drones.²² The new rules require federal agencies to review their current policies and create additional policies as may be needed in order to ensure adequate protection of personal, private data collected via surveillance flights and ensure compliance with existing constitutional or statutory privacy and free speech protections. Agencies are directed to release an annual report disclosing locations of surveillance drone operations and to conduct follow-up policy audits every three years. Information collected by an agency’s drone surveillance operations may only be used when consistent with an authorized purpose and any data containing personal identifiable information must be destroyed after 180 days unless expressly required for an agency’s ongoing authorized mission.²³ **Public entities and higher education institutions should review and address their surveillance collection and retention policies in light of the February, 2015 White House privacy memorandum.**

¹⁹ 78 FR 68360, published November 14, 2013

²⁰ <http://www.gpo.gov/fdsys/pkg/FR-2015-02-23/pdf/2015-03544.pdf>; *Operation and Certification of Small Unmanned Aircraft Systems*; Proposed Rule, 14 CFR Parts 21,43, 45, et al. (published Monday, February 23, 2015)

²¹ <http://www.gpo.gov/fdsys/pkg/FR-2015-02-23/pdf/2015-03544.pdf>; *Operation and Certification of Small Unmanned Aircraft Systems*; Proposed Rule, 14 CFR Parts 21,43, 45, et al. (published Monday, February 23, 2015)

²² <http://www.whitehouse.gov/the-press-office/2015/02/15/presidential-memorandum-promoting-economic-competitiveness-while-safegua>

²³ <http://www.whitehouse.gov/the-press-office/2015/02/15/presidential-memorandum-promoting-economic-competitiveness-while-safegua>



State and Local Oversight

States have limited authority to enact and enforce drone-related legislation. Control over flight and safety in the NAS are under the federal government and FAA purview. Therefore federal law will preempt any *state or local law* regarding the operation of a drone in NAS.²⁴ States may regulate the use of unmanned aircraft by state or local law enforcement organizations and may pass legislation that addresses general privacy concerns, such as voyeur or nuisance protections that include the surveillance data collected by drones.²⁵ This is resulting in variations state by state. Florida, Utah, and Montana prohibit law enforcement agencies from using drones without first obtaining a probable cause warrant or in an emergency.²⁶ Virginia lawmakers imposed a moratorium on all state and local law enforcement drone use through July, 2015, regardless of whether a warrant has been issued or an emergency exists.²⁷ In Wisconsin, it is a misdemeanor for a private individual to use a drone to “photograph, record, or otherwise observe another individual in a place where the individual has a reasonable expectation of privacy.”²⁸

In 2014, 35 states considered unmanned aircraft-related legislation and 2015 is shaping up to be no different.²⁹ Privacy and the use of captured surveillance images are the main focus for a majority of the state and local government proposals. The Virginia state Senate and House of Representatives have both passed legislation to prohibit and limit law enforcement use of drones; those bills are currently pending revisions. Georgia already has three drone-related bills pending in its current legislative session; all bills include language restricting the collection and use of drone surveillance images. The Washington state House of Representatives passed two drone surveillance related bills at the beginning of March, one of which requires law enforcement agencies to obtain legislative approval prior to the purchase of drones and to obtain a warrant for any nonemergency uses (the bills are pending in the state Senate).³⁰ In 2013, Charlottesville, Virginia was the first city to pass anti-drone legislation. Not to be outdone, the cities of Berkeley, California; Deer Trail, Colorado; Iowa City, Iowa; Pierce County, Washington and Rancho Mirage, California have all introduced proclamations to regulate the domestic use of drones.³¹ **Public entities and higher education institutions need to be aware of local and state regulations—especially because these will continue to evolve over the coming years.**

²⁴ 49 U.S. Code § 40103(a)(1)

²⁵ Wells C. Bennett, *Civilian Drones, Privacy, and the Federal-State Balance*, Brookings Institute, September 2014

²⁶ Wells C. Bennett, *Civilian Drones, Privacy, and the Federal-State Balance*, citing Fl. Stat. § 934.50; Ut. Code § 63G-18-101; Mt. Code Ann. § 46-5-109-110

²⁷ <http://www.washingtontimes.com/news/2014/oct/10/drones-cant-be-used-va-search-warrants-ag/#/> (Virginia Attorney General confirming the moratorium through July, 2015)

²⁸ Wisc. Stat. Ann. § 942.10

²⁹ 2014 State Unmanned Aircraft Systems (UAS) Legislation, NCSL (www.ncsl.org/research/civil-and-criminal-justice/current-uas-state-law-landscape.aspx)

³⁰ http://www.thenewtribune.com/2015/03/04/3670313_washington-house-passes-bill-to.html

³¹ Institute for National Security and Counterterrorism (INSCT)

Drone Usage by Federal Agencies, States, Universities and Law Enforcement

Federal Agencies

Customs and Border Protection, which has the largest U.S. drone fleet outside the Defense Department, flew nearly 700 surveillance missions on behalf of other agencies from 2010 to 2012.³² The drone flights were used in disaster relief and in the search for marijuana crops, methamphetamine labs and missing persons, among other missions not directly related to border protection.³³

State Agencies and Universities

Drone research and test flights have provided financially beneficial public-private research partnerships for state agencies and public universities, particularly in the agriculture and safety industries. The Georgia Department of Transportation funded a \$75,000 research study by Georgia Tech to evaluating drone use monitoring highway vehicle flow and accident investigations. Kansas State University at Salina uses its COAs for agriculture research projects, studying aerial wheat crop pest detection methods in one instance. One of the COA conditions for their research flights includes approval of the homeowner or landowner prior to flying the drones overhead. Virginia Tech, one of the designated UAS Operational Test Sites, has partnered with 10 news media companies including The Washington Post, Gannett, The New York Times Co., and the Associated Press, to research and test the safe operation and use of drones in news gathering. In addition to the six UAS Operational Test Sites, the FAA is in the process of selecting designated “Centers of Excellence for Unmanned Aircraft Systems.” Such designations could generate research and grant funding for the designated locations. Georgia Tech, one of the universities vying for a Centers of Excellence designation, has partnered with CNN to also research safety issues with news gathering drone flights.



Law Enforcement

Law enforcement agencies across the country are exploring use of drones for use in areas such as traffic monitoring, search and rescue missions, and crime scene photography, but are hesitant with regard to surveillance uses. In general, law enforcement can use drones to survey anything that is visible to the human eye without a warrant. However, there are drones on the market that have structure penetrating technology which can uncover details that are not visible to the naked human eye. Local law enforcement agencies cite the need for clarification of state guidelines before incorporating surveillance uses into every day operations. Law enforcement agencies are also keeping a close eye on the Proposed Regulations as they move through the approval process. As currently published, law enforcement agencies could skip the cumbersome COA application process and instead utilize third-party commercial contractors for conducting drone operations. The commercial operators would not be subject to the same flight operation disclosures as required with COA applications. The Proposed Regulations are still subject to comments and revisions, but permitting commercial drone operation would enable agencies to further save on drone acquisition, operation, and maintenance costs.

³² Craig Whitlock and Craig Timberg, Border-patrol drones being borrowed by other agencies more often than previously known (The Washington Post, January 14, 2014)

³³ Craig Whitlock and Craig Timberg, Border-patrol drones being borrowed by other agencies more often than previously known (The Washington Post, January 14, 2014)

Drone Unknowns—Coverage, Liability, Acceptable Use

Operation of drones either directly or through third party contractors exposes entities to a myriad of risks and potential liabilities, ranging from the operation of the drones to the collection and protection of all data collected. All contracts and agreements with third parties relating to the use of drones should contain provisions outlining the proposed flight operations and data privacy protections, ensuring compliance with all applicable federal, state and local requirements. Public entities are not automatically immune from liability in the event of a data breach. In addition to any federal requirements, 45 states each have their own data breach statutes. As a general rule under various data breach statutes, entities can be held liable when third-party business associates fail to use common data protection standards. Notification costs alone required per a state statute can strain an entity's budget and financial resources.

In addition to incorporating minimum data protection provisions in all contracts, entities should also include hold harmless and release provisions for third party actions. The National Transportation Safety Board (NTSB) confirmed in a landmark November 2014 decision that the FAA has the authority to levy fines and other penalties for unsafe drone operations.³⁴ There, a third party operator capturing film footage of the campus on behalf of the University of Virginia was fined \$10,000 for “unsafe operations” (the case later settled for a reduced fine of \$1,100).³⁵

Before utilizing drones, entities should, at a minimum, consider the following coverages when evaluating their exposures:

General Liability: Some insurers will provide coverage for drones at no additional charge while other insurers are currently excluding such coverage. Before owning or operate a drone, coverage related to invasion of privacy claims should be assessed.

Property Liability: Coverage for the drone itself is not guaranteed if it is damaged; a property insurer may or may not cover this type of mobile equipment.

Aircraft or Aviation Liability: Drone liability coverage may be purchased from the aviation marketplace. Public entities considering use of drones directly or through third part contractors should become familiar with applicable FAA regulations and state statutes.

Cyber Risk Liability: Cyber liability insurance addresses gaps in coverage for expenses that may arise in the aftermath of a data breach. Depending on the policy, covered expenses may include the legal costs and costs associated with notifying all of the impacted individuals.

FAA Corrects Drone Folklore

MYTH #1

The FAA doesn't control airspace below 400 feet.

FACT

The FAA is responsible for the safety of the U.S. airspace from the ground up. This misrepresentation may originate with the idea that manned aircraft generally must stay at least 500 feet above the ground or because of the rules for model aircraft.

MYTH #2

Commercial UAS flights are okay if I'm over private property and stay below 400 feet.

FACT

The FAA published a Federal Register notice in 2007 that clarified the agency's policy: You may not fly a UAS for commercial purposes by claiming that you're operating according to the Model Aircraft guideline (below 400 feet, three miles from an airport, away from populated areas). Commercial operations are only authorized on a case-by-case basis. A commercial flight requires a certified aircraft, a licensed pilot and operating approval.

MYTH #3

Commercial UAS operations are a “gray area” in FAA regulations.

FACT

There are no shades of gray in FAA regulations. Anyone who wants to fly an aircraft—manned or unmanned—in U.S. airspace needs some level of FAA approval. Private sector (civil) users can obtain an experimental airworthiness certificate to conduct research and development, training and flight demonstrations. Commercial UAS operations are limited and require the operator to have certified aircraft and pilots, as well as operating approval.

For more myths visit [Busting Myths about the FAA and Unmanned Aircraft-Update](#).

³⁴ *Huerta v. Pirker*, NTSB Docket CP-217 (November 18, 2014)

³⁵ <http://www.wsj.com/articles/u-s-federal-aviation-administration-settles-with-videographer-over-drones-1421960972>

Resources

Current Unmanned Aircraft State Law Landscape

<http://www.ncsl.org/research/civil-and-criminal-justice/current-uas-state-law-landscape.aspx>

U.S. Department of Transportation Federal Aviation Administration, Air Traffic Organization Policy, July 2014

http://www.faa.gov/documentLibrary/media/Notice/N_JO_7210.873_Unmanned_Aircraft_Operations.pdf

ACLU Domestic Drones

<https://www.aclu.org/blog/tag/domestic-drones>

National Conference of State Legislatures, 2014 State Unmanned Aircraft Systems (UAS) Legislation.

<http://www.ncsl.org/research/civil-and-criminal-justice/2014-state-unmanned-aircraft-systems-uas-legislation.aspx>

Institute for National Security and Counterterrorism, Syracuse University, Domesticating the Drone

<http://uavs.insct.org/1948-2/>

References

1. **Protecting Privacy from Aerial Surveillance: Recommendations for Government Use of Drone Aircraft.** December 2011. Report by Jay Stanley and Catherine Crump
2. **Recommended Guidelines for the use of Unmanned Aircraft,** International Association of Chiefs of Police, and Aviation Committee. August 2012.
3. **FAA Modernization and Reform Act of 2012.** H.R. 658 – 112th Congress (2011-12)
4. **FAA Aerospace Forecast Fiscal Years 2013-2033**
5. **Border-patrol drones being borrowed by other agencies more often than previously known,** January 14, 2014, Craig Whitlock and Craig Timberg, The Washington Post
6. **FAA News & Updates. Busting Myths about the FAA and Unmanned Aircraft,** February, 26, 2014
7. **Rich Williams, *Current Unmanned Aircraft State Law Landscape*,** September 16, 2014, National Conference of State Legislatures



Arthur J. Gallagher & Co.

Two Pierce Place
Itasca, IL 60143-3141

Gallagher
Public
Sector

About the Team

This publication was written by Elizabeth Wharton and Scott Thomason and edited by Dorothy Gjerdrum.

Scott Thomason, National Director, Gallagher Public Sector

Scott Thomason is an Area Vice President for Arthur J. Gallagher Risk Management Services, Inc. based in Atlanta, Georgia and is a National Director for the Gallagher Public Sector. He leads Gallagher's Southeast efforts working on large self-insured governmental entities, large and small schools, public-private venture firms, public entity risk pools, charter schools and other public sector accounts. He brings over 25 years of experience to the Gallagher team with expertise in risk financing, risk analysis, risk innovation and creative program design.

Scott is considered one of the leading public entity and educational risk experts in the Southeast. His speaking experience includes elected officials training, risk financing and retention level analysis and risk management. Scott is also an active participant in national associations such as PRIMA, AGRIP, ASBO and URMIA and many of their state chapters.

Elizabeth Wharton, Attorney at Law, Hall Booth Smith, P.C.

Elizabeth Wharton focuses her practice on guiding clients through business transactions, public policy and contracting matters and providing effective legal solutions to achieve their goals. Prior to HBS, Elizabeth gained legal experience as in-house counsel for an information technology security company where she represented developer and lender clients as an associate with a top-tier international law firm, and as counsel for the Senate Judiciary Committee during the Georgia General Assembly's 2010 Legislative Session. Elizabeth is involved in the business transactions, government affairs, real estate and education practice groups with HBS. She is a regular blog contributor and presenter on technology, legislative and regulatory policy and governance matters.

Dorothy Gjerdrum, Senior Managing Director, Gallagher Public Sector

Dorothy Gjerdrum is the leader of Gallagher's largest client practice group, which includes cities, counties, K-12 public schools, state governments, special districts and public sector pools. She has 25 years of public sector risk management experience.

From 2008-2014, Dorothy was the Chair of the US Technical Advisory Group to ISO 31000 which is responsible for representing the interests of the United States risk management community in the standards development process. In addition to leading Gallagher Public Sector, Dorothy is a leading ERM consultant for cities, counties, public school districts, community colleges and public universities. She is a frequent speaker on ERM and ISO 31000 and its application in the public sector.

For questions, please contact:

Scott Thomason

scott_thomason@ajg.com

Elizabeth Wharton

ewharton@hallboothsmith.com

Dorothy Gjerdrum

dorothy_gjerdrum@ajg.com