**Legislative Task Force on**

**Unmanned Aircraft Systems**

**Report to the Legislature**

**(January 15, 2014)**

**DRAFT November 25, 2013**

**Task Force Members**

Representative Shelley Hughes, Co-Chair

Senator Donny Olson, Co-Chair

Lt. Steve Adams, Department of Public Safety

McHugh Pierre / Mike O’Hare, Department of Military and Veterans’ Affairs

Greg Walker and Ro Bailey, Alaska Center for Unmanned Aircraft Systems Integration at the University of Alaska Fairbanks

Steve Colligan, Academy of Model Aeronautics – Alaska Chapter

Steve Strait, Aviation Advisory Board

**Table of Contents**

[EXECUTIVE SUMMARY 1](#_Toc373161448)

[INTRODUCTION 2](#_Toc373161449)

[Background 3](#_Toc373161450)

[REVIEW SUMMARY 3](#_Toc373161451)

[SAFETY GUIDELINES 4](#_Toc373161452)

[PRIVACY CONCERNS 4](#_Toc373161453)

[Privacy and Civil Liberties Consideration 5](#_Toc373161454)

[Homeland Security Privacy Impact Assessment 6](#_Toc373161455)

[Alaska State Law and Personal Privacy 6](#_Toc373161456)

[Self-Regulation by Three National Organizations 9](#_Toc373161457)

[Technical Operations Guidelines 10](#_Toc373161458)

[Benefits to Alaska 11](#_Toc373161459)

[RECOMMENDATIONS 12](#_Toc373161460)

**APPENDICES**

A

B

C

# EXECUTIVE SUMMARY

The Legislative Task Force on Unmanned Aircraft Systems (UAS) was formed under House Concurrent Resolution No. 6 to review regulations and guidance regarding UAS and provide recommendations for a comprehensive state policy for unmanned aircraft that protects privacy and allows the use of unmanned aircraft systems for public and private applications.

Being sensitive to public concern, the Legislative Task Force on UAS (LTFUAS) reviewed multiple potential UAS scenarios focusing on economic development, law enforcement, anticipated mission types, and safety. The Task Force evaluated existing privacy laws for Alaska without recommending duplicative law for UAS, considered ways to encourage the economic development and safe uses of UAS in Alaska, and supported public education to reduce fear and embrace UAS to be used in life safety and other beneficial applications.

The Task Force concluded that the FAA is adequately addressing the safety concerns of integrating unmanned aircraft systems in the National Air Space (NAS). Existing guidelines clearly state the requirements of the aircraft, pilot training and responsibilities, and the expectations of the Test Sites (to be selected). The rules outlined in the guidelines provided the Task Force assurance that unmanned aircraft can be operated safely in Alaska.

The Task Force recommends the following:

* Law enforcement agencies adopt the IACP guidelines
* Formation of a public review panel to establish broad categories of approved UAS use
* Require high visibility paint scheme for aircraft

As we move forward, particularly but not exclusively in the event Alaska is chosen as an FAA test site for UAS Integration, LTFUAS further recommends immediate emphasis on:

* 1. management of the test ranges,
  2. economic development opportunities, and
  3. public education regarding UAS.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Shelley Hughes Donny Olson

# INTRODUCTION

The Legislative Task Force on Unmanned Aircraft Systems (UAS) was formed under House Concurrent Resolution No. 6 and charged with the duties of:

1. reviewing regulations and guidance from the Federal Aviation Administration (FAA) regarding UAS;
2. providing written recommendations, together with suggested legislation, for a comprehensive state policy for unmanned aircraft that protects privacy and allows the use of unmanned aircraft systems for public and private applications; and
3. submitting a final report to the legislature.

The Legislative Task Force on UAS (LTFUAS) met **[include dates]** twice via teleconference and twice in person to respond to the concerns Alaskans have raised regarding unmanned aircraft use in Alaska. This *DRAFT* report presents the findings of the Task Force as required by HCR6, SLA13. The LTFUAS:

1. reviewed regulations and guidance from the FAA, International Association of Chiefs of Police, and many other recommendations for UAS operations;
2. received hours of public testimony and written public testimony; and
3. compiled recommendations and suggested legislation for the use of unmanned aircraft systems for public and private applications in Alaska that are protective of privacy.

The result of these meetings is this Executive Summary, report of findings, and documentation supporting the decisions of the LTFUAS.

The LTFUAS considered two approaches to regulating the use of UAS in Alaska:

* Restrict the industry and adopt exemptions for specific kinds of approved uses, or
* Generally allow UAS operations in Alaska and adopt the necessary privacy, operations, and other guidelines that seem necessary to protect Alaskans.

The Task Force adopted the second approach and emphasized that educating the public will be an important part of integrating this technology safely and for the benefit of Alaskans.

The Task Force concluded that the FAA is adequately addressing the safety concerns of integrating unmanned aircraft systems in the National Air Space (NAS). FAA Guideline N 8900-227 spells out the details of operating UAS by clearly stating the requirements of the aircraft, pilot training and responsibilities, and the expectations of the Test Sites (to be selected). The rules outlined in the guidelines provided the Task Force assurance that unmanned aircraft can be operated safely in Alaska.

The FAA also recently released its Final Privacy Requirements, November 2013. The privacy document from the FAA clearly identified that while it governs the NAS, local governments will assume the responsibility of addressing privacy concerns.

Alaskans are fortunate to live in a state where the constitution and state law provide some of the greatest privacy protections compared to other states. As the Task Force reviewed multiple scenarios for misuse of the UAS, we determined that existing laws would apply, are sufficiently protective of privacy, and penalties are already in place to address inappropriate behavior.

When studying the many possible scenarios for misuse, the Task Force returned repeatedly to the premise that an unmanned aircraft is a tool; the operator needs to be considered for breaches of privacy or harming another.

This report presents the findings of the LTFUAS resulting from task force meetings, public testimony, research, and information from industry experts in pursuit of the assigned duties listed above.

## Background

This technology is growing rapidly worldwide, and UAS are currently used across the United States for a variety of beneficial purposes. The Task Force approach is to responsibly embrace the positive uses without overregulating the industry and thus hindering economic opportunity. In addition to accepting the use of UAS in Alaska, the Task Force recognizes that public perception is greatly influenced through media reports, such as military flights in war zones. The public appear hesitant to allow UAS in Alaska due to fear of invasion of personal privacy and overreaching law enforcement.

# REVIEW SUMMARY

“Since the early 1990s, unmanned aircraft systems (UAS) have operated on a limited basis in the National Airspace System (NAS). Until recently, UAS mainly supported public operations, such as military and border security operations. The list of potential uses is now rapidly expanding to encompass a broad range of other activities, including aerial photography, surveying land and crops, communications and broadcast, monitoring forest fires and environmental conditions, and protecting critical infrastructures.

**FAA ‘Roadmap’**

“Ultimately, UAS must be integrated into the NAS without reducing existing capacity, decreasing safety, negatively impacting current operators, or increasing the risk to airspace users or persons and property on the ground any more than the integration of comparable new and novel technologies.”

The FAA created the Unmanned Aircraft Systems Integration Office to facilitate integration of UAS safely and efficiently into the NAS. Toward that goal, the FAA is collaborating with a broad spectrum of stakeholders, which includes manufacturers, commercial vendors, industry trade associations, technical standards organizations, academic institutions, research and development centers, governmental agencies, and other regulators.”[[1]](#footnote-1)

## SAFETY GUIDELINES

The Task Force studied the FAA Guidelines for the Operations of Unmanned Aircraft Systems and participated in a presentation of the guidelines from Ro Bailey, Deputy Director of the Alaska Center for Unmanned Aircraft Systems Integration at the University of Alaska Fairbanks and comments from representatives of the FAA. Document number N 8900.227 provides the most current guidelines for federal approval of operating unmanned aircraft.[[2]](#footnote-2)

The Task Force recognizes that the FAA manages the safety of the national airspace and has adopted extensive guidelines regarding aircraft certification, pilot training and certification, and approval process for flights (or missions). N 8900.227 also provides detailed requirements for the operations of pending test sites and the current approval of flights in designated areas for specific purposes. The FAA pre-approves UAS missions and awards a Certificate of Authorization (COA) that identifies the details of the mission. This process is tightly scrutinized, and the entity flying the UAS is accountable to the FAA under the details of the COA.

The COA approval process gives the Task Force confidence that safety of the national airspace is adequately considered and that UAS missions will not invade personal privacy or operate inappropriately.

It is the opinion of the Task Force that no additional statutory or regulatory requirements are needed for FAA-approved missions.

## PRIVACY CONCERNS

**FAA Final Privacy Requirements**

On February 22, 2013 the FAA published and requested public comment on the proposed privacy requirements for UAS test sites that the FAA will establish pursuant to the FAA Modernization and Reform Act of 2012.

The FAA received 99 comments through Regulations.gov and 53 comments through the public engagement session.

Federal Aviation Administration Final Privacy Requirements, November 7, 2013

The FAA recently published its Final Privacy Requirements, Nov 7, 2013 (Appendix X) regarding unmanned aircraft. The FAA recognizes that there is substantial debate and difference of opinion among policy makers, industry, advocacy groups, and members of the public as to whether UAS operations at the Test Sites will raise novel privacy issues that are not adequately addressed by existing legal frameworks.

The public comments were grouped into ten categories, and the FAA provided a response to each category. You can view all categories, comments and responses in the document provided in Appendix X titled …

**Excerpts from the FAA Final Privacy Requirements:**

*There was substantial difference of opinion among commenters as to whether the UAS operations and manned aircraft operations present different privacy issues that justify imposing special privacy restrictions on UAS operations at the Test Sites. In addition, there was substantial difference of opinion regarding what elements would be appropriate for a Test Site privacy policy.*

**Test Site Requirements**

1. Test site operators must maintain a record of all UAS operating in the test sites;

2. Test site operators must require every UAS operator in the Test Site to have a written plan for the operator’s use and retention of data collected by the UAS; and

3. Test site operators must conduct an annual review of test site operations to verify compliance with stated privacy policy and practices and share those outcomes annually in a public forum with an opportunity for public feedback.

*The FAA has determined that it should not impose privacy requirements beyond those in the Final Privacy Requirements for the following reasons.* ***First****, there are many privacy laws and applications of tort law that may address some of the privacy issues that arise from UAS operations at the Test Sites.*

***Second****, the FAA believes that the Test Sites operators will be responsive to local stakeholders’ privacy concerns and will develop privacy policies appropriately tailored to each Test Site.* ***Third****, if UAS operations at a Test Site raise privacy concerns that are not adequately addressed by the Test Site’s privacy policies, elected officials can weigh the benefits and costs of additional privacy laws or regulations. Forty-three states have already enacted or are considering legislation regulating use of UAS.*

*Conclusion:*

*Based on the comments submitted, the FAA intends to require each Test Site operator to comply with all of the privacy requirements included in the Draft Privacy Requirements as well as the following additional privacy requirements:*

1. *Test site operators must maintain a record of all UAS operating in the test sites;*
2. *Test site operators must require every UAS operator in the Test Site to have a written plan for the operator’s use and retention of data collected by the UAS; and*
3. *Test site operators must conduct an annual review of test site operations to verify compliance with stated privacy policy and practices and share those outcomes annually in a public forum with an opportunity for public feedback.*

It is the opinion of the Task Force that privacy policy is adequate through the FAA requirements for the use of UAS in the Test Sites.

### Privacy and Civil Liberties Consideration

The FAA is implementing a UAS test site program to help the FAA gain better understanding of operational issues relating to UAS. Although the FAA’s mission does not include developing or enforcing policies pertaining to privacy or civil liberties, experience with the UAS test sites will present an opportunity to inform the dialogue in the Interagency Policy Committee (IPC) and other interagency forums concerning the use of UAS technologies and the areas of privacy and civil liberties.

*The Fourth Amendment is central to the privacy issues with respect to government UAS operation. Although the Supreme Court has never explicitly considered the question of UAS privacy, there is a long list of relevant precedents. Among them are several cases from the 1980s that specifically considered aerial observations and the Fourth Amendment.*

### Homeland Security Privacy Impact Assessment

U.S. Customs and Border Protection (CBP) is responsible for guarding nearly 7,000 miles of land border, 2,000 miles of coastal waters and 95,000 miles of maritime border. CBP employs several types of aircraft to achieve its mission objectives including UAS. COAs have been authorized in Arizona, Texas, Florida and North Dakota. When deploying resources for operations, the Office of Air and Marine must determine the availability of aircraft type and the integration of the requested activity into its flight operations.

**Homeland Security**

95,000 miles of maritime border security includes joint operations with the United States Coast Guard. Some of those miles include Alaska coastline.

Homeland Security addressed privacy in the Privacy Impact Assessment published September 9, 2013. A summary of privacy concerns addressed in this document includes:

1. The collection and use of data from aerial surveillance remains within the scope of its authorities to protect the border and provide support for law enforcement for law enforcement activities, while continuing to preserve a person’s right to privacy.
2. UAS present a perceived risk because they are able to fly for longer periods of time and conduct surveillance relatively undetected. While UAS can fly for longer periods of time, they are equipped with the same technology to conduct surveillance that is presently deployed on manned aircraft.
3. Concern for the security of the UAS itself and the potential for hijacking of the unmanned aircraft is managed by the close monitoring of ground control and satellite communication by encrypted data. If one ground station were to lose contact, a second ground station is equipped to pick up the UAS and continue operations.

### Alaska State Law and Personal Privacy

The State of Alaska and its local governments cannot dictate the use of the national airspace but can consider rules that better define the FAA guidelines, can consider legal repercussion for entities found in violation of adopted laws, and can provide for specific privacy laws regarding the use of UAS in Alaska.

The State of Alaska Constitution provides privacy protection, “although not unlimited, has been held to be broader than the protection afforded by the United States Constitution. Both the Alaska Constitution and the Fourth Amendment to the United States Constitution require a warrant by a governmental agency for the search of a place where a person has a reasonable expectation of privacy.”[[3]](#footnote-3)

**Legal Services**

**Constitutional Protection of Privacy:** The Constitution of the State of Alaska explicitly protects the right of privacy against government intrusion. Art. I, sec. 22 provides: “The right of the people to privacy is recognized and shall not be infringed. The legislature shall implement this section.”

**Alaska Statutory Protections:**

AS 11.41.270 Stalking, nonconsensual conduct prohibits monitoring by technical means

AS 11.61.116 Sending an explicit image of a minor

AS 11.61.120(a)(6) Harassment: publishing or distributing certain images

AS 11.61.123 Indecent viewing or photography

AS 11.76.113 Misconduct involving confidential information in the first degree

AS 11.76.115 Misconduct involving confidential information in the second degree

Although much attention regarding UAS privacy focuses on government use and the Fourth Amendment, it is non-governmental use that is likely to raise some of the most significant privacy challenges in coming years. For private entities, the key constitutional question is the extent of their First Amendment privilege to gather information.

Civil use of unmanned aircraft will fall under the federal and state laws including such provisions as trespassing, invasion of privacy, intrusion upon seclusion, publication of private facts, stalking and harassment, and business privacy.

The Task Force, with guidance from Legislative Legal Services, considered many scenarios of possible violations of state and federal law that might occur with the use of unmanned aircraft. The Legal Services memo outlining the areas of statute that protect personal privacy can be found in Appendix X.

Privacy protection scenarios considered by the Task Force include but are not limited to:

**1. If data is gathered by a government agency, it is a public record. However, AS 40.20.120 provides certain protections for private information. Use of inadvertently captured information in a criminal prosecution may depend on who captures the information and whether the person whose actions have been captured has a reasonable expectation of privacy.**

It was discussed that data captured by a UAS would be treated similarly to data captured by other technology such as cell phones, manned aircraft, satellite images, voice recorders, etc. Case law is substantial in determining if the person would be considered to have a reasonable expectation of privacy and when a warrant would be required to obtain and use any data collected.

**2. As technology continues to advance beyond ‘normal’ application of current laws, drafting new laws must adopt a balanced approach that recognizes the inherent difficulty in predicting the future.**

The Task Force determined that we cannot foresee the future applications of technology (of UAS or other technologies) therefore, creating restrictions in law based on assumptions is not recommended.

**Observations From Above: UAS and Privacy**

This document was published in the Harvard Journal of Law and Public Privacy by John Villasenor, a senior fellow in Governance Studies and the Center for Technology Innovation, the Brookings Institution.

The Task Force discussed many of the scenarios posed by the author when considering the need for Alaska law.

**3. How should Alaska manage unintentionally captured images or data?**

Discussion concluded that there are adequate statute, case law and data retention guidelines that resolved the concerns of the Task Force.

**4. The tie between safety and privacy is tightest with respect to rules requiring the operator of a UAS to be able to see the aircraft at all times. Public UAS operated in association with the expedited authorizations in Section 334(c )(2)(C ) of FMRA have a “line of sight” requirement.**

The Task Force assumes that FAA regulations adopted in the next several years will continue to require visual line of sight operation. “Sense and avoid” technology will become more mature and some non-line-of-sight missions may be permitted by the FAA. Non-line-of-sight operations and other unknown technological advances may bring new challenges that will require the legislature to review industry guidelines and state laws in the future.

**5. Unmanned aircraft may bring efficient advances to law enforcement; however, the public seems to be highly sensitive to law enforcement using unmanned aircraft.**

After reviewing many possible uses of UAS, the Task Force determined that existing law already affords the public with adequate protections.

* Routine Technology: The use of UAS is treated much the same as any other technological tool used to protect the public. The Department of Public Safety has adopted the IACP Guidelines for UAS, and the Task Force found those guidelines to be superior for rules of law enforcement use.
* Public Navigable Airspace: The question of what constitutes “public navigable airspace” for UAS operated by the government is central to privacy policy. The Task Force found that almost every law enforcement scenario discussed was already protected by existing law.

**Law Enforcement**

Public protection will benefit greatly from unmanned aircraft for the purposes of search and rescue, crash scene documentation time, natural disaster monitoring, wildfire management, amber and silver alerts, hostage situations and other life safety extremes. Some efforts will require warrants to proceed and some will be allowed under a COA.

* Role of Imaging Technology: Rules and case law exist that protect citizens from inappropriate use of capturing data that is a “great more than the human eye could ever see.”
* Extended Surveillance: Law enforcement does not intend to use UAS for standard patrol activities at this time. Limiting flight hours was not seen as an acceptable control because long flights may be necessary in the event of search and rescue or natural disaster remediation operations.
* Obtaining a Warrant: After much discussion, it was decided that using UAS to gather data would require a warrant in similar situations as using any other data gathering device (such as voice recording, photography, and thermal imaging with manual technology). No additional laws are required to obtain a warrant for UAS data gathering.
* Under no circumstance would a UAS be armed. FAA guidelines do not allow anything to be dropped from an unmanned aircraft.
* Law enforcement is planning to use high-visibility marking on any UAS they will use. Application of lights and/or hi-vis paint is being considered.
* It is apparent that public education is necessary for all agencies using UAS but sensitivity is heightened for law enforcement uses.

It is the opinion of the Task Force that existing privacy laws are adequate to govern the use of unmanned aircraft.

**Voluntary Approaches**

The International Association of Chiefs of Police (IACP) adopted model guidelines for the use of UAS for law enforcement purposes.

The Association for Unmanned Vehicle Systems International (AUVSI) Code of Conduct calls for a commitment to “respect the privacy of individuals.”

Academy of Model Aeronautics has also adopted operational policies and guidelines for advanced flight systems used in radio controlled model aircraft.

It is the opinion of the Task Force that if Alaska is chosen as one of the FAA Test Sites, we will have the opportunity to participate in the use of UAS in a variety of ways that would put Alaska in the position to establish policy guiding the use of UAS for the rest of the United States to consider.

### Self-Regulation by Three National Organizations

The Task Force adopted the IACP with one modification and excerpts from the AUVSI Code of Conduct.

IACP – International Association of Chiefs of Police Recommended Guidelines for the use of Unmanned Aircraft was adopted in August 2012. The Alaska Department of Public Safety has also adopted these guidelines as their doctrine with the exception of increasing the flight approval responsibility from a “supervisor” to the director’s office.

AUVSI – Association for Unmanned Vehicle Systems International; “As an industry, it is incumbent upon us to hold ourselves and each other to a high professional and ethical standard. As with any revolutionary technology, there will be mishaps and abuses; however, in order to operate safely and gain public acceptance and trust, we should all act in accordance with these guiding themes and do so in an open and transparent manner. We hope the entire UAS industry will join AUVSI in adopting this industry Code of Conduct.”

AMA – Academy of Model Aeronautics Policies for Radio Controlled Model Aircraft Operations Utilizing First Person View, Failsafe, Stabilization and Autopilot Systems guides model aircraft operators.

The same way that the FAA does not regulate model aeronautics, the Task Force does not intend to adopt requirements of hobbyist activities using UAS.

It was discussed that a notice should be provided at the time of purchase of each model aircraft to review the AMA flight operation guidelines for appropriate use of model aeronautics. The Task Force did not adopt a requirement for notice regarding hobbyists because so many aircraft are purchased outside of Alaska and would not be required to provide the notice.

[Need to add something about integrating model aeronautics and UAS policy.]

1. Should Alaska adopt some industry-relevant voluntary approaches of self-managed rules of UAS?

International Association of Chiefs of Police Guidelines for UAS, AUVSI Code of Conduct, and the Academy of Model Aeronautics rules were considered and generally accepted by the Task Force.

## Technical Operations Guidelines

International Civil Aviation Organization (ICAO), a special agency of the United Nations, promotes “the safe and orderly development of international civil aviation throughout the world. It sets standards and regulations necessary for aviation safety, security, efficiency, and regularity, as well as aviation environmental protection.”

**UAS Operations Guidelines**

Technical rules for operating unmanned aircraft systems are clearly identified at a global and federal level. “A number of Civil Aviation Authorities have adopted the policy that UAS must meet the equivalent levels of safety as manned aircraft…”

The goal of the ICAO in addressing unmanned aviation is to provide the fundamental international regulatory framework to support routine operation of UAS throughout the world in a safe, harmonized, and seamless manner comparable to that of manned operations.

“A number of Civil Aviation Authorities have adopted the policy that UAS must meet the equivalent levels of safety as manned aircraft… In general, UAS should be operated in accordance with the rule governing the flight of manned aircraft and meet equipment requirements applicable to the class of airspace within which they intent to operate… To safely integrate UAS in non-segregated airspace, the UAS must act and respond as manned aircraft do. Air Traffic, Airspace and Airport standards should not be significantly changed. The UAS must be able to comply with existing provisions to the greatest extent possible.”[[4]](#footnote-4)

FAA Guidelines for the Operations of Unmanned Aircraft N 8900-227 specifically sets the rules for the technical operations of flying unmanned aircraft.

The FAA has established guidelines for the certification and airworthiness of the aircraft, certification of the pilot including additional instruction in operating specific UAS, flight operations with the Test Sites, management of the Test Site and certificates of authorization for particular missions.

The Task Force is confident in the FAA guidelines in protecting the safety of the national airspace.

UAF Center for Unmanned Aircraft Systems Integration, RT&D is a nationally recognized program that has shown responsible use of UAS for more than ten years. The University has applied to the FAA to be selected as one of the six federal test sites.

(Was selected as one of the FAA’s six Test Sites… December 31, 2013)

## Benefits to Alaska

Economic Benefit

Policy Development

Expedited Timeline for Test Range Use and Approved Missions

**University of Alaska Fairbanks Center for Unmanned Aircraft Systems Integration, Research Testing and Development**

The University of Alaska Fairbanks has been involved in UAS missions for more than ten years. It has participated in research and data gathering operations from Prudhoe Bay to South Africa.

The Alaska Legislature indicated its support in the University’s efforts by passage of HCR6 in the 2013 session. The resolution identified many of the good uses of UAS in Alaska and established this task force to recommend statutory changes.

Encourage UAF pilot training program for UAS

Hi-vis markings for law enforcement

Insurance for civil operators (license and bonding)

Education – public awareness

Market Alaska “open for business” for UAS

Audits of missions – FAA Privacy Policy requirement

Test Site operations manager position – FAA Privacy Policy requirement also requires a Chief Privacy Officer at Test Site

Incentive grants

Research appropriation to UAF

Definitions

# RECOMMENDATIONS

The Task Force supports its recommendations to the legislature by considering and adopting general guidelines from the following reports from the FAA: (1) Guidelines for Operations of UAS N 8900-227, (2) Comprehensive Plan to integrate UAS in National Airspace, and (3) Final Privacy Requirements. The Task Force also adopted the International Association of Chiefs of Police (IACP) UAS Guidelines as appropriate rules for law enforcement in Alaska (Appendix A).

In addition to the FAA documents, the Task Force considered a report from Legal Services that identified Alaska’s privacy laws and Constitutional protections of privacy to determine if there might be a scenario created through the use of UAS that would not be protected by existing privacy laws. The Task Force also recognized that in the event Alaska is chosen as an FAA test site for UAS Integration, an emphasis on management of the test ranges, economic development, and public education needed immediate attention.

In summary, the Task Force recommends the following:

* law enforcement agencies adopt the IACP guidelines
* form a public review panel that will establish broad categories of approved UAS use
* require high visibility paint scheme for aircraft
* If Alaska is chosen as an FAA Test Site for UAS Integration, emphasize
  + management of the test ranges,
  + economic development opportunities, and
  + public education regarding UAS.

**Appendix X**

**Unmanned Aircraft System Operations Industry “Code of Conduct”**

**Unmanned Aircraft System Operations**

**Industry “Code of Conduct”**

The emergence of unmanned aircraft systems (UAS) as a resource for a wide variety of public and private applications quite possibly represents one of the most significant advancements to aviation, the scientific community, and public service since the beginning of flight. Rapid advancements in the technology have presented unique challenges and opportunities to the growing UAS industry and to those who support it. The nature of UAS and the environments which they operate, when not managed properly, can and will create issues that need to be addressed. The future of UAS will be linked to the responsible and safe use of these systems. Our industry has an obligation to conduct our operations in a safe manner that minimizes risk and instills confidence in our systems.

For this reason, the Association for Unmanned Vehicle Systems International (AUVSI), offers this Code of Conduct on behalf of the UAS industry for UAS operation. This code is intended to provide our members, and those who design, test, and operate UAS for public and civil use, a set of guidelines and recommendations for safe, non-intrusive operations. Acceptance and adherence to this code will contribute to safety and professionalism and will accelerate public confidence in these systems.

The code is built on three specific themes: Safety, Professionalism, and Respect. Each theme and its associated recommendations represent a “common sense” approach to UAS operations and address many of the concerns expressed by the public and regulators. This code is meant to provide UAS industry manufacturers and users a convenient checklist for operations and a means to demonstrate their obligation to supporting the growth of our industry in a safe and responsible manner. By adopting this Code, UAS industry manufacturers and users commit to the following:

Safety

* We will not operate UAS in a manner that presents undue risk to persons or property on the surface or in the air.
* We will ensure UAS will be piloted by individuals who are properly trained and competent to operate the vehicle or its systems.
* We will ensure UAS flights will be conducted only after a thorough assessment of risks associated with the activity. This risks assessment will include, but is not limited to:
* Weather conditions relative to the performance capability of the system
* Identification of normally anticipated failure modes (lost link, power plant failures, loss of control, etc.) and consequences of the failures
* Crew fitness for flight operations
* Overlying airspace, compliance with aviation regulations as appropriate to the operation, and off-nominal procedures
* Communication, command, control, and payload frequency spectrum requirements
* Reliability, performance, and airworthiness to established standards
* Professionalism
* We will comply with all federal, state, and local laws, ordinances, covenants, and restrictions as they relate to UAS operations.
* We will operate our systems as responsible members of the aviation community.
* We will be responsive to the needs of the public.
* We will cooperate fully with federal, state, and local authorities in response to emergency deployments, mishap investigations, and media relations.
* We will establish contingency plans for all anticipated off-nominal events and share them openly with all appropriate authorities.

Respect

* We will respect the rights of other users of the airspace.
* We will respect the privacy of individuals.
* We will respect the concerns of the public as they relate to unmanned aircraft operations.
* We will support improving public awareness and education on the operation of UAS.

As an industry, it is incumbent upon us to hold ourselves and each other to a high professional and ethical standard. As with any revolutionary technology, there will be mishaps and abuses; however, in order to operate safely and gain public acceptance and trust, we should all act in accordance with these guiding themes and do so in an open and transparent manner. We hope the entire UAS industry will join AUVSI in adopting this industry Code of Conduct.

**Appendix XX**

INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE

AVIATION COMMITTEE

Recommended Guidelines for the use of Unmanned Aircraft

BACKGROUND:

Rapid advances in technology have led to the development and increased use of unmanned aircraft. That technology is now making its way into the hands of law enforcement officers nationwide.

We also live in a culture that is extremely sensitive to the idea of preventing unnecessary government intrusion into any facet of our lives. Personal rights are cherished and legally protected by the Constitution. Despite their proven effectiveness, concerns about privacy threaten to overshadow the benefits this technology promises to bring to public safety. From enhanced officer safety by exposing unseen dangers, to finding those most vulnerable who may have wandered away from their caregivers, the potential benefits are irrefutable. However, privacy concerns are an issue that must be dealt with effectively if a law enforcement agency expects the public to support the use of UA by their police.

The Aviation Committee has been involved in the development of unmanned aircraft policy and regulations for several years. The Committee recommends the following guidelines for use by any law enforcement agency contemplating the use of unmanned aircraft.

DEFINITIONS:

1. Model Aircraft - A remote controlled aircraft used by hobbyists, which is manufactured and operated for the purposes of sport, recreation and/or competition.
2. Unmanned Aircraft (UA) – An aircraft that is intended to navigate in the air without an on-board pilot. Also called Remote Piloted Aircraft and “drones.”
3. UA Flight Crewmember - A pilot, visual observer, payload operator or other person assigned duties for a UA for the purpose of flight.
4. Unmanned Aircraft Pilot - A person exercising control over an unmanned aircraft during flight.

COMMUNITY ENGAGEMENT:

1. Law enforcement agencies desiring to use UA should first determine how they will use this technology, including the costs and benefits to be gained.
2. The agency should then engage their community early in the planning process, including their governing body and civil liberties advocates.
3. The agency should assure the community that it values the protections provided citizens by the U.S. Constitution. Further, that the agency will operate the aircraft in full compliance with the mandates of the Constitution, federal, state and local law governing search and seizure.
4. The community should be provided an opportunity to review and comment on agency procedures as they are being drafted. Where appropriate, recommendations should be considered for adoption in the policy.
5. As with the community, the news media should be brought into the process early in its development.

SYSTEM REQUIREMENTS:

1. The UA should have the ability to capture flight time by individual flight and cumulative over a period of time. The ability to reset the flight time counter should be restricted to a supervisor or administrator.
2. The aircraft itself should be painted in a high visibility paint scheme. This will facilitate line of sight control by the aircraft pilot and allow persons on the ground to monitor the location of the aircraft. This recommendation recognizes that in some cases where officer safety is a concern, such as high risk warrant service, high visibility may not be optimal. However, most situations of this type are conducted covertly and at night. Further, given the ability to observe a large area from an aerial vantage point, it may not be necessary to fly the aircraft directly over the target location.
3. Equipping the aircraft with weapons of any type is strongly discouraged. Given the current state of the technology, the ability to effectively deploy weapons from a small UA is doubtful. Further, public acceptance of airborne use of force is likewise doubtful and could result in unnecessary community resistance to the program.
4. The use of model aircraft, modified with cameras, or other sensors, is discouraged due to concerns over reliability and safety.

OPERATIONAL PROCEDURES:

1. UA operations require a Certificate of Authorization (COA) from the Federal Aviation Administration (FAA). A law enforcement agency contemplating the use of UA should contact the FAA early in the planning process to determine the requirements for obtaining a COA.
2. UA will only be operated by personnel, both pilots and crew members, who have been trained and certified in the operation of the system. All agency personnel with UA responsibilities, including command officers, will be provided training in the policies and procedures governing their use.
3. All flights will be approved by a supervisor and must be for a legitimate public safety mission, training, or demonstration purposes.
4. All flights will be documented on a form designed for that purpose and all flight time shall be accounted for on the form. The reason for the flight and name of the supervisor approving will also be documented.
5. An authorized supervisor/administrator will audit flight documentation at regular intervals. The results of the audit will be documented. Any changes to the flight time counter will be documented.
6. Unauthorized use of a UA will result in strict accountability.
7. Except for those instances where officer safety could be jeopardized, the agency should consider using a “Reverse 911” telephone system to alert those living and working in the vicinity of aircraft operations (if such a system is available). If such a system is not available, the use of patrol car public address systems should be considered. This will not only provide a level of safety should the aircraft make an uncontrolled landing, but citizens may also be able to assist with the incident.
8. Where there are specific and articulable grounds to believe that the UA will collect evidence of criminal wrongdoing and if the UA will intrude upon reasonable expectations of privacy, the agency will secure a search warrant prior to conducting the flight.

IMAGE RETENTION:

1. Unless required as evidence of a crime, as part of an on-going investigation, for training, or required by law, images captured by a UA should not be retained by the agency.
2. Unless exempt by law, retained images should be open for public inspection.

1. Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap. 2013. U.S. Department of Transportation, Federal Aviation Administration. First Edition—2013. [↑](#footnote-ref-1)
2. FAA documents (2) [footnote-reference – get ref data]; Notice N 8900.227, Subj: Unmanned Aircraft Systems (UAS) Operation Approval. Effective Date 7/30/13, Cancellation Date 7/30/14. [↑](#footnote-ref-2)
3. Legal memo [footnote-reference – get ref data] [↑](#footnote-ref-3)
4. Roadmap page 11 [get footnote ref data] [↑](#footnote-ref-4)