# DRONES A Report on the Use of Drones by Public Safety Agencies—and a

Wake-Up Call about the Threat of Malicious Drone Attacks

# DRODNES A Report on the Use of Drones by Public Safety Agencies—and a Wake-Up Call about the Threat of Malicious Drone Attacks

TIM

This project was supported, in whole or in part, by cooperative agreement number 2016-CK-WX-K009 awarded to PERF by the U.S. Department of Justice, Office of Community Oriented Policing Services. The opinions contained herein are those of the author(s) or contributor(s) and do not necessarily represent the official position or policies of the U.S. Department of Justice. References to specific individuals, agencies, companies, products, or services should not be considered an endorsement by the author(s), the contributor(s), or the U.S. Department of Justice. References to supplement discussion of the issues.

The internet references cited in this publication were valid as of the date of publication. Given that URLs and websites are in constant flux, neither the author(s), the contributor(s), nor the COPS Office can vouch for their current validity.

This resource was developed under a federal award and may be subject to copyright. The U.S. Department of Justice reserves a royalty-free, nonexclusive, and irrevocable license to reproduce, publish, or otherwise use and to authorize others to use this resource for Federal Government purposes. This resource may be freely distributed and used for noncommercial and educational purposes only.

#### Recommended citation:

Police Executive Research Forum. 2020. Drones: A Report on the Use of Drones by Public Safety Agencies—and a Wake-Up Call about the Threat of Malicious Drone Attacks. Washington, DC: Office of Community Oriented Policing Services.

Published 2020

# CONTENTS

Letter from the Director of the COPS Office
Letter from the Executive Director of PERF
Acknowledgments
Executive Summary
Overview
The research behind this report
Key findings and recommended practices
Malicious use of drones
Risks in moving too slowly
Introduction
State of the field and policy analysis 1
Addressing community concerns about privacy
Project overview
Methodology
1. Pre-Implementation Considerations
Laws and regulations: Federal, state, and local
Community outreach
Selecting drone equipment
Funding considerations
2. Establishing a Drone Program
Staffing your drone team
Drone team training
Standard operating procedures

3. Malicious Use of Drones
Law, policy, and regulations limit law enforcement's use of certain technologies to counter drones63
New federal law
New authority on remote identification is critical
New law provides little to no role for local police
The risks of moving too slowly
Educating Drone Hobbyists to Reduce the Number of Unauthorized Drones at Major Events
Recommendations for preventing and responding to the malicious use of drones
Conclusion. Local Law Enforcement Agencies are Learning to Use Drones; Now They Must Focus on Stopping Malicious Drone Attacks
Police use of drones
Malicious use of drones by terrorists and other criminals
Appendix A. Conference Participants
Appendix B. List of Agencies that Provided their UAS Standard Operating Procedures to PERF
Appendix C. Palm Beach County Sheriff's Office Template for Writing Search Warrants for Using Drones97
About PERF
About the COPS Office

# LETTER FROM THE DIRECTOR OF THE COPS OFFICE

#### Colleagues:

Unmanned Aerial Systems (UAS) have rapidly changed the state of play in the public safety theater. Inappropriate use and deployment of UASs and their operators present a serious threat to public safety and order. The same technology also offers tremendous opportunities to improve safety outcomes for our communities and for our sworn law enforcement practitioners and other public safety first responders. The COPS Office is committed to collecting, documenting, and disseminating the best available information on UASs for state, local, tribal, and territorial (SLTT) law enforcement agencies.

Last year, the COPS Office, the U.S. Department of Homeland Security (DHS), and the Police Executive Research Forum (PERF) convened a two-day conference for experts across the law enforcement community on drones, their use and implementation, and attendant policy and operational issues. Representatives from several agencies presented on several topics:

- Regulations, community concerns, budgetary matters, and promising practices for setting up programs for use of drones in law enforcement
- Recommendations for operating such a program, including training and staffing
- Counter-use matters, such as detection and disabling technology and dangerous illegal drone use by bad actors

This report summarizes the information discussed at that conference and also presents lessons learned and promising practices gathered from interviews, policy reviews, and survey data. The presentations and discussions from this event have informed all of our UAS work going forward, and we appreciate the ongoing support and engagement from PERF, our colleagues at DHS, and all of the conference participants as we navigate this new frontier in law enforcement.

We recognize that UASs present unique challenges both for our SLTT practitioners, and we are here for the duration. The need for this report was driven by the field and the report itself is for the field. We hope that you find it useful and that you will engage with us as we develop our resources for using and managing UASs.

Sincerely,

Phil Keith Director Office of Community Oriented Policing Services

# LETTER FROM THE EXECUTIVE DIRECTOR OF PERF

#### Colleagues:

As I write this, the United States is in the midst of the COVID-19 pandemic, which is putting tremendous strains on everyone, including police departments. Police leaders are working overtime to maintain services and protect public safety, while also focusing on protecting their employees against infection and managing staffing shortages. Other issues in policing are taking a back seat to the pandemic crisis.

However, the topic of this report—police use of Unmanned Aircraft Systems, or drones—has relevance even during the COVID-19 crisis. For example, drones are being used by the Elizabeth (New Jersey) Police Department to disperse crowds and enforce social distancing rules. The Daytona Beach (Florida) Police Department is using two drones equipped with loudspeakers to communicate with the public without getting too close. In the United Kingdom and across Europe, police are using drones to monitor people's movements and enforce lockdown orders. And in Israel, police are using drones to confirm that those who tested positive for COVID-19 are self-isolating.

When the COVID-19 pandemic abates and conditions begin to return to normal, police agencies will turn their focus to other issues of drones raised in this report. There are two separate aspects of this: (1) the policy and operational considerations of police agencies using drones to advance public safety, and (2) the need for police to have certain legal authority and technical capabilities for disabling drones when they present a threat to public safety.

Drones are quickly becoming one of the most innovative and effective technologies used by police agencies today. Yet, despite the exponential increase in the number of agencies using drones, there is still a lack of clarity on how police should launch a drone program.

To address these questions and produce policy guidance for law enforcement agencies, the Police Executive Research Forum (PERF), with support from the U.S. Department of Justice's Office of Community Oriented Policing Services (COPS Office) and the U.S. Department of Homeland Security (DHS), held a two-day conference in February 2019 in Washington, D.C. This meeting featured more than 200 police chiefs, sheriffs, officers, scholars, stakeholder groups, representatives from federal agencies, and other experts to discuss the policy and operational issues regarding the implementation and use of drones.

On the first day of PERF's conference, participants discussed what agencies need to consider before starting a drone program. For example, what laws and regulations must police agencies comply with? How should police interact with and involve the community before purchasing drones? What type of drones should police purchase, and what other equipment, such as cameras, should be attached to the drone?

On the second day of PERF's conference, participants addressed a more urgent issue—how federal, state, and local law enforcement agencies must respond to the malicious use of drones—i.e., when they are used in a manner that threatens public safety. Although there is technology available to counter threatening drones, local police agencies do not have the legal authority to use it, because accidental misuse could cause as much damage as a hostile drone. Despite these legal limitations, the public expects that local police agencies will respond and protect the community if a drone threatens public safety.

This report documents the promising practices and lessons discussed by the conference participants. The recommendations in this report will help police agencies that are interested in implementing a drone program, and will provide guidance on how to respond when a drone threatens the safety of the community.

Sincerely,

Church Wexler

Chuck Wexler Executive Director Police Executive Research Forum

# ACKNOWLEDGMENTS

PERF would like to thank the U.S. Department of Justice's Office of Community Oriented Policing Services (COPS Office) and the U.S. Department of Homeland Security's (DHS) Office for State and Local Law Enforcement (OSLLE) for supporting this research into drones. We are grateful to COPS Office Director Phil Keith and Deputy Director Rob Chapman and to OSLLE Deputy Assistant Secretary Brian Dorow for recognizing the increasingly important role that this technology plays in advancing the work of law enforcement agencies and other first responders. At the same time, the COPS Office and OSLLE recognize the other critical issue addressed in this report: the severe threat to public safety when terrorists or other criminals use drones as weapons. Director Keith has been an outspoken advocate of drone programs and getting ahead of the serious threat of malicious use of drones. And we want to especially thank Brendan Groves, Senior Counsel to the Deputy Attorney General, who provided his invaluable expertise on the legal authorities in this area. We are also grateful for the support and guidance provided by our program manager at the COPS Office, Helene Bushwick.

We would also like to thank the law enforcement agencies that participated in our survey on drones. Their thoughtful responses guided our research and agenda for a two-day conference in Washington, D.C., in February 2019. We are grateful to the more than 200 police chiefs, sheriffs, scholars, and other professionals who participated in our conference (see appendix A for a list of participants). These leaders provided valuable information about their experiences with drones and provided an insightful two-day discussion of the benefits of drones, as well as the new threats this technology has created.

Thanks also go to the more than 50 police executives and department personnel who shared their drone policies with PERF and participated in interviews with PERF staff. Their candid assessments of how this technology has impacted their agencies shaped the findings in the publication.

Finally, credit is due to PERF staff members who conducted the survey, prepared for and hosted the conference, conducted interviews, and helped write and edit this publication, especially Director of Technical Assistance Jessica Toliver; Director of Communications Craig Fischer; Assistant Director of Communications James McGinty; Senior Research Associates Lisa Mantel and Dave McClure; Senior Research Assistant Adam Kemerer; Research Assistants Hyla Jacobson and Adam Kass; and Research Interns Tatiana Lloyd-Dotta and Shira Moolten.



# EXECUTIVE SUMMARY

## **Overview**

This report is about two opposite but related issues: (1) the use of drones by police agencies to protect public safety and (2) the use of drones by malicious actors to commit various crimes such as acts of terrorism. Thus, the story of drones is about two radically different sides of the same coin.

This report should be seen as two separate reports.

The bulk of the document, chapters 1 and 2, provides guidance to police and sheriffs' departments about how to identify the ways in which drones could facilitate their work and how to create a drone program to accomplish those goals.

The remainder of the document, chapter 3, is about the malicious use of drones. As of early 2020, the United States is extremely vulnerable to drone attacks because only in late 2018 were federal law enforcement agencies given the legal authority to use the most effective types of technologies to detect and mitigate drone threats. Local police and sheriffs' departments still are unable to purchase or use most counter-drone technologies because of concerns they might break the law when employing them and the danger of interference with air traffic in the National Airspace System.

This is not merely oversight by Congress and federal agencies; there are important reasons for limiting drone detection and mitigation technologies. Careless or unskilled use of these technologies could result in disaster. For example, technologies that use radio signals to jam an incoming malicious drone or seize control of it, improperly used, might interfere with radio signals used by commercial or private airplanes or air traffic controllers.

A number of federal and local law enforcement agencies have begun to explore counter-drone strategies at major events and mass gatherings such as the Super Bowl. But this work is still developing. Federal, state, and local lawmakers and government officials, including law enforcement officials, should accelerate their efforts to address these issues as soon as possible.

The drone strikes against oil facilities in Saudi Arabia in September 2019, which temporarily disrupted approximately half of that kingdom's oil production capacity, demonstrate how much harm can be done by the malicious use of drones. The United States must not wait until it suffers a drone attack to undertake large-scale efforts to develop strategies by law enforcement agencies at all levels of government for (1) identifying drone threats and (2) mitigating drone threats in real time.

## The research behind this report

In 2018 and 2019, the Police Executive Research Forum (PERF), with support from the U.S. Department of Justice's (DOJ) Office of Community Oriented Policing Services and the U.S. Department of Homeland Security's (DHS) Office for State and Local Law Enforcement, conducted research, disseminated a survey of law enforcement agencies, and hosted a two-day forum to discuss police use of drones and the police response to the threat of drones being used maliciously.

This project consisted of three major components: (1) an informal survey of 860 law enforcement agencies nationwide; (2) interviews with more than 50 police executives and personnel in agencies that operate a drone program or have plans to implement one; and (3) a two-day national conference in which police executives, federal stakeholders, and other experts from across the country discussed and debated the considerations associated with police use of drones. The purpose of this report is to assist police agencies interested in establishing their own drone programs.<sup>1</sup>

# Key findings and recommended practices

This report is divided into three chapters:

- 1. Pre-Implementation Considerations
- 2. Establishing a Drone Program
- 3. Malicious Use of Drones

Following are some of the key findings and recommendations detailed in this report.

<sup>1.</sup> This report is intended to document the results of the February 2019 conference and to disseminate and share information across the state, local, tribal, and territorial law enforcement community. It does not create any legal rights or obligations and has no legally binding effect. This report may not be used for the purpose of coercing persons or entities outside of the Federal Government into taking any action or refraining from any action.

# PRE-IMPLEMENTATION CONSIDERATIONS

The use of drones, or unmanned aircraft systems (UAS),<sup>2</sup> in the policing profession has been on the rise since approximately 2016 as drones have become more readily available. Law enforcement agencies who have deployed drones say there are many benefits associated with using these devices. They note that drones are useful for search and rescue missions, disaster response, crowd monitoring, traffic collision reconstruction, crime scene reconstruction, and investigating armed and dangerous suspects.

However, many community members have legitimate concerns about the use of drones by anyone, including the police, because of the privacy issues that occur when small, lightweight devices with video cameras can fly almost anywhere. Thus, some considerations for police agencies interested in using drones to advance public safety include undertaking a methodical process of explaining their plans publicly; holding public meetings and other forums in which community members can express their concerns; and working with the community to reach acceptable compromises or consensus approaches to issues such as defining the purposes of police drones, managing the use and possible storage of video or other data obtained by drones, and addressing the public's legitimate concerns and questions.

Prior to implementing a drone program, state and local agencies must consider a number of factors that will impact the operations of their program, including federal, state, and local laws and regulations; conducting community outreach; selecting drone equipment; and funding the drone program.

<sup>2.</sup> The U.S. Department of Defense and the Federal Aviation Administration use the term *unmanned aircraft system* (UAS), as do aviation and air traffic organizations worldwide, to emphasize the importance of more than just the crewless aerial vehicle—that is, the software, ground control stations, data links, etc. This report will use the term *UAS* interchangeably with the more colloquial *drone* but will not use UAV, RPAV, or other less comprehensive terms.

#### Federal, state, and local laws and regulations

- Research all federal, state, and local laws and regulations that will dictate your agency's drone use before starting your program. Work with your agency's legal team to ensure drone team members understand the laws and regulations they must follow.
- Consider obtaining both a part 91 certificate of authorization and a part 107 license from the Federal Aviation Administration (FAA) to conduct your program's drone operations for maximum use and flexibility.
- In states and municipalities with restrictive legislation, reach out to fellow agencies in the area to learn how the limitations affect their operations.
- Prepare templates for search warrants facilitated by the use of drones and applications for waivers of certain limitations that sometimes affect drone operations (an example warrant template is included from one jurisdiction in appendix C to this report).

#### Community outreach

- Engage with the community before implementing a drone program to ensure support for the program.
  - Proactively reach out to community organizations that are likely to have reservations about drone use, such as civil liberties or privacy interest groups, prior to program implementation. This can help the agency to get ahead of concerns, address them properly, and avoid misunderstandings.
  - Solicit feedback from community stakeholders to ensure that community concerns are addressed properly.
  - Host outreach events during a variety of days and times to ensure that a large majority of community members will be able to attend such events.
- Communicate with the public and community stakeholders about the authorized and official purposes of your drone program to ease privacy concerns about uses of drones and alleviate concerns about unauthorized uses or purposes.
  - Stress that the use of drones is to promote public safety and not for loosely defined surveillance purposes.
  - Use print, broadcast, and social media to inform and engage the public.
  - Involve your agency's public information officer to share information widely.

• Be transparent about your agency's drone policies and practices both prior to and after implementation. For example: Posting your drone policy on the department's website and releasing video of successful drone deployments (when footage can be made public) can reassure the community about your purpose and intent.

#### Selecting drone equipment

- Decide on the goals and purposes of your drone program and establish the operational parameters and specifications of features and capabilities you need to inform your purchase of drone equipment.
  - Regardless of your specific drone model needs, start small, use inexpensive models first, and test your equipment prior to program implementation.
  - Implement your drone program on a trial basis with a set time for a formal evaluation process. This process allows flexibility to make changes to the scope of services and equipment needed for your program before final implementation.
  - Take incremental steps as you develop your program to allow time to solicit community feedback and adjust as necessary.
  - Funding will naturally affect any agency's decision-making. Some drones and their associated technology are expensive in addition to the personnel hours and IT support that each program requires.

#### Funding and outfitting a drone program

- In budgeting for a drone program, consider the initial equipment costs as well as the long-term training, maintenance, and upgrade costs that come with maintaining drones.
- Engage the community in supporting drone use to help secure funding for your program.
- Conduct a cost-benefit analysis to demonstrate cost savings associated with drone use. Drones can be far more cost-effective than helicopters in performing certain functions.
- Look into potential grants or community partnerships to help offset program costs.

## ESTABLISHING A DRONE PROGRAM

#### Staffing your drone team

- Create the drone team roles based on your agency's individual needs and any state or local regulations or requirements.
- Consider training drone pilots from different units to ensure that expertise will be available for response to any type of incident, e.g., accident reconstruction, special weapons and tactics (SWAT), or missing persons.
- Determine how many drone pilots should be certified based upon the size of your jurisdiction as well as the incident types that the drone team will be responsible for responding to.
- Use both sworn and nonsworn personnel to reduce costs and maximize expertise.

#### Drone team training

- Require drone training for all agency personnel who will be assisting with drone procedures to ensure operational proficiency.
- Include the following topics if developing your own training protocols:
  - Methods of conducting safe flight operations under exigent circumstances
  - Crew Resource Management and a risk assessment-based model for decisions about whether to accept or decline a UAS flight request
  - Missions and fleet management
  - Operational guidelines for UAS pilots and technicians within an agency
  - An understanding of the role the FAA plays in public safety regulatory compliance
  - Rules of evidence related to UAS operations and agency requirements
  - How to present UAS-collected data in court to further justice
  - Methods to ensure compliance with Constitutional protections regarding free speech, privacy, and civil liberties

- Purchase inexpensive drones for new pilots to practice with during initial training.
- Train visual observers in different units (such as bomb squad or accident reconstruction personnel) to ensure someone arrives on scene in a timely manner.
- Set ongoing training requirements so team members remain proficient in drone operations and up to date on FAA rules and regulations.

# **Malicious use of drones**

All law enforcement agencies, whether or not they wish to begin a program for using drones for their own purposes, must consider a related but far more difficult challenge: how to anticipate, prevent, detect, and respond to the criminal use of drones, including use by terrorists. For example, terrorists could use drones to drop a bomb or spray a poisonous gas over large crowds of people at a public event. Drones also can be extremely effective at reconnaissance for criminal purposes because they can fly past bollards, checkpoints, and other security mechanisms.

Unfortunately, laws and public policy governing drones lag far behind the development of new counter-drone technology. Until late 2018, efforts by any U.S. law enforcement agency at the federal, state, or local level to use certain new counter-drone technology to disable or destroy threatening drones were severely hampered by federal law. Drones are considered a type of aircraft, so federal laws designed to protect airplanes and helicopters from attack also criminalized actions to destroy or disable threatening drones. Further, drones are equipped with computers, so drones—even drones being used to commit crimes—were protected by laws designed to prevent computer hacking.

Fortunately, in October 2018, Congress approved a new federal law—the Protecting Emerging Threats Act of 2018 as codified in the FAA Reauthorization Act of 2018—that gives certain federal agencies, namely the DHS and the DOJ, important new authority to detect, identify, monitor, and track drones without prior consent; to warn the operator of a drone, including by passive or active and direct or indirect physical, electronic, radio, and electronic means; to disrupt or seize control of a potentially threatening drone; to seize or otherwise confiscate the drone; and if necessary to use reasonable force to damage or destroy a threatening drone. The new authority for the FAA to regulate drones through rulemaking requiring remote identification is a separate but related critical issue contained in the FAA Reauthorization Act of 2018. Implementing "remote identification" will mean that law enforcement agents can immediately be alerted electronically to the presence of a particular drone and can read the electronic "signature" of the drone and receive information about the identity of the operator. This will help agents distinguish drones of hobbyists and legitimate organizations, such as TV news drones, from potential threats.

Local police are left out of the new anti-drone law. The new federal law does not provide authority to state and local police to disable threatening drones. Only certain federal agencies are given these new powers. That said, state and local police agencies can apply to seek assistance from DHS and DOJ which can use their authorities under the act upon request from the chief executive officer of the state or territory concerned.

One reason for Congress's reluctance to provide new authorities to thousands of local police agencies is that counter-drone technologies can be technologically challenging. For example, one method of disabling a threatening drone is to jam the airwaves in the area with radio signals that stop the operator from controlling the drone. However, there is a risk that such jamming signals could interfere with other critical radio systems, such as those that allow airline pilots to communicate with ground controllers. Thus, there are concerns that an overly aggressive police action against a possible drone threat might result in an airliner crash or other catastrophe.

However, the federal officials at PERF's meeting said that state and local police and sheriffs' departments do have general authority under the Constitution to take action to protect public safety in exigent circumstances. They gave the example of a drone that appears to be moving to drop an explosive device on a crowd of people, comparing that to the threat of a suicide bomber or truck racing toward a crowd of people. Ultimately, local police can take action to protect the public against imminent threats, commensurate with the exigency of the threat and their agency's existing policies and procedures.

Importantly, local jurisdictions can work to enact laws prohibiting or restricting the takeoff or landing of drones at certain locations to mitigate the use of drones in those sensitive areas. Such restrictions can be very helpful, because many drone operators have no malicious intent, even when their actions can be dangerous. It may not occur to them that their use of drones can make it more difficult for the police to protect the public.

For example, police see drones during major gatherings such as sports events and outdoor concerts, and they are kept busy trying to track down the drone operators and tell them they must land their drones and cease operations. By enforcing local ordinances against drones at certain locations, police

may be able to sharply reduce the number of potentially harmless but problematic drone incidents. This will enable police to focus their attention on the drone sightings that might involve an intent to do harm.

Some local police agencies are moving to explore their options and prepare themselves for a drone threat against a large crowd of people. As of 2018, there were more than 200 counter-drone technologies on the market.<sup>3</sup> Many of these technologies are not sold to local police, because manufacturers know that local police are not authorized to use them. But some local agencies are beginning to test devices that they can acquire consistent with existing legal authorities. The New York City Police Department (NYPD), for example, acquired and used a drone detection system at the New Year's Eve celebration at Times Square on December 31, 2018.

# **Risks in moving too slowly**

Experts at PERF's conference called for intensive efforts to "catch up" with the new risks posed by drones. Some noted that the United States has been fortunate not to have experienced a major drone attack to date but said there is little capability to stop such an attack, especially with limited local police authority.

In early 2020, federal law enforcement agencies have begun testing sophisticated drone detection and mitigation technologies at large-scale or sensitive events, such as national political conventions, international summits, and high-profile public gatherings such as the Super Bowl. But federal agencies lack the resources to help local police or other law enforcement agencies protect against drone attacks at countless other events that routinely attract tens of thousands of spectators, such as concerts and sports events.

Local police *are* allowed to use certain types of technologies, such as non-radio frequency-based drone detection systems, including radar-based systems, acoustic systems that can detect the sound of a drone in the air, and sophisticated camera systems. When local police detect drones flying where they are not allowed to fly, such as over a baseball stadium, they often are able to find the drone operators and force them to land the drones. Local police should continue to use such systems consistent with existing legal authorities, in systems of systems for holistic risk detection and risk mitigation, to increase their familiarity with how drones work and prepare for the day when they will be allowed to use better technologies.

<sup>3.</sup> Arthur Holland Michel, *Counter-Drone Systems* (Annandale-on-Hudson, NY: Center for the Study of the Drone at Bard College, 2018), <u>https://dronecenter.</u> <u>bard.edu/files/2018/02/CSD-Counter-Drone-Systems-Report.pdf</u>.

State and local law enforcement officials also should bring these issues to the attention of their local, state, and federal lawmakers. The United States needs a much greater sense of urgency to address the threat of malicious drones. This report is intended to be a "wake-up call" to spur action.

# INTRODUCTION

# State of the field and policy analysis

With a rapid influx of new technologies, the work of policing looks very different from what it was as recently as 2010. New technologies, such as facial recognition software and a wide variety of computer applications facilitated by high-speed broadband wireless systems, have greatly advanced law enforcement's capabilities. At the same time, however, criminal offenders have used technologies to create new types of crime, such as ransomware attacks, or have used technology to find new ways of committing old crimes, such as car theft and thefts from banks.

Because police departments' time and financial resources are limited, it is important to understand the capabilities and limitations of various new technologies, including laws, regulations, and policies applicable to their use, as well as their costs and benefits. In this way, law enforcement agencies can make the best decisions about which new technologies to deploy.

Law enforcement agencies that have deployed drones say there are many benefits associated with using these devices. *Drone* is an informal name for devices known as unmanned aerial vehicles (UAV), unmanned aircraft systems (UAS), and small unmanned aircraft systems (sUAS). The term UAS refers to the entire system for using a drone, including the aircraft and the ground control unit, while UAV refers only to the vehicle itself.

Drones are small unmanned aircrafts that can be remotely controlled or can fly autonomously via preplanned flight plans. They typically carry cameras that can transmit video or still images to their operators.

Drones have been used by the U.S. military in overseas contingency operations since 2000. In more recent years, many police and sheriffs' departments have acquired drones and used them for search and rescue missions, disaster response, crowd monitoring, traffic collision reconstruction, crime scene reconstruction, investigating armed and dangerous suspects, and other applications.

# "The use of drones is limited only by one's creativity."

— Deputy Chief Tony Zucaro, Virginia Beach Police Department

## Addressing community concerns about privacy

The use of drones by police agencies raises important questions about privacy and trust. Before implementing a drone program, law enforcement agencies must work to obtain their communities' support and understanding of why, how, when, and where police believe that drones should be deployed. Police should have written plans and guidelines about what types of incidents or situations may result in use of a drone, the specific purposes drones will be used for, what types of video footage or other information will be collected and stored, how the information will be protected, who will have access to it, and other considerations. Obtaining community support and buy-in for the limited use of drones will help to ensure that relationships of trust with community members remain strong while allowing police to take advantage of the capabilities of this extremely useful new technology.

Agencies also must consider the many practical questions associated with drone deployments, including the significant financial costs of purchasing and maintaining drone hardware and software, training drone team members, and establishing standard operating procedures that adhere to federal, state, and local laws.

# **Project overview**

Even as police use of drones increases, many questions about this technology have yet to be answered. To address these questions and produce policy guidance for law enforcement agencies, the Police Executive Research Forum (PERF)—with support from the U.S. Department of Justice's (DOJ) Office of Community Oriented Policing Services and the U.S. Department of Homeland Security (DHS)—conducted research, disseminated a survey to law enforcement agencies, and hosted a twoday national conference to discuss promising practices and lessons learned from drone deployments by leading departments as well as the separate issue of what law enforcement agencies must begin to do to reduce the threat of malicious use of drones by criminals, terrorists, or criminal organizations for criminal acts (e.g., to attack members of the public or commit acts of mass destruction).

## Methodology

This project consisted of three major components: (1) the results of an informal survey of 860 law enforcement agencies nationwide; (2) interviews with police executives and personnel in agencies that operate drone programs; and (3) a national conference in Washington, D.C., in which police executives, federal officials, and other experts from across the country discussed the many considerations associated with police use of drones.

#### SURVEY

To determine the state of the field, PERF distributed surveys to 860 police departments across the nation in September 2018. Questions addressed topics such as seeking community input, hardware and software implementation considerations, state and local legislation regarding police use of drones, standard operating procedures, and training requirements.

PERF received responses from 282 departments (a 33 percent response rate). The use of drones is undoubtedly a growing trend, with 47 percent of respondents using drones and another 34 percent reporting that although they do not currently use drones, they are interested in purchasing them in the future.

Of the 123 agencies that reported using drones, nearly 90 percent reported having a written policy governing their department's drone use. However, these policies varied greatly. Some respondents reported that they were hesitant to implement a written policy because of a lack of guidance on what a policy should include. This reluctance highlighted the need for a set of standards and best practices regarding law enforcement's use of drones.

#### INTERVIEWS

Next, PERF staff members interviewed more than 50 police executives and members of departments who have implemented—or have considered implementing—a drone program. These interviews revealed lessons learned and promising practices that are captured within this report. As part of this process, PERF also collected and reviewed policies and standard operating procedures concerning the use of drones from agencies across the country. These model policies are referenced through this publication and can be found in the appendices to assist agencies interested in establishing a drone program.

## NATIONAL CONFERENCE

Finally, PERF convened a two-day conference for more than 200 police chiefs, sheriffs, officers, scholars, stakeholder groups, representatives from federal agencies, and other experts to discuss the policy and operational issues regarding the implementation and use of drones.

This publication synthesizes information presented and discussed by the conference participants; lessons learned; and promising practices gathered from the interviews, policy reviews, and survey data. The goal of this publication is to provide law enforcement agencies with guidance on the implementation of a drone program.

The first chapter outlines pre-implementation considerations for agencies interested in establishing a drone program. The pre-implementation considerations discussed include (1) the federal, state, and local regulations that agencies must comply with; (2) effective community outreach methods; (3) benefits of a trial period; (4) promising practices for purchasing program equipment; and (5) estimating the financial costs of a program and conducting a cost/benefit analysis.

The second chapter presents recommendations and promising practices for operating a drone program, including drone team staffing, training team members, and drafting standard operating procedures.

The third chapter discusses the danger of malicious use of drones by criminal offenders, counterdrone technology, current legislation governing the use of technologies to detect and disable threatening drones, and the urgent need for police organizations to begin preparing and responding to unlawful drone use including terrorist attacks.

The department members referenced throughout this publication are those who attended the February 2019 conference, provided policies for PERF's review, or were interviewed by PERF in early 2019.<sup>4</sup> A list of participants from the February 2019 conference is included at appendix A.

<sup>4.</sup> The titles listed throughout this document reflect officials' positions at the time of the February 2019 conference.

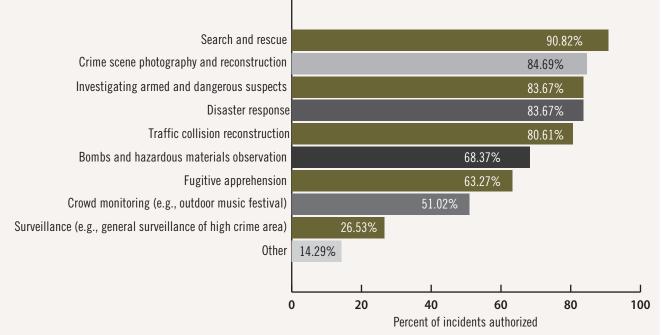
# 1. PRE-IMPLEMENTATION CONSIDERATIONS

## Common purposes for using drones in policing

Drones can be used for many purposes in policing. However, the authorized drone uses for each department may be limited by state and local statutes or ordinances or by internal policies that a police department adopts to reflect community values about privacy or other issues.

PERF's survey revealed the most common purposes of drones in responding agencies, as shown in figure 1.

#### Figure 1. Incidents authorized for drone use



Other uses of drones in policing include the following:

- Supporting officers serving warrants, which often is a high-risk activity for officers
- Hostage negotiations
- Assisting other government agencies
- · Obtaining video footage for recruitment or other materials
- K-9 backup
- Inspections of police radio towers

# Laws and regulations: Federal, state, and local

Prior to implementing a drone program, it is essential that local law enforcement agencies understand the federal, state, and local regulations that govern their use of drones. The Federal Aviation Administration (FAA) establishes and enforces most regulations regarding drone use in the United States. Law enforcement agencies also must abide by any state and local legislation governing drones. Therefore, it is important to research all federal, state, and local regulations within your agency's jurisdiction to ensure that your program will function lawfully and without legal challenges. Agencies should work with their legal advisors to ensure that drone team members understand the laws and regulations they must follow.

# FEDERAL REGULATIONS: PART 107 LICENSE AND PART 91 CERTIFICATE OF AUTHORIZATION

The FAA is responsible for establishing, monitoring, and enforcing the federal regulations associated with drone use. Agencies interested in developing their own drone program have two regulatory options for operation:

- 1. Have individual operators obtain a part 107 license.<sup>5</sup>
- 2. Have the agency obtain a part 91 certificate of authorization (COA) so they can self-certify their operators.<sup>6</sup>

There are advantages and disadvantages to each option, which is why many agencies choose to pursue both.<sup>7</sup>

A part 107 license "allows operations of drones or unmanned aircraft system (UAS) under 55 pounds at or below 400 feet above ground level . . . for visual line-of-sight operations only."<sup>8</sup> Part 107 has a number of other restrictions, including not being allowed to fly a drone at night. Some flight restrictions associated with a part 107 license can be overcome by applying for waivers. However, this can be a slow process, with no guarantee that a waiver will be approved.

In order to become part 107 certified, each drone pilot for the agency needs to pass the FAA's Aeronautical Knowledge Test to obtain a Remote Pilot Certificate.

The major benefit of the part 107 license is that it is less burdensome than the part 91 COA and allows the agency to quickly begin testing drones and working to establish a program.

<sup>5.</sup> Operation and Certification of Small Unmanned Aircraft Systems, 14 C.F.R. § 107 (2017), <u>https://www.govinfo.gov/content/pkg/CFR-2017-title14-vol2/</u> <u>xml/CFR-2017-title14-vol2-part107.xml</u>; "Fact Sheet – Small Unmanned Aircraft Regulations (Part 107)," press release, Federal Aviation Administration, July 23, 2018, <u>https://www.faa.gov/news/fact\_sheets/news\_story.cfm?newsld=22615</u>.

<sup>6. &</sup>quot;Certificates of Waiver or Authorization (COA)," Federal Aviation Administration, last modified April 25, 2019, <u>https://www.faa.gov/about/office\_org/headquarters\_offices/ato/service\_units/systemops/aaim/organizations/uas/coa/</u>.

<sup>7. &</sup>quot;Unmanned Aircraft Systems: Frequently Asked Questions," Federal Aviation Administration, last modified December 9, 2019, <u>https://www.faa.gov/uas/</u> resources/faqs/.

<sup>8. &</sup>quot;Unmanned Aircraft Systems: Operate a Drone, Start a Drone Program," Federal Aviation Administration, last modified February 14, 2019, https://www.faa.gov/uas/public\_safety\_gov/drone\_program/.

By contrast, operating under a part 91 COA allows an agency to "self-certify UAS and operators for flights performing governmental functions."<sup>9</sup> This means that it is up to the police agency to set standards for determining whether someone is ready to be a pilot, because they do not need to take the FAA's Aeronautical Knowledge Test. The downside of applying for a COA is that it sometimes takes months for the FAA to process the request. Many agencies have their drone operators obtain a part 107 license while waiting for their COA to be granted.

Ultimately, it benefits the agency to have a COA because it allows more flexibility in operations, especially when near an airport or controlled airspace.

#### The Benefits of a COA for the New York City Fire Department

The New York City Fire Department (FDNY) uses tethered drones\* and sees the advantages of using a COA for its operations. "There are advantages of using a COA for a place like New York City, where about 65 percent of the airspace is highly restricted," said Tim Herlocker, former Director of the FDNY Emergency Operations Center. "The COA gives us the ability in advance to work out the rules in which we will fly in that airspace. It also gives me the ability to decide the skillset that my pilots need, as opposed to being a [part] 107[–licensed] pilot and just needing to pass the FAA exam. I can set my own standards as to how we train them."

A COA provides authorization for activities that are prohibited by part 107, such as flying at night, flying beyond the visual line of sight, flying over people, flying at altitudes above 400 feet above ground level, and flying in controlled airspace.

Under a part 107 license, the drone is considered a civil aircraft for commercial operations, whereas under a COA, the drone is considered a public aircraft that is only used for governmental purposes. Michael O'Shea, UAS Integration Office Program Manager for the FAA, explained the fundamental difference between the two:

"A COA is a public aircraft operation, so everything you do has to be entirely government. For example, supporting your SWAT [special weapons and tactics] team and taking crime scene photos are considered governmental. However, doing a demonstration for an elementary school would not be considered governmental, so that could not be done under a COA and would have to be done under a 107."

<sup>\*</sup> A tethered drone is a drone that is connected through a flexible wire or cable to a person, ground, or object while it is airborne. The tether often includes the power supply, eliminating the need for a battery, which might otherwise need to be replaced on longer missions.

<sup>9. &</sup>quot;Unmanned Aircraft Systems: Operate a Drone, Start a Drone Program" (see note 7).

To assist agencies with deciding which options to pursue, the FAA has a "User Identification Tool"<sup>10</sup> on its website. The tool allows law enforcement agencies to answer a few simple questions about their intended drone uses and obtain guidance about which regulatory option or options may work best for their agency.

O'Shea of the FAA is a proponent of agencies obtaining both a part 107 license and a COA. "We get questions all the time, should we be a part 107 operator, or should we get a COA and operate that way?" he said. "Right now, we generally suggest that agencies do both. They give you different advantages."

#### Part 107 license

#### Pros

- · Shorter process to receive license and start drone operations
- Requirement to pass the FAA Aeronautical Knowledge Test ensures that all drone pilots will have the same base level of education on drone operations
- Can be used for law enforcement activities as well as non–law enforcement activities, such as demonstrating to the public how drones operate

#### Cons

- Has many restrictions on drone operations; bars flying at night, flying over people, flying beyond the visual line of sight, flying in controlled airspace, and flying at altitudes above 400 feet
- · Must apply for waivers each time pilot wants to use drone for a restricted use

#### Part 91 COA

Pros

- · More flexibility in operations, especially near an airport or controlled airspace
- · Police agencies can self-certify their own drone pilots and tailor drone training to their own standards

#### Cons

- Applying for the COA can be a lengthy process
- Under a COA, drones can only be used for governmental purposes

# STATE AND LOCAL REGULATIONS

In addition to the FAA regulations, numerous state and local governments have enacted laws governing law enforcement agencies' use of drones.

<sup>10. &</sup>quot;Unmanned Aircraft Systems: User Identification Tool," Federal Aviation Administration, last modified February 15, 2019, <a href="https://www.faa.gov/uas/getting\_started/user\_identification\_tool/">https://www.faa.gov/uas/getting\_started/user\_identification\_tool/</a>.

#### **PERF survey results**

PERF's survey revealed that approximately 37 percent of respondents' state, county, or municipal governments had enacted legislation governing police use of drones.

A number of participants at the PERF conference discussed the restrictions they must comply with under state legislation. Florida, for example, enacted the Freedom from Unwanted Surveillance Act in 2015, which prohibits law enforcement agencies' use of drones with three broad exceptions:

- 1. To counter a high risk of a terrorist attack by a specific individual or organization if the U.S. Secretary of Homeland Security determines that credible intelligence indicates that there is such a risk.
- 2. If the law enforcement agency first obtains a search warrant signed by a judge authorizing the use of a drone.
- 3. If the law enforcement agency possesses reasonable suspicion that, under particular circumstances, swift action is needed to prevent imminent danger to life or serious damage to property, to forestall the imminent escape of a suspect or the destruction of evidence, or to achieve purposes including, but not limited to, facilitating the search for a missing person.<sup>11</sup>

"The law has absolutely dictated how we deploy our drones," said Sergeant Thomas Tompkins of the Polk County (Florida) Sheriff's Office. "We use our drones for priority one calls, such as burglaries, or robberies that are in progress, because they fit into the third exception to the ban. However, we would like to use our drones to monitor the large crowds of people that gather to observe spring training for our baseball team, but that doesn't fit under any of the exceptions."

Captain Ken Voiret of the Palm Beach County (Florida) Sheriff's Office (PBCSO) said his agency has been able to deploy drones on numerous occasions. "We have successfully written between 30 to 40 warrants that allow us to use drones during crime scenes, traffic reconstruction, and surveillance," Voiret said. "To streamline the process of writing warrants and getting them approved by a judge, the PBCSO, in conjunction with the Palm Beach State Attorney's Office, has created templates to make the process slightly less time-consuming."<sup>12</sup>

Agencies in Virginia operate under limits established by state legislation. Virginia House Bill No. 2125, which passed in 2015, requires law enforcement agencies to obtain a warrant before using a drone for any purpose, except in certain defined circumstances. Exceptions include Amber Alerts, Silver (or

<sup>11.</sup> Freedom from Unwanted Surveillance Act, Fla. Stat. § 934.50(4) (2015), <u>http://www.leg.state.fl.us/statutes/index.cfm?App\_mode=Display\_</u> <u>Statute&Search\_String=&URL=0900-0999/0934/Sections/0934.50.html</u>.

<sup>12.</sup> See appendix C for the PBCSO template.

senior) Alerts, and Blue Alerts,<sup>13</sup> incidents in which "use of an unmanned aircraft system is determined to be necessary to alleviate an immediate danger to any person," and non–law enforcement purposes such as "damage assessment, traffic assessment, flood stage assessment, and wildfire assessment."<sup>14</sup>

It is important to know and understand any limitations on drone use imposed by state or local laws before initiating any plans for a drone program. PERF is aware of one department that purchased several drones only to discover that their use was tightly restricted by state law. The agency gave some of the drones to a state emergency management agency that could use them and retained two for use in traffic accident reconstruction.

## RECOMMENDATIONS FOR LAW, POLICY, AND REGULATIONS

- Research all federal, state, and local laws and regulations that may limit your agency's use of drones before starting your program. Work with your agency's legal advisors to ensure that members of your drone team understand the laws and regulations they must follow.
- Consider obtaining both a part 91 COA and a part 107 license to conduct your program's drone operations for maximum use and flexibility.
- In states with legislation, reach out to other agencies to learn how the regulations operate and how they are using drones.
- Prepare templates for warrants and waivers to streamline the process of applying for exceptions.
- In states without specific legislation, advocate with state legislatures to influence future legislative content so that future laws offer you the most flexibility to employ drones to accomplish your mission and promote public safety, while balancing privacy rights and concerns that the public raises.

## **Community outreach**

Fostering strong relationships of trust with the community is an essential part of policing. These relationships are built on transparency and cooperation between the police and the communities they serve. Therefore, it is important when implementing the use of a new technology, such as drones, that police agencies have a comprehensive community outreach strategy.

<sup>13.</sup> Blue Alerts are a system for apprehending suspects in cases involving the death or serious injury of a law enforcement officer.

<sup>14.</sup> Code of Va. 19.2–60.1 (2015), https://law.lis.virginia.gov/vacode/title19.2/chapter5/section19.2-60.1/.

The strategy should include genuine efforts to solicit community members' views; explain the police department's planned approach and reasons for the use of drones; provide detailed assurances about privacy, accountability, and other issues of concern; and ensure that questions and concerns are adequately addressed.

"Getting public support is one of the most important factors to a successful drone program," said Sgt. Tompkins of the Polk County Sheriff's Office, one of the earliest agencies to adopt a drone program.

Comments by participants at PERF's conference and survey respondent data indicate that community members are more accepting of police use of drones if the agency is transparent about policies and intended uses from the very beginning of any implementation efforts.

"We knew we had to get community support if we were to develop a drone program. We knew we had to be 100 percent transparent to the community, including civil rights leaders, from the start. We went into community meetings, we brought people into our CompStat meetings so they could see how drones could be useful, and we did a news conference where we talked about how and why we wanted to develop a drone program."

---- Sergeant Tim Ehrenkaufer, Daytona Beach (Florida) Police Department

Captain Vern Sallee of the Chula Vista (California) Police Department found that slowly developing plans for a drone program was helpful to fostering the public's trust. "We did not go out and purchase our drone right away. Instead we reached out to members of the public and stakeholder groups to consider their perspectives and to share our vision for the program. We held town halls and invited the media to see what we were doing. We also met with the ACLU [American Civil Liberties Union] and read their publication about drones. All this happened before we ever bought our first drone or started any operations," Sallee said.

Staff Sergeant Don Chapman said this approach also worked for the Vancouver (British Columbia) Police Department, which recently purchased their drones after almost two years of preimplementation efforts:

"We did not want to immediately purchase our drones at the risk of having our program shut down because it did not have community support or did not run smoothly. We took the time to look at all the existing drone programs in the major Canadian cities to see what they had in place, what mistakes they had made, and how they addressed community concerns. We put in our due diligence before developing our own program."

### EXPLAINING THE BENEFITS OF A DRONE PROGRAM

It is helpful to make sure that your community understands the life-saving capabilities and other benefits of a drone program. The Hampton (Virginia) Police Department, for example, noted that its drone program would help the city's disaster preparedness efforts. When there is flooding, drones can fly to areas that cannot be reached by cars or trucks. "The community was accepting, because Hampton is in a low-lying area and has a serious hurricane risk," said Chief of Police Terry Sult.

Major Christian Quinn of the Fairfax County (Virginia) Police Department (FCPD) said that at some of the public outreach meetings the department arranged, some community members had concerns about his agency's plans to use drones. "However, when they had the opportunity to see the type of equipment we were considering using and learned that we intended to use the drones for situations such as helping to find an elderly person with dementia who had wandered off, that changed a lot of people's minds," he said.

Officials from many agencies at the PERF conference noted that community members' concerns about privacy and other issues can be addressed if police are clear about how they wish to define the authorized and nonauthorized uses of drones. For example, Fairfax County posted an information page online about its planned drone program, which listed nine types of missions that would be authorized—such as search and rescue, damage assessments from disasters, crash reconstruction, and hazardous materials responses. Equally important, the information page listed four types of missions that the drone program would not permit, including random surveillance or intimidation of any individual or group.<sup>15</sup>

<sup>15. &</sup>quot;Provide Your Feedback on Public Safety Drones in Fairfax County," Fairfax County, Virginia, last modified January 7, 2019, <a href="https://www.fairfaxcounty.gov/news2/drones-in-fairfax-county/">https://www.fairfaxcounty.gov/</a> news2/drones-in-fairfax-county/.

#### Examples of drone use for search and rescue

- In April 2019, the Collier County (Florida) Sheriff's Office deployed six drones to aid in the search for a 77-year-old man who had been missing for more than two hours after wandering from his residence. The search area was divided into six grids, with one drone assigned to each section. Within 30 minutes, police found the man and returned him to safety.\*
- In August 2019, the Fremont (California) Police Department used a drone to find a Deaf 17-year-old boy who had run away from school. The search took place at night, and police successfully used the drone's infrared camera to spot the boy in a field and safely recover him.<sup>†</sup>

\* Collier County Sheriff's Office, "Drone-Led Rescue a First for CCSO," press release, April 17, 2019, <u>https://www.colliersheriff.org/Home/Components/News/</u> <u>News/40660/1929</u>.

+ "Specialized Fremont Police Drone Helps Find Missing Deaf Teen," CBS SF Bay Area, February 21, 2019, <u>https://sanfrancisco.cbslocal.com/2019/02/21/</u> fremont-police-drone-helps-find-missing-deaf-teen/.

## METHODS OF OUTREACH

Successful community outreach initiatives create an open dialogue for community members to ask questions and raise issues while allowing the agency to address concerns in a constructive manner.

Many agencies recommend a combination of outreach initiatives. Captain John Orr of the Virginia Beach (Virginia) Police Department (VBPD) described his department's approach:

"We prepared a presentation for the city council, which was open to the public, where we outlined our intentions, spoke of our mission capabilities, outlined some budget challenges, and outlined our community engagement plans. Despite some questions regarding security issues, the city council unanimously supported our proposed program.

"Then we conducted focus groups with community members, and we posted information on our website and used social media prior to implementation. These community outreach methods worked well for us, because we won community support and support from our elected officials."

#### Public forums, community presentations, and demonstrations of drones

Many police leaders at the PERF conference said they conducted public forums to discuss their plans for drone programs. To accommodate the schedules of as many community members as possible, agencies recommend holding public forums on different days and times. "We held two public forums at headquarters, during different days of the week and different times, to make sure it was accessible to a wider audience," said Sergeant Max Nowinsky of the Savannah (Georgia) Police Department. The FCPD, which conducted pre-implementation efforts for its drone program for several months, credited public forums as its most successful outreach method. Six public meetings helped to clarify the goals of the drone program, address privacy concerns of community members, and define how the drones will be used.

"The crowds were engaged at each session," said Major Christian Quinn of Fairfax County. "They asked a lot of questions and provided some recommendations. Many of the questions revolved around our intended uses, budget implications, and some privacy concerns. The comments we received were generally supportive. This process adds time and is labor-intensive, but there is great value in having public input. We use this time to build community support and address concerns."

Along with public forums, many agencies said that making presentations at community meetings is an effective way to engage with the public. "We spoke about our intended use of drones at a Tomorrow's Neighborhood Today (TNT)<sup>16</sup> meeting, which is a community group," said First Deputy Chief Joe Cecile of the Syracuse (New York) Police Department.

Some agencies, including the Polk County Sheriff's Office, have conducted demonstrations of drones in the community. "We did drone demonstrations in our elementary schools, middle schools, and high schools," said Sgt. Tompkins of Polk County. "We also did demonstrations at community meetings. Our goal is to be transparent with the community by letting them see the drones and ask questions."

#### Involving community stakeholders

Working directly with stakeholder groups before implementing a drone program is another promising practice that agencies recommended. Building strong relationships with stakeholders through solicitation of feedback and guidance helped agencies gain community-wide support for their drone programs.

The Prince William County (Virginia) Police Department, for example, shared a draft version of its drone policy with 40 different community stakeholder groups such as the ACLU, local attorneys, and church groups and asked for feedback before writing a final version. "We encouraged them to respond with any questions or concerns about our policy," said Lieutenant Gregory Pass of Prince William County.

The FCPD has involved community stakeholders throughout its entire pre-implementation process through the creation of a Drones Task Force. The task force is made up of representatives from a variety of groups such as community associations, the FAA, the National Association for the

<sup>16. &</sup>quot;Who We Are," Tomorrow's Neighborhoods Today, accessed February 10, 2020, http://www.tomorrowsneighborhoodstoday.org/.

Advancement of Colored People (NAACP), the ACLU, local business owners, and many others.<sup>17</sup> The Audubon Society also was interested and was included on the task force, because drones can be useful for terrain mapping and wildlife management. During the first task force meeting, the FCPD introduced the program to the group, described potential uses of drones, and answered questions. The task force also held a meeting to discuss legal and privacy concerns. "I would describe the conversations as productive, and definitely not adversarial," Major Quinn said.

The FCPD found that involving stakeholders during this process has been a valuable investment when issues arose. For example, airspace issues are complex in Fairfax County because of its proximity to Washington, D.C., and numerous airports. "Some of the stakeholders on our task force are knowledgeable about these airspace restrictions and provided informed guidance on the subject," Major Quinn said.

Many agencies have found it helpful to contact stakeholder organizations that may have privacy concerns about drones to ask for their input up front, before decisions are made and a drone program is implemented. "You are showing respect to their viewpoint. If you never reach out, you never open that communication," said Captain Sallee of the Chula Vista (California) Police Department.

Vancouver Police Sgt. Don Chapman described his agency's process:

"We went to the British Columbia Civil Liberties Association (BCCLA) and advised them that we were in the process of examining a Remotely Piloted Aircraft System (RPAS) program. It was important that we painted a clear picture of the intent of the program, what the drones were going to be used for, how they were going to be deployed, and of equal importance what we were not going to be using them for.

"We invited BCCLA to participate in the process and make policy recommendations for us to consider. We also worked with the Office of the Information and Privacy Commissioner (OIPC) for British Columbia and provided them with a 13-page Privacy Impact Assessment (PIA). The document outlined the purpose and scope of our RPAS program, defined the intended uses of the RPAS, outlined photographic and video use/retention, and provided technical information pertaining to data warehousing and security.

<sup>17.</sup> The task force is composed of more than 40 community stakeholders.

"Based on the information provided, the OIPC stated that they were satisfied that our program would be compliant with the Freedom of Information and Protection of Privacy Act. This helped mitigate their privacy concerns and allow a smooth implementation of the program."

### **Example stakeholder organizations to consult**

- The ACLU and other civil liberties and privacy interest groups
- All public safety departments
- Church groups
- · Citizens advisory boards
- FAA
- Hospitals
- Local attorneys
- Local business owners and the local Chamber of Commerce
- Local parks authority
- NAACP and other civil rights organizations
- Neighborhood Watch groups
- Other local community groups
- Schools

### Working with the news media and using social media

Many police agencies worked with newspapers and broadcast news media to share information about drone programs. And participants at PERF's conference also recommended using the police department's social media accounts to explain the benefits of a drone program.

The Michigan State Police (MSP), for example, invited news organizations to a media day about drones. "Once we received our Certificate of Authorization in 2015, we hosted a media day to show the community our drones," said MSP Lieutenant Colonel Chris Kelenske. "We had more than 30 news media cameras present." The MSP has continued this openness with the media. "Any time a news agency contacts us, we are willing to discuss our program, show them our drones, and demonstrate them," Kelenske said.

The Leesburg (Virginia) Police Department and the Surprise (Arizona) Police Department both tasked their Public Information Officers (PIO) with getting word out to the community about the creation of a drone program. "Our PIO invited the media and community to see a demonstration of the drone that we purchased, which resulted in a local news story about our UAS program. As a result of our proactive outreach, we received positive feedback and support from the community," said Leesburg Deputy Chief of Police Vanessa Grigsby.

Commander Randy Rody of Surprise said that social media can help police departments win support for a program. "In addition to a community survey, our PIO [used] social media to solicit feedback on our UAS program and offered three methods for communication: in writing, over the phone, or in person at a public forum. Attendance at the public forum was nominal and overwhelmingly supportive."

# ADDRESSING PRIVACY CONCERNS

Police agencies told PERF that privacy concerns are the biggest source of apprehension about drones expressed by community members. However, clearly stating that drones will not be used as a general surveillance tool alleviates many concerns. Education and transparency are key to achieving community trust and support for a drone program.

Major Quinn of the FCPD said, "Departments shouldn't underestimate the extent to which community members may internalize issues, especially when it comes to technology and privacy concerns. I've listened to people at public meetings discussing nude sunbathing in their back yards. This highlights the extent to which people personalize issues and can dwell on worst-case scenarios that could personally affect them, however unlikely. We have to acknowledge these concerns and sometimes make concessions. With our drone program, we found common ground and points to move forward on, such as minimizing the amount of data we would record or retain."

To ease privacy concerns, the Daytona Beach Police Department implemented a policy to not record video footage from drones unless they are specifically authorized to do so by the unit supervisor. Sergeant Timothy Ehrenkaufer said this issue often came up in meetings with community members. "People would ask, 'Are you going to fly over my yard when you are looking for someone, record the video, and then come back and arrest me later for having pot in my backyard?" he said. "We addressed those concerns by telling them no, that we are not going to record the video. We will livestream it to the pilot and command staff, and then move on. We're not going to use it later to come back and prosecute them."

# RECOMMENDATIONS FOR COMMUNITY OUTREACH

- Engage with the community before implementing a drone program to increase understanding and support for the program.
  - Proactively reach out to community organizations that are likely to have reservations about drone use, such as civil liberties groups, prior to program implementation. Make legitimate efforts to understand community members' concerns and modify your plans when appropriate.
  - Actively solicit feedback from community members and organizations before finalizing the drone policy to ensure that community concerns are addressed.
  - Host outreach events on various days and times and at various locations, to ensure that most community members are able to participate.
- Provide specific information to the public about the purposes for which drones will be used and purposes for which they will not be used. This can help to prevent unnecessary conflicts and ease community members' concerns about privacy and other issues.
  - Stress that the use of drones is to promote public safety and not for nonspecific, random surveillance purposes.
  - Work with print and broadcast news media organizations to disseminate your messages, and use your social media accounts to inform and engage the public about your plans.
  - Involve your agency's PIO to ensure that your messages are disseminated widely.
- Be clear and transparent about your agency's drone policies and practices prior to and after implementation of your program.
  - For example, post drafts and the final version of your drone policy on the department's website. After drone deployments have begun, release video of successful drone operations, when footage can be made public.

# **Selecting drone equipment**

### Using drones in serving arrest warrants

In June 2019, the Lodi (California) Police Department successfully used their drone to capture a suspect who fled when police attempted to serve him with an arrest warrant. The drone helped to locate the suspect and guide officers to his location, where they made the arrest.\*

<sup>\*</sup> Rob Malcolm, "Lodi Police Utilizing Their Eye In The Sky To Fight Crime," CBS Sacramento, June 4, 2019, https://sacramento.cbslocal.com/2019/06/04/ lodi-police-drone-fight-crime/.

The process of selecting drones and related equipment can be overwhelming for an agency. There are many options on the market today, in an array of sizes and capabilities. Models vary from palm-sized quadcopters to large six-rotor machines capable of lifting and delivering a heavy box. Prices range from approximately \$800 for a basic model to \$85,000 for a robust model with a high-definition infrared camera.

There are also a number of tools that can be added to the aircraft such as bright spotlights, thermal imaging, scene mapping, and automatic sharing on media platforms. The abundance of options can make finding the right equipment a challenge.

Participants at the PERF conference shared lessons they have learned to make the process easier for agencies developing a drone program. In order to select and purchase the best drones for your agency, it is important to keep in mind the following key considerations:

- 1. Operational parameters: What will the drones be used for?
- 2. Operational specifications: What technology or equipment is needed to achieve mission goals?

Investigator Karen Box of the Robertson County (Texas) Sheriff's Office urged agencies to proceed slowly and carefully to avoid costly mistakes. "Do your research, take the classes, get some training before jumping in. Otherwise you may purchase something that you don't need or can't use," she said. That advice was echoed by many of the experienced practitioners at the conference.

Tim Herlocker, former Director of FDNY's Emergency Operations Center, offered important advice to those just starting a drone program. "You should always go in with the expectation that you're going to crash your drone," he said. He pointed out that in an urban setting, dense building infrastructure and signal interruption cause drones to fall from the sky. Knowing the limitations of your drone is essential, Herlocker said, and it is advisable to start with small, inexpensive models and purchase larger models later, after officer training has been completed and operators are more skilled and experienced.

"We started out cheap, and we'll go to the larger, more expensive models once we determine the value of the devices and the operational parameters," Hampton Chief of Police Terry Sult said. His agency uses inexpensive, off-the-shelf drones to allow the drone pilots to become familiar with flying the aircraft.

# BEGIN WITH A SMALL PROGRAM AS A TEST

An evaluation period allows an agency to decide if pursing a drone program is worth the time, effort, and money that must go into it. "We did a process of incremental steps to bring the program to full delivery," said VBPD Deputy Chief Tony Zucaro.

The VBPD evaluated its program by examining the following factors:

- The cost of equipment
- Training
- Service delivery and capability
- The reduced cost of operating a drone rather than a helicopter
- Mission capabilities and operations
- Return on investment

At the completion of this evaluation, the VBPD decided to move forward with its drone program.

### **PERF survey results**

PERF's survey revealed that approximately 31 percent of respondents first deployed their drones on a trial basis.

# MISSION GOALS AND LEGISLATIVE RESTRICTIONS

Budgeting for a drone program and selection of equipment must begin with defining the circumstances in which drones will be used by your agency and the technical requirements to support your desired functions. For example, if you plan to conduct low-light or late-night searches for suspects or missing persons, you will want a thermal sensor mounted with your camera that can send a live feed to the pilot.

As another example, if your city or region consists largely of restricted airspace or is subject to laws that strictly limit drone use to crash investigation and scene mapping, your agency will likely only need simple drones with limited range and a basic camera array.

Some fire departments and police departments use tethered drones for certain missions, such as tactical situations that typically last several hours, because tethered drones can stay in the air indefinitely. The tether provides the drone's power supply and also helps to keep it in range and under control. A nontethered drone, on the other hand, might require multiple battery changes to keep it aloft for the duration of hours-long incidents.

When looking at which types of aircraft are best suited to your missions, agencies should review the operational specifications of various models and find the best fit for their individual purposes. The following performance measures should be factored into your decision-making process:

- **Durability.** Plan on having crashes and needing to replace rotor blades and belts. As a program is implemented, there will likely be mishaps as pilots get used to navigating and manipulating drones in different environments. Having a sturdy drone that can withstand some common errors and has replaceable parts can help keep a drone program sustainable.
- **Battery life.** Speed, weight of components, and altitude all affect battery life. Many drones with an infrared camera or thermal sensor that sends a live feed back to the pilot can fly for only 20 to 30 minutes depending upon conditions of use.

### The importance of battery life

It is essential to consider battery life in the context of the anticipated uses of a drone.

For example, Sergeant Timothy Ehrenkaufer of the Daytona Beach Police Department used a drone to respond to a call about a fleeing burglary suspect. The suspect was jumping from rooftop to rooftop, and Ehrenkaufer was able to track the suspect and guide a patrol unit on the ground. But because the pursuit continued for more than an hour, Ehrenkaufer had to land the drone, install fresh batteries, and relaunch it more than once.

In a scenario like this one that requires a long flight time, it is worthwhile to have multiple drones on hand to avoid the risk of losing sight of the subject while a battery is changed.

- **Distance.** How far can a drone travel from the operator while maintaining a reliable signal from the controller? And what are your protocols and requirements regarding keeping the drone within sight of the operator?
- **Payload.** What do you intend to attach to the drone as part of its operational package? The heavier the components, the larger and stronger the drone must be. For example, search and rescue organizations use six-rotor drones that can deploy items such as blankets and life vests to those in need.

An agency may need to purchase different drone models for different missions. Testing and experimenting with less expensive models first will help you make the best investment in your aircraft.

# RECOMMENDATIONS FOR SELECTING EQUIPMENT

- Establish the operational parameters and specifications of your drone program to inform your purchase of drone equipment.
- Start small and test your equipment prior to program implementation.
- Implement your drone program on a trial basis with a set time for a formal evaluation process. Plan to have flexibility to make changes to the scope of services and equipment needed for your program before final implementation.
- Take incremental steps as you develop your program and continue to solicit community feedback and modify the program as necessary (see "Community Outreach" section for guidelines).
- Funding limitations will impact agencies' decision-making, except in very small programs with limited purposes for drones. Many drones and their associated technologies are expensive, and personnel hours and information technology (IT) support can also be costly. See "Funding Considerations" for discussion of how some agencies have obtained assistance with the costs of their drone programs.

# **Funding considerations**

Drones can offer many benefits to law enforcement agencies, but the costs can also be significant. In addition to the initial cost of purchasing one or more drones, agencies must also allocate funding and staffing resources for training, program administration, and drone data management and storage needs.

# COST OF IMPLEMENTATION

The price of drones currently (in early 2020) ranges from several hundred dollars for a basic model to more than \$85,000 for a robust model with advanced technology. For some agencies, those costs make it a challenge to implement a drone program.

### **PERF survey results**

The PERF survey revealed that 39 percent of respondents that did not have drones cited cost as a primary reason.

The Wilmington (Delaware) Police Department established its program in 2014 and has invested approximately \$200,000 in drones and related equipment since its inception.

Implementing a drone program comes with steep initial costs as well as long-term costs, which an agency needs to consider when deciding on the front end if a drone program is sustainable.

"Procurement of new equipment and spare parts needs to be factored into the cost as the program grows and capabilities are expanded," said Deputy Chief Tony Zucaro of the VBPD.

### Costs of a drone program in Scottsdale, Arizona

#### **Program background**

The Scottsdale (Arizona) Police Department's (SPD) UAS program, developed in 2015, has a drone team of five pilots and a program manager. The drone team, located in the Tactical Operations Section, primarily works a Monday– Friday schedule with a pilot on call at all times for emergency response. The SPD's program includes three aircraft: one DJI Inspire 1 equipped with a forward-looking infrared (FLIR) thermal imaging camera and two DJI Mavic Pros. This three-aircraft fleet provides both day and night capabilities as well as a limited indoor flight capability. The SPD operates its drones under a part 107 license and has received waivers for nighttime and non–line of sight operations. The department also has acquired authorizations to operate within all local airspace.

#### **Equipment and maintenance costs**

Sgt. Austen George of the SPD provided details on the cost of his department's program and highlighted important considerations for agencies interested in implementing their own programs:

"First, agencies should be aware that all remote aircraft require a host of additional equipment in order to maintain operational capability. As an example, SPD's DJI Inspire 1 aircraft includes six additional batteries and chargers, two remote controllers, two high-definition ruggedized displays, a Pelican case, multiple types of cameras, and a supply of replacement rotors. These ancillary items increase the final cost of the aircraft significantly and need to be considered when budgeting for procurement.

"Second, in order to minimize downtime, increase coverage, and remain operational in the event of an aircraft failure, a minimum of two complete systems should be purchased. This means additional training costs as well, as pilots must be available to operate the drone.

"Third, maintenance is also a significant cost consideration, not only in costs associated with hardware replacement but also investment in maintaining the software upon which these devices rely heavily. Each aircraft should undergo a system check at a minimum of once a week. All firmware must be updated, batteries checked for wear, and the airframe and rotors must be inspected for damage. This procedure must also be completed prior to each deployment and should be itemized in a pre-flight checklist."

Table 1 provides a breakdown of initial costs associated with creating a basic UAS program with two aircraft and two pilots, based on the SPD's program costs.

### Table 1. Costs of standing up a drone program

Equipment and training	Cost
Equipment and training	COSI
Aircraft with HD camera	\$2,000-\$5,000
FLIR camera	\$10,000-\$15,000
Batteries	\$200 x 6 = \$1,200
Props	\$150
HD monitors	\$700 x 2 = \$1,400
Additional remote	\$700
Pelican case	\$500
VHF transceiver	\$400
FAA RPIC license exam fee	\$250
Ground school per student	\$500-\$2,000
Estimated total for two systems	\$35,000-\$55,000

The costs of maintaining a drone program will far exceed the initial implementation expenses. Equipment will age and require replacement, additional pilots will require training, and emerging technology will prompt the purchase of additional aircraft. Recurring funding should be put in place to sustain the program and allow for improvements, with the understanding that some technology will require special funding well beyond this. A rule of thumb suggested by participants would be to budget 20 percent of the initial expense annually to maintain the existing equipment and personnel.

The costs of pilots' time must also be added to the costs of a drone program.

### COSTS AND BENEFITS OF USING DRONES

Many agencies have found their use of drones to be cost-effective in the long run. Jesse Panuccio, Principal Deputy Associate Attorney General in the DOJ, said, "It comes as no surprise that law enforcement and public safety agencies are now using drones in a number of ways. Drones are far less expensive to operate than helicopters or airplanes, and they can fly in areas that traditional aircraft cannot reach."

"We strongly support the limited and effective use of drones to improve visibility, situational awareness, and deputy safety for priority one calls. During our first year and a half of operating, we've flown more than 750 missions, resulting in 31 suspects being arrested and five missing or endangered people being found. We are saving tens of thousands of dollars deploying drones as opposed to our piloted agency helicopters. In many situations, our drones are more versatile and effective than a helicopter."

With an initial investment of less than \$10,000, the VBPD purchased two drones to add to its Aviation Unit, which already consisted of two patrol helicopters. To meet their program needs, officials spent an additional \$800 for an upgraded drone camera. Then they conducted a trial and evaluation study, including a cost-benefit analysis of implementing a full drone program.

"During the evaluation of our trial period, we looked at the cost of equipment, the cost of operating drones versus helicopters, and the return on investment. We found that the hourly operating costs of drones were significantly less than operating a traditional helicopter aircraft and would bring us a considerable return on our investment," said Deputy Chief Tony Zucaro.

Sergeant David Maitlen of the Torrance (California) Police Department offered an example of how a drone can help protect officer safety while avoiding situations that might result in a lawsuit against a police department:

"Our department received a call about a stolen car. The car stopped and the driver got out, but a passenger was still in the car and was nonresponsive to our commands to exit. We considered using a dog to drag the passenger out, but decided to use a drone instead. With the drone near the passenger-side window, we could see that the passenger was passed out, possibly from drugs. The drone also showed us which car doors were locked and which were unlocked. So the drone gave the officers a live view of what they would encounter, so they would know if there were risks to approaching the car.

"We explain to city officials that in situations like this, drones can protect officer safety and reduce legal liability. If we had used a dog to drag the passenger out of the car, there might have been injuries and a lawsuit. With a \$400 drone, we avoided all that."

Presenting these types of cost-benefit analyses can help police departments to win support and funding for their drone program.

# PARTNERING WITH OTHER GOVERNMENT AGENCIES

Before launching a drone program of their own, many police agencies may benefit by approaching other agencies in their own jurisdiction or police departments in nearby jurisdictions to discuss whether the costs of operating a program might be shared. The Metropolitan Police Department (MPD) in Washington, D.C., does not currently have a drone program but is considering future implementation. "The MPD participates in a citywide UAS working group that was established by the mayor to look at potential drone usage not only for law enforcement but also for the fire department and other government agencies like the Department of Consumer and Regulatory Affairs," said Assistant Chief Jeffery Carroll of the MPD.

### City of Virginia Beach drone program—a model for agency partnerships

The VBPD's drone program is a part of the larger drone program in the city government. The fire department, the Office of Emergency Management, and the Communications Office / Visitor and Convention Bureau also participate. The police department owns two drones and has six certified drone pilots, and there are six drones and 21 certified pilots in the other departments.

The police department was the first to acquire drones and is responsible for administrative oversight of the entire program. It was up to the police to work out the logistics of the program, including developing the policy and creating training protocols. Once the VBPD established its individual drone program and worked out the kinks, it helped the other city departments to create their programs. "Each of the city agencies had a number of individuals who had operated drones for their personal use, but they were not certified as drone pilots. We helped develop a program and built a 40-hour in-house training to help them get certification and establish their drone programs and protocols," said Deputy Chief Tony Zucaro.

Each city department provides different mission capabilities. "In Virginia Beach, we use drones as much for public utility use and emergency management as we do for law enforcement," said Captain John Orr. Table 2 shows some examples of drone operations in various city departments.

Police Department	Fire Department	Office of Emergency Management	Communications Office / Visitor and Convention Bureau
Accident reconstruction	Emergency scenes	Operations center's immediate situational awareness	Promotional videos
Tactical SWAT operations	Structure fires	Identifying tornado paths	Special events
Intelligence and evidence gathering	Hazardous material incidents	Special events management	Virtual tours
Traffic and crowd management	Damage assessments	Search and rescue (land and water)	Project documentation (construction)

#### Table 2. City of Virginia Beach examples of drone operations\*

\* This is not a comprehensive list of all authorized drone deployments. Some types of operations may be completed by multiple departments. For example, in addition to the Office of Emergency Management, the police and fire departments also use drones for search and rescue missions.

City department personnel work together to provide drone assistance to the residents and visitors in Virginia Beach. Any employee in the police department, as well as any city employee, can request a drone. All non-time sensitive requests are put in a queue and are managed by the individual city agencies.

# FUNDING SOURCES

Participants at PERF's conference discussed several strategies that their departments have used to fund drone programs.

 The DOJ's Office of Justice Programs (OJP) provides Justice Assistance Grant (JAG) funding to state and local jurisdictions. Matt Dummermuth, who heads OJP, said there is a general prohibition on using JAG funds for drones but added that "waivers are allowed if you can put together a request for why you need the drone and have documentation from the FAA showing you are allowed to use it."

- 2. The Norman (Oklahoma) Police Department was struggling to get its program moving because of concerns about high initial costs and long-term funding. "One option that we evaluated was to purchase the devices in partnership with a joint regional drug task force," said Norman Police Captain Brent Barbour. "Under that concept, the task force would purchase, own, and maintain the devices, while our agency would provide the manpower, training, and experience to operate them for both agencies' needs. Details and specifics would be managed through a Memorandum of Understanding (MOU) between the two agencies. We decided not to take that route, but it was an example of the possibilities we considered."
- 3. Managing the data storage costs associated with drone use can be an additional cost for an agency. Hampton Police Chief Terry Sult said that his department has been able to use video storage capabilities of its body-worn camera program to store drone video footage that becomes evidence in a criminal case. "We have been able to integrate drone videos that we capture as evidence into our regular evidence.com system," Sult said. "This has allowed us to absorb some of the hidden costs of data storage."

# SUMMARY OF RECOMMENDATIONS FOR FUNDING

- Establish your agency's drone program goals and operational parameters to determine how costly your drone program will be.
- Consider the initial equipment costs as well as the long-term training, maintenance, and upgrade costs that come with maintaining a drone program.
- Engage the community in supporting drone use to help secure funding for your program.
- Conduct a cost-benefit analysis to demonstrate cost savings associated with drones. Drones can be costly, but the costs of drones should be compared to the costs of other equipment, such as helicopters and fixed-wing aircraft, that are often used in the absence of drones. Drones also provide important benefits in protecting officer safety and public safety, and in reducing risks and the potential for lawsuits.
- Investigate options for grants or community partnerships to reduce program costs.

# 2. ESTABLISHING A DRONE PROGRAM

# Staffing your drone team

### Example of using a drone to resolve a "suicide by cop" incident

In February 2018, a woman armed with a handgun was behaving erratically in a parking lot in Stafford, Virginia.\* When Stafford County sheriff's deputies arrived, the woman attempted to commit "suicide by cop," waving her firearm and telling the deputies to shoot her. For the next four hours, deputies used a drone to closely monitor the woman's behavior from a safe distance. The video images were so clear that deputies could gauge the woman's changing mood over time, and they could see when her finger was on the trigger of her gun. They were able to resolve the incident without using lethal force against the woman.

Ensuring that your drone team is staffed with qualified people is crucial to any agency's drone operations. There are a variety of ways in which this staffing can be accomplished, depending on an agency's individual needs.

Most agencies employ a "tandem" team consisting of a pilot and a visual observer:

- **Pilot.** The pilot controls the drone and in most situations is required to keep it within his or her visual line of sight to avoid any collisions with people, buildings, trees, telephone poles and electrical lines, bridges, birds, other drones, or other obstacles.
- **Visual observer.** Because it can be difficult for the pilot to maintain eye contact with the drone while also looking at the hand-held control device to obtain information about the drone's altitude, remaining battery power, a live video feed from the drone's camera, etc., most police departments provide for a visual observer to assist the pilot. The visual observer is charged with constantly watching the drone and the area around the drone and alerting the pilot to potential hazards.

Many drone controllers have a built-in video screen or can be connected to a smartphone or tablet to provide a live feed from a video camera on the drone. But a drone camera's field of view is limited, so it cannot be relied upon to avoid all obstacles. Persons operating a drone with a part 107 license are generally prohibited from operating a drone beyond the operator's visual line of sight.

<sup>\*</sup>Clarence Williams, "She Pointed a Gun at Police and Asked to Die; They Used Drones to Intercede Instead," *The Washington Post*, February 11, 2018, https://www.washingtonpost.com/local/public-safety/she-pointed-a-gun-at-police-and-asked-to-be-shot-they-used-drones-to-intercedeinstead/2018/02/11/419587c2-0acc-11e8-8890-372e2047c935\_story.html.

Drone teams often have other members, including the following:

- **Team leader**, who is responsible for overseeing the operational status of the program, assigned equipment and staff, and policy and program development.
- **Camera/video/sensor operator**, who monitors the video feed and any other information being transmitted from the drone.
- **Safety and security officer**, who protects the other members of the drone team. Because drone operators and visual observers must maintain an intense focus on the drone, in a dangerous situation they may need someone to monitor the situation on the ground and protect the drone team against any potential threats.

#### **PERF survey results**

The PERF survey revealed that more than 90 percent of respondents had a pilot in command and a visual observer on their drone team.

The MSP drone team uses the tandem model because its COA requires that they use observers. They have trained observers around the state, so the drone pilot and observer can quickly connect and deploy the drone.

Under ideal circumstances, the Surprise Police Department will use a four-person team consisting of a pilot, a visual observer, a video/sensor operator, and a security officer. In instances where all four roles cannot be filled, minimum requirements call for a pilot and visual observer.

### FULL-TIME VERSUS PART-TIME DRONE OPERATIONS

A majority of agencies told PERF that they do not have a full-time drone unit or full-time drone pilots. Most agencies have officers in the field who are trained as drone pilots, who deploy drones when needed.

#### **PERF survey results**

The PERF survey revealed that only 7 percent of respondents had department personnel assigned full-time to a drone unit.

Many agencies have incorporated drone operations into existing units. The VBPD's drone operations, for example, are located within the department's Aviation Unit, which was established in 1974 for the department's helicopter operations. Because the Aviation Unit members already were FAA-certified commercial pilots and many had experience with drone operations, it was a smooth transition when the department created a drone program.

Agencies may find it beneficial to have drone pilots in a variety of units spread across the agency's jurisdiction. Most of the Irving (Texas) Police Department's 22 drone pilots are patrol officers. This staffing allows them to have a licensed drone pilot available in their North and South Districts when incidents calling for a drone arise. The department has four patrol officers with part 107 certifications on duty at all times. Two officers respond to a scene; one serves as the pilot and the other as the visual observer. "It's good to have our drone pilots in patrol, because they're usually the first on the scene," Irving Police Assistant Chief Samuel Hall said.

### SWORN VERSUS CIVILIAN DRONE OPERATORS

There is some debate about whether drone operators need to be sworn officers. Civilian employees often are less costly than officers, because they have not received the extensive training that all officers receive. But Captain Vern Sallee of the Chula Vista Police Department said that cost is not the only consideration. "Sworn officers are certainly a more expensive resource," he said, "but they also have greater expertise to interpret the video they're seeing, describe relevant elements to other officers, and decide what the drone should be doing to generate the most valuable information."

Civilian employees can have other supporting roles in drone operations. For example, the MSP uses civilian Geographic Information System employees to process drone data collected from the crime scenes and disasters.

# RECOMMENDATIONS FOR STAFFING

- Create the drone team roles based on your agency's individual needs and any state or local laws, policies, or regulations.
- Consider training drone pilots from different units to ensure expertise are available for response to any type of incident, e.g., accident reconstruction, SWAT, or missing persons.
- Determine how many pilots should be certified based upon the size of your jurisdiction as well as the incident types that the drone team will be responsible for responding to.
- Use both sworn and nonsworn personnel to minimize costs and maximize expertise.

### **Drone team training**

Having a strong training protocol in place is critical to the success of an agency's drone program. It is important that drone team members have a detailed understanding of the drones they will be operating and the airspace they will be operating in. Michael O'Shea, Program Manager in the FAA's Unmanned Aircraft Systems Integration Office, advises agencies to determine the purposes of their drone program before developing their training protocol. "The mission must drive the operations. The technology should not drive the operations. Police departments also need to decide how they are going to operate. Will they operate under a part 107, under a Certificate of Authorization, or both?" Many details of a training program will depend on the missions that drones will be used for and the authorizations of drone team members.

### Part 107 versus part 91 COA

#### Part 107 operating rules

- Drones must weigh less than 55 pounds, including payload, at takeoff.
- Drones must be kept within visual line of sight.
- Drones must be flown at or below 400 feet; during daylight or civil twilight with anti-collision lighting; and less than 100 miles per hour.

#### Part 91 COA

- Allows more flexible and advanced drone operations, especially when near an airport or in controlled airspace.
- The applicant's entire program is considered when applying for this authorization, including how the pilots will be certified, operating environments, and procedures for obtaining access into airspace with local air traffic facilities.
- This process of applying for a COA can be very lengthy—up to 60 days—especially in waiting for the FAA to approve a Public Declaration Letter, which certifies the agency as a governmental entity.

# DRONE TRAINING PROTOCOLS

There is no "one size fits all" approach to drone training program development.

The structure of an agency's training will often depend upon its size and which FAA regulatory option they are operating under. If police employees are using drones under a part 107 license, they must pass an FAA's examination and obtain a Remote Pilot Certificate. However, if a police department is operating under a part 91 COA, it can self-certify its pilots.

Although there is not one training protocol that works best for all agencies, it is important that the training give drone team members the necessary knowledge and skill to successfully operate the agency's drones.

The Polk County Sheriff's Office provides extensive training to officers before they take the part 107 test. "First, we do an 80-hour class that includes a basic ground school, an overview of policy and state statutes, and some practical flying," said Polk County Sgt. Tompkins. "After the 80-hour course, the pilots take the part 107 test. Once they have their part 107 license, it takes another one to two months of additional training before they are considered operational. We do four hours of training every other week, totaling 15 to 20 hours before a pilot is signed off as being operational."

Other agencies, such as the Torrance Police Department, structure their training differently. "People apply to get into the drone program, and we conduct interviews with them," said Torrance Sgt. Maitlen. "We select good candidates, who must then pass the part 107 test to move on. Those who pass are given two days of in-house training on the FAA rules and regulations. After that, they conduct practice flights with senior members of the drone team. It usually takes about six months to one year before they can deploy by themselves."

#### In-house versus external training

To train drone team members, some agencies provide their own in-house training, and other agencies use training from an external vendor, such as another law enforcement agency, the drone manufacturer, or a private vendor.

Lieutenant William Saunders of the Southeastern Pennsylvania Transportation Authority (SEPTA) Transit Police Department runs an in-house training program for drone pilots consisting of classroom time and flight time, which is similar to the training structure in many other agencies. "Pilot candidates attend my classes," Saunders said. "Those who demonstrate an aptitude for flying drones are encouraged to test for the FAA part 107 license. Once obtained, all pilots participate in on-the-job training, continuing pilot education, and UAS training."

For agencies with small drone programs, it may be easier to look to an outside training program for guidance. "Currently, I am the only person in my agency who is a drone pilot," said Investigator Karen Box of the Robertson County Sheriff's Office. "I took my training through the Texas A&M Engineering Extension Service's class, Introduction to sUAS—Public Safety,<sup>18</sup> which is a three-day course to prepare pilots to take the part 107 exam. The training taught me a lot about drones, including how to choose which drone to purchase. Without the course, I might have purchased a drone that would not have worked as well for my agency's purposes."

Numerous agencies, such as the Miami Beach (Florida) Police Department, use a combination of in-house and external training. "Our department takes pride in the certification process for our sUAS pilots," said Sergeant Anthony Loperfido of Miami Beach. "All of our officers are required to complete a 40-hour, in-house, FAA part 107 test preparation course. This course is taught by our senior sUAS pilots who have extensive knowledge of Public Safety sUAS operations. The 40-hour course includes an in-depth review of FAA regulations, department policy, the City of Miami Beach–approved FAA COA, and many public safety topics surrounding sUAS operations. Once they complete this portion of the training, each student must complete 40 hours of observed flight time alongside one of our already certified sUAS pilots.")

<sup>18. &</sup>quot;sUAS for Public Safety Personnel," Texas A&M Engineering Extension Service, accessed February 11, 2020, https://teex.org/class/sap151/.

"We try to encourage people to actually learn to be pilots, and then take the test. Then you pass the test because you are a pilot, not because you trained specifically for the test."

--- Michael O'Shea, Program Manager, FAA Unmanned Aircraft Systems Integration Office

### **Training topics**

There are core topics that should be included in every agency's drone training. Many agencies have sought advice from the Wilmington Police Department, which has a very reputable drone training program. Sergeant Adam Ringle, the department's Director of UAS Flight Operations, advised that all drone training programs for public safety should include the following:

- Methods of conducting safe flight operations under exigent circumstances
- Drones crew resource management and a risk assessment-based model to accept or decline a UAS flight request
- How to choose the right aircraft for your missions and fleet management
- Operational guidelines for UAS pilots and technicians in a police agency
- A baseline understanding of the FAA's role in public safety regulatory compliance
- Rules of evidence related to drone operations and agency requirements
- How to successfully present drone-collected data in court so the evidence is admitted into the record and appropriately understood by all parties

Training needs to provide the drone team with aeronautical knowledge as well as operational skills to successfully conduct drone deployments. Training also must cover the agency's drone policy and any state or local laws regarding police use of drones.

### **Hints and tips**

A number of agencies recommended purchasing inexpensive drones to use as practice during training.

"We bought some cheap drones on Amazon that people could practice with when they're first starting out so they could get a feel for flying drones. And it doesn't cost us much if we have an occasional crash," said Assistant Chief Samuel Hall of the Irving Police Department.

#### Visual observers

Some agencies have specific training hour requirements depending on the drone team member's role. Under the Miami Beach Police Department's training protocols, someone can act as a visual observer after 40 hours of classroom training and passing the part 107 test. To become pilot, they need to complete an additional 40 hours of flight time.

The MSP operates under both a COA and part 107. Most of the agency's missions are subject to the requirements of the COA, which include having a visual observer. The MSP has found it useful to train observers across the state so there are people who can get to a scene quickly. "We trained our bomb squad, our arson investigators, and our accident reconstructionist on drones," said MSP Lt. Col. Kelenske. "Those are the three groups that call us most often for service and are spread throughout the state, so usually one of them is already at the scene or their way to it."

# ONGOING TRAINING

Many agencies expressed a need to continue training after drone team members become operational. The Polk County Sheriff's Office requires its drone pilots to participate in four-hour training sessions every two weeks, totaling 96 training hours per year. The Daytona Beach Police Department has training sessions for their pilots every month as well as special training sessions throughout the year that focus on nighttime operations. Continuous training keeps drone team members proficient in drone operations and up to date on FAA rules and regulations.

### RECOMMENDATIONS FOR TRAINING

- Require drone training for all agency personnel who will be assisting with drone operations.
- Include the following topics in your own training protocols:
  - Methods of conducting safe flight operations under exigent circumstances
  - Drones crew resource management and a risk assessment-based model to accept or decline a UAS flight request
  - How to choose the right aircraft for your missions and fleet management
  - Operational guidelines for UAS pilots and technicians in a police agency
  - A baseline understanding of the FAA's role in public safety regulatory compliance
  - Rules of evidence related to UAS operations and agency requirements
  - How to present UAS-collected data in court to facilitate admissibility of the data and understanding by the fact finder

- Purchase inexpensive drones for new pilots to practice with during initial training.
- Train pilots and visual observers in patrol and from various units (e.g., bomb squad or accident reconstruction personnel) to ensure fast response times.
- Set ongoing training requirements so team members will remain proficient in drone operations and up to date on FAA rules.

# Standard operating procedures

Following is an outline of elements that should be included an agency's drone program's standard operating procedures (SOP). Within each section, we have included sample language and suggested components to help guide agencies as they implement their programs. However, agencies must tailor their SOPs according to their specific program objectives and any local regulations.

PERF staff reviewed the SOPs of 24 agencies to compile these recommendations. See appendix B for the list of agencies that provided their SOPs to PERF.

### PURPOSE

This section should include one to two sentences explaining the topic and purpose of the SOPs.

#### Sample language

The purpose of this written policy is to establish guidelines for the use of small Unmanned Aircraft Systems (UAS) to support public safety operations by the department.<sup>19</sup>

### DEFINITIONS

Include definitions for terms that are specific to UAS and not common knowledge within the department or to the public.

#### **Proposed definitions**

- Above ground level (AGL). Height measured with respect to underlying ground surface.
- **Certificate of Authorization (COA).** A document issued by the Federal Aviation Administration (FAA) to a public operator authorizing a specific UA activity.
- **Federal Aviation Administration (FAA).** The national aviation authority of the United States, with powers to regulate all aspects of American aviation.

<sup>19.</sup> This language comes from the Scottsdale (Arizona) Police Department's SOP, on file with PERF.

- **Night flight.** Flight of a UAS that occurs between the hours of one half hour after sunset and one half hour before sunrise.
- Unmanned Aircraft System (UAS). An uncrewed aircraft of any type that can sustain directed flight, commonly referred to as an unmanned aerial vehicle (UAV) or drone, and all associated elements, including communication links, sensing devices, and components that control the aircraft.
- **Remote pilot in command (RPIC).** An individual who has full control over the drone during flight and is responsible for the overall flight operations.
- VO (visual observer). A crew member for a flight mission who serves as a second set of eyes, monitoring the UAS in flight in order to support the RPIC.

# POLICY

Include in this section a summary of the department's goals for UAS usage and identify the scope of operations.

### Sample policy language:

All police department employees involved in the operation of department owned UAS will adhere to the procedures and restrictions outlined within this policy. It is the policy of this agency to use UAS for the focused and limited purpose of criminal investigations, public safety, and training. A UAS will only be operated for a specific mission when it can be done safely and effectively. Operation of the department UAS will be in accordance with department policy, state law, FAA regulations, and in accordance with the parameters of the COA. Department-owned UAS will only be used for legitimate law enforcement and public safety purposes.

# STAFFING

This section should include an overview of the staffing requirements for the UAS team and the flight crew during UAS deployments.

#### Sample staffing section components

- Chain of command (will vary between larger and smaller departments and size of UAS program)
- Position responsibilities and duties (will vary between larger and smaller departments and size of UAS program)
- Flight crew personnel (identifies the minimum number of team members required for UAS deployment)

#### Sample language: Chain of command

- The department Unmanned Aerial Systems Unit (UASU) will operate within the Operations Bureau under the direction of a commander identified by the Chief of Police.
- The Operations Bureau Commander, in coordination with the UASU Commander, will identify a UASU coordinator.
- In the absence of the UASU Commander, team members involved in UASU operations will be responsible to the on-duty watch commander or specific incident commander for operational assignments.<sup>20</sup>

Sample language: Position responsibilities and duties

- UAS Unit Commander. The commander is responsible for the following tasks:
  - Oversight and coordination of the UAS program, members, and equipment in accordance with department policy
  - The safe, legal, and efficient deployment and operation of UAS devices
  - Ensuring department supervisors are provided training and updates on UAS procedures and capabilities
  - Participating in the selection and removal of UAS program members and identifying specific program assignments as outlined in this document<sup>21</sup>
- UAS Unit Coordinator. The coordinator is responsible for the following tasks:
  - The safe, legal, and efficient deployment and operation of a UASU device
  - Ensuring department members have the opportunity to participate in observer orientation training so they can safely and effectively assist in UAS program operations
  - Coordinating and ensuring completion of required team member training
  - Ensuring all program related documentation and reporting is completed as required
  - In the legal officer's absence, contacting the program coordinator regarding the legal officer's responsibilities.
  - All other UAS program related tasks assigned by the Program Commander<sup>22</sup>

<sup>20.</sup> This language comes from the Norman (Oklahoma) Police Department's SOP, on file with PERF.

<sup>21.</sup> This language comes from the Norman (Oklahoma) Police Department's SOP, on file with PERF.

<sup>22.</sup> This language comes from the Norman (Oklahoma) Police Department's SOP, on file with PERF.

- Legal Officer. The legal officer will be a UAS operator assigned to or removed from the position by the team commander. The legal officer is responsible for the following tasks:
  - The safe, legal, and efficient deployment and operation of a UAS device
  - Ensuring the UAS programs operations are being conducted within the current legal requirements from local, state, and federal standards
  - Preparing annual training and updates to the department, program members, and other identified persons or groups as deemed necessary to ensure compliance with legal and regulatory guidelines, including FAA COAs; the legal officer shall work with the jurisdiction's legal staff to prepare these updates
  - Obtaining and maintaining necessary COAs for operations within the jurisdiction's limits and any other anticipated areas of operation<sup>23</sup>
- Maintenance Officer. The maintenance officer will be an RPIC who is assigned to the position by the team commander. In the maintenance officer's absence, the UASU Coordinator shall be contacted regarding maintenance or equipment related matters. The maintenance officer will be responsible for the following tasks:
  - The safe, legal, and efficient deployment and operation of a UAS device
  - The proper maintenance and repair of all UAS devices
  - Ensuring team members have necessary training and tools for basic evaluations, inspection, and necessary routine operational maintenance of team equipment
  - Ensuring proper reporting and documentation of all maintenance or equipment-related matters are properly documented as required by this document, department policy, or the coordinator's direction
  - All other UASU program related tasks assigned by the unit commander or coordinator<sup>24</sup>

<sup>23.</sup> This language comes from the Norman (Oklahoma) Police Department's SOP, on file with PERF.

<sup>24.</sup> This language comes from the Norman (Oklahoma) Police Department's SOP, on file with PERF.

- Technical Advisor. If determined necessary, the unit commander may seek appointment of one or more technical advisors to the program. Examples of a UASU technical advisor may include private or commercial pilots, legal advisors, and those possessing specific skills related to the program operations.
  - The need for a technical advisor shall be made by the commander to enhance or advance the program's mission.
  - Selection of an advisor, specific tasks, and requirements for selection shall be determined by the Operations Bureau Commander and UASU Commander.
  - The UASU Commander may terminate the role of a technical advisor at any time in accordance with department policy and the needs of the program.<sup>25</sup>
- RPIC. The RPIC is solely responsible for the flight team's actions.
  - The RPIC is authorized to refuse any flight request based on current meteorological conditions, physiological conditions, or for any other concern that the RPIC believes will affect flight safety.
  - Should the RPIC refuse a flight for any reason, they shall inform the Division Program Coordinator (DPC) as soon as possible of such refusal and the reason for refusal.
  - The RPIC is responsible for the safe conduct of all flights, including the following:
    - Flight planning and preparation, including pre-flight inspections of UAS and equipment
    - Weather briefing
    - Flight operations, including control of course, air speed, altitude, and duration
    - Timely reporting of new or previously unknown hazards to safe flight
    - Post-flight inspection
    - After each deployment, maintaining and making appropriate entries in UAS logbooks and reports

<sup>25.</sup> This language comes from the Norman (Oklahoma) Police Department's SOP, on file with PERF.

- VO. The VO is responsible for performing assignments given by the relevant program supervisor, or in their absence, the RPIC.
  - The VO assists the RPIC in the safe conduct of all flights, including the following:
    - See-and-void operations of the UAS, remaining in contact with RPIC, and communicating any obstacles the aircraft might encounter
    - If the flight becomes a hazard to ground personnel or other aircraft, immediately notifying the RPIC
    - During any phase of flight, if the VO notices a malfunction with the aircraft, immediately notifying the RPIC
    - All other program tasks assigned by the RPIC or program supervisor
- Flight Crew Personnel
  - Flight crews should consist of one trained UAS RPIC and preferably at least one VO.
  - A VO shall always be used if the personnel are available.
  - If the personnel are not available, the UAS RPIC shall consider that operating a UAS without a VO creates an environment of heightened risk.

### REQUIRED TRAINING

This section outlines the department's UAS training requirements. Please see the section on "Training" in chapter 2 for detailed guidance.

#### Sample training section components

- Flight hours
- RPIC initial training
- RPIC proficiency training
- VO Training

#### Sample language

- Flight hours training
  - The person manipulating the controls should have a minimum 20 hours of flight time with a similar aircraft, preferably documented in a logbook.
  - RPIC initial training
  - Option 1. Prior to operating a department owned UAS, pilots must successfully pass the FAA aeronautical test and obtain the FAA remote pilot certification in accordance with 14 C.F.R. part 107. Pilots will attend and successfully complete formal training to prepare for the aeronautical knowledge test.
  - Option 2. All personnel selected to be RPICs that will be flying law enforcement missions shall be properly trained and have obtained their FAA part 107 Remote Pilot Certificate. The RPICs will have an up-to-date working knowledge of the airspace intended for operations, air traffic control communication requirements, and specific UAS aerodynamic factors and the ability to obtain and interpret weather information. All RPICs shall be proficient with the role and functions of an observer as well.
  - Option 3. Agency personnel who are assigned UAS equipment must complete an agencyapproved training program to ensure effective use, operations, and the proper calibration and performance of the equipment.<sup>26</sup>
- RPIC proficiency training:
  - To maintain proficiency, all RPICs shall conduct at least one training flight, including one takeoff and landing, each month. Training flights shall be documented.
  - An RPIC is also required to pass a refresher test on the FAA part 107 every 24 months.
- VO training
  - Agency personnel who are assigned as a VO and are not certified as an RPIC must complete an agency-approved training program to ensure that they can effectively perform the duties of a VO as outlined in the department SOP and COA.<sup>27</sup>

<sup>26.</sup> This language comes from the Tennessee Bureau of Investigation's SOP, on file with PERF.

<sup>27.</sup> This language comes from the Tennessee Bureau of Investigation's SOP, on file with PERF.

## AUTHORIZED TYPES OF MISSIONS

This section should include a description of the types of missions for which your department is authorized to use its UAS.

#### Sample mission types

- Crime scene processing
- Cross-agency aid
- Damage assessment (man-made or natural event)
- Disaster response
- Fire or explosives
- Infrastructure inspections
- Major traffic accident investigations
- Monthly training flights
- Public relations
- Search and rescue missions
- Special events or public safety assessments
- Tactical deployment
- Terrorism response

### Sample language

- Crime scene processing
  - Provide aerial mapping support to assist in crash reconstruction.
  - Provide aerial mapping and photographing to analyze crime scenes.
  - Enhanced non-surveillance operations that will provide officer safety during crime scene searches.<sup>28</sup>

<sup>28.</sup> This language comes from the Fairfax County (Virginia) Police Department's UAS program manual, on file with PERF.

- Cross-agency aid
  - Following official requests, the deployment of the department UASU may be authorized by a program supervisor or watch commander. Requests must be fully evaluated for approval in accordance with department policies, legal authority, other available resources, and community expectations.
  - Participation in mutual aid requests should involve the establishment of a unified or joint command in accordance with common industry standards. All deployments will be continually evaluated for changing situations or information that may alter reasonable participation in the incident.
  - Fire department
    - Grass fires
    - Hazardous materials situations
    - Large structural fires
    - Storm siren maintenance and inspections
    - Water rescues
  - Public works
    - Congestion
    - Detours
    - Review of traffic patterns in areas of construction
    - Roadway and bridge inspections
    - Other areas of concern
  - Other governmental or private agencies may request assistance through routine processes including MOUs or during emergency situations. Any request for use of the department UAS unit will require the approval for use by the watch commander or the UASU Commander.<sup>29</sup>
- Damage assessment (natural or man-made event)
  - Structural, flood related, environment, transportation, pipeline breaks, and rail incidents.
  - Enhanced search grids through onboard software.<sup>30</sup>

<sup>29.</sup> This language comes from the Norman (Oklahoma) Police Department's SOP, on file with PERF.

<sup>30.</sup> This language comes from the Fairfax County (Virginia) Police Department's UAS program manual, on file with PERF.

- Disaster response
  - To assist decision makers (incident command staff, first responders, city, county and state officials) in understanding the nature, scale, and scope of an incident and for planning and coordinating an effective response.
  - Fire or explosives
  - Aerial management and coordination for large outside fires to help determine the extent of coverage and identify structures, exposures or other infrastructure that may be impacted.
  - Assist fire investigators in assessing and documenting fire scenes for an overall scope of the scene.
  - Assist in evaluating hazards [and] structure's integrity and helping to ensure scene safety.
  - Assist in helping account for personnel on the fire ground.
  - Assist in post-blast investigations in locating blast scene radius and areas impacted by an explosion.
  - Explosive ordinance detection (EOD) and security.
  - Overflight of structure fires (residential and commercial) by providing a 360-degree view for the incident commander.
  - Provide real-time aerial video footage of large-scale incidents.<sup>31</sup>
- Infrastructure Inspections
  - Inspections and documentation of critical infrastructure including department radio towers, facilities, lighting devices, and other related needs as approved by the program supervisors.<sup>32</sup>
- Major traffic accident investigations
  - Provide real-time traffic impact assessment and 3D mapping due to vehicle crashes or significant events (such as road backups or alternate routes of travel, weather, or evacuations).<sup>33</sup>

<sup>31.</sup> This language comes from the Fairfax County (Virginia) Police Department's UAS program manual, on file with PERF.

<sup>32.</sup> This language comes from the Norman (Oklahoma) Police Department's SOP, on file with PERF.

<sup>33.</sup> This language comes from the Fairfax County (Virginia) Police Department's UAS program manual, on file with PERF.

- Monthly training flights
  - Documentation, monitoring, assistance, and review of department training including basic academy, in-service training, and other necessary situations as determined by the training staff and program supervisors.
- Public relations
  - Enhancements to brochure and other marketing tools.
  - High definition video and photographic capability for media events.<sup>34</sup>
- Search and rescue missions
  - Allow for limited tracking of search teams in an area.
  - Identify potential hazards for search teams and vehicles.
  - Provide a large-scale overview of the search area.
  - Provide photographic and video capability and analysis.
  - Scene awareness and life safety to identify potential hazards to responders.
  - Search for endangered or critical missing individuals to assist missing persons investigations, Amber Alerts, and Silver Alerts, as well as other search and rescue missions.<sup>35</sup>
- Special events and public safety assessments
  - Bridging digital communications and observations.
  - Forensic documentation.
  - Perimeter security.
  - Races, festivals, large public gatherings (when authorized).<sup>36</sup>
- Tactical deployment
  - To support the tactical deployment of officers and equipment in emergency situations (e.g., incidents involving hostages and barricades, support for large-scale tactical operations, and other temporary security situations).

<sup>34.</sup> This language comes from the Fairfax County (Virginia) Police Department's UAS program manual, on file with PERF.

<sup>35.</sup> This language comes from the Fairfax County (Virginia) Police Department's UAS program manual, on file with PERF.

<sup>36.</sup> This language comes from the Fairfax County (Virginia) Police Department's UAS program manual, on file with PERF.

- Terrorism response
  - To counter a high risk of a terrorist attack by a specific individual or organization if the U.S.
     Secretary of Homeland Security determines that credible intelligence indicates that there is a risk.

### In Chula Vista, police at headquarters send drones directly to a scene

The drone program of the police department in Chula Vista is unique; it is the first "drones as a first responder" (DFR) program in the United States.\* In most police departments, an officer at the scene requests a drone, and a drone operator transports a drone to the scene and operates it. In Chula Vista's DFR model, drones are operated by pilots at police headquarters, and they respond directly to priority 1 (emergency) and priority 2 (urgent) calls. A drone often arrives on scene before officers.

Originally, drones were limited to a one-mile radius from headquarters, so they could be flown within visual line of sight of an operator as required by the FAA. However, in May 2019, Chula Vista became the first police department in the nation to be granted a Beyond Visual Line of Sight Waiver by the FAA over an urban environment. Operators now deploy from two launch sites and can range about 1.5 miles from each launch site. This arrangement has provided the department with coverage over 17 of the 52 square miles of the city. Approximately 70 percent of the department's calls for service are to locations within those 17 square miles.

The drone provides real-time video feeds to a radio-equipped pilot at headquarters as well as to first responders, who can view the footage using an application on their cell phones. This capability increases safety and efficiency for responding officers, because they can see video of the scene before they arrive.

In 2018 and the first nine months of 2019, drones in Chula Vista responded to 849 calls for service involving 117 arrests. In one case, a drone gathered vital information about a domestic violence suspect who was in a canyon. The footage allowed officers to monitor the suspect as they formulated a plan to safely take him into custody.

An additional benefit of using drones as first responders is that they can help clear calls without the need to tie up ground units. In 18 months, drones cleared 195 calls. In those cases, a police department employee informs the 911 caller that the call was cleared by drone. For example, a drone operator can evaluate a scene and determine that the suspect in a disturbance call has left.

On the other hand, in at least one case, a responding drone resulted in a call being assigned a higher priority level.

\*"UAS Drone Program," Chula Vista Police Department, accessed February 11, 2020, <u>https://www.chulavistaca.gov/departments/police-department/programs/</u> uas-drone-program.

# ACCIDENTS

This section should include the department protocol for handling UAS-related accidents.

#### Sample accidents components

- FAA accident reporting guidelines
  - An outline of the guidelines for reporting accidents to the FAA under FAA 107.9 following an accident

- Flight termination
  - Flight termination process during emergency situations
- Reporting within the department
  - Whom to report the accident to within the department
- Types of accidents
  - Loss of global positioning system (GPS) signal
  - Lost link procedures
  - Loss of visual contact
  - Low battery

#### Sample language

- FAA accident reporting guidelines
  - FAA accident reporting guidelines shall be followed as required under the following circumstances. Such reports shall be reported through the UAS supervisors for review before their submission and must be submitted to the FAA within 10 days of the incident.
    - Serious injury to any person or loss of consciousness; or
    - Damage to any property, other than the UAS, unless one of the following conditions is satisfied:
      - The cost of repair (including materials and labor) does not exceed \$500
      - The fair market value of the property does not exceed \$500 in the event of total loss<sup>37</sup>

<sup>37.</sup> This language comes from the Norman (Oklahoma) Police Department's SOP, on file with PERF.

- Flight termination
  - If flight termination must be executed in the event that all other contingencies have been exhausted and further flight of the aircraft cannot be safely achieved or other potential hazards exist that require immediate discontinuation of the flight, the UAS RPIC may initiate the intentional and deliberate process of performing Controlled Flight Into Terrain (CFIT).<sup>38</sup>
- Reporting within the department
  - All accidents or mishaps shall be recorded in the post flight report and to UAS unit supervisors. Additional documentation may be required through the department's professional standards reporting system.<sup>39</sup>
- Types of accidents
  - Loss of GPS signal
    - Should the UAS lose GPS signal during autonomous operations, the UAS RPIC must immediately command the UAS into manual mode and land as soon as practical. If positive control of the UAS cannot be maintained and the UAS departs the operation area or the UAS poses a risk to life or property, the UAS RPIC will issue an Engine Kill command.<sup>40</sup>
  - Lost link procedures
    - Lost link procedures shall be followed in accordance with the COW/COA, department UAS emergency procedures (checklist), and manufacturer instructions.
    - Immediate notification to a local airspace authority should be considered.<sup>41</sup>
  - Loss of visual contact
    - If visual contact with the UAS is lost, the UAS RPIC shall command the aircraft into a hover mode and the UAS crewmembers shall try to re-establish visual contact. If visual contact cannot be re-established within a reasonable amount of time determined by the RPIC, lost link procedures shall be executed.<sup>42</sup>

<sup>38.</sup> This language comes from the Tennessee Bureau of Investigation's SOP, on file with PERF.

<sup>39.</sup> This language comes from the Norman (Oklahoma) Police Department's SOP, on file with PERF.

<sup>40.</sup> This language comes from the Tennessee Bureau of Investigation's SOP, on file with PERF.

<sup>41.</sup> This language comes from the Norman (Oklahoma) Police Department's SOP, on file with PERF.

<sup>42.</sup> This language comes from the Tennessee Bureau of Investigation's SOP, on file with PERF.

- Low battery
  - A low battery emergency is triggered when the battery is depleted to a point that may affect the safe return of the UAS; the RPIC will land the UAS as soon as possible.
  - Loss of UAS Power (Engine Failure)/UAS Crash: In case of an engine failure, the UAS will
    not be able to maintain flight. UAS flight crew will immediately attempt to locate the UAS,
    assess the scene for injuries, and render first aid if necessary.<sup>43</sup>

# PROCEDURES

This section should include a description of the procedures required for UAS operation from start to finish.

### Sample procedure components

- Agency reports and flight logs
- Flight procedures
- Landing procedures
- Launch procedures
- Perimeter management
- Preflight expectations
  - Authorization for flights
  - Planning for flights
  - Inspection of UAS
  - Preflight check expectations (checklist)
- Post flight procedures
  - Post flight documentation, including agency report and/or flight log
- Safety procedures

<sup>43.</sup> Source: Tennessee Bureau of Investigation's SOP, on file with PERF.

- Search warrants
- State and federal regulations
- Weather
  - Develop weather safety guidelines, especially pre-flight
  - Maintenance, i.e., who will maintain the aircraft and how to maintain the aircraft

### Sample language

- Agency reports and flight logs
  - All agency reports should include the following:
    - Date of UAS deployment
    - Name of UAS operator (RPIC)
    - Purpose of UAS deployment
    - Whether a search warrant was requested and obtained
    - Results of UAS deployment
    - Duration of UAS deployment
    - Any other pertinent information<sup>44</sup>
  - Flight log: The RPIC is responsible for creating a flight log for each flight. The flight log should include the relevant case file number, the purpose for the flight, the approving supervisor name, and other flight team member names. The flight log should be a part of the program investigative files and entered into the online flight management tool and/or other electronic format for collecting the log data. The RPIC will also maintain flight logs for training and maintenance missions.<sup>45</sup>

<sup>44.</sup> This language comes from the Cumberland County (Maine) Sheriffs Office's SOP, on file with PERF.

<sup>45.</sup> This language comes from the Tennessee Bureau of Investigation's SOP, on file with PERF.

- Flight procedures
  - Although the UAS can be flown autonomously, the RPIC will monitor the aircraft, base station, and payload systems to ensure the aircraft is flying as designed and maintains the proper altitude.
  - After liftoff, crew members shall perform tasks according to their job assignment while communicating clearly and effectively to monitor the UAS.<sup>46</sup>
- Landing procedures
  - The RPIC is responsible for confirming either that the mission objective has been met or the mission is to unsafe to continue prior to landing the aircraft.
  - The RPIC will communicate with the VO to confirm no obstacles are in the flight path of the aircraft and the home location prior to giving the command for the UAS to return home.
  - The VO will monitor the aircraft to ensure proper landing. If the aircraft is not landing as desired, the VO will notify the RPIC who will determine whether to abort landing.
  - The RPIC is responsible for ensuring contact is made with the proper tower in accordance with FAA guidelines.<sup>47</sup>
- Launch procedures
  - The RPIC should launch, operate, and recover from preset locations so that the aircraft will fly according to mission plan.<sup>48</sup>
  - Prior to the launch of the UAS, the RPIC is responsible for ensuring the checklist is complete and the aircraft and ground station are safe to operate. The RPIC will communicate with the VO to confirm that the area is visibly clear of any safety hazards or obstacles such as low-flying air traffic prior to lift off.
  - The RPIC is responsible for ensuring all notifications to the appropriate air traffic control facility and local authorities have been made in accordance with the rules and guidelines set forth by the FAA.<sup>49</sup>

<sup>46.</sup> This language comes from the Torrance (California) Police Department's SOP, on file with PERF.

<sup>47.</sup> This language comes from the Torrance (California) Police Department's SOP, on file with PERF.

<sup>48.</sup> This language comes from the Athens-Clarke County (Georgia) Police Department's SOP, on file with PERF.

<sup>49.</sup> This language comes from the Torrance (California) Police Department's SOP, on file with PERF.

- Perimeter management: It is the job of the RPIC to ensure that all flight operations are within the FAA-issued airspace waiver and authorization parameters and UAS flight limits. Flight boundaries should be reviewed prior to commencing flight operations. In addition, the RPIC should identify the following:
  - Primary takeoff and landing site: Typically the primary landing shall be the same as the launch site but they can be separate locations. The RPIC has final authority for any approaches to the primary site and can elect to reject an approach deemed unsafe.<sup>50</sup>
  - Alternate landing sites: The RPIC shall designate at least one alternative landing site. In the event that a landing is not possible, and the primary landing site is deemed unsafe, procedures to utilize the back-up site will be invoked.<sup>51</sup>
  - Emergency landing sites: The RPIC may optionally designate an alternate landing site whereby the aircraft may be landed directly in the case of an emergency. The alternate landing site should be located so as to provide minimal risk if the aircraft is required to vacate airspace. If the RPIC deems it necessary, the UAS may be flown to this site and landed without regard to the risk to the flight equipment or the aircraft. The safety of persons, manned aircraft, and property should be prioritized over the risk to UAS equipment.<sup>52</sup>
  - Flight over populated areas: The RPIC should make every effort to select a landing site that avoids flight over populated areas.<sup>53</sup>
  - Landing safety and crowd control: All landing sites should be maintained and operated in the same manner as the launch sites. A buffer of at least 10 feet should be maintained at all times between aircraft operations and all nonessential personnel (all personnel other than the UAS operator or RPIC and the VO).<sup>54</sup>
- Pre-flight check expectations
  - Authorization: Every deployment of the department's UASU, including its members or equipment shall be done in accordance with department policy and this SOP. A determination and authorization for deployment of the UASU will be made by the UAS unit supervisor or other department-designated supervisor.<sup>55</sup>

<sup>50.</sup> This language comes from the Athens-Clarke County (Georgia) Police Department's SOP, on file with PERF.

<sup>51.</sup> This language comes from the Athens-Clarke County (Georgia) Police Department's SOP, on file with PERF.

<sup>52.</sup> This language comes from the Athens-Clarke County (Georgia) Police Department's SOP, on file with PERF.

<sup>53.</sup> This language comes from the Athens-Clarke County (Georgia) Police Department's SOP, on file with PERF.

<sup>54.</sup> This language comes from the Athens-Clarke County (Georgia) Police Department's SOP, on file with PERF.

<sup>55.</sup> This language comes from the Norman (Oklahoma) Police Department's SOP, on file with PERF.

- Planning
  - The flight crew should be familiarized with all available information pertaining to the flight, such as takeoff/landing, the operational limitations of part 107, weather conditions, hazards, temporary flight restrictions (TFR), etc.
  - The RPIC will ensure the location for takeoff and emergency landing is adequate upon arrival at the location. At least one emergency landing area should be identified before the start of operations.
  - RPIC should be aware of all surroundings if an emergency landing is necessary. This includes the ability to recover the UAS.<sup>56</sup>
- Inspection
  - Before the first flight of the day, verify all batteries are fully charged.
  - Check the airframe for signs of damage, and its overall condition.
  - Check the propeller or rotor blades for chips, cracks, looseness, and any deformation.
     A propeller must be replaced if any abnormalities are identified.
  - Check that camera(s) and mounting systems are secure and operational.
  - Perform an overall visual check of the aircraft prior to arming any power systems.
  - Repair or replace any part found to be unsuitable to fly during the pre-flight procedures prior to takeoff.
  - Once equipment is powered on, RPIC should ensure all hardware firmware is up to date.<sup>57</sup>
- Example pre-flight checklist
  - Necessary documents: pilot certificate, aircraft registration, UAS flight manual
  - Suitable weather conditions
  - Check air frame for cracks, ensure screws are tight

<sup>56.</sup> This language comes from the Athens-Clarke County (Georgia) Police Department's SOP, on file with PERF.

<sup>57.</sup> This language comes from the Athens-Clarke County (Georgia) Police Department's SOP, on file with PERF.

- Propeller or rotor not damaged, tightly fixed
- Batteries fully charged and securely mounted
- Check firmware status of all hardware
- Communications (data link) check
- Ensure GPS module has GPS "fix"
- Check mission flight plan
- If applicable, "Return Home" and "Emergency Landing" locations selected and loaded to the Ground Control Station (GCS) and aircraft
- Ensure sensors are calibrated and right setting is loaded
- Complete flight crew briefing
- Launch site free of obstacles
- Recheck wind direction before launch
- Confirm phone number to nearest air traffic control facility in event of emergency<sup>58</sup>
- Post-flight procedures
  - The RPIC is responsible for performing an equipment check, weather report, and any other documentation relating to the mission and area of operations at the completion of all UAS operations.
  - It is the responsibility of the RPIC to ensure an investigative report is completed in order to document any flight categorized as "investigative operations."
  - Flights categorized as "training" or "maintenance" do not require an investigative report.<sup>59</sup>

<sup>58.</sup> This language comes from the Athens-Clarke County (Georgia) Police Department's SOP, on file with PERF.

<sup>59.</sup> This language comes from the Tennessee Bureau of Investigation's SOP, on file with PERF.

- Safety
  - General safety: All on-site team members involved in an operation shall be responsible for following all necessary steps to ensure the safety of all involved persons and property. This includes the safety of all employees, community members, animals, department and nondepartment property.<sup>60</sup>
  - Distractions: RPICs and VOs shall ensure they do not become distracted from their flight operation tasks. Potential distractions include the use of phones, computers, or other electronic items. Operators are prohibited from using any of these devices while flight operations are in progress. RPICs and VOs should avoid situations that would impede vision or hearing as well as any clothing that would interfere with safe operation of the UAS.<sup>61</sup>
  - Reporting safety concerns: Any UASU team member who becomes aware of a safety-related concern or situation shall immediately notify the RPIC and VO of the specific concern. Team members should work to safely mitigate all concerns. If the situation is not resolved, the on-site team members shall immediately cease operations and notify the supervisor in charge of the operation to request immediate assistance. All concerns and situations should be reported to the supervisor as soon as reasonable.<sup>62</sup>
- Search warrants
  - Prior to the flight, the police department must first obtain a search warrant signed by a judge authorizing the use of a UAS. The flight may be launched without a warrant, however, if an Assistant Special Agent in Charge or above approves the flight based upon the existence of an exception to the warrant requirement consistent with state law.<sup>63</sup>
    - This does not apply to UAS deployments for the following:
      - Purposes other than the investigation of crime, including aerial photography for the assessment and documentation of crashes and other scenes, forest fires and other fire scenes, flood stages, and storm damage
      - Search and rescue operations when the department determines that use of a UAS is necessary to address an immediate danger to any person or for related training exercises.<sup>64</sup>

<sup>60.</sup> Source: Norman (OK) Police Department's SOP, on file with PERF.

<sup>61.</sup> This language comes from the Norman (Oklahoma) Police Department's SOP, on file with PERF.

<sup>62.</sup> This language comes from the Norman (Oklahoma) Police Department's SOP, on file with PERF.

<sup>63.</sup> This language comes from the Tennessee Bureau of Investigation's SOP, on file with PERF.

<sup>64.</sup> This language comes from the Cumberland County (Maine) Sheriffs Office's SOP, on file with PERF.

- State and federal regulations
  - The UAS unit must obtain applicable authorizations, permits, certificates, and licenses required by the FAA prior to deploying or operating the UAS, all of which shall be maintained and be current.<sup>65</sup>
    - The RPIC must hold a current FAA certificate that evidences that the pilot meets the minimum standards required for operation of a UAS.
    - Any operation of a UAS must comply with all FAA requirements and guidelines, such as obtaining a Certificate of Authorization or Waiver from the FAA, and any other applicable city or state law.
- Weather
  - Before each flight, the RPIC and VO should ensure that they gather enough information about the existing and anticipated weather conditions throughout the entire mission environment. As best practice, they should use FAA approved weather resources such as the following:
    - Meteorological Terminal Aviation Weather Reports (METARs)<sup>66</sup>
    - Terminal Area Forecasts (TAF)
    - To obtain the latest and most current weather conditions, Notices to Airmen (NoTAM) and TFRs, the RPIC should obtain a local aviation briefing at:
      - 1-800-WXBRIEF or
      - <u>www.1800WXBRIEF.com</u>
  - Wind direction plays a major role in flight operations. The RPIC should take precautions to ensure that wind conditions do not exceed the aircraft limits stated in the aircraft manual and specifications. An anemometer is a low-cost, simple-to-use tool that can be used to estimate wind speed and determine if it is within the necessary limits to fly the UAS.

<sup>65.</sup> This language comes from the Tennessee Bureau of Investigation's SOP, on file with PERF.

<sup>66.</sup> Aviation Weather Center. "METARs." https://www.aviationweather.gov/metar.

- The RPIC should ensure that the flight will occur within the weather requirements specified in part 107.51, c–d:
  - The minimum flight visibility from the control station is no less than three statute miles
  - UAS remains at least 500 feet below a cloud and at least 2,000 feet horizontally from a cloud
  - Majority of FAA authorizations require a Visual Line of Sight (VLOS) between the aircraft and RPIC and the aircraft and VO at all times, though the FAA can produce waivers under part 107 for certain types of night-time or beyond-line-of-sight operations.<sup>67</sup>
- Weather must be continually evaluated to ensure safe flight operations.<sup>68</sup>
- A weather report will be completed at the end of the mission.
- Maintenance
  - Maintenance must be up to date prior to launch.
  - Accurate UAS maintenance reporting is the responsibility of the RPIC, who will forward the information to the supervisor or their designee in accordance with the manufacturer recommendations.
  - When maintenance is performed, a test flight shall be conducted and documented in accordance with the manufacturer's instructions.
  - The RPIC will not fly any aircraft that does not meet airworthiness requirements following the preflight inspection.
  - Timely maintenance and accurate reporting are required for mission availability and safety.<sup>69</sup>

<sup>67.</sup> This language comes from the Athens-Clarke County (Georgia) Police Department's SOP, on file with PERF.

<sup>68.</sup> This language comes from the Norman (Oklahoma) Police Department's SOP, on file with PERF.

<sup>69.</sup> This language comes from the Tennessee Bureau of Investigation's SOP, on file with PERF.

## A typical Michigan State Police drone deployment

The MSP uses drones for a variety of purposes. Most deployments are for fire scene assistance, collision reconstruction, and crime scene photography. The MSP has conducted presentations across the state to inform other police agencies and fire departments of their drone capabilities. These agencies call the MSP when they need to utilize their drone services. As of August 2019, the MSP had three drones strategically located in the state to provide the best response time. The MSP also was preparing to deploy two additional drones.

The MSP's drone deployment process begins with a request for an air asset. A member of the aviation unit reviews the request and decides which type of asset (fixed-wing, helicopter, or drone) is most appropriate. Decision factors include duration of the mission, the amount of discretion required, technological capabilities of the platform, and legal issues.

If the MSP decides that a drone is the most appropriate air asset, the current and forecasted weather at the call location is assessed to determine whether a drone deployment would be in compliance with FAA regulations. If weather conditions are acceptable, a NoTAM is filed with the FAA. Next, an operator and visual observer drive to the scene. Sometimes a visual observer is already on scene, because the MSP trains members of the local bomb squads, fire investigators, and traffic reconstruction team members to fulfill that role.

## RESTRICTIONS

Any restrictions placed on UAS operations should be outlined in this section. Such restrictions may include mission authorizations, specific equipment, areas of operation, and surveillance parameters.

### Sample language

- Authorization
  - Only a UAS authorized by the department may be deployed by qualified agency personnel (as set forth in this policy) for agency operations.
  - The UAS shall be deployed and used only to support official law enforcement and public safety missions.
  - The UAS shall not be operated in an unsafe manner or in violation of FAA rules.

- Equipment
  - The UAS shall not be equipped with or used to deploy weapons of any kind.
  - Written approval by the chief or sheriff or his or her designee must be obtained prior to the procurement of a UAS equipped with any of the following items:
    - Any sense-enhancement technology
    - Facial recognition technology
    - High-powered listening devices
    - High-powered zoom lenses
    - Night-vision technology
    - Thermal imaging technology
    - Video analytics<sup>70</sup>
- Populated areas: FAA part 107.39 does not permit UAS flights over persons not directly involved in the operations. Flights taking place over populated areas, heavily trafficked roads, or open-air assemblies of people are not allowed under regulation (unless through waiver). If the mission dictates that flight operations be conducted in such areas, the RPIC will need to obtain a waiver prior to flight.<sup>71</sup>

<sup>70.</sup> This language comes from the Cumberland County (Maine) Sheriffs Office's SOP, on file with PERF.

<sup>71.</sup> This language comes from the Athens-Clarke County (Georgia) Police Department's SOP, on file with PERF.

- Video surveillance
  - UAS video surveillance equipment shall not be used for the following activities:
    - To conduct random surveillance activities
    - To target a person based solely on individual characteristics, such as race, ethnicity, national origin, religion, disability, gender, or sexual orientation
    - To harass, intimidate, or discriminate against any individual or group<sup>72</sup>
    - To conduct personal business of any type<sup>73</sup>
  - To protect individual privacy rights, drone operators shall not intentionally photograph or record any individual inside a building or motor vehicle.<sup>74</sup>

## EVIDENCE DATA COLLECTION

This section documents the department's protocols for evidence collected by the UAS. Policies should address storage, access, privacy protections, and how information or evidence will be released to the public.

## Sample language

- Restrictions
  - Because of privacy concerns, UAS video transmitted while traveling to and from the target location will only be viewed live for navigational purposes and not recorded.
  - When reasonable, video will be recorded once the UAS has arrived at the target location and the camera is focused in a direction that is not intended to purposely infringe on the public's reasonable expectation of privacy.<sup>75</sup>

<sup>72.</sup> This language comes from the Fairfax County (Virginia) Police Department's UAS Program Manual, on file with PERF.

<sup>73.</sup> This language comes from the Chula Vista (California) Police Department's SOP, on file with PERF.

<sup>74.</sup> This language comes from the University of Massachusetts at Amherst Police Department's SOP, on file with PERF.

<sup>75.</sup> This language comes from the Scottsdale (Arizona) Police Department's SOP, on file with PERF.

- Storage
  - At the conclusion of operational deployments, the RPIC uploads video footage to the designated department location for video evidence.<sup>76</sup>
  - Prior to their duplication and further dissemination, any audio or video recordings, photographs, or any other such documentation resulting from the deployment of a UAS must be reviewed to determine whether such further dissemination may occur.
  - Any audio or video recordings obtained during the deployment of a UAS that are deemed unnecessary by the designated supervisor of the UAS program will be destroyed or dealt with in a manner consistent with the department policy on record retention.
- Public information
  - All UAS recordings will be released to other agencies, media, and members of the public through routine request procedures in accordance with department policy and state law.<sup>77</sup>

<sup>76.</sup> This language comes from the Scottsdale (Arizona) Police Department's SOP, on file with PERF.

<sup>77.</sup> This language comes from the Norman (Oklahoma) Police Department's SOP, on file with PERF.

## 3. MALICIOUS USE OF DRONES

Previous sections of this report provide guidance for police and sheriffs' departments interested in implementing drone programs, including model policies, promising practices, and lessons learned. This chapter discusses a more difficult challenge: how federal, state, and local law enforcement agencies must learn how to anticipate, prevent, and respond to the criminal use of drones by malicious actors.

Drones provide many new capabilities for criminals, including terrorists. For example, drones can be used by criminals to conduct reconnaissance to facilitate crimes such as robbery, theft, or sexual assault. Drones can also be used to drop firearms, narcotics, or other contraband into correctional facilities. Even more alarming, terrorists could use drones to drop a bomb, shoot firearms, or spray a poison gas over large crowds of people at a concert, sports event, or other gathering. Drones also can be extremely effective at reconnaissance, because they can fly past bollards, checkpoints, and other security mechanisms.

# Law, policy, and regulations limit law enforcement's use of certain technologies to counter drones

Unfortunately, until recently, efforts by any law enforcement agency at the federal level to disable threatening drones were severely hampered by existing federal laws.

- 1. Drones are considered a type of aircraft, so federal laws designed to protect airplanes and helicopters from attack or interference also criminalized actions to destroy or disable drones.
- 2. Drones are equipped with computers, so drones—even drones being used to commit crimes were protected by laws designed to criminalize computer hacking.

Drones are a unique type of new technology, occupying a grey area between laws and regulations originally enacted for other technologies, namely airplanes and helicopters, radio waves, and cyberspace. Writing new laws and regulations specifically for drones could have unpredictable implications for those technologies. So far, Congress has taken a more limited approach of modifying existing laws.

## New federal law

Fortunately, in October 2018, Congress approved a new federal law—the Preventing Emerging Threats Act, part of the Federal Aviation Administration Reauthorization Act (FAARA) of 2018—that gives the DOJ and the DHS important new counter-drone authority:

- To detect, identify, monitor, and track drones
- To warn the operator of a drone that is in restricted airspace

- To disrupt or seize control of a potentially threatening drone
- If necessary, to damage or destroy a threatening drone in various ways<sup>78</sup>

## New authority on remote identification is critical

In addition, the FAARA also mandates—in conjunction with the FAA Extension, Safety, and Security Act of 2016—that the administrator of the FAA, in coordination with the National Aeronautics and Space Administration (NASA) and in consultation with unmanned aircraft systems industry stakeholders, develop a plan to implement UAS traffic management (UTM) services. An essential component of the UTM currently under design by the FAA and NASA is automatic remote identification (Remote ID) of drones. UTM, incorporating the ability to automatically ascertain the identity of a drone's operator, is considered an especially important element of future drone management in the National Airspace System. Typically, at a large event such as a marathon or an outdoor concert, law enforcement agencies providing security may detect multiple drones approaching the event over the course of several hours. Remote ID means that law enforcement agents can immediately be alerted electronically to the presence of a particular drone so they can read the electronic "signature" of the drone and receive certain information—for example, the name and identity of the operator. This will help the law enforcement agents distinguish drones properly registered under Remote ID as belonging to hobbyists from drones that are potential threats operated by criminals. If a drone approaches the event without this automatic identification system, it will alert the agents that the drone is not registered, which can be considered a factor in determining whether the drone constitutes a threat. However, as of September 2019, regulations to fully implement the new federal law were still being worked out.

Furthermore, another concern is that drone detection systems that rely on remote identification will not detect drones manufactured by companies that have not provided their electronic "signatures" to allow easy detection. Additionally, criminals, including terrorists, may hand-build drones that do not have a radio frequency (RF) signature and will thus escape detection by RF-based systems. Drones also can be designed to fly a pre-planned flight path without remote control by an operator or use of GPS to guide its path; those drones would not receive or transmit RF signals, so they would not be detected by current RF-based detection technologies.

<sup>78.</sup> Preventing Emerging Threats Act of 2018, Pub. L. No. 115–254, §§ 1601–1603, 132 Stat. 3522–3530 (2018), https://www.congress.gov/115/plaws/publ254/PLAW-115publ254.pdf.

Finally, another concern is that a single company, DJI—a Chinese company—controls a large share of the worldwide drone market (as much as 85 percent by some estimates). There are significant concerns that Chinese-manufactured technologies may contain hardware or software components (or both) that are antithetical to U.S. interests. Such drones could create vulnerabilities in any computer networks they connect with. Systems intended to detect or interdict these drones could be thwarted by foreign actors, and information collected by these drones could be surreptitiously shared with foreign actors.

## New law provides little to no role for local police

The Preventing Emerging Threats Act of 2018 does not provide any new authority to state and local police to disable or destroy threatening drones. Only certain federal agencies are given these new powers, although the act contemplates DHS and DOJ support of state, local, territorial, or tribal law enforcement upon appropriate request from the chief executive officer of the state or territory.

In part, the new authority was limited to federal agencies because of concerns that counter-drone technologies are technologically unsafe. For example, one method of disabling a threatening drone is to jam the airwaves in the area with radio signals that stop the operator from controlling the drone. However, there is a risk that such jamming signals could interfere with other critical radio systems, such as those that allow airline pilots to communicate with ground controllers and receive information that helps them to land or take off safely. Thus, there are concerns that police action against a possible drone threat might result in an airliner crash or other catastrophe.

Participants at PERF's meeting said that this is one reason why Congress was not prepared to extend the authority to use counter-drone technologies to local police. In fact, even drone detection systems that are designed to identify the radio signals between a drone and its controller on the ground may violate certain federal laws, federal officials at PERF's meeting said. However, the federal officials at PERF's meeting said that state and local police and sheriffs' departments do have general authority under the Constitution to take action to protect public safety in exigent circumstances. They gave the example of a drone that appears to be moving to drop an explosive device on a crowd of people and compared that to the threat of a suicide bomber or truck racing toward a crowd of people. Ultimately, local police can take reasonable action to protect the public against imminent threats, proportionate to the nature of the exigent threat and consistent with existing agency policies and procedures.

Some local police agencies are moving to explore their options and prepare themselves for a drone threat against mass gatherings. As of 2018, there were more than 200 counter-drone technologies on the market.<sup>79</sup> Some agencies are beginning to test various devices.

<sup>79.</sup> Holland Michel, "Counter-Drone Systems" (see note 3).

## The risks of moving too slowly

Experts at PERF's conference called for intensive efforts to "catch up" with the new risks posed by drones. Some noted that the United States has been fortunate not to have experienced a major drone attack to date but said there is little to stop such an attack, especially with local police authority so limited. Federal agencies can use their new authority under the 2018 law to help local police manage a relative handful of major events, such as the Super Bowl, they noted. But every day, there are countless routine events in American cities that draw tens of thousands of people, and there is no way that federal agencies can involve themselves in all of those events.

## New federal law gives DOJ and DHS legal authority to take down threatening drones

The FAA Reauthorization Act of 2018, which became law on October 5, 2018, provides new legal authority for federal agencies to identify and mitigate drone attacks. The following is Congress's official summary of this new authority:

**DIVISION H—PREVENTING EMERGING THREATS** 

#### **Preventing Emerging Threats Act of 2018**

(Sec. 1602) This division amends the Homeland Security Act of 2002 to authorize the Department of Homeland Security (DHS) and the Department of Justice (DOJ) to each authorize specified personnel to act to mitigate a credible threat that an unmanned aircraft system or unmanned aircraft (drone) poses to the safety or security of facilities or assets identified regarding potentially impacted airspace located in the United States, through a risk-based assessment.

"The actions authorized in subsection (a) are the following:

- (A) During the operation of the unmanned aircraft system, detect, identify, monitor, and track the [drone], without prior consent . . .
- (B) Warn the operator ....
- (C) Disrupt control of the [drone], without prior consent ....
- (D) Seize or exercise control of the [drone].
- (E) Seize or otherwise confiscate the [drone].
- (F) Use reasonable force, if necessary, to disable, damage, or destroy the [drone]."\*

<sup>\*</sup> Preventing Emerging Threats Act of 2018, Pub. L. No. 115–254, § 1602 (b), 132 Stat. 3522–3523 (2018), <u>https://www.congress.gov/115/plaws/publ254/PLAW-115publ254.pdf</u>.

At PERF's meeting, a number of key participants made presentations, including the following:

- John Miller, NYPD Deputy Commissioner of Intelligence and Counterterrorism, provided analysis of threats by international terrorists as well as "homegrown" terrorists who have been sharing information about drone technologies online.
- Terence Monahan, NYPD Chief of Department, described the challenges New York City is facing in protecting against drone attacks at events like the New Year's Eve celebration at Times Square.
- Cathy Lanier, former Chief of Police in Washington, D.C., and currently Vice President for Security for the National Football League (NFL), worked with federal agencies to protect against drone attacks and other threats at the 2019 Super Bowl in Atlanta and offered her perspectives on providing security at those types of major events.
- Brendan Groves, Senior Counsel to the Deputy Attorney General at the DOJ, detailed the current limits of local police authorities to prevent or respond to drone attacks.
- Angela Stubblefield, Deputy Associate Administrator for Security and Hazardous Materials Safety at the FAA, discussed the FAA's role in regulating drones, especially with respect to federal and local law enforcement agencies' authorities.

## WE HAVE A MAJOR GAP IN OUR RESPONSE TO USE OF DRONES FOR TERRORISM

NYPD Deputy Commissioner of Intelligence and Counterterrorism John Miller

If you think about the changing modes of terrorism and changes in technology, those changes are extraordinarily quick. The threats and the technologies change by the day. But if you think about the speed of policy development and legislation, that's much slower.

The NYPD has a very deep bench and a big bag of tools. So there's very little that happens that we can't reach into the tool bag and say, "We can handle this." We have bomb squads, hostage teams, hazardous materials (hazmat) people. But the drone issue is moving quickly. In 2014, we had 82 drone incidents in New York City. In 2016, we had 416. And in 2018, up until September, we had 1,649 drone incidents.

Most of these incidents are just hobbyists playing with drones, and they fall out of the sky, and sometimes they land in sensitive places. Usually when we find the wreckage of a drone, we can find the operator just by watching the video that the drone was capturing. If you rewind to the beginning of the video, usually it includes images of the drone operator, and by looking at the background, you can figure out where he was standing and find out who he is.

### Terrorists have been using drones since 2013

If you look at terrorists' use of drones, the first ISIS drone use started around 2013. Sometimes people say, "We need to stop talking about drones, because we're going to give the terrorists ideas." But the police leaders in this room know that the terrorists have already figured out that drones are a major new tool. Drones are all over terrorists' propaganda, their films. ISIS, in particular, has bragged about their use of drones in the field, and their videos include instructions about how to use drones to kill people.

Our bad guys in the United States are watching these terrorist propaganda videos. It is simply a matter of time before this propaganda reaches the "lone wolf" types over here.

### Drones offer multiple new capabilities for terror

From a terrorist's standpoint, drones are accessible. Anyone can buy them. And they work. You don't need a suicide bomber if you can use an inanimate object to fly your bomb into your target. You don't have to waste an operator with a suicide attack. And it's repeatable; you can do this over and over again. You can drop the ordnance and blow something up, and maybe even keep the drone. Or if you blow up the drone with the ordnance, you can just buy another drone.

Penetration is another major advantage of drones. Drones can get inside to where a suicide bomber can't go or where a vehicle bomber may be blocked. All of our bollards and delta barriers and security checkpoints will have trouble interdicting a flying object.

Another advantage of drones is perseverance, in terms of surveillance. You can leave a drone up for great lengths of time and collect valuable intelligence about a target. Helicopters are very expensive, and airplanes don't take very good pictures because of the altitude, but drones are ideal in many situations.

Another key use of drones has been reconnaissance, targeting, and guidance, where the drone will actually serve as the eyes and ears—for example, guiding a large vehicle bomb through the streets to avoid barriers or obstacles.

And the psychological impact is at the heart of this discussion, because we know about this threat, we're aware of it, but there's very little we can do about it. It's relatively low tech, very cheap, and extremely high impact.

## We need to step up to this major challenge and do it quickly

We won't see big headlines until the first drone attack happens in the United States or in London or Paris. In New York City we have major events with hundreds of thousands of people attending and so many other events like baseball games with tens of thousands. Right now, when we learn about a drone, we can only go out and try to find the operator, but we can't stop a drone with a payload in mid-flight. It's a real gap for us.

What really keeps me up at night is the fact that drones are extraordinarily simple pieces of technology for the bad guys to use. But stopping drones is an extremely complicated issue for law enforcement to navigate. We have to operate under all the rules, but they don't have any rules slowing them down.

### Technologies can disrupt or disable threatening drones, but local police agencies can't buy it

The manufacturers won't sell the technology to local police, because they know the law says we don't have the authority to use it. And there are reasons behind that. Technology meant to disrupt a drone can have the unintended impact of disrupting flight safety systems onboard airplanes or air navigation services. So we have to avoid creating a safety hazard by trying to address a potential security threat.

We need to get into the business of having people with the training and technology to interrupt radio signals for a limited purpose over a limited area, and understanding what the limits of that are, what's too high, too low, too wide, and too strong a signal, so you don't affect other things.

### We're in a race to implement technologies before we suffer a major attack

This is very complex territory, but it's not insurmountable. This is a thing where the right experts, the right legislation, and the right authorities given to the people with the right training can make this possible. This is reachable.

But we are nowhere close to it now, and the cat is out of the bag. The bad guys know the game, and they don't have any rules, so we're about to see this happen. It's not if, it's when, because the terrorist groups are advertising it toward the lone wolves now.

The new legislation last October moved us forward, but we need to move much further. Whether we do that before the bad thing happens, or because a bad thing happened, is really up to us.

## WE HAVE HUNDREDS OF MAJOR EVENTS IN NYC, SO WE CAN'T RELY ON FEDERAL AGENCIES TO PROTECT US EVERY TIME

### NYPD Chief of Department Terence Monahan

If you think about the potential for an attack against your city using a drone, and if you aren't petrified by what John Miller just told us, you're kidding yourself.

So far, the United States has been lucky; we haven't seen drone attacks. But it's happened around the world, so it's something that we need to get ahead of. We need to figure out how to mitigate this threat.

The NYPD focused on this last year for the New Year's Eve event at Times Square. This was the first time we tried to detect drones. We bought some technology: the AeroScope<sup>80</sup> from FLYMOTION, which is a device that detects drones made by DJI,<sup>81</sup> the leading manufacturer of drones, which represents about 80 percent of the drones market.

With our AeroScope up, if a DJI drone came into the space that we had geofenced around Times Square, we would know about the drone, and we would know where the operator was. So we had teams set up at different locations around Times Square, and if we detected anyone putting a drone up in the air, we sent the response team out to find the operator.

But under current laws, that's all we could do—grab the drone operator and get him to bring his drone down. There was nothing we could do legally to prevent the threat from happening in the first place or to take direct action against a threat.

Last October, Congress passed H.R. 302, which for the first time gives federal agencies the authority to seize control of threatening drones or destroy them. There are different approaches to how this might work, like putting up an electronic "shield" that would disrupt drone signals or "spoofing" a drone, where you take control of it.

These anti-drone technologies haven't really been tested in urban environments in the United States. They have been tested in other countries, and our Department of Defense has some of these technologies.

<sup>80. &</sup>quot;AeroScope – DJI Drone Detection System," FLYMOTION, accessed February 12, 2020, https://flymotionus.com/news/aeroscope-dji-drone-detection/.

<sup>81. &</sup>quot;DJI Camera Drones," DJI, accessed February 12, 2020, https://www.dji.com/camera-drones.

But for the NYPD and other police departments, the problem is that I cannot buy this technology. I can't use this technology. We can only do it with our federal partners at DOJ and DHS. But when you look at New York City, I've got the Yankees, I've got the Mets, I've got all sorts of major events where we have large groups of people to protect against drone attacks. So for me to have to drag in my federal partners to use anti-drone technologies when we have major events almost every day, that's going to be a problem for us. We can't rely on federal agencies to come out and help us every time.

## TODAY'S DRONE DETECTION TECHNOLOGY WILL NOT ALWAYS GIVE US ENOUGH ADVANCE WARNING

Senior Vice President for Security Cathy Lanier, NFL

I started my first counter-drone working group as Chief of Police in Washington, D.C., in 2011. So it's very frustrating to me that eight years later, we still don't have a solution, and it's just as frustrating for me now at the NFL.

With the new legislation passed in October 2018 allowing DHS and DOJ to test anti-drone technologies, we had an opportunity in February 2019—with the Super Bowl in Atlanta—to work with the Federal Bureau of Investigation (FBI) and DHS and DOJ and FAA to deploy drone countermeasures, for the first time ever on U.S. soil.

If you've never been to a Super Bowl, it's more than just the game itself. It's 10 days of events in about 26 different venues. On game day, there was an entire team of people to mitigate any drones that came into the airspace. We had the ability to track drones up to 50 miles out, and on game day our no-fly zone was 30 miles out. And they could mitigate a threat within a one-mile to three-mile radius.

There were 74 drones observed in the days leading up to the Super Bowl. They were running after drones constantly. There were 10 drones observed on game day, and in fact the Blue Angels flyover was disrupted by a drone. The Blue Angels actually had to elevate their altitude because of a drone.

The technology we were using, the Air Force Research Lab's Ninja,<sup>82</sup> essentially redirects a drone to a different home. So if a nefarious drone comes into the airspace, the system would identify, track, locate, and then redirect it to a different home base, where there would be a hazmat team of bomb technicians waiting.

<sup>82. &</sup>quot;Catching RPAs Using Actual Nets and Other AFRL Innovations at Lab Day," *Air Force Magazine*, May 19, 2017, <u>http://www.airforcemag.com/Features/</u> <u>Pages/2017/May%202017/Catching-RPAs-Using-Actual-Nets-and-Other-AFRL-Innovations-at-Lab-Day.aspx</u>.

All of that sounded good, but the Ninja was only estimated to have a success rate of 50 to 60 percent for this Super Bowl event because of all the other RF activity going on that can interfere with the Ninja's radio signals.

So I started thinking, "What if a drone comes in and we get word that it's one of the 40 percent that does not get intercepted? Some drones can travel at more than 100 miles per hour, so we might only have three to five minutes to react and disable the drone. We have hundreds of thousands of people in all these open areas and heavy queue lines. There is no protective measure I can take in just a few minutes. For example, would it make sense to open all the doors and pull people inside the stadium? That might just scare people and cause a stampede.

Even disseminating word about the threat to all of the police and security people would be impossible in three to five minutes. We had dozens of police departments involved, 25 different federal law enforcement agencies, and 6,000 private security guards from four different companies. How are we going to communicate that we've got a threat arriving in three to five minutes? There were four different radio systems with 14 to 16 different radio channels being used at any given time. We had 13 different command centers operating at the Super Bowl, so which command center gets the word? We asked the smart analysts at the FBI to put together a graphic showing our communications plan, and they produced a plan that was well thought-out, but the reality was that there was no preventive measure that we could have employed, period.

## DOJ expert Brendan Groves explains the limits of local police agencies' legal authorities on drones

At PERF's conference, Brendan Groves, Senior Counsel to the Deputy Attorney General at the DOJ, explained the various types of counter-drone technologies that exist and what state and local law enforcement agencies can and cannot do with these capabilities.

There are two core capabilities in counter-drone technology: **detection** and **mitigation**.

Detection of drones: What can state and local police do, legally?

There are two basic categories of drone detection systems:

1. RF detection – Most drones are controlled from the ground by an operator holding a controller device. The controller communicates with the drone via radio signals. Thus, one type of drone detection technology scans the RF spectrum to identify a drone and its controller.

- 2. Non-RF detection These tools use other approaches to detecting drones, such as
- radar-based systems;
- acoustic systems that can "hear" a drone in the air and identify the make and model of the drone, with varying levels of precision;
- sophisticated cameras, with electro-optical and thermal imaging.

In general, local police can use non-RF capabilities, provided that any required regulatory approvals are obtained. Law enforcement agencies interested in using these tools must conduct a thorough legal review. For instance, agencies must obtain a license from the Federal Communications Commission (FCC) before obtaining or using a radar. If the radar is installed near an airport, the local agency should also contact the FAA and ensure it will not interfere with airport operations.

When using drone detection capabilities, Groves recommended that agencies consider using and integrating multiple methods—combining radar with electro-optical and infrared (EO/IR) cameras or combining lawful RF detection tools with acoustic sensors, for instance. This "system-of-systems" approach reduces the risks inherent in relying on any single sensor, which is unlikely, standing alone, to detect drones with perfect accuracy. Sensors work best in combination.

**RF detection tools present additional complications**. Before purchasing or using these tools, law enforcement agencies must conduct a detailed legal review. The tool must comply with federal and state electronic surveillance laws, such as the federal Wiretap Act (18 U.S.C. §2511) and Pen/Trap Act (18 U.S.C. §3121 et seq.). In general, these laws require a warrant or court order before anyone, including local, state, and federal law enforcement agencies, may intercept "electronic communications." Violations of the electronic surveillance laws are punishable by criminal and civil penalties.

Some vendors may claim their technology is legal because it is purely "passive" and does not obtain the "content" of communications. That may be misleading, because the federal Pen/Trap Act prohibits the interception of *non*-content information associated with electronic communications. If you imagine RF signals as a letter, non-content information would be the information on the outside of the envelope: the addresses of the sender and recipient. Violations of the Pen/Trap Act are serious and may give rise to criminal and civil liability.

#### Mitigating threatening drones: What can state and local police do?

As with detection of drones, there are two categories of devices that can mitigate drone threats:

1. Kinetic—These tools use physical force of some kind to stop the drone (i.e., a net gun or an interceptor drone).

2. Non-kinetic—These tools use a variety of non-physical means to disable or redirect the drone, such as jamming, hacking, and spoofing the electronic controls of the drone.

As a general matter, outside of truly exigent circumstances, the use of any mitigation tool by local or state law enforcement agencies probably is illegal.

Federal law makes it a crime to disable or destroy an aircraft—and Congress has arguably defined "unmanned aircraft" as a type of aircraft. (18 U.S.C. § 32 Destruction of aircraft or aircraft facilities)

What if the drone is simply hacked and redirected, instead of disabled or destroyed? Not so fast: Certain companies sell systems capable of taking control of drones by hacking their onboard computer systems. But federal laws make computer hacking a crime. (18 U.S.C. § 1030 Fraud and related activity in connection with computers) Second, many other companies sell systems capable of jamming the signals between drones and their controllers. However, FCC laws and regulations strictly prohibit jamming, unless authorized by the FCC.

# TECHNICAL ISSUES WITH DRONES QUICKLY GET COMPLICATED

Angela H. Stubblefield, FAA Deputy Associate Administrator for Security and Hazardous Materials Safety

### Remote identification

The FAA is working as expeditiously as possible to implement a remote identification rule to address many of the concerns regarding unauthorized UAS operation. Remote identification will enable threat discrimination by providing information about the UAS and the current location of its ground control station, which will facilitate effective, real-time law enforcement response, education, and civil or criminal enforcement (or both)—all of which will substantially reduce future clueless or careless operations.

### Local police authority in exigent circumstances

UAS cannot be legally operated in a way that endangers individuals, property, or other aircraft. These types of UAS operations may also violate applicable state and local laws such as assault, criminal trespass, or injury to persons or property. Locating the operator to safely land the unauthorized UAS is optimal as it provides the opportunity to discern operator intent and provide education or enforcement (or both) on applicable laws and regulations. The FAA cautions against the use of active drone detection or mitigation technologies without consulting legal counsel for a thorough evaluation of the legal and operational risks.

### Technical limitations of counter-drone technologies

The impact of some UAS mitigation systems could pose a greater threat to other aircraft, people on the ground, and air navigation services and infrastructure than the unauthorized UAS threat they are intended to mitigate. For example, not all counter-UAS technologies are able to target only noncompliant, threatening UAS and could impact an authorized UAS operation or degrade performance of onboard manned aircraft systems or ground-based communications, navigation, or surveillance infrastructure. Furthermore, some UAS react to counter-UAS systems in ways that could endanger other aircraft or people on the ground.

## Educating Drone Hobbyists to Reduce the Number of Unauthorized Drones at Major Events

Many participants at PERF's conference noted that public education is a key part of stopping unauthorized drone use. This has public safety implications, because it is difficult enough for law enforcement agencies to protect against drone attacks at large public events. It becomes more difficult if the skies are cluttered with "innocent" drones being flown by hobbyists. If police can reduce the large numbers of unauthorized drones at public events, it will help them to focus on the small number of drones that may be a threat.

"[Because] local law enforcement is prohibited from using counter-drone technology, education is all we really have right now to mitigate errant flights from the clueless, the careless and the criminal," said Detective Vince D'Angelo of the Las Vegas (Nevada) Metropolitan Police Department. "I have encountered a lot of people who say, 'Oh, I didn't know I'm not allowed to fly here,' or 'I didn't think it was a big deal.' In Las Vegas we had a person who landed a drone on an active airport runway. We worked closely with the FAA on it, and they just levied a \$14,700 fine on that individual."<sup>83</sup>

The FAA believes that public education and outreach are key to reducing the incidents of errant UAS operations in the National Airspace System. In addition, the FAA works closely with and stands ready to assist federal, state, local, tribal and territorial law enforcement agencies through its Law Enforcement Assistance Program, or LEAP. The FAA has published an extensive online Public Safety and Law Enforcement Toolkit<sup>84</sup> designed to assist law enforcement and public safety entities in operating and responding to situations involving UAS.

## CITIES CAN BAN TAKEOFFS AND LANDINGS OF DRONES ON THEIR PROPERTY, AND WE WOULD LIKE TO HAVE REMOTE IDENTIFICATION

NYPD Lieutenant in Charge of UAS Countermeasures Art Mogil

One of the biggest challenges is how to make people aware of how drones can be dangerous. We've had an exponential increase in the number of reported drone detections. We have had approximately 1,600 illicit drone detections called into 911 just in the past three years, and there are probably 100 times as many incidents not being called in.

<sup>83. &</sup>quot;Video Emerges of Drone Flying Dangerously Close to Plane Landing in Las Vegas," AJC.com, February 4, 2018,

https://www.ajc.com/news/national/video-emerges-drone-flying-dangerously-close-plane-landing-las-vegas/H2D7jqsX6ARiPduz9nVS2I/.

<sup>84. &</sup>quot;Public Safety and Law Enforcement Toolkit," Federal Aviation Administration, last modified September 4, 2019, <u>https://www.faa.gov/uas/public\_safety\_gov/public\_safety\_toolkit/</u>.

### Banning drone takeoffs and landings in certain locations

We've been trying to approach this from the standpoint of what local police agencies can do. In many areas, local municipalities have laws that go beyond federal laws. Right now we have on our books an administrative code violation called Unlawful Avigation.<sup>85</sup> This city law prohibits anyone from flying an unmanned aircraft system anywhere within the five boroughs or territories of New York City by restricting takeoffs and landings unless it's been specifically approved by the Port Authority of New York and New Jersey or the New York City Department of Transportation. And the law also gives the Police Commissioner of New York City the authority to issue rules based on this law.

### Automatic identification of drones and operators

Also, we interpret section 366 of the new FAARA as requiring the FAA to provide state and local police with guidance and resources on how to identify and respond to public safety threats posed by drones. We would like to see some kind of system so we are able to identify who is operating a drone. In New York City, we have 8.5 million people in a 300-square-mile area. Because everything is so dense, in New York we'll probably only have seconds to respond to a threat; to be generous, you could say we'll have a minute. So that means that some kind of designated decentralized authority needs to be made at a local level, to be able to respond that quickly.

**Angela H. Stubblefield**: If I could comment on what Art said, yes, states and localities generally have the authority to regulate takeoffs and landings of drones within their jurisdictions; however, the FAA maintains responsibility over the airspace, and state and local restrictions on takeoff and landing cannot be so restrictive that they effectively block all access to the airspace.

## LOCAL POLICE ARE THE BOOTS ON THE GROUND WHO WE NEED TO PROTECT PEOPLE AT LARGE GATHERINGS

Kenneth Edmonds, Director, Government Relations and Public Policy, National Football League

The bill that Congress passed in 2018 was a major step forward, but it is not sufficient. What needs to happen now, before it's too late, is that we need to put a framework in place where the authority that has been extended to DHS and DOJ can be extended to local law enforcement, with the proper supervision, training, and best practices. DHS, DOJ, and the FAA are our partners, but it's the local law enforcement agencies that are our boots on the ground.

<sup>85.</sup> Avigation in and over the city, New York City Administrative Code §10-126, http://ny.elaws.us/law/adc t10 ch1 sec.10-126.

Detection and mitigation of drone threats isn't a panacea, but they should be in the toolbox, because any time there's a regular season football game, a baseball game, a NASCAR event, or a marathon, we need to take steps to protect the tens or hundreds of thousands of people attending these mass gatherings.

## THE LAW ENABLES PRIVATE PROPERTY OWNERS TO PETITION THE FAA TO HAVE SENSITIVE LOCATIONS DESIGNATED NO-DRONE ZONES

#### Lisa Ellman, Executive Director, Commercial Drone Alliance<sup>86</sup>

I work with many clients, including Major League Baseball, which is fully aligned with the NFL on the points that have been made here today. I also work with many companies that are very focused on these UAS security issues. I represent commercial drone users, including the Commercial Drone Alliance as well as companies that are affected by drone uses.

There are many benefits to commercial drones, but all technologies can be used for good and for bad—and unauthorized drones present critical safety and security issues. The drone industry is working to bring technology solutions to these issues. We have talked a lot about remote identification, because until fall [2018], the FAA actually didn't have the legal authority to require remote identification of most drone operators. We supported giving the FAA the ability to regulate all UAS as necessary for safety and security, including requiring remote identification—and that law was changed late [in 2018].

Now that the FAA has that legal authority, the industry is working with the FAA to get a comprehensive remote identification framework implemented expeditiously. We need to be able to distinguish friend from foe and mitigate potential drone threats while enabling the commercial drone marketplace to expand safely and securely.

<sup>86.</sup> The Commercial Drone Alliance defines itself as "an independent 501(c)(6) nonprofit organization led by key members of the commercial drone industry. We work collectively to merge policy with innovation to create relevant rules for operation. We educate on the economic benefits, humanitarian gains, safe and responsible use and technology requirements of commercial drones.""Enabling Commercial Drones,"The Commercial Drone Alliance, accessed February 12, 2020, <u>https://www.commercialdronealliance.org/</u>.

### Letting property owners seek no-fly zones over their property

One thing we haven't mentioned yet today is section 2209 of the 2016 FAA Extension Act,<sup>87</sup> which required the FAA to develop a process through which private property owners can apply to have themselves designated no-fly zones, prohibiting or restricting drones from flying over their property. Private industry is very focused on this new authority and we are anxious to see the FAA implement it.

**Angela Stubblefield, FAA**: Yes, section 2209 of the FAA Extension, Safety, and Security Act of 2016 directs the FAA to establish a process to allow applicants to petition the Administrator of the Federal Aviation Administration to prohibit or restrict the operation of an unmanned aircraft in close proximity to limited categories of fixed site facilities. The FAA has initiated rule-making to implement this provision. This effort is expected to provide an opportunity for state and local governments as well as private sector entities to come to the FAA and ask for a 2209 designation over eligible facilities. Until the rule-making process is complete, the FAA may consider requests for Special Security Instructions implemented as temporary flight restrictions (TFR) based on national security interests by agreement between FAA and DOD or a U.S. federal security or intelligence agency pursuant to 14 C.F.R. § 99.7. Rule-making is necessary to establish a process for other entities to request similar assistance.

# Recommendations for preventing and responding to the malicious use of drones

There are few options for local police agencies interested in investing in anti-drone technologies. The FAA Reauthorization Act of 2018 provides new legal authority for federal agencies to identify and mitigate drone attacks; however, the 2018 law does not provide new authority to state and local police agencies to disable or destroy malicious drones.

## WHY ARE LOCAL POLICE BEING RESTRICTED?

Drone mitigation technologies exist, but they have not been thoroughly tested in urban environments in the United States. Technology meant to disable a threatening drone can have the unintended impact of disrupting other radio-based technologies, such as flight safety systems onboard airplanes or air navigation services. So federal lawmakers have been hesitant to authorize major changes in the status quo with respect to enabling state and local authorities to use these mitigation technologies.

<sup>87.</sup> The law allows for such bans or restrictions to be given to owners or operators of "critical infrastructure, such as energy production, transmission, and distribution facilities and equipment; oil refineries and chemical facilities; amusement parks; and other locations that warrant such restrictions." FAA Extension, Safety, and Security Act of 2016, Pub.L. 114–90, § 2209 (b)(1)(C), 130 Stat. 634 (2016), https://www.congress.gov/114/plaws/publ190/PLAW-114publ190.pdf.

## SIX ACTIONS THAT LOCAL POLICE AND SHERIFFS' AGENCIES CAN TAKE NOW

- 1. Use available technologies. Local police can purchase drone detection technologies that are not based on detecting the radio signals between a drone and its operator, taking care to understand the limitations presented by existing legal authorities. Potential tools available to local police include radar systems, acoustic sensors that can "hear" the sound of an approaching drone and in some cases even identify the model of drone, and camera systems.
- **2. Be aware that local police can take action against a clear terrorist threat.** Police have general authority to take action to protect the public in exigent circumstances. For example, in the case of a drone that is clearly being used in a terrorist attack, police can consider taking reasonable action to mitigate that threat, proportionate to the nature of the exigent circumstance and consistent with their agency's policies and procedures.
- **3. Restrict the use of drones over sensitive locations.** Local jurisdictions can enact laws prohibiting or restricting the takeoff or landing of drones at certain sensitive locations. Such restrictions can be very helpful, because many drone operators have no malicious intent, but their actions can be dangerous. It does not occur to them that their use of drones can make it more difficult for the police to protect the public.

For example, police see drones during major gatherings such as sports events and outdoor concerts, and they are kept busy trying to track down the drone operators and tell them they must land their drones and cease operations.

By strictly enforcing local ordinances against drone takeoffs and landings at certain locations, police may be able to sharply reduce the number of these "harmless" but problematic drone sightings. This will enable police to focus their attention on the drone sightings that might more likely involve an intent to do harm.

**4.** Request assistance from federal agencies to help manage extremely large or sensitive events. Police should not expect to receive federal help for all events that are large but routine,

such as major league baseball, football, or soccer games. But by requesting assistance where deemed necessary, local law enforcement agencies will highlight the need for additional resources and authorities in this area and present federal agencies with the opportunity to provide assistance to the extent that resources permit.

- **5. Contact federal, state, and local lawmakers.** Police chiefs, sheriffs, and other law enforcement agency leaders are well-respected experts on public safety issues whose views are given great weight by elected officials. Many lawmakers and policy makers have little or no awareness of the potential threats against the United States by malicious drones. Law enforcement officials can help sound an alarm and focus national, state, and local attention on these threats.
- **6. Report dangerous drone operations to the FAA.** The FAA is gathering data on these types of incidents.

## CONCLUSION. LOCAL LAW ENFORCEMENT AGENCIES ARE LEARNING TO USE DRONES; NOW THEY MUST FOCUS ON STOPPING MALICIOUS DRONE ATTACKS.

Police agency use of drones for public safety purposes and police agency efforts to combat the malicious use of drones are two entirely different matters, which is why PERF's conference on drones required two days of discussions.

## **Police use of drones**

On the first day, we discussed the many ways in which federal, state, and local law enforcement agencies can use drones to advance public safety. Drones can assist with search and rescue missions, disaster response, monitoring of crowds at large public events, traffic collision reconstruction, crime scene reconstruction, and investigating armed and dangerous suspects.

## PRIVACY ISSUES

The use of drones by police raises important questions about privacy and trust. Many people have understandable privacy concerns about anyone, including police agencies, having the technical capability to fly small, lightweight devices—which typically are equipped with video cameras—almost anywhere they wish. And many people are concerned that police agencies may use drones to obtain evidence in ways that violate the Fourth Amendment ban on unreasonable searches and seizures.

These issues can be complex, but they are similar to issues that police executives have managed in the past with regard to other new technologies. The key is to begin the process by soliciting the views of your communities and involving interested stakeholders in the development of policies and implementation plans. Police agencies considering the use of drones for public safety should hold public hearings, and they should provide other mechanisms for community members to share their views—such as a dedicated email address or other online system to accept comments, because not everyone has time to attend public hearings. Police should present their initial plans for a drone program, listen to any concerns of community members, revise their programs as appropriate, and move forward with a drone program at a deliberate pace. This report details many of the issues that police agencies should address, such as what types of incidents and situations drones will be used for, what (if any) video or other information will be collected and stored, how data will be protected, and who will have access to it.

## LARGER COSTS AND EVEN LARGER BENEFITS

The public safety benefits that have already been documented and the cost/benefit analyses that many agencies have completed indicate that in many environments the cost of drone use is worth the investment. Drone programs can be expensive—but if the alternative is using helicopters or airplanes, drones generally are much less expensive. Drones also can be much more effective than other aircraft because drones are smaller, quieter, and less disruptive and can hover at close range to the persons or situations being observed.

## Malicious use of drones by terrorists and other criminals

On the second day of PERF's conference, participants addressed the other aspect of the issue of drones and policing, which is different and far more urgent: how federal, state, and local law enforcement agencies must quickly undertake intensive efforts to protect against the threat of criminals, including terrorists, using drones to commit crimes.

## UNTHINKABLE THREATS OF MASS KILLINGS

The NYPD's top counterterrorism official, John Miller, told participants at PERF's meeting that it is only a matter of time before terrorists try to use drones in a potentially devastating attack—for example, at a World Series Game, outdoor concert, New Year's Eve or Fourth of July gathering, or other event where tens or hundreds of thousands of people have gathered. International terrorist groups already have been posting videos online demonstrating how such an attack could be carried out, Miller warned.

## A NEW FEDERAL LAW FINALLY TAKES THE FIRST STEP

Even though malicious drone threats have been recognized as an urgent issue for years, many law enforcement agencies are just now beginning to consider how they might prevent such attacks, because until recently, federal laws criminalized taking countermeasures. In October 2018, Congress enacted a new law giving certain federal agencies in the DOJ and the DHS the legal authority to use technologies that can detect the presence of drones; track them; quickly learn the identity of their operators; and disrupt, seize control of, or destroy potentially threatening drones.

## LOCAL POLICE ARE LARGELY LEFT OUT OF THE NATIONAL RESPONSE

Unfortunately, the new law does not provide this new legal authority to state and local police agencies. This omission is largely due to the fact that use of these counter-technologies, especially the technologies for disrupting a drone threat, can be complicated and difficult and the results can be uncertain. Clumsy or unskilled use of some technologies could result in public safety disasters, so the federal action by Congress to date has been limited in scope.

## local police do have some authority to act

One of the most effective systems for detecting drones is based on detecting the radio signals between a drone and its operator. Such RF-based systems can now be used only by federal law enforcement authorities.

Local police departments, however, are legally authorized to use certain other types of technologies to detect drones, such as radar-based systems, acoustic sensors that can "hear" the sound of an approaching drone and in some cases even identify the model of drone, and camera systems.

Local jurisdictions also have the authority to prohibit or limit takeoffs and landings of drones at certain sensitive locations. Thus, cities can prevent drones from flying near large gatherings such as major league sports games and outdoor concerts. By enacting and strictly enforcing such ordinances, local police may be able to sharply reduce the numbers of drones at such events so they can better focus their attention on the drone sightings that may more likely be malicious.

## NEW TECHNOLOGIES ARE FINALLY BEING TESTED BY FEDERAL AGENCIES

Federal agencies, with their new legal authorities, have begun to use drone detection and mitigation technologies—sometimes in conjunction with state and local police at major events designated as Special Event Assessment Rating (SEAR) events and National Special Security Events (NSSE). These designations include events such as the Super Bowl, national political conventions, and international summits.

However, local police executives at PERF's conference noted that the vast majority of major events in their cities—even events attended by 100,000 people or more—do not receive these special security designations. In addition, there are not nearly enough federal officials to cover all of the local events that could be targeted by a lone-wolf terrorist or terrorist group for a drone strike.

## DANGER LEVEL: HIGH

Thus, the current level of danger is high, officials said at PERF's conference. State and local police should begin the process of acquiring drone detection devices that they can lawfully use, learning how to use them, and working to protect major events against drone attacks unilaterally and in concert with federal law enforcement officials. The drone strikes against oil facilities in Saudi Arabia in September 2019, which temporarily disrupted approximately half of that kingdom's oil production capacity, demonstrate how much harm can be done by the malicious use of drones.

The United States must not wait until it suffers a drone attack to undertake large-scale efforts to develop systems by law enforcement agencies at all levels of government for (1) identifying drone threats and (2) mitigating such threats in real time.

Local law enforcement agencies have sharply limited authority on this issue. But local police can take six types of actions now:

- **1. Use available technologies.** Local police can purchase drone detection technologies that are not based on detecting the radio signals between a drone and its operator. Tools available to local police include radar systems, acoustic sensors that can "hear" the sound of an approaching drone and in some cases even identify the model of drone, and camera systems.
- **2. Local police can take action against a clear terrorist threat.** Police have general authority to take action to protect the public in exigent circumstances. In the case of a drone that is clearly being used in a terrorist attack, police can consider taking reasonable action to mitigate that threat, proportionate to the nature of the exigent circumstance and consistent with their agency's policies and procedures.
- **3. Restrict the use of drones over sensitive locations.** Local jurisdictions can enact laws prohibiting or restricting the takeoff or landing of drones at certain sensitive locations.

By strictly enforcing such ordinances, police can sharply reduce the number of "harmless" but problematic drone sightings at large public gatherings. This will enable police to focus their attention on the drone sightings that might more likely involve an intent to do harm.

- **4. Request assistance from federal agencies to help manage extremely large or sensitive events.** By requesting assistance often, local law enforcement agencies will highlight the need for additional resources and authorities in this area and present federal agencies with the opportunity to provide assistance to the extent that resources permit.
- **5. Contact federal, state, and local lawmakers.** Many lawmakers and policymakers have little or no awareness of the potential threats against the United States by malicious drones. Law enforcement officials can help sound an alarm and focus national attention on these threats.
- **6. Report dangerous drone sightings to the FAA.** The FAA is gathering data on these types of incidents, which can be used to demonstrate the magnitude of the problem to Congress.

## APPENDIX A. CONFERENCE PARTICIPANTS

PERF, the COPS Office, and DHS convened this two-day conference on February 20–21, 2019, in Washington, D.C., to discuss the policy and operational issues regarding the implementation and use of drones. The titles listed here reflect attendees' positions at the time of the conference.

Jon Adler Director, Bureau of Justice Assistance

**Randolph Alles** Director, U.S. Secret Service

Nino Amirfar Chief, Turlock (CA) Police Department

Shawn Andersen Deputy Chief, Las Vegas (NV) Metropolitan Police Department

Patrick Archbald Deputy Chief, University of Massachusetts Police Department

## Margaret Baldinger

Captain, Waterfront Commission of New York Harbor

### Nick Barbknecht

Advisor, Intergovernmental Affairs, U.S. Department of Homeland Security

**Brent Barbour** Captain, Norman (OK) Police Department

Matthew Barger Program Analyst, U.S. Department of Homeland Security

**Charles Barstow** Captain, City of Milton (GA) Police Department James Basinger Major, Pennsylvania State Police

### **Ryan Berry**

Policy Advisor, Office of the Secretary of Defense, Homeland Defense Integration & Defense Support of Civil Authorities

### **Stephen Birnie**

Commander, University of South Carolina Division of Law Enforcement and Safety

### Travis Boltjes

Colonel, U.S. Department of Defense

#### **Christopher Boness**

Professional Staff Member, Senate Homeland Security and Governmental Affairs Committee

#### **Trevor Bosco**

Detective, Waterfront Commission of New York City

**Michael Bouchard** Sheriff, Oakland County (MI) Sheriff's Office

## Karen Box

Investigator, Robertson County (TX) Sheriff's Office

**Romeo Brandani** Special Agent, U.S. Secret Service

### **Josh Bronson**

Director of Training, International Association of Campus Law Enforcement Administrators

### Adam Brown

Sergeant, Surprise (AZ) Police Department

**Scott Brunner** Deputy Assistant Director, Federal Bureau of Investigation

**Maggie Brunner** Program Director, National Governors Association

**Thurston Bryant** Special Assistant to the Director, Bureau of Justice Assistance

**Jim Bugel** Vice President, AT&T Public Safety Solutions

**Tim Burkett** Major, Louisville (KY) Metro Police Department

Helene Bushwick Supervisory Policy Analyst, Office of Community Oriented Policing Services

**Jeffrey Cannon** Section Chief, Federal Bureau of Investigation

Jeffery Carroll Assistant Chief, Metropolitan Police Department, Washington, D.C.

Joe Cecile 1st Deputy Chief of Police, Syracuse (NY) Police Dept

**Neil Cervenka** Lieutenant, Turlock (CA) Police Department

**Shawn Chamberlain** Chief, Lee County (FL) Port Authority

### **Mark Champoux**

Principal Deputy Assistant Attorney General, U.S. Department of Justice, Office of Legal Policy

### **Rob Chapman**

Deputy Director, Office of Community Oriented Policing Services

### **Brett Chapman**

Social Science Analyst/Policing, National Institute of Justice

**Don Chapman** Staff Sergeant, Vancouver (BC) Police Department

### **RaySean Clark**

Branch Chief, Policy, Doctrine, and Tactics, Federal Protective Service, U.S. Department of Homeland Security

### Kym Craven

Executive Director, National Association of Women Law Enforcement Executives

#### Kelbi Culwell

Associate Director, U.S. Department of Homeland Security

#### Pat Cunane

Detective, Gloucester Township (NJ) Police Department

#### **Jim Daly**

Program Manager, Virginia Center for Policing Innovation

#### Vince D'Angelo

Detective, Las Vegas (NV) Metropolitan Police Department

### **Ed Daniel**

Captain, Montgomery County (MD) Police Department

# **Al Davis**

Deputy Agency Director, Texas A&M Engineering Extension Service

# John Dejarnette

Organizational Development Coordinator, University of Cincinnati

# **Kathleen Deloughery**

Program Manager, DHS Science and Technology Directorate

# **Julie Dickerson**

Attorney Advisor, Office of Law and Policy, National Security Division, U.S. Department of Justice

# **Michael Diekhoff**

Chief, Bloomington (IN) Police Department

### **Brian Dorow**

Deputy Assistant Secretary, U.S. Department of Homeland Security, Office for State and Local Law Enforcement

# John Drake

Deputy Chief, Metropolitan Nashville (TN) Police Department

# **Matt Dummermuth**

Principal Deputy Assistant Attorney General, Office of Justice Programs

## Jeff Ebersole

Assistant Director, International Association of Chiefs of Police

# **Veronica Ector**

Chief of Staff, Homeland Security Investigations

## Joshua Ederheimer

Deputy Director, Federal Protective Service, U.S. Department of Homeland Security

# **Kenneth Edmonds**

Director, Government Relations and Public Policy, National Football League

#### **Timothy Ehrenkaufer**

Sergeant, Daytona Beach (FL) Police Department

#### **Chris Elliott**

Lieutenant, University of Cincinnati

#### Lisa Ellman

Executive Director, Commercial Drone Alliance and Hogan Lovells

# Sarah Estill

Social Science Analyst, Office of Community Oriented Policing Services

**Joe Eyerman** UAS Researcher, RTI International

# Lori Farrell

Air Traffic Security Coordinator, Federal Aviation Administration

#### **Jason Figueroa**

Lieutenant, Gila River (AZ) Police Department

# **Victor Galladora**

Sergeant, Montgomery County (MD) Police Department

#### **Dan Gettinger**

Co-Director, Center for the Study of the Drone

#### **Arthur Gibson**

Security Specialist, U.S. Department of Homeland Security

# **Brent Goodwin**

Deputy Assistant Director, Homeland Security Investigations

# Donald Goulet

Captain, Cumberland County (ME) Sheriff's Office

# **Louis Grever**

Executive Director, Association of State Criminal Investigative Agencies (ASCIA)

# Vanessa Grigsby

Deputy Chief, Leesburg (VA) Police Department

# **Ryan Grothe**

Technician, Denver (CO) Police Department

# **Brendan Groves**

Senior Counsel to the Deputy Attorney General, U.S. Department of Justice

#### Samir Guerrero

Major, Miami Beach (FL) Police Department

#### Samuel Hall

Assistant Chief of Police, Irving (TX) Police Department

# **Brodny Hall**

Senior Federal Air Marshal, Transportation Security Administration Federal Air Marshal Service, Joint Vulnerability Assessments Unit

# **Kurtis Hallstrom**

Commander, Saint Paul (MN) Police Department

# **Chris Hardee**

Chief Counsel for Policy, National Security Division, U.S. Department of Justice

#### Joe Heaps

Senior Physical Scientist, National Institute of Justice

#### **Brian Henderson**

Captain, Volusia County (FL) Sheriff's Office

# **Tim Herlocker**

Former Director, Emergency Operations Center, New York City Fire Department

# **Robin Hicks**

Director, Homeland Defense Capability Development, Office of the Under Secretary of Defense for Research and Engineering

# **Melvin High**

Sheriff, Prince George's County (MD) Office of Sheriff

# Gary Hill

Special Agent in Charge, Drug Enforcement Administration

#### Joshua Holtzman

Director, National Security Programs and Incident Response, Federal Aviation Administration

# Sean Hook

Executive Director, USAF/FAA Airspace Management, Leidos (FAA Contract Support)

# **Patrice Howard**

Social Science Research Analyst, Office of Community Oriented Policing Services

# **Travis Hull**

Sr. Public Safety Products Advisor, First Responder Network Authority Mary Hyland Deputy Executive Director, U.S. Customs and Border Protection

Joanna Ip Assistant Director, Homeland Security Investigations

**Hyla Jacobson** Research Assistant, Police Executive Research Forum

# **Elise Jarvis Wilson**

Director, Law Enforcement Outreach and Community Security, Anti-Defamation League (ADL)

**Sean Jennings** Captain, Pennsylvania State Police

Jeffrey Johnson Commander, Roanoke County (VA) Police Department

#### **Jerrold Jones**

High Tech Crime Specialist, National White Collar Crime Center

John Jordan Sergeant, Suffolk County (NY) Sheriff's Office

Paul Joyal Managing Director, National Strategies

Adam Kass Intern, Police Executive Research Forum

# Nick Katz

Sergeant, Gloucester Township (NJ) Police Department

# **Phil Keith**

Director, Office of Community Oriented Policing Services

#### **Brian Keith**

Protective Security Advisor, DHS Cybersecurity and Infrastructure Security Agency (CISA)

#### **Chris Kelenske**

Lieutenant Colonel, Michigan State Police

#### **Keith Kelley**

Captain, Athens-Clarke County (GA) Police Department

# Adam Kemerer

Research Assistant, Police Executive Research Forum

#### **Jason Kepp**

Division Director, Federal Protective Service, U.S. Department of Homeland Security

#### Kyle Kinnaman

Police Officer, City of Mesa (AZ) Police Department

### **Brett Kooharian**

Corporal, Arlington County (VA) Police Department

# Frank Korinek

Director of Governmental Affairs, Motorola Solutions, Inc.

**Scott Kurfis** Special Agent, U.S. Secret Service

**Christian Kuyper** Commander, Roanoke County (VA) Police Department

**Michael Laird** Corporal, Arlington County (VA) Police Department

**Donald Lambert, Jr.** Captain, Henrico County (VA) Police Division

Anthony Landato Lieutenant, City of Mesa (AZ) Police Department

**Cathy Lanier** Senior Vice President, National Football League

**David Lee** Supervisory Asylum Officer, U.S. Department of Homeland Security

**Todd Limerick** Sergeant, Dallas (TX) Police Department

Tatiana Lloyd-Dotta Intern, Police Executive Research Forum

Sasha Lohn General Counsel, St. Petersburg (FL) Police Department

**Anthony Loperfido** Sergeant, Miami Beach (FL) Police Department

**David Maggard, Jr.** Chief, Los Angeles World Airport, Airport Police Division **Daniel Mahoney** 

Deputy Director, Northern California Regional Intelligence Center

**David Maitlen** Sergeant, Torrance (CA) Police Department

Alexander Manjasek Detective, Daytona Beach (FL) Police Department

**Michael Manley** Captain, Vermont State Police

# Linda Mansour

Director of Engagements, U.S. Department of Homeland Security, Office for State and Local Law Enforcement

# Lisa Mantel

Senior Research Associate, Police Executive Research Forum

## Sydney Marshall

Policy Analyst, U.S. Department of Homeland Security, Office for State and Local Law Enforcement

# Dave McClure

Senior Research Associate, Police Executive Research Forum

#### **Robert McCullough**

Colonel, Baltimore County (MD) Police Department

# **James McGinty**

Assistant Director of Communications, Police Executive Research Forum

#### **Carol Might**

Air Traffic Security Coordinator, Federal Aviation Administration

# **Chau Miles**

Associate General Counsel, Office of Community Oriented Policing Services

John Miller Deputy Commissioner, New York City Police Department

#### **Evan Mishler**

Digital Design and Technology Specialist, Virginia Center for Policing Innovation (VCPI)

**Art Mogil** Lieutenant, New York City Police Department

**Robert Molloy** Captain, Boston University Police Department

**Terence Monahan** Chief, New York City Police Department

#### **Christopher Moore**

Branch Chief, Federal Protective Service, U.S. Department of Homeland Security

**Shawn Moore** Sergeant, Methuen (MA) Police Department

# **Steven Mucklow**

Special Assistant to the Deputy Assistant Secretary of Defense, Office of the Secretary of Defense

**Richard Myers** Executive Director, Major Cities Chiefs Association

**Max Nowinsky** Sergeant, Savannah (GA) Police Department

Joseph O'Connor Chief, Concord (MA) Police Department **Thomas O'Reilly** Executive Policy Advisor, Center on Policing

John T. Orr Captain, Virginia Beach (VA) Police Department

#### **Michael O'Shea**

UAS Integration Office Program Manager, Federal Aviation Administration

**Kimberly Owens** Lieutenant, Dallas (TX) Police Department

#### **David Oyler**

Deputy Chief, Wilmington (NC) Police Department

# Altmann Pannell

Director of Government and External Relations, International Association of Campus Law Enforcement Administrators

# L. Scott Parker

Chief, Emerging Threats Section, DHS Cybersecurity and Infrastructure Security Agency (CISA)

#### **Greg Pass**

Lieutenant, Prince William County (VA) Police Department

#### Joe Perez

President Local Chapter, Hispanic American Police Command Officers Association— National Capitol Region

# **Todd Porter**

Assistant Section Chief, Federal Bureau of Investigation

# Serge Potapov

Supervisory Air Marshal in Charge, Transportation Security Administration Federal Air Marshal Service, Security Services and Assessments Division

**Ron Prater** Executive Director, Big City Emergency Managers

Silver Joy Prout Associate Director, U.S. Department of Homeland Security

**Matthew Puia** 

Sergeant, Arlington County (VA) Police Department

**Christian Quinn** Major, Fairfax County (VA) Police Department

**Sue Ramanathan** Senior Counsel, Senate Homeland Security and Governmental Affairs Committee

**David Rausch** Director, Tennessee Bureau of Investigation

Robert Ravida Lieutenant, Montgomery County (MD) Police Department

John Ray Director, Texas A&M Engineering Extension Service—LAW Division

**Tim Richardson** Senior Legislative Liaison, Fraternal Order of Police

# **Alexander Richmond**

Officer, Methuen (MA) Police Department

#### **Janet Riffe**

Manager, Enforcement Standards & Policy, Federal Aviation Administration

Adam Ringle

Director of UAS Flight Operations, Wilmington (DE) Police Department

Michael Robertson Officer, Norman (OK) Police Department

**Randy Rody** Commander, Surprise (AZ) Police Department

Matt Rogers Sergeant, Michigan State Police

# Shelly Roman

UAS Airspace Operations Porgram Manager, Federal Aviation Administration

## David Rosado

Chief, Hartford (CT) Police Department

#### Kara Rose

Senior Police Advisor, Bureau of International Narcotics and Law Enforcement Affairs, U.S. Department of State

#### **Colin Ross**

Attorney Advisor, U.S. Department of Justice, National Security Division

# **James Rust**

Lieutenant, Manassas City (VA) Police Department

# **Vern Sallee**

Captain, Chula Vista (CA) Police Department

# **William Saunders**

Lieutenant, Southeastern Pennsylvania Transit Authority Police Department

# **Kevin Saupp**

Director, U.S. Department of Homeland Security Office of Intelligence and Analysis

## **Matthew Scheider**

Assistant Director, Office of Community Oriented Policing Services

#### **Patrick Schmidt**

Chief of Staff, Intergovernmental Public Liaison, U.S. Customs and Border Protection

# **Kurt Schoeps**

Lieutentant, Volusia County (FL) Sheriff's Office

# **Chrishonna Scott**

Policy Analyst, U.S. Department of Homeland Security, Office for State and Local Law Enforcement

# Shahid Shabazz

Senior Security Specialist, U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA)

#### **Michael Sharkey**

Chief, Suffolk County (NY) Sheriff's Office

Isaac Siekierski Superintendent, Israel National Police

# **Richard Slavin**

Assistant Chief, Scottsdale (AZ) Police Department

#### **Matthew Slawson**

Police Officer, Torrance (CA) Police Department

# Michael Snawder

Captain, Richmond (VA) Police Department

# **Deborah Spence**

Assistant Director, Office of Community Oriented Policing Services

#### **Al Stiehler**

Chief of Operations, Metropolitan Transportation Authority (NY) Police Department

#### Angela Stubblefield

Deputy Associate Administrator for Security & Hazardous Materials Safety, Federal Aviation Administration

## **Terry Sult**

Chief, Hampton (VA) Police Division

## Katharine (Katy) Taylor

Counsellor, Security and Counter Terrorism Science & Technology, British Embassy

#### Jason Thody

Assistant Chief, Hartford (CT) Police Department

#### **Scott Thomson**

Chief, Camden County (NJ) Police Department

#### **Jessica Toliver**

Director, Technical Assistance Division, Police Executive Research Forum

#### **Thomas Tompkins**

Sergeant, Polk County (FL) Sheriff's Office

# **Christopher Troiano**

Lieutenant, Concord (MA) Police Department

**Carissa VanderMey** Senior Advisor, U.S. Department of Homeland Security

# Joshua Vayer

Director, Uniformed Operations Division, Federal Protective Service, U.S. Department of Homeland Security

**Gary Vogue** Captain, Pennsylvania State Police

Kenneth Voiret Captain, Palm Beach County (FL) Sheriff's Office

# **Kenneth Walburn**

Captain, Metropolitan Nashville (TN) Police Department

# **David Warfield**

Avionics and C4ISR Specialist, U.S. Coast Guard, Aviation Forces

# **Chuck Wexler**

Executive Director, Police Executive Research Forum

# **Tyler Wotring**

Director of High-Tech Initiatives, National White Collar Crime Center

# Steven Woznyk

Assistan Chief of Police, Yale University Police Department

# **Chris Wuchenich**

Chief, University of South Carolina Division of Law Enforcement and Safety

#### **Kevin Zodrow**

Master Police Officer, Leesburg (VA) Police Department

# Anthony (Tony) Zucaro

Deputy Chief, Virginia Beach (VA) Police Department

# APPENDIX B. LIST OF AGENCIES THAT PROVIDED THEIR UAS STANDARD **OPERATING PROCEDURES TO PERF**

- Athens-Clarke County (GA) Police Department Scottsdale (AZ) Police Department
- Chula Vista (CA) Police Department
- Cumberland County (ME) Sheriff's Office
- Daytona Beach (FL) Police Department
- Fairfax County (VA) Police Department
- Gloucester Township (NJ) Police Department
- Leesburg (VA) Police Department
- Michigan State Police
- Norman (OK) Police Department
- New York City Police Department
- Prince William County (VA) Police Department
- Robertson County (TX) Sheriff's Office
- Savannah (GA) Police Department

- Seminole County (FL) Sheriff's Office
- Southeastern Pennsylvania Transit Authority Police Department
- St. Petersburg (FL) Police Department
- Tennessee Bureau of Investigation
- Torrance (CA) Police Department
- University of Massachusetts at Amherst Police Department
- University of Cincinnati Department of Public Safety
- University of South Carolina Division of Law Enforcement and Safety
- Virginia Beach (VA) Police Department
- Wilmington (DE) Police Department



# APPENDIX C. PALM BEACH COUNTY Sheriff's office template for writing Search warrants for using drones

# IN THE COUNTY/CIRCUIT COURT OF THE FIFTEENTH JUDICIAL CIRCUIT IN AND FOR PALM BEACH COUNTY, FLORIDA

# SEARCH WARRANT AUTHORIZING THE USE OF A DRONE UNDER F.S. 934.50

THE STATE OF FLORIDA COUNTY OF PALM BEACH

IN THE NAME OF THE STATE OF FLORIDA, TO ALL AND SINGULAR:

The Sheriff of Palm Beach County, Florida, and the Sheriff's Deputies and/or any police officer in Palm Beach County, Florida, within whose jurisdiction the aforesaid property to be searched is found, or the Commissioner of the Florida Department of Law Enforcement, or any of his duly constituted Agents.

WHEREAS, a complaint on oath and in writing, supported by affidavit of a credible witness or witnesses has this day been presented to me, and upon examination of the affidavit and application for this search warrant and other proofs submitted, I am satisfied that probable cause exists that the laws of the State of Florida are being violated within the [**property or area or premises and its curtilage**] located in Palm Beach County described as:

# DESCRIBE PROPERTY OR AREA OR PREMISES TO BE SURVEILLED BY THE DRONE

Being the [**property or area or premises and its curtilage**] of, or occupied by, or under the control of:

\*Name

Therefore, the remote use of a Drone is authorized to gather aerial video and/or aerial photographs of the above described [**property or area or premises and its curtilage**] and all items, objects and individuals within the above described [**property or area or premises and its curtilage**]

Further, those authorized to execute this search warrant or assist in the execution of this search warrant are authorized to conduct remote monitoring of the Drone and to capture aerial video and/ or aerial photographs of the above described [**property or area or premises and its curtilage**] and all items, objects and individuals within the above described [**property or area or premises and its curtilage**] for the purpose of obtaining evidence relevant to proving that a crime has been committed.

These items, objects and/or individuals are particularly described as:

# DETAIL AS BEST YOU CAN THOSE THINGS YOU BELIEVE THE AERIAL VIDEO AND/OR AERIAL PHOTOGRAPHS WILL CAPTURE

(1)

Which is being kept or used in violation of Florida Law, to wit:

## \*List crime(s) and specific statutes

NOW THEREFORE, the Sheriff of Palm Beach County, Florida, and the Sheriff's deputies and/or any police officer in Palm Beach County within whose jurisdiction the aforesaid [**property or area or premises and its curtilage**] is found, or the Commissioner of the Florida Department of Law Enforcement, or any of his duly constituted Agents, are hereby commanded with lawful and proper assistance as may be necessary in the name of the State of Florida,

To enter onto any part of the [**property or area or premises and its curtilage**] described above, for the purpose of capturing images of items, objects and actions of individuals through aerial video and/or aerial photographs and to do so surreptitiously to avoid detection.

AND that good cause has been shown that this use of the Drone should be done in the daytime or the nighttime, as the exigencies may demand or require, or on Sunday. You are hereby commanded to remotely and continuously operate and monitor the Drone and use the Drone to remotely capture images of items, objects and actions of individuals through aerial video and/or aerial photographs for a period of [**time frame of use of the drone**]

Palm Beach County Sheriff's Office Template

AND that the Affiant or any other person authorized to execute or assist in the execution of this search warrant are authorized to remotely and continuously operate and monitor the Drone and use the Drone to remotely capture images of items, objects and actions of individuals through aerial video and/or aerial photographs consisting of:

# DETAIL AS BEST YOU CAN THOSE THINGS YOU BELIEVE THE AERIAL VIDEO AND/OR AERIAL PHOTOGRAPHS WILL CAPTURE

(1)

FURTHER, the Court directs that the Affidavit and Application for the search warrant to be kept in the custody of the executing agency until further order of the court or until release by the executing agency. This will maintain the integrity of the ongoing investigation, pursuant to F.S. 119.071(2)(c)1 and *Wooling* v. *Lamar*, 764 So. 2d 765, 768 (Fla. 5th DCA 2000).

The original of the warrant, together with the original inventory, shall be returned and filed with the Clerk of the Court as stated above within ten (10) days of the issuance of this warrant. Further, any Property seized or taken shall be impounded for use as evidence at any trial of any criminal or penal cause growing out of the having or possession of said Property.

WITNESS MY HAND AND SEAL this \_\_\_\_\_ day of \_\_\_\_\_\_, in the year 20\_\_\_\_.

[Name of Judge] Fifteenth Judicial Circuit in and for Palm Beach County, Florida

Agency Name	
Agency Case #	Reviewing Prosecutor:



# ABOUT PERF

The **Police Executive Research Forum** (PERF) is an independent research organization that focuses on critical issues in policing. Since its founding in 1976, PERF has identified best practices on fundamental issues such as reducing police use of force, developing community policing and problem-oriented policing, using technologies to deliver police services to the community, and evaluating crime reduction strategies.

PERF strives to advance professionalism in policing and to improve the delivery of police services through the exercise of strong national leadership, public debate of police and criminal justice issues, and research and policy development.

In addition to conducting research and publishing reports on our findings, PERF conducts management studies of individual law enforcement agencies, educates hundreds of police officials each year in a three-week executive development program, and provides executive search services to governments that wish to conduct national searches for their next police chief.

All of PERF's work benefits from PERF's status as a membership organization of police officials, academics, federal government leaders, and others with an interest in policing and criminal justice.

All PERF members must have a four-year college degree and must subscribe to a set of founding principles, emphasizing the importance of research and public debate in policing, adherence to the Constitution and the highest standards of ethics and integrity, and accountability to the communities that police agencies serve.

PERF is governed by a member-elected president and board of directors and a board-appointed executive director. A staff of approximately 30 full-time professionals is based in Washington, D.C.

To learn more, visit PERF online at www.policeforum.org.



# ABOUT THE COPS OFFICE

The **Office of Community Oriented Policing Services (COPS Office)** is the component of the U.S. Department of Justice responsible for advancing the practice of community policing by the nation's state, local, territorial, and tribal law enforcement agencies through information and grant resources.

Community policing begins with a commitment to building trust and mutual respect between police and communities. It supports public safety by encouraging all stakeholders to work together to address our nation's crime challenges. When police and communities collaborate, they more effectively address underlying issues, change negative behavioral patterns, and allocate resources.

Rather than simply responding to crime, community policing focuses on preventing it through strategic problem-solving approaches based on collaboration. The COPS Office awards grants to hire community policing officers and support the development and testing of innovative policing strategies. COPS Office funding also provides training and technical assistance to community members and local government leaders, as well as all levels of law enforcement.

Since 1994, the COPS Office has invested more than \$14 billion to add community policing officers to the nation's streets, enhance crime fighting technology, support crime prevention initiatives, and provide training and technical assistance to help advance community policing. Other achievements include the following:

- To date, the COPS Office has funded the hiring of approximately 130,000 additional officers by more than 13,000 of the nation's 18,000 law enforcement agencies in both small and large jurisdictions.
- Nearly 700,000 law enforcement personnel, community members, and government leaders have been trained through COPS Office–funded training organizations.
- To date, the COPS Office has distributed more than eight million topic-specific publications, training curricula, white papers, and resource CDs and flash drives.
- The COPS Office also sponsors conferences, round tables, and other forums focused on issues critical to law enforcement.

COPS Office information resources, covering a wide range of community policing topics such as school and campus safety, violent crime, and officer safety and wellness, can be downloaded via the COPS Office's home page, <u>www.cops.usdoj.gov</u>. This website is also the grant application portal, providing access to online application forms.



In February 2019, the COPS Office, the Police Executive Research Forum (PERF), and the U.S. Department of Homeland Security (DHS) convened a two-day conference in Washington, D.C., to discuss the policy and operational issues regarding the implementation and use of drones. This publication synthesizes information presented and discussed by the conference participants; lessons learned; and promising practices gathered from interviews, policy reviews, and survey data for the purpose of providing law enforcement agencies with guidance on implementing a drone program.



U.S. Department of Justice Office of Community Oriented Policing Services 145 N Street NE Washington, DC 20530

To obtain details about COPS Office programs, call the COPS Office Response Center at 800-421-6770.

Visit the COPS Office online at www.cops.usdoj.gov.