ROADMAP TO IMPLEMENTING AN

Effective Unmanned Aircraft System (UAS) Program

COPS
Community Oriented Policing Services
U.S. Department of Justice

Police Executive Research Forum

ROADMAP TO IMPLEMENTING AN

Effective Unmanned Aircraft System (UAS) Program

This project was supported, in whole or in part, by cooperative agreement 2019-CK-WX-K020 awarded to Police Executive Research Forum 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. Rather, the references are illustrations 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:
Mantel, Lisa. 2020. *Roadmap to Implementing an Effective UAS Program*. Washington, DC: Office of Community Oriented Policing Services.

Published 2020

Contents

Letter from the Director of the COPS Office v

Letter from the Executive Director of PERF vii

Overview 1

Planning and Preparation—What to Consider Before You Begin 3

Step 1. Determine your agency's needs 3

Step 2. Engage the community 4

Step 3. Identify sources of funding 6

Step 4. Review state and federal laws and regulations 8

Implementation—Building Your Drone Program 11

Step 5. Select and purchase your drone and associated equipment 11

Step 6. Staff your drone team 12

Step 7. Train your drone team 13

Step 8. Develop standard operating procedures 14

Conclusion 17

Appendix A. State and Local UAS Working Group Members 19

Appendix B. Security Implications of Drone Programs 21

Appendix C. Training and Other Resources 23

About PERF 25

About the COPS Office 27

Letter from the Director of the COPS Office

Colleagues,

We are very pleased to release *Roadmap to Implementing an Effective Unmanned Aircraft System (UAS) Program* with our partners at the Police Executive Research Forum (PERF). Drones, as UAS are generally known, present one of the most exciting frontiers in law enforcement by giving departments an essential tool with which to gather vital situational data without placing law enforcement professionals in harm's way. I am personally committed to providing law enforcement agencies with the assistance they need to use this game-changing technology.

Our UAS portfolio has been informed by my own first-hand encounters with successful and innovative UAS programs across the country. Site visits to the Drones as a First Responder program in Chula Vista, California, and the agencies working on our southern border illustrated the urgent need for guidance in both the use and countering malicious use of drones for state, local, tribal, and territorial (SLTT) law enforcement agencies. In 2019, we hosted a forum that convened practitioners, law enforcement stakeholder groups, federal partners, and international peers. The findings from that forum were compiled into *Drones: A Report on the Use of Drones by Public Safety Agencies—and a Wake-Up Call about the Threat of Malicious Drone Attacks* which was released early this year. That report served as the foundational text for our work since. We also participate in federal working groups with the Federal Bureau of Investigation; the Bureau of Alcohol, Tobacco, Firearms, and Explosives; the Drug Enforcement Administration; and the U.S. Marshals Service, complemented by the military knowledge of UAS technology, to ensure that we are representing your needs and interests in this rapidly evolving theater.

In January 2020, the Office of Community Oriented Policing Services (COPS Office) convened a working group with representatives from innovative SLTT UAS programs, law enforcement stakeholder groups, and federal partners. The primary purpose of this working group is to identify the most pressing needs pertaining to SLTT UAS deployment and produce guidance for our peers in the field. This roadmap contains resources identified by working group members as essential to starting a drones program as well as their own invaluable lessons learned. It will help departments scope their mission, navigate permissions and paperwork, engage with their communities, and protect their data. This and all following deliverables from the SLTT UAS Working Group are grounded in the COPS Office's philosophy of deliverables "by the field, for the field."

This roadmap is the first of a series of deliverables identified by your peers as essential to expanding the safe and appropriate use of UAS technology. The deliverables will form a body of best practices for SLTT agencies using or managing the public's use of drones. I urge any agency considering a UAS program to carefully read this roadmap and contact the resources include within, who stand ready and willing to assist.

I want to thank the staff and leadership of PERF and our federal partners for their work in its creation.

Phil Keith
Director
Office of Community Oriented Policing Services

Letter from the Executive Director of PERF

Dear colleagues:

Earlier this year, the Police Executive Research Forum (PERF) released *Drones: A Report on the Use of Drones by Public Safety Agencies—and a Wake-Up Call about the Threat of Malicious Drone Attacks*.[1] This comprehensive report was based in part on a two-day conference that PERF held in 2019 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).

At our conference, more than 200 police chiefs, sheriffs, officers, scholars, stakeholder groups, representatives of federal agencies, and other experts discussed the issues that public safety agencies need to consider before starting a drone program. Participants also addressed how federal, state, and local law enforcement agencies must respond to the malicious use of drones by bad actors.

I'm pleased that we are now releasing *Roadmap to Implementing an Effective Unmanned Aircraft System (UAS) Program,* which is a companion piece to our earlier report. Our new report is an eight-step guide to planning a drone program, starting with evaluating whether your agency needs a drone program and, if so, for what purposes. Other key steps include consulting with your community, identifying funding sources, and researching the laws and regulations that would impact your program. After that essential preparation, you can begin the work of purchasing drone equipment, staffing and training your drone team, and writing standard operating procedures (SOP).

In light of the heightened scrutiny of police agencies these days, our step 2—Engage the community—is especially important. Any police agency considering a drone program must be completely transparent with the community about how they are thinking about the key issues, including the purposes of the program, the limitations on use of drones that you are considering, privacy issues, accountability, and any other concerns that the community may have.

The steps and tips included in this guidance are based on the promising practices and lessons learned by leaders in the field. I want to thank the members of the State, Local, Tribal, and Territorial UAS Working Group for their expertise in developing the *Roadmap to Implementing an Effective Drone Program*. I also want to thank

1. Police Executive Research Forum, *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, 2020), https://cops.usdoj.gov/RIC/ric.php?page=detail&id=COPS-W0894.

the COPS Office for making this work possible and Director Phil Keith for his leadership on this issue. Drones have tremendous potential for saving lives, but to tap into that potential, you must ensure that your program is carefully controlled and managed and that you have strong support in your community for your stated goals and purposes. Our new roadmap report can help you achieve that.

Sincerely,

Chuck Wexler

Chuck Wexler
Executive Director
Police Executive Research Forum

Overview

The Police Executive Research Forum (PERF), with support from the U.S. Department of Justice Office of Community Oriented Policing Services (COPS Office) and in consultation with the State and Local Unmanned Aircraft Systems (UAS) Working Group,[2] developed this roadmap to assist public safety agencies with implementing an effective UAS, or drone, program.[3] The use of drones by law enforcement and other public safety agencies has been increasing since 2010—and even more so since 2015—yet little guidance is available for police executives to consider in establishing a drone program.

For more detailed guidance, including recommendations, best practices, and lessons learned, please reference the COPS Office and PERF's 2020 report on public safety agencies' use of drones.[4]

In addition, the U.S. Department of Justice in autumn 2019 issued its new policy on the use of UAS,[5] which can serve as a model for law enforcement and public safety agencies to employ UAS in a responsible, appropriate, and effective way to protect the public while promoting national values and the rule of law.

While the guidance in this publication is framed in steps, it is important to understand that these steps need not occur in a rigid, sequential manner. Rather, this is meant to be a continuous process. For example, continued action on some of the steps may be necessary based on new or changing conditions. As an illustration of new conditions, many public safety agencies employed drones in response to civil unrest or the challenges presented by the COVID-19 pandemic; when faced with such new conditions, public safety agencies must work with their communities and seek advice of counsel to protect privacy and civil liberties (e.g., First Amendment interests) in this new context. In addition, continued refinement of standard operating procedures and best practices is necessary throughout the life of a drone program to ensure that policy, training, and best practice continues to evolve.

---

2. Members of the group are listed in appendix A.
3. 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 document will use the term UAS interchangeably with the more colloquial term *drone*, but will not use the terms *unmanned aerial vehicle* (UAV), *remotely-piloted airship vehicle* (RPAV), or other less comprehensive terms.
4. PERF (Police Executive Research Forum), *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, 2020), https://cops.usdoj.gov/RIC/ric.php?page=detail&id=COPS-W0894.
5. "9-95.100 - Department of Justice Policy on the Use of Unmanned Aircraft Systems," U.S. Department of Justice, last modified November 2019, https://www.justice.gov/jm/9-95000-unmanned-aircraft-systems-uas.

Planning and Preparation—What to Consider Before You Begin

Step 1. Determine your agency's needs

The first step is to determine **whether your agency needs a drone.** Answer the following questions:

- How will your agency use the drone? Consider the various use cases for drone missions, including the following:
  - Bombs and hazardous materials observation
  - Crime scene photography and reconstruction
  - Disaster response
  - Ensuring safety at mass gatherings
  - Fugitive apprehension
  - Investigating armed and dangerous suspects
  - Search and rescue
  - Traffic collision reconstruction
  - Training missions
- How often do you anticipate using the drone?
  - Is there a neighboring agency with a drone program whose services you can request or join as a partnering agency?
  - Can you partner with a neighboring agency or other public safety agency within your jurisdiction (e.g., the fire department, emergency management) to jointly build a drone program?

Recommendations

- **Identify the goals and objectives of your agency's drone program**. This will help you determine the operational parameters of the program, including the size of the program, capital and operating costs, number and type of drones to purchase, and the associated equipment you will need.
- **Consider establishing mutual aid agreements with neighboring agencies with a single point of contact for dispatching**. This will allow your agency to share resources and personnel regionally or statewide.

Step 2. Engage the community

The next step in implementing a drone program is to **engage with your community**. Many state, local, tribal, and territorial public safety agencies have found that seeking public understanding and support is key to a successful drone program.

Recommendations

- Before you purchase your drone, consult with community organizations and other stakeholders, and work to ensure that their concerns are understood and are addressed through an open and transparent process. Proactively reach out to organizations that are likely to have helpful perspectives or reservations about drone use (e.g., the American Civil Liberties Union (ACLU), civic groups, other civil liberties or privacy interest groups).
    - **Tip.** Be prepared to provide detailed, substantive answers to questions about what type of information police intend to collect during drone missions and how you will store, protect, and retain the data you collect.

> "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 and read their publication about drones. All this happened before we bought our first drone or started any operations."
>
> *– Captain Vern Sallee, Chula Vista (CA) Police Department*

- **Communicate with other stakeholder organizations** in your community. Following is a checklist of suggested organizations to contact, which can be tailored to your jurisdiction's unique needs:
  - All public safety departments (e.g., fire, emergency medical services (EMS), campus security)
  - Church groups
  - Citizen community advisory boards
  - Civil liberties and privacy rights organizations
  - Federal Aviation Administration (FAA)
  - Federal law enforcement agencies operating in your area (e.g., U.S. Attorney's Office, Federal Bureau of Investigation (FBI) Field Office)
  - Groups with wildlife concerns such as the National Audubon Society
  - Hospitals
  - Local business organizations
  - Local parks authority
  - Major airports (including tower staff) and airport management agencies
  - National Association for the Advancement of Colored People (NAACP) and other civil rights organizations
  - Neighborhood Watch groups
  - Other local community groups specific to your area
  - Other local government agencies (e.g., public works, emergency management)
  - Prosecutors and criminal defense attorneys
  - Schools
- **Engage with local governing bodies** (e.g., mayor, city council, city manager, county commissioners) to explain how police would like to use drones to promote public safety.

- **Communicate with the public** about your plans for defining the authorized and official purposes of your drone program and what types of uses you intend to prohibit. This information may help to avoid misunderstandings and reduce levels of opposition.
  - **Tip.** Stress that the use of drones is to promote public safety and not for loosely defined surveillance purposes.
  - **Tip.** Use print, broadcast, and social media to inform and engage the public. *Involve your agency's public information officer* to share information widely. Ensure that your message is going to reach the target audience.
- **Be transparent** about your agency's plans for drone policies and practices. This should continue after the program has been implemented.
  - **Tip.** Post your agency's plans for drones on your department's website when the program is being considered, and post the final details about policies on your website after the program has been approved and implemented.
  - **Tip.** If permissible by law, release video of successful drone deployments to reassure the community about your agency's purpose and intent. In addition, share the drone mission flight log with public by posting it on your agency's website (with the exception of any missions that are sensitive or would compromise a criminal investigation).
- **Respond to community concerns and recommendations.** After public input has been solicited and gathered, work with local elected officials to review the situation and make decisions about final policies and plans. Transparency is essential. Publicly announce all decisions about any revisions to the initial plans, and post the final policies and plans on police and city websites with explanations and background information.

Step 3. Identify sources of funding

The third step is to **identify sources of funding** for your agency's drone program. This includes the initial costs as well as ongoing costs to sustain the program. Many agencies with sophisticated programs suggest a "crawl, walk, run" approach; in other words, start with a small program and gain experience before expanding it.

Recommendations

- **Establish the goals and operational parameters** of your agency's drone program. This will help determine the true costs of the program.
  - **Tip.** Begin with the minimum amount of equipment needed to achieve your agency's mission. Once you master that, consider possible expansion of the program if needed.

- When establishing the financial needs of a drone program, **consider the initial equipment costs as well as the ongoing costs**, including long-term training, maintenance, and upgrade costs.
  - **Tip.** Do not forget the ancillary equipment required to make your drone functional (e.g., a thermal camera, spotlight, data storage, a vehicle to transport the drone).
- **Consider alternative funding sources** that could help support a drone program.
  - **Tip.** Consider foundations, grants, or community partnerships to help offset program costs. If you are using a federal grant to purchase a drone, ensure that the manufacturer meets the requirements of the federal grantor.
- **Carefully evaluate offers of donated UAS, or UAS for "free" evaluation periods.** Law enforcement and public safety agencies must be attuned to the cybersecurity and supply chain risks associated with UAS, and factor those risks into purchase and fielding decisions. Foreign-manufactured UAS companies have occasionally offered to donate UAS to state and local law enforcement entities, often during public emergencies—most recently including the COVID-19 pandemic. Vendors may also occasionally offer "free" evaluation periods where an agency is permitted to "test drive" a UAS. However, these "free" systems often involve having to install or use proprietary software or hardware components that could introduce vulnerabilities into or compromise agency computer systems (including "over-the-air" because most systems include radio frequency transmitters and receivers) and may provide unauthorized "backdoors" into critical public safety networks. (See appendix B for additional discussion about the security implications of using drones.)
- **Conduct a cost-benefit analysis.** In addition to estimating all of the immediate and long-term costs of a drone program, consider the potential benefits derived from drone use (e.g., more successful searches for missing persons; faster accident reconstruction leading to briefer road closures).
  - **Tip.** Consult neighboring agencies to determine if costs can be shared between agencies that jointly own and operate a drone program.
  - **Tip.** If your agency deploys fixed-wing aircraft or helicopters, consider the extent to which drones might perform certain missions more easily and at lower cost than crewed aviation. Drones likely will not replace crewed aircraft entirely, but the costs of drones may be offset to some extent by savings in reduced use of crewed aircraft.

> "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."
>
> *– Interim Chief Tony Zucaro, Virginia Beach (VA) Police Department*

Step 4. Review state and federal laws and regulations

An additional step to take before implementing a drone program is to **research all federal, state, and local laws and regulations** applicable to your agency's jurisdiction to ensure that your program will function lawfully and without legal challenges.

You must also determine which FAA regulatory option you will use for operation:

- Have individual operators obtain an **FAA Part 107 Remote Pilot Certificate** under 14 CFR Part 107.[6]
- Have your agency obtain a **FAA Part 91 Certificate of Authorization (COA)** so you can self-certify your operators under 14 CFR Part 91.[7]

There are advantages and disadvantages to each option, which is why many agencies choose to pursue both.

6. "Fact Sheet—Small Unmanned Aircraft Regulations (Part 107)," press release, Federal Aviation Administration, last modified June 21, 2016, https://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=20516.
7. "Certificates of Waiver of Authorization (COA)," Federal Aviation Administration, last modified April 25, 2019, https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/systemops/aaim/organizations/uas/coa/.

Recommendations

- **Consult with your agency's legal department** to determine if there are legal restrictions on the use of drones by law enforcement and to ensure that drone team members understand the laws and regulations they must follow.
  - For example, police agencies in Virginia are limited by state legislation[8] that requires law enforcement agencies to obtain a warrant before using a drone for any purpose, except in certain defined circumstances.
  - In Florida, lawmakers enacted the Freedom from Unwanted Surveillance Act[9] in 2015, which prohibits law enforcement agencies' use of drones, with several broad exceptions.
- **Use the** FAA's User Identification Tool[10] to determine which regulatory option is right for your agency.
  - **Tip.** Consider applying for both an FAA Part 107 Remote Pilot Certificate and a Part 91 COA for maximum use and flexibility.
- If applicable, **consult with neighboring agencies** to learn how legal limitations affect their operations and how they manage those limitations.
- **Prepare templates for search warrants** based on the contemplated use of drones as necessary,[11] and applications for waivers of certain limitations that sometimes affect drone operations. A template for writing a search warrant can be found in appendix C to the COPS Office and PERF report, *Drones: A Report on the Use of Drones by Public Safety Agencies—and a Wake-Up Call About the Threat of Malicious Drone Attacks.*[12]
- **Know your neighbors,** including the U.S. Department of Defense, U.S. Department of Energy, and other federal facilities that have permanent airspace restrictions. For example, the National Capital Region around Washington, D.C., is covered by the Flight Restricted Zone (FRZ), which requires special waivers and notifications before a law enforcement flight can take place.
  - **Tip.** Consult the FAA, which lists sensitive areas where flights are prohibited.[13]

---

8. Virginia State Code § 19.2-60.1, https://law.lis.virginia.gov/vacode/title19.2/chapter5/section19.2-60.1/.
9. Florida Statue 934.50, https://www.flsenate.gov/Laws/Statutes/2015/934.50.
10. "User Identification Tool," Federal Aviation Administration, last modified May 7, 2020, https://www.faa.gov/uas/getting_started/user_identification_tool/.
11. For example, if required by state or local law or if, after conferring with legal counsel, the specific contemplated use implicates the Fourth Amendment to the United States Constitution (e.g., given the ability of UAS to get much closer to a home than manned aircraft or if sensors are used on the UAS that intrude into an area where an individual has a reasonable expectation of privacy a warrant wifould likely be constitutionally required). However, the Supreme Court has repeatedly ruled that aerial surveillance, provided it remains within certain parameters, is not a search under the Fourth Amendment, and therefore a warrant is not constitutionally required. (*Florida* v. *Riley*, 488 U.S. 445 (1989); *California* v. *Ciraolo*, 476 U.S. 207 (1986); *Dow Chem. Co.* v. *United States*, 476 U.S. 227 (1986)).
12. PERF, *Drones* (see note 4).
13. "Where Can I Fly?" Federal Aviation Administration, last modified October 19, 2018, https://www.faa.gov/uas/recreational_fliers/where_can_i_fly/airspace_restrictions/.

Implementation—Building Your Drone Program

Step 5. Select and purchase your drone and associated equipment

The next step is to **select and purchase your drones and related equipment**. This can be challenging because there are many options in an array of sizes, capabilities, and costs.

To select and purchase the best drones for your agency, it is important to keep in mind the following key considerations:

- **Operational parameters.** What will the drones be used for?
- **Operational specifications.** What technology or equipment is needed to achieve mission goals?
- **Operational security.** Based on the platform you select, are you potentially exposing your agency's systems to cybersecurity threats? Can you successfully mitigate the risks? (There are risks associated with drones that are manufactured in a foreign country or data platforms in which video footage or other data are accessible by servers in a foreign country. See appendix B, Security Implications of Drone Programs.)

Recommendations

- **Consider the operational parameters and specifications of your drone program** to help inform the purchase of your drone and associated equipment.
  - What will you use the drone for? (See step 1. "Determine your agency's needs.")
  - What special features and capabilities do you need (e.g., bright spotlights, thermal imaging, scene mapping, automatic sharing on media platforms)?
  - What are the typical weather conditions in your area?
  - How do you plan to transport the drone and store data?
- **Often, "less is more."** The more complex the drone system is, the more complicated and expensive it can be to operate and maintain it. Consider starting with simple and easy-to-learn systems and evolve the program as you gain more experience.

- **Consider durability and battery life** as you evaluate which drones to purchase.
  - **Tip.** Look for vendors with proven experience that will be in the drone industry for the foreseeable future. This will allow you to obtain necessary parts and repairs in the future.
- **Consider mission management solutions** for supporting operational requirements, including report generation, image storage and management, image analysis, etc.
- **Be aware of the security risks** (including the potential exposure of private or sensitive data) when operating drones that were designed or manufactured in a foreign country or where the data is stored, transferred to, or accessible by servers in a foreign country.
  - **Tip.** Coordinate with your agency's network security personnel to identify mitigation strategies before using any foreign-made UAS.
- **Strongly consider procuring drones made domestically** or by trusted allies, although each purchase decision will depend on the specific use case, mission requirements, and assessed risks.
- **Implement your drone program on a trial basis for a specified period of time** (e.g., 180 days).
  - **Tip.** Use an inexpensive and small platform drone when first starting out. Many drones have been accidentally damaged or destroyed during training.
- Conduct a formal evaluation of the trial period. An evaluation period will allow your agency to decide if pursuing a drone program is worth the time, effort, and money that must go into it.
- C**onsider the insurance requirements** for your UAS fleet.
  - **Tip.** In addition to UAS insurance specifically to cover the drone and basic liability of UAS operations, it may be necessary to include specific schedules of aircraft registration numbers or pilots in your agency's general law enforcement liability policy.
  - **Tip.** Consider obtaining insurance to cover UAS operations when using a partner agency's drones through mutual aid agreements.

Step 6. Staff your drone team

Ensure that your drone team is staffed with qualified people. 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 at a minimum of a remote pilot in command and a visual observer. Other team roles include team leader, camera/video/sensor operator, and safety and security officer.

- The **remote pilot in command** controls the drone and in most situations is required to keep it within his or her visual line of sight.

- The **visual observer** assists the pilot by maintaining visual contact with the drone and the area around the drone and by alerting the pilot to potential hazards.
- The **team leader** is responsible for overseeing the operational status of the program, assigning equipment and staff, and policy and program development.
- The **camera/video/sensor operator** monitors the video feed and any other information being transmitted from the drone.
- The **safety and security officer** protects the other members of the drone team.

Recommendations

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

Step 7. Train your drone team

The next step is to ensure that **drone team members receive comprehensive training**, including a detailed understanding of the drones they will be operating and the airspace they will be operating in. The structure of your training will depend on several factors, including

- your agency's size;
- which FAA regulatory option you are operating under;
- the missions that your drones will be used for;
- the authorizations of your drone team members.

Some agencies conduct training internally while other agencies are trained by an external provider. As noted in previous steps, you must first determine the purpose of your drone program before developing a training protocol.

Recommendations

- **If you develop your own training protocols,** be sure to include the following topics:
  - A baseline understanding of what role the FAA plays in public safety regulatory compliance
  - Aviation safety—an aviation safety program or aviation safety management system
  - Crew resource management and a flight risk assessment tool to accept or decline a UAS flight request
  - Fleet management—how to choose the right aircraft for each mission
  - How to present UAS-collected data in court
  - Legal and policy instruction on compliance with FAA regulatory standards, the Fourth Amendment's application to aerial surveillance (and to any sensors that may be employed on the UAS), and privacy and civil liberty implications of using UAS and conducting aerial surveillance
  - Methods of conducting safe flight operations, including under pressing circumstances
  - Operational guidelines for UAS pilots and technicians within an agency
  - Rules of evidence related to UAS operations and agency requirements
- **Require drone training** for all agency personnel who will be part of the approval chain for using drones or who will assist with drone procedures to ensure operational proficiency.
  - **Tip.** Purchase inexpensive drones for new pilots to practice with during initial training. (See step 5 "Select and purchase your drones and associated equipment.")
  - **Tip.** Set ongoing training requirements so team members remain proficient in drone operations and up to date on FAA rules and regulations.
  - **Tip.** Train visual observers in different units (such as bomb squad or accident reconstruction personnel) to ensure someone arrives on scene promptly. (See step 6. "Staff your drone team.")

Step 8. Develop standard operating procedures

It is important to **document your agency's policies and standard operating procedures (SOP)** regarding drone use. Request that your agency's legal counsel and your local prosecutor's office review and provide input on the policies and SOPs. This will help to ensure compliance with your jurisdiction's laws and regulations, improve transparency, provide assurance to the public that operations are being conducted lawfully and with legal oversight, and reduce the possibility that evidence collected by drones will be deemed inadmissible at trial. To ensure accountability, make sure that all staff members receive a copy of the policies and SOPs and are trained on them.

Recommendations

- **Review model policies** and sample language when developing your own SOPs. Sample language can be found in the COPS Office and PERF report, *Drones: A Report on the Use of Drones by Public Safety Agencies—and a Wake-Up Call About the Threat of Malicious Drone Attacks.*[14]
- **Tip.** Consult other agencies and use their SOPs as a starting point.
- **Make sure your SOPs include the following components:**
  - Authorized types and purposes of missions
  - Aviation safety
  - Definitions
  - Evidence data collection and storage
  - Information collection, retention, and dissemination
  - Legal guidance on search, seizure, and aerial surveillance activities
  - Privacy and civil liberties considerations
  - Procedures
  - Purpose
  - Required training
  - Restrictions on use of UAS
  - Staffing
- **Consider posting your drone policies on your agency's website** to ensure transparency and build community trust.
- **Be flexible and willing to change** as your program develops.

14. PERF, *Drones* (see note 4).

Conclusion

Organizations must be able to adapt to changing circumstances and learn from mistakes. Agencies choosing to implement a drone program must remain flexible, inventive, and adaptable. Technology changes fast, and agencies must continue to change with it to stay ahead of threats and drone countermeasures. Thus, it is important to continuously refine policy, best practices, and tactics as you build your drone program and incorporate new technology into your daily operations.

Appendix A. State and Local UAS Working Group Members

Gregory Ahern
Sheriff, Alameda County (CA) Sheriff's Office

Brian Bahlau
Lieutenant, Michigan State Police

Michael Brown
National Sheriffs' Association

Robert Chapman
Deputy Director, COPS Office

Ileana Ciobanu
Senior Counsel, DOJ Office of Legal Policy

Nicole Corbin
Lieutenant, California Department of Corrections and Rehabilitation

Matthew Cronin
National Security & Cybercrime Coordinator, Executive Office for United States Attorneys

Rodolfo Cuevas
Massachusetts Department of Transportation

Sarah Estill
Social Science Analyst, COPS Office

Charles Guddemi
D.C. Homeland Security and Emergency Management Agency

Joseph Heaps
Senior Physical Scientist, National Institute of Justice

Hyla Jacobson
Research Assistant, PERF

Kevin Jinks
Senior Counsel, DOJ Office of Legal Policy

Phil Keith
Director, COPS Office

Roxana Kennedy
Chief, Chula Vista (CA) Police Department

Tom Madigan
Commander, Alameda County (CA) Sheriff's Office

David Maitlen
Sergeant, Torrance (CA) Police Department

Lisa Mantel
Deputy Director of Technical Assistance, PERF

Ben Miller
Director, Colorado Center of Excellence for Advanced Technology Aerial Firefighting

Art Mogil
Lieutenant, New York City (NY) Police Department

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

Michael O'Shea
UAS Integration Office Program Manager, Federal Aviation Administration

Christian Quinn
Major, Fairfax County (VA) Police Department

Ray Reed
Master Police Officer, Virginia Beach (VA) Police Department

Janet Riffe
Manager, Enforcement Standards & Policy Division, Federal Aviation Administration

Adam Ringle
Sergeant, Wilmington (DE) Police Department

Don Roby
Training Program Manager, Airborne Public Safety Association

Matt Rogers
Sergeant, Michigan State Police

Vern Sallee
Captain, Chula Vista (CA) Police Department

Martin Sayre
Commander, St. Cloud (MN) Police Department

Matthew Scheider
Assistant Director of Research and Development, COPS Office

David Simon
Captain, Michigan State Police

Jessica Toliver
Director of Technical Assistance, PERF

Duane Tompkins
Sergeant, Polk County (FL) Sheriff's Office

Robert Tracy
Chief, Wilmington (DE) Police Department

Chuck Wexler
Executive Director, PERF

Tony Zucaro
Interim Chief, Virginia Beach (VA) Police Department

Appendix B. Security Implications of Drone Programs

Public safety agencies must understand the cybersecurity and supply chain risks associated with certain foreign-made technology, as well as the relevant restrictions based on the sources of funding they receive.

Public safety agencies must also recognize that legislatures and executives at the federal and state levels are moving to limit public agencies' purchase and deployment of certain foreign-made UAS in light of the risks they present. These risks include the following:

- **Operators.** Inexperienced operators can place an organization's UAS device and its data at risk if they do not follow established procedures for securing the UAS before, during, and after flight. Both transmitted and stored data are vulnerable when the device, its components, or its transmission feed are not properly secured by the operator.
- **Manufacturers and vendors.** An organization's information is at risk if it employs technology corrupted by malware or performs automatic data transmission to a third party. Manufacturers and vendors of UAS, their firmware, and software applications potentially can build in malware or collect data from UAS devices without an organization's knowledge.
- **Data theft.** Organizations are susceptible to theft of information if the UAS device and the organization's network are not properly secured and if the communication feed on which the UAS is operating is unencrypted. The potential data at risk to exposure from using a UAS includes location data, personally identifiable information (PII), phone/tablet data, video and pictures, biometric data, and flight logs and telemetry data.
- **Network intrusion.** UAS—as with other connected "internet of things" devices—can expose organizations to network breaches, which could lead to unauthorized access to agency internal data sets and other information. Malware incorporated into software, firmware, or hardware modules within the UAS supply chain may potentially spread to an agency network depending on its design and how data is retrieved from the UAS.
- **Wireless communications.** UAS and their controllers may be susceptible to various local wireless attacks because they communicate using a number of protocols, and are impacted by whether or how the communications are encrypted.

- **Foreign law enforcement and foreign government cooperation.** While companies operating within any country are typically expected to comply with applicable law and government regulations, foreign governments may require companies to disclose far more information than the U.S. government without significant legal protection for customers. UAS data is often sent to servers controlled by or accessible to the UAS manufacturing company or third-party application vendor. For UAS designed, manufactured, or supplied abroad, company internet servers may be located in the United States or in foreign countries (or both). Data servers run by or accessible to foreign companies, especially those located in foreign countries, may be susceptible to foreign law enforcement and government seizure without the benefit of the types of legal protections under U.S. law.

Appendix C. Training and Other Resources

- FAA (Federal Aviation Administration). *Drones in Public Safety: A Guide to Starting Operations*. Washington, DC: Federal Aviation Administration, 2019. https://www.faa.gov/uas/public_safety_gov/media/Law_Enforcement_Drone_Programs_Brochure.pdf.
- FAA. *Emergency Situations*. Last modified August 27, 2020. https://www.faa.gov/uas/advanced_operations/emergency_situations/.
- FAA. "How to Start a Drone Program." YouTube, July 9, 2019. https://www.youtube.com/watch?v=Rp1yTzJt7ZU.
- Police Executive Research Forum. *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, 2020. https://cops.usdoj.gov/RIC/ric.php?page=detail&id=COPS-W0894.
- U.S. Department of Justice. *9-95.100 – Department of Justice Policy on the Use of Unmanned Aircraft Systems*. Last modified November 2019. https://www.justice.gov/jm/9-95000-unmanned-aircraft-systems-uas.

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 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 the Senior Management Institute for Police, 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, who share information and open their agencies to research and study. PERF members also include 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.

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, www.cops.usdoj.gov. This website is also the grant application portal, providing access to online application forms.

State, local, tribal, and territorial law enforcement agencies, as well as members of the community, have been increasing their use of unmanned aircraft systems (UAS)—also known as drones—because of their increasing utility and efficiency. In early 2020, the COPS Office launched a working group comprising leaders in the field, both local and federal, to identify and create vital resources for law enforcement agencies using and confronting the use of drones. This publication is a roadmap on how agencies can plan, establish, and implement drone programs.

COPS
Community Oriented Policing Services
U.S. Department of Justice

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**.

e092017965
Published 2020