



City of Phoenix

ADMINISTRATIVE REGULATION	A.R. NUMBER Revised 1.56
	FUNCTION General Page 1 of 13
SUBJECT UNMANNED AIRCRAFT SYSTEMS (UAS) POLICY	EFFECTIVE DATE June 2, 2022
	REVIEW DATE
1. PURPOSE	
<p>The City of Phoenix (“City”) is committed to embracing technologies that improve service delivery to the public while protecting the safety and privacy of its residents. The integration of Unmanned Aircraft Systems (UAS) technology by the City in accordance with Federal Aviation Administration (FAA), Cyber Security and Infrastructure Security Agency (CISA), National Institute of Standards and Technology (NIST) and Federal Trade Commission (FTC) is intended to enhance existing departmental capabilities and service to the community.</p> <p>The City of Phoenix is dedicated to the security, safety, and the preservation of life of residents and employees. The UAS program is intended to provide an enhanced level of operational capability, safety, and situational awareness and reduce the risk of injury. The UAS program will be utilized in a responsible, legal, and transparent manner to maintain the public trust. The UAS program will be operated to ensure and protect the rights and privileges of the public, including protecting the fundamental rights to free speech and expression; the freedom to assemble and protest, and protect against unreasonable search and seizure.</p>	
2. SCOPE OF POLICY	
<p>This policy is intended to improve the efficiency of departmental operations, ensure the security of employees, residents, real and personal property, and respect and protect the privacy expectations of the public. This policy shall provide a framework and direction for all City departments approved by City management to implement UAS technology to meet their respective department mission objectives. Each City department is responsible for the development and integration of their own UAS program to meet the needs of the department and the City while ensuring that the department is following the policy set forth in this UAS Policy.</p>	
3. DEFINITIONS	
<p>Cyber Security and Infrastructure Security Agency (CISA): An agency within the United States Department of Homeland Security serving as the Nation’s risk advisor, working with partners to defend against today’s threats and collaborating to build a more secure and resilient infrastructure for the future.</p>	
<p>Department: City department pre-approved by City management to deploy an Unmanned Aircraft System in the National Airspace System.</p>	

Federal Aviation Administration (FAA): An agency within the United States Department of Transportation that is the lead aviation authority in the United States providing for the safe and efficient use of navigable airspace.

Global Positioning System (GPS): A global positioning system uses signals from satellites to find the position of an object.

National Airspace System (NAS): Consist of (a) the common network of United States airspace; (b) air navigation facilities, equipment, and services; (c) airports, landing areas; (d) aeronautical charts, information, and services; (e) related rules, regulations and procedures; (f) technical information; and (g) manpower and material.

National Institute of Standards and Technology (NIST): An agency within the United States Department of Commerce that provides solutions for measurements, standards, and legal metrology that ensures measurement traceability, enables quality assurance, and harmonizes documentary standards and regulatory practices.

Personal Identifying Information (PII): includes a person's date of birth, social security number, personal telephone number, home address, personal e-mail address, financial account information, passwords, access codes, or any official state or government-issued driver's license or identification number.

Privacy: The rights and obligations of the City with respect to the collection, protection, use, disclosure, and retention of personally identifying information for individuals and entity-identifying information for entities, such as businesses and organizations as provided in A.R. 1.95. In addition, a UAS shall be deployed to ensure and protect the privacy of citizens, including the rights to free speech and assembly under the US and Arizona constitutions, as well as protecting against unreasonable search and seizure guaranteed by the US and Arizona constitutions.

Restricted City Information (RCI): Information for which unauthorized access, modification, or loss could have a negative effect on the City or the public. Examples include sensitive public infrastructure and/or utility information, all information exempt from public disclosure under state or federal public records laws, customer databases, employee personnel records and information, selected procurement information, licensed proprietary or copyrighted information, and security information.

Unmanned Aircraft System (UAS): A small, unmanned aircraft and its associated elements (including communication links and control components) when used together create a system required for safe and efficient operation.

Unmanned Aircraft Vehicle (UAV): An aircraft without a human pilot aboard; UAVs are a component of an UAS.

While an UAV is used to describe the aircraft itself, the term UAS represents the system of equipment, personnel, and the associated elements necessary for the operation of such aircraft. For the purposes of this policy, UAV, and UAS are all collectively referred to as UAS when referring to a complete system.

4. PROGRAM ADMINISTRATION AND GOVERNANCE STRUCTURE

The City UAS Program will be governed by an UAS Executive Committee that will be supported by a subcommittee known as the Technical, Security and Privacy (TS&P) Subcommittee.

4.1 Program Administration

The City UAS program oversight will be administered by the City Manager's Office, or a designee, who shall appoint an Administrative Manager.

4.2 Administrative Manager

The Administrative Manager is responsible for day-to-day administrative responsibilities that include but are not limited to: (1) scheduling meetings; (2) providing reports; (3) taking meeting notes and publishing them.

4.3 Notice & Agenda

The Administrative Manager will prepare the notice, agenda, and minutes of the UAS Executive Committee meetings. A member of the UAS Executive Committee and TS&P subcommittee chair may add an item to the agenda 14 working days prior to the UAS Executive Committee meeting for its consideration. In emergencies, items may be added no later than 24 hours before the meeting.

5. UAS PROGRAM MEMBERS

The UAS program shall be comprised of permanent members and rotating members.

5.1 Member Admission and Approval

Any department may apply for membership to the UAS program and the UAS Executive Committee may admit members with a simple majority vote. An aspirant member must complete the following to be considered for a membership:

- Submit a written request for UAS program membership with an explanation on why a UAS program is needed and the impact that a UAS program would have on the department's mission;
- Must agree to follow UAS policies and governing and reporting structure.

5.1.1 Application Evaluation Factors

The UAS Executive Committee has the authority to deny or consider applications for membership status. If the Committee decides to consider approval of an application, an application assessment needs to be conducted by the TS&P Subcommittee and provide its recommendation to the Chairperson, who will forward it to the UAS Executive Committee for final deliberation.

5.2 Member Removal and Replacement

City departments are only authorized to fly UAVs if they are members of the UAS program in a good standing. The UAS Executive Committee has the authority to remove a member from the UAS program when it is determined that the department willfully violates UAS policies and/or is in violation of any federal, state, or local laws.

6. UAS EXECUTIVE COMMITTEE

The UAS Executive Committee develops, establishes, and approves policies for the UAS program for which all participating members must comply. The UAS Executive Committee approves participation in the UAS program and approves all departmental Standard Operating Procedures (SOPs) upon recommendation from the TS&P Subcommittee.

6.1 Executive Committee Membership

The UAS Executive Committee shall be made up of six permanent staff members, three rotating staff members and two community members, one with privacy/civil liberties expertise preferred and one at large. The permanent members will be the Assistant City Manager, Fire Chief, Police Chief, Aviation Director, Chief Assistant City Attorney and Chief Information Officer. The rotating member to the UAS Executive Committee shall be selected from current members of the UAS program. When community seats are vacant, an interested community member must submit an application with an explanation of why they want to serve on the Executive Committee.

6.2 Chair and Vice Chair of Executive Committee

The Chair and Vice Chair of the UAS Executive Committee shall be from the permanent members of the UAS Executive Committee.

The Chair of the UAS Executive Committee shall serve as the presiding officer for a two-year term. The Chair may not serve more than two consecutive terms.

The Fire Chief shall serve as the inaugural Chair of the UAS Executive Committee for a two-year term. Thereafter, the UAS Executive Committee will elect another member from the UAS Executive Committee as Chair for a two-year term.

The UAS Executive Committee must elect one of the permanent members as the Vice Chair for a two-year term. The Vice Chair will perform the role and responsibilities of the Chair when the Chair is absent or unable to fulfill his/her duties.

The UAS Executive Committee will elect a temporary presiding officer from the attending UAS Executive Committee in the event both the Chair and Vice Chair are absent or unable to fulfill their duties.

6.3 Meetings Frequency

The UAS Executive Committee shall meet quarterly, at a minimum, except to the extent the Committee determines to meet more frequently.

6.4 Special Called Meetings

A member of the UAS Executive Committee may call a special meeting with the consent of the Chair provided five working days' advance notice is given. In emergency circumstances, a meeting may be called with less than five days of advanced notice.

6.5 Quorum

A quorum is required to hold an official UAS Executive Committee meeting. A quorum is formed when a simple majority of the UAS Executive Committee members are present for the meeting.

6.6 Meeting Attendance

The UAS Executive Committee members may attend and participate in a meeting in person, by teleconference, or by video-conference.

6.7 Rules for Conducting Meeting

The UAS Executive Committee shall adopt bylaws to establish rules for its proceedings. The handling of a meeting item not specifically covered by the Committee's bylaws shall be decided by the presiding officer. If after the close of the hearing and during its deliberations the Committee determines that any ruling of the presiding officer was in error, it may reopen the hearing or take other actions as it deems appropriate to correct the error. All decisions of the presiding officer are subject to a majority vote of the Committee.

6.8 Voting Methodology

Each member attending the UAS Executive Committee meeting must vote on all items before the Committee, unless the member has a good-faith reason to abstain from voting and has explained their rationale to the Committee.

6.9 Voting

Each member of the UAS Executive Committee can cast only one (1) vote per action item. The Chair and Vice Chair are voting members in all items.

A vote must pass by the affirmative vote of a simple majority of the attending members during a meeting, except those matters which require super-majority approval.

In case of a tie in votes on any motion, the motion fails.

6.10 Super-Majority Voting

A two-third affirmative vote is required for certain issues of fundamental importance. The following items shall require Super-Majority voting:

- Termination of a member from the UAS program;
- Procuring UAS outside of the recommended list;
- Approving procedures below the minimum requirements of this A.R.

6.11 Waiver

A member of the UAS program may submit a waiver application to the TS&P Subcommittee for its review and recommendation to the UAS Executive Committee for its consideration of a particular item justifying the need to deviate from the approved list.

6.12 A waiver is granted with the consent of two-thirds of the attending members of the UAS Executive Committee.

6.13 Escalation and Conflict Resolution

In the event an item that requires securing a super-majority of the attending members of the UAS Executive Committee, the item or the issue can be escalated to the City Manager for a ruling.

7. TECHNICAL, SECURITY AND PRIVACY (TS&P) SUBCOMMITTEE

The role of the TS&P Subcommittee of the UAS program is to advise and provide recommendations to the UAS Executive Committee as they consider items put before them.

7.1 Composition of the TS&P Subcommittee

- This subcommittee shall be led by Information Technology Services (ITS) along with representation from Fire and Police Department UAS Program Managers, PFD Technical Services, PPD Information Technology Bureau and the Aviation Department. A representative from the City Attorney and the Risk Management departments will be part of this subcommittee.

7.2 Responsibilities

The TS&P Subcommittee is responsible for, but not limited to the following:

- Review and recommend membership applications;
- Review and provide guidance on developing departmental SOPs and make recommendations to the UAS Executive Committee for its approval;
- Review and recommend disposition on waiver requests;
- Review and recommend storage and data handling of departmental UAS program;
- Establish minimum requirements to protecting PII;
- Establish minimum requirements to protect the civil liberties of the general public, including the freedom of speech and assembly; protect against unreasonable search of seizure; and protect public's expectations of privacy.

7.3 Subcommittee Rule

The TS&P Subcommittee shall adopt bylaws to establish rules for its proceedings and develop a process for intaking SOPs from participating member departments where the lifecycle of the SOP review and approval process shall not take more than 90 days.

7.4 Subcommittee Meetings

The TS&P Subcommittee shall meet monthly except to the extent that the subcommittee determines to meet more or less frequently.

7.5 Meeting Attendance

The TS&P Subcommittee members may attend and participate in a meeting in person, by teleconference, or by video-conference.

8. DEPARTMENTAL STANDARD OPERATING PROCEDURES; REVIEW AND APPROVAL

This policy requires each department to develop and adopt written SOPs to accomplish department objectives in a manner consistent with the City's overarching UAS policy.

- 8.1 Each department with a UAS program will work in conjunction with the FAA and City of Phoenix Aviation Department regarding restrictions to operating on or near City-owned airports. In addition to complying with the FAA Low Altitude Authorization and Notification Capability process (LAANC), the UAS operator must notify the Aviation Department Airport Duty Manager (602) 273-3388 prior to conducting any operation that

occurs on airport property, or that exceeds any maximum altitude published on a FAA UAS Facility Map within 5 nautical miles of an airport.

- 8.2 To ensure protection of the civil liberties of the general public, including the fundamental, constitution, and legal rights of all citizens, departments will work in conjunction with the City Manager's Office and the Law Department.
- 8.3 To ensure proper storage and access to data, information and images, departments will work in conjunction with the IT Department.
- 8.4 To ensure public access to data, information and images, departments will work in conjunction with the Communications Office and the Law Department.

While departments may not develop procedures falling below the minimum requirements listed under the Policy Requirements section of this policy unless approved by a super-majority of the Executive Committee, departments may implement additional requirements when necessary to meet the needs of each department.

- 8.5 **SOP Approval Process**
Each department must submit their SOPs to the TS&P Subcommittee for review. Departments must receive clearance or affirmative recommendation on all SOPs from the TS&P Subcommittee before it can be placed on the UAS Executive Committee's quarterly meeting for their approval. All SOPs must be reviewed, recommended, or rejected within 90 days of submission to the TS&P Subcommittee.

9. POLICY REQUIREMENTS

The privacy and safety of Phoenix residents, businesses, visitors, and the general public are the top priorities of this policy. Departmental SOPs must be consistent with this policy and must comply with all federal, state, and local laws, as well as the requirements in A.R. 1.90 and 1.95.

- 9.1 **Privacy, Civil Rights, and Civil Liberties**
The City prohibits the use or operation of a UAV or the UAS in a manner that violates federal, state, or local laws, and prohibits the collection, use, retention, or dissemination of any information in any manner that would:
 - 9.1.1 Impinge on the right to free speech under the First Amendment of the US Constitution and/or Article 2, § 6 of the Arizona Constitution and the right against unreasonable search and seizure under the Fourth Amendment US Constitution and/or Article 2, § 8 of the Arizona Constitution. In addition, UAS shall not be used to violate any constitutional right of any citizen, including Victim's Rights, due process of law, the right to petition and assembly, or the right worship or religion:
 - 9.1.1.1 A UAV or UAS shall not be used or operated to violate a person's 4th Amendment protection against unreasonable search and seizure. Prolonged or extensive tracking or surveillance that reveals non-public information, such as detailed locations, affiliations, or movements is impermissible. Generally, if a person can conduct surveillance with authority or a warrant, a UAV or UAS can

also conduct the surveillance. Conversely, a drone may not be used to circumvent a search warrant;

9.1.1.2 A UAV or UAS shall not be used or operated to violate a person's reasonable expectation of privacy. Factors to include are locations that are not open to public use; where a person is an owner and has a right to control access and exclude others, or a location where a person has taken normal precautions to maintain privacy. A person does not have a reasonable expectation of privacy out in public or openly accessible places, or in places that can be viewed by the normal eye;

9.1.1.3 Incidental and transitory capture of information and images do not violate the 4th Amendment or an expectation of privacy. For example, aerial flyovers of homes, neighborhoods, or businesses in route to an incident are allowable, but unnecessary and unauthorized stationary surveillance or hovering over of a person or place, without the appropriate authority, is not allowed.

- 9.1.2 Harass, coerce, or discriminate against persons based upon their ethnicity, race, gender, national origin, religion, sexual orientation, or gender identity, in violation of law;
- 9.1.3 Search for specific faces or utilizing face surveillance technologies or software of any kind;
- 9.1.4 Be for personal use of any type.

9.2 To preserve individual's privacy, civil rights and civil liberties, each department is required to follow best practice guidelines developed by the applicable federal or state agency or relevant industry or professional organization. Department's SOPs must address following:

- 9.2.1 Provide prior notice to public of general timeframe and location of when UAS will be operated will be provided except when that is not possible or reasonable for public safety operations;
- 9.2.2 Take reasonable care and due diligence when operating UAS or collecting and storing covered data;
- 9.2.3 Develop an information management plan that ensures collection, use, storage and dissemination of collected data in adherence to A.R. 1.90, A.R. 1.95, and Arizona public records laws. Consideration must be given to reasonable expectations of privacy, as those circumstances may arise;
- 9.2.4 Implement an administrative, technical, and physical data securing program that meets ITS' minimum information security standard;
- 9.2.5 Ensure compliance with evolving federal, state, and local UAS laws by updating departmental SOPs.

Each departments SOPs must address how they will handle public record requests and specifically describe how and where the public can file complaints, which shall include the City Manager's Office and the City's Integrity Line. Each departments SOPs also must address record management and retention processes while complying with A.R. 1.61. These SOPs shall be reviewed and approved by the Law Department prior to submission for approval by the Executive Committee.

9.3 Security

Security is paramount to having a successful UAS program. ITS will establish minimum standards/requirements for department UAS programs. Departments are required to develop SOPs that address these security standards/requirements to include, among other things, the following areas:

- 9.3.1 Identify Security controls addressing various drone inputs connected to the enterprise network;
- 9.3.2 Where and how data will be stored – what controls are in place to address various regulatory requirements for data access and usage, depending on the type of data, and how the data will be accessed or disseminated;
- 9.3.3 Identify security controls addressing access to data and information;
- 9.3.4 Identify security controls addressing cloud hosted application and data;
- 9.3.5 Must address data protection mechanism during at rest, in use, and in motion;
- 9.3.6 Must address firmware upgrade process, describing specific security controls that are in place.

10. STORAGE

Each department is required to consult with ITS for their UAS storage need. In consultation with ITS, the department is to develop a storage architecture plan that needs to be submitted to the TS&P Subcommittee for their review. Data stored should be mission critical and should be stored for a limited amount of time and comply with applicable records retention laws and policies. The time of storage, location of storage, and who shall have authorized access to data shall be considered depending on the source and type of data and shall be specified in the department SOP.

11. ACCEPTABLE UAS FOR THE CITY OF PHOENIX

The City UAS Program members shall only procure and operate UAS' from the United States Department of Defense (DoD) approved fleet of UAS. DoD's Defense Innovation Unit has recommended a few UAS makers who meet the stringent security standards of the DoD. **Any requests for deviations from the DoD recommended fleet of UAS' shall be submitted in writing to the UAS TS&P Subcommittee for review and recommendation to the UAS Executive Committee, who will make the final waiver determination. It is required that departments obtain a waiver from the City's UAS governing body before procurement and ultimate use of UAS' not previously found on the DoD approved fleet list. UAS' previously purchased by departments prior to this policy which do not comply with the DoD approved fleet list must follow the same waiver approval process.**

12. TRAINING, CERTIFICATION, AND REGISTRATION

All City department UAS pilots/observers must complete all required training and certifications in accordance with FAA guidelines, Code of Federal Regulations, and all applicable laws prior to the deployment of any UAV.

All UAS deployed by the City must be registered as required by the FAA, the Code of Federal Regulations, and all applicable law.

All UAVs deployed by the City must be labeled with the City of Phoenix logo.

All UAS Training, Certification, and Registration documents will be maintained by each City department operating a UAS program.

12.1 Safety

All UAS operated by City departments will only be operated in a safe manner and in accordance with all FAA guidelines. Due regard for the safety of department personnel, the public, navigable airspace, and surrounding property will take priority over the need for deployment.

13. PROHIBITED USES

For the purpose of conducting City's business, all City department personnel are prohibited from self-deploying or piloting any UAS platform not owned by the City department and/or for which such personnel do not possess the appropriate FAA certification to operate.

Prohibited uses may include, but are not limited to the following:

1. Any use that violates federal, state, or local laws, regulations, or ordinances;
2. Deployment and operation of UAS outside of FAA guidelines;
3. Deployment and use of UAS for other than for official City purposes;
4. Use of personal equipment during UAS operations;
5. Use of UAS to carry hazardous materials;
6. Equipping UAS with any type of weapons, or modifying a UAS to deploy any projectile, biological, or chemical agent;
7. Operating outside of approved flight plan;
8. Operating UAS on, or in the immediate vicinity of any airport without prior approval;
9. To conduct unauthorized surveillance activities;
10. Deployment of the UAS in violation of the United States Constitution, federal laws and/or regulations;
11. Deployment of the UAS in violation of the Arizona Constitution, state laws and/or regulations, or City ordinances, policies or requirements;
12. In conditions that exceed the manufacturer's recommended limitations, including but not limited to range, ceiling, wind strength, and battery charge;
13. To intentionally pursue, harass, disturb, or destroy wildlife;
14. Any use by any person without the proper waiver or license to operate a UAV or UAS;
15. Any unauthorized mission, use, or deployment of a UAV or UAS.

Note - Deployment of a UAS in restricted air space or within the immediate vicinity of an airport will require all necessary waivers and approvals.

13.1 No Fly Zones / "No Drone-Zones"

All UAS flights conducted by City department personnel will be conducted in accordance with existing FAA guidelines governing flight operations within the NAS.

Each department seeking to deploy UAS technology shall determine the necessity of deploying within a designated "no-fly" zone, and if necessary, will contact the FAA for authorization before deploying.

14. INVENTORY AND MAINTENANCE

14.1 Inventory Management

Each City department will designate a UAS Program Manager responsible for establishing an inventory management system for records keeping of UAS equipment assigned to their department. Although the following list is not all inclusive, Program Managers will be responsible for tracking the following UAS information:

- 14.1.1 All purchasing documentation for each UAS platform to include the serial number, make, and model;
- 14.1.2 The location and department employee the UAS are assigned to, and where it is stored;
- 14.1.3 A description of any complimentary technologies assigned to each UAS platform (i.e., FLIR, sensor technology, etc.);
- 14.1.4 A tracking schedule for each unit for when new software/firmware updates are due or when completed;
- 14.1.5 Developing a warranty schedule for each unit and schedule for repairs with the authorized vendor support team.

14.2 Maintenance

Department UAS Program Managers will oversee and coordinate the maintenance of their department's fleet. Warranty work, repairs and service will be handled by the UAS manufacturer or a certified third-party vendor that has been approved by the UAS manufacturer.

The UAS Program Manager is responsible for any general maintenance or updates of their UAS before and after each flight to ensure a state of operational readiness is maintained. Any maintenance exceeding the UAS Program Manager's ability on-site will be referred to the manufacturer for repairs.

14.3 Storage and Transport

City department personnel responsible for deploying UAS will ensure the equipment is properly secured to prevent against physical theft or damage during transport and storage. Specific consideration will be given to the following:

- 14.3.1 UAS will not be left unattended in vehicles during deployments or when not in use;
- 14.3.2 UAS will only be stored in approved containers/cases and transported in accordance with manufacture recommendations;
- 14.3.3 To preserve battery life and prevent propeller warping, every effort will be made to protect the UAS from intense heat and direct sunlight;
- 14.3.4 When UAS in stored, battery must be charged.

15. LIABILITY INSURANCE

City of Phoenix Risk Management is the only department authorized to place insurance coverage on any City-owned UAS. City liability coverage must be in place for each UAS prior

to deploying. The City's liability insurance policy only covers the UAS and pilots which have been added to the policy.

To add a UAS pilot to the City policy, an application must be completed and submitted to Risk Management for each pilot and UAS.

The applications can be obtained directly from Risk Management who will submit the application along with any supporting information to the City's insurance carrier for approval. Risk Management will make notification to the applicant once they have been successfully added to the policy.

16. TRANSPARENCY

The City is committed to promoting transparency regarding the use of UAS technology by City department's activities within the NAS by following best practices published by the FTC. City departments using UAS shall follow existing City policies regarding Public Record Requests for UAS flight information (A.R. 1.61 Revised). Departments will maintain their own data and adhere to department's information management plan. The UAS program led by the UAS Executive Committee will continue to update the public and city leadership as technology evolves or significant changes are made to the UAS program.

17. COMPLIANCE/OVERSIGHT

The Chief Information Security Officer (CISO) is responsible and accountable for implementing security apparatus that assures confidentiality, integrity and availability of information (A.R. 1.84).

The City Auditor Department is empowered to conduct periodic audits to evaluate department's compliance with approved policies, A.R.s, and SOPs. The City Auditor is empowered to conduct periodic audits to evaluate a departments compliance related to information security (A.R. 1.84 and 1.90). CISO and City's Auditor Department will make available to the City Manager's Office and the UAS Executive Committee any security control deficiencies, any violation, abuse, or misuse of UAS technologies by the UAS program members.

Each department shall be responsible for the development and delivery of training for its personnel assigned to a UAS program to include all recurring training and documentation.

18. VIOLATION OF THIS ADMINISTRATIVE REGULATION

Violations of this administrative regulation, especially violations involving privacy or civil rights infringements, will be taken very seriously. Allegations of violations will be fully investigated. Any person found to have violated this A.R. shall be subject to disciplinary action, up to and including suspension or termination of employment.

19. APPENDIX

1. A.R. 1.61 Records Management Program
2. A.R. 1.84 Information Security Management

3. A.R. 1.95 Privacy Program
4. DOD Approved list of UAS.
<https://www.diu.mil/autonomy-blue-suas>
5. CISA Cybersecurity Best Practices for Operating Commercial Unmanned Aircraft Systems
<https://www.cisa.gov/sites/default/files/publications/CISA%20Cybersecurity%20Best%20Practices%20for%20Operating%20Commerical%20UAS%20%28508%29.pdf>
6. Federal Aviation Administration (FAA) Part 107
[Certificated Remote Pilots including Commercial Operators \(faa.gov\)](https://www.faa.gov/air_traffic/flight_info/aeronav/digest刊物/part107)
7. Federal Trade Commission Best Practice
[Careful Connections: Keeping the Internet of Things Secure | Federal Trade Commission \(ftc.gov\)](https://www.ftc.gov/privacy/connected-devices)
8. National Institute of Standards and Technology (NIST) 800-53 (Rev. 5)
[SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC \(nist.gov\)](https://www.nist.gov/sp/800-53)

20. QUESTIONS

Questions regarding this Administrative Regulation (AR) should be directed to the Fire Department at 602-262-7110.

Jeffrey Barton, City Manager

By: 
Ginger Spencer
Deputy City Manager