



## U.S. Department of the Interior (DOI)

### Office of Aviation Services (OAS)

## Unmanned Aircraft Systems (UAS) Best Practices for Responsible Operations

**Opportunities:** Unmanned aircraft systems (UAS) offer unprecedented access to data, information, knowledge, and supported action that heretofore has only been available to agencies with significant and expensive aviation, sensor, and data processing resources and highly trained aviation and remote sensing personnel. UAS/drones have “democratized” access to the 3rd dimension with low cost, highly capable aircraft that require little if any training to successfully fly in support of a wide range of agency missions. This has enabled agencies to put aviation resources directly in the hands of highly specialized field personnel. The explosive growth of the consumer and commercial drone market has also fueled the dramatic development of newer, more capable, smaller, and lighter-weight sensors and attendant data processing software. Together, they provide agencies with the ability to achieve significant enhancements in **Sensing**, which promotes better and more transparent decision making, improvements in **Safety** by

removing personnel from traditionally hazardous mission environments, increased **Savings** through reduced acquisition, training, maintenance, and operating costs, and more responsive **Service**, particularly for missions that do

not follow regular, predictable occurrences and demands.

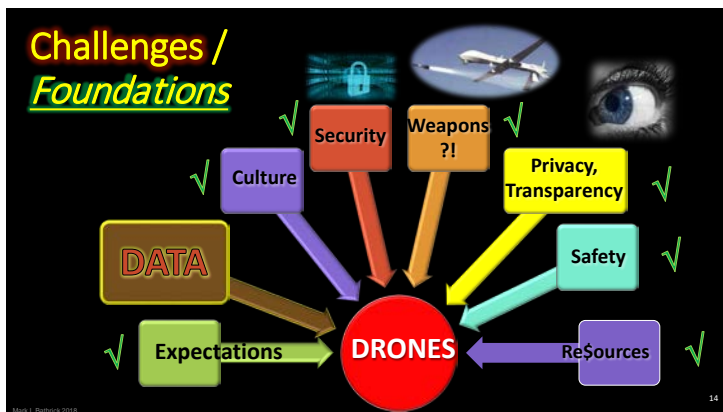
### What is the Problem to be Solved?

1. Close / eliminate gaps in current outcomes?
2. Traditional aviation was desired, but ill-suited?
3. “Leap-Frog” opportunity?

[HTTPS://WWW.DOI.GOV/AVIATIONUAS](https://www.doi.gov/aviationuas)

**Challenges:** Many of the attributes that underpin the unique opportunities drones offer to agencies also serve as the origin of the challenges they face.

Drones have a long history as weapons of war and intelligence gathering. These images have been magnified and solidified in pop culture. The unique ability of drones to put highly capable aviation assets into the hands of those with little to no aviation experience increases the risk of safety mishaps and airspace violations. Likewise, highly experienced aviators without UAS program experience may not appreciate the data processing, security, and privacy, issues that manned aircraft rarely deal with. Agencies that are successful in integrating drones into their aviation operations are able to bring together executive leadership and an assembled team with experience and vision in [aviation, security, privacy, and culture](#). Those agencies that fail to assemble and empower a team with these competencies will eventually find itself the unfortunate subject of various oversight audits, media articles, and congressional interest of the wrong variety.



**1. Organizational Structure and Oversight:**

Federal agencies that employ aviation in support of their missions must provide the requisite level of management and oversight structure to meet applicable legal and regulatory requirements. Many agencies' flight operations fall under the legal definition of Public Aircraft Operations (PAO) as defined in 49 U.S.C. § 40102(a)(41), 49 U.S.C. § 40125, and FAA Advisory Circular

**Legal Requirements Drive OAS Roles and Responsibilities**

1. Code of Federal Regulations (14 CFR)
2. OMB regulatory requirements
  - A-11, A-76, A-94, A-123, A-126
3. GSA Federal Management Regulations (FMR)
  - FMR 102-33

- Apply to all Federally funded aviation activities
- Establish requirements for OAS roles and responsibilities
  - Establish Departmental flight standards for management, administration, operations, safety, accident reporting, training, aircrew qualifications, maintenance, finance, etc.

00-1.1B. The FAA has no regulatory authority over PAO, which means agencies are responsible for oversight of their aviation operations, including aircraft airworthiness and any unique operational requirements. Similarly, government agencies that contract for aviation services assume all responsibility for oversight of PAO they perform. Within DOI, the Office of Aviation Services (OAS), part of the Office of the Secretary, serves in this management and oversight role. Comprising only 78 Full Time Equivalents (FTE), OAS oversees hundreds of manned and unmanned fleet aircraft and hundreds of contracts supporting access to over 1,000 commercial aircraft supporting DOI missions from Puerto Rico across all 50 States to the Western Pacific Territories. Key to OAS's ability to do so much with so few personnel is the 1,000+ cumulative years of aviation experience resident within OAS. Strong, experienced executive leadership with a proven history of building and managing high risk aviation programs in a collaborative environment is key to program success. Unity of management and oversight is also critical. Drones are high visibility in the public's eye and potential privacy, safety, waste or other issues of misuse will quickly damage an agency UAS program's reputation.

It must be remembered, UAS are simply a unique category/class of aircraft. They are



defined as aircraft by Congress and should be managed as much like manned aircraft (e.g. acquisition, inventory procedures, operating standards, training, safety, mishap and hazard reporting, etc.) as possible. Agencies that seek to treat them different than aircraft will double their work and halve their success. UAS should also be

treated as the name implies as a system, comprised of a vehicle, sensors/payload, and processing elements. Focusing solely on one element of the system rather than the system as a whole will result in disappointing results.

2. **Mission Set Differentiation:** With UAS, it is important to understand the mission sets you plan to employ drones on and the relative security risk of each. Regardless of the mission, all agency drones should incorporate encrypted control links and encrypted payload links. Also, agencies should establish standards/policies for data sharing with equipment, software, and supporting analysis processing providers. Interior's requirement is that we decide the type and amount of data we share.

**Publicly releasable data** is the lowest sensitivity UAS mission set. If the data being collected is going to be released to the public or would be subject to a

Freedom of Information Act request (FOIA), then use of UAS with known or risks of inherent data sharing with manufacturers might be permissible. It is important to note that while the transfer of UAS-acquired publicly releasable data to foreign servers might not undermine specific operations, it could result in an erosion of public trust in agency UAS operations and cyber security. Additionally, it should be noted that open-source, non-sensitive unclassified data can often be used to assemble a product that could be seen as sensitive or even classified.

**Sensitive** data should only be collected by UAS that ensure no unwanted data is shared with manufacturers.

**Personally Identifiable Information (PII)** should only be collected by UAS that

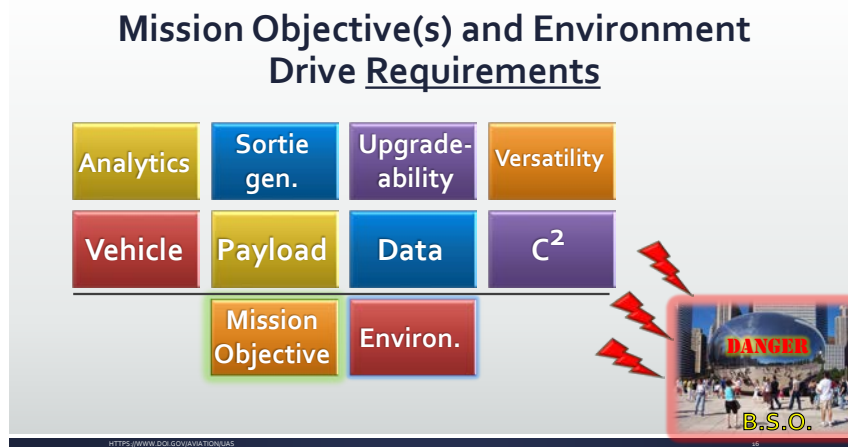
ensure no unwanted data is shared with manufacturers. Additionally, PII requires special handling once it is collected. Ensure trained personnel and PII compliant systems are used in these operations.



**Classified** data should only be collected by UAS specifically tested and authorized to collect such data. As with PII, classified data requires special handling once it is collected. Ensure trained personnel and classified data compliant systems are used in these operations. DOI has not currently been asked to support UAS missions involving classified data.

### 3. **System Requirements Determination and Discipline:**

A strong, documented, and widely shared mission-based UAS requirements document is essential to ensuring your UAS program is efficient, effective, and able to pass the scrutiny of management and security oversight agency audits and reviews.



ONLY UAS that meet the written and approved requirements document should be acquired. Beware the seductive “*bright shiny object*” (BSO) of the “*latest and greatest*” new drone. ALL UAS should be acquired through a centralized office practiced in the management and legal and regulatory compliance of government aircraft programs. Even though the cost of a UAS may be below the purchase card threshold, they should not be procured by individuals using this method, but through a designated central office. Agencies that fail to develop and stick to strong, written and approved mission-based requirements will end up with an unmanageable collection of diverse UAS, increasing the safety, security, and mismanagement risk. As aircraft, ALL Federal UAS flight activities and costs must be logged and reported in accordance with applicable CFR’s, OMB Circulars, and Federal Management Regulations.

There are THREE critical security requirements that every agency UAS should meet.

- (1) **Encrypted control links** prevent the easy “hijacking” of agency drones. Without this, agency drones run the risk of being taken over by a nefarious actor and flown where they are not intended or intentionally crashed. This can result in security and privacy breaches, damage to personnel and property as well as embarrassment to the agency. Applies to fleet and contracted UAS.
- (2) **Encrypted payload links** prevent the easy interception of UAS-acquired data by unauthorized parties. Without this, live streaming UAS data is vulnerable to interception and exploitation. Applies to fleet and contracted UAS.
- (3) **Enterprise control of data sharing** ensures only that data the agency wishes to share with UAS vehicle/payload/software processing companies is transferred. Agencies should take a number of steps to ensure the data sharing


controls are not countermanded at the operational level. These include policy, training, hardware/software lockouts, and signed acknowledgement of operator responsibilities to avoid “jail-breaking” the enterprise level data sharing controls. Applies to fleet and contracted UAS.

**Example UAS Requirements Categories:**



1. Platform weight.
2. Platform size.
3. Flight duration.
4. Service ceiling.
5. Max operating winds.
6. Min launch area.
7. Min recovery area.
8. Takeoff mode req'd.
9. Operating temperature.
10. Maintainability.
11. Day, night.
12. Auxiliary launch and/or recovery equipment
13. Propulsion / fuel restrictions.
14. Noise limits.
15. Range.
16. Special markings.
17. Operate in precipitation.
18. Training and manuals.

 **Example C<sup>2</sup> Requirements**

- |                                       |                                 |
|---------------------------------------|---------------------------------|
| 1. Control link range.                | 8. Operating crew members.      |
| 2. Control link frequency.            | 9. Payload link range.          |
| 3. Control link security.             | 10. Payload link frequency.     |
| 4. Programmable lost link capability. | 11. Payload link security.      |
| 5. Common ground control station.     | 12. Payload link bandwidth.     |
| 6. Direct pilot mode.                 | 13. Onboard recording capacity. |
| 7. Semi-autonomous mode.              | 14. Geo-fencing capability.     |
- 

35


Mark L Bathrick 2015

 **Example Payload Requirements**

- |                                      |                                |
|--------------------------------------|--------------------------------|
| 1. Weight.                           | 9. Ease of removal.            |
| 2. Form factor.                      | 10. Interoperability.          |
| 3. Power required.                   | 11. External data connections. |
| 4. Connectors.                       | 12. Resolution.                |
| 5. Fixed or gimbaled.                | 13. Speed.                     |
| 6. Onboard storage.                  | 14. Overlap.                   |
| 7. Payload triggering mechanism.     | 15. Matched to mission.        |
| 8. Integration with vehicle systems. | 16. EMI / EMC.                 |

36

Mark L Bathrick 2015



## Example **Data & Ancillary** Requirements

<b>Data</b>	<b>Ancillary</b>
1. Format.	8. System maintenance – organic or service.
2. Bandwidth.	9. System simulator.
3. Storage.	10. Flight planning software.
4. Manual or automated analytics.	11. Sortie generation rate.
5. Output format.	12. Upgradability.
6. Integration with other systems.	13. Reliability.
7. Security.	14. Availability.

Mark L. Gatzrick 2015 37

4. **UAS Policy:** Successful agency UAS programs are founded on strong agency manned aviation programs. Remembering that UAS are simply a unique category/class of aircraft, UAS programs should strive to only develop UAS policy that is not already covered by established manned aircraft policy. As an example, Federal laws and regulations already speak to the accepted processes, procedures, and management of aircraft justification, fleet acquisition, contracting, safety, management, etc. By using existing agency aviation policy as a foundation, organizations reduce the time to develop it while also reducing the chance for errors that attempting to develop stand-alone UAS policy will result in. As an example, DOI has 310 pages of aviation policy that has served as the basis for over 45 years of professional and safe aviation mission support to the Department. In building our UAS program, DOI relied on this first and only needed to add 26 pages of additional, UAS-specific policy ([Operational Procedures Memorandum 11 - OPM-11](#)). OPM-11 recognizes unique attributes and vulnerabilities of UAS and addresses them in a concise manner, while reinforcing that UAS are aircraft by using long-established agency aircraft policy as a foundation for UAS operations.
  
5. **Training:** Having a comprehensive training program, tailored to the unique attributes of drones and drone use and the constituency of operators and management involved is critical to building and sustaining a successful UAS program. Some specific elements to consider include:



**Aviation for Non-Aviators** - Integrating drones into your agency's aviation mission tool kit will result in **at least a 50% increase** in the number of agency employees engaged in aviation, either as operators or as supervisors/managers/executives overseeing these personnel and operations. Not only must your agency be prepared to efficiently handle this increased training and oversight requirement, but you must ensure the training is tailored to the unique characteristics of this new constituency. As most of the new personnel using UAS in your agency won't be traditional manned pilots with years of experience in aviation, your training must be structured to give them the tools they'll need to be safe and successful in their mission and as representatives of your agency. One way we drive this in DOI is by insisting all prospective DOI drone operators first obtain their Part 107 commercial drone operator's certification from the FAA. Additionally, recognizing they lack the training and experience of manned aircraft pilots, we emphasize **airspace responsibilities**, their **responsibilities for people and property on the ground beneath them**, and work to instill the **safety management system (SMS) culture** that is core to manned aviation safety programs. We also incorporate elements of this training into the manager training we already require for all supervisors/managers/executives who are responsible for aviation within elements of the agency.

**Information Security** - An effective UAS training program must include the subject of information security. Discussions of the importance of encrypted control and payload links, enterprise data management, the potential vulnerabilities of using unauthorized third-party applications, and the need for cradle-to-grave control of data, based on its sensitivity level should be part of this training element.

**Privacy and Outreach** - Embedded public perceptions of drones as tools of the military and intelligence communities and their unique ability to obtain high volumes of high resolution data that were previously unobtainable by manned aircraft necessitates a thoughtful discussion of privacy and outreach in any agency UAS training course. Training should include



discussions regarding the right to privacy and the specific requirements of the [2015 Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems](#). Training should also include



discussions regarding the value of and the techniques to employ effective pre and post mission outreach to the public whenever possible. Pre-mission outreach to the public, followed by post-mission reports, articles, data, etc. goes a long way to

1. Agency policies and procedures for **collection** and **use, retention, and dissemination**, of **information** collected through unmanned aircraft in the National Airspace System (NAS).
2. No collection, use, retention, or dissemination of data that would violate the **First Amendment** or would **discriminate** against persons based upon their ethnicity, race, gender, national origin, religion, sexual orientation, or gender identity.
3. Federal agencies must ensure effective **oversight**.
4. To promote transparency, agencies will **publish** information **within one year** describing how to access their **publicly available policies** and procedures implementing the PM.
5. Requires agencies to **examine** their UAS **policies** and **procedures prior** to the **deployment of new UAS technology**, and at **least every three years**, to ensure that protections and policies keep pace with developments.

assuaging public fears surrounding “government drone operations” and has even proven useful in generating support for these operations across additional mission applications. To see proof of this, you only need to consider that after 19,000 UAS mission flights DOI has conducted across public lands Interior stewards in 37 States, the Department has **not** experienced one complaint from the public. Additionally, Interior’s drone program has been the subject of over [50 positive news articles from the Washington Post, Wall Street Journal, and other notable news outlets](#), while receiving [high praise from Senators in public testimony](#).

**Disciplined Execution** – “A great idea, poorly executed, is NEVER a great idea” (Mark Bathrick, 2006). All your great plans, policy, training, etc. are for naught if your program lacks the disciplined execution and closed loop feedback mechanisms (like those in the ISO 9001-2015 standard) that promotes consistent and repeatable results.



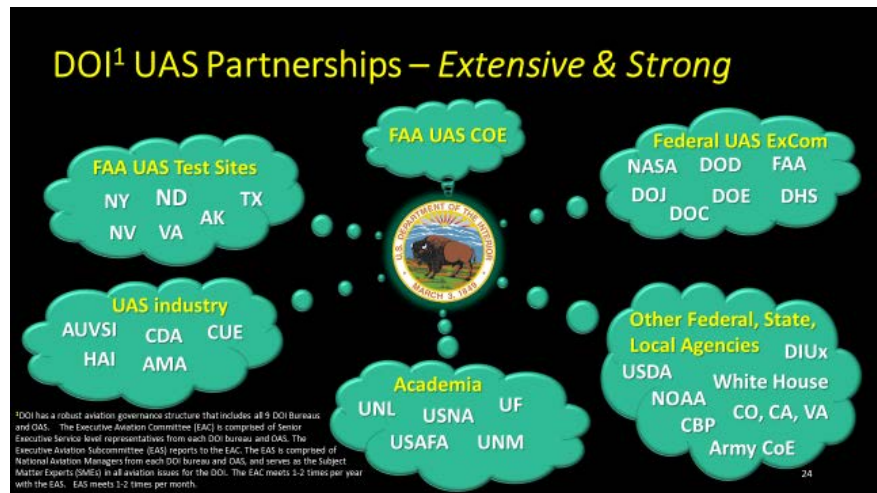
6. **UAS Program Transparency & Outreach** must not only be part of the training curriculum for agency drone operators, program managers, supervisors, and executives, but it must be integral to the agency’s UAS program strategy for a successful and secure program. As an example, Interior’s transparency and outreach strategy also includes detailed flight reporting requirements by agency pilots that supports detailed reporting that is included on our various [public UAS webpages](#). In doing this as an agency, we have steadily built trust with the media and the public that our [“Drones for Good”](#) program is responsibly and safely run. This has freed up time and resources that would have otherwise been spent on addressing media/public concerns/complaints, allowing us to focus on program enhancements, including data security enhancements. [Interior’s annual UAS Use Report](#) is a good example of this transparency and outreach.
7. **“Terrestrial” Data Security**: UAS data security doesn’t end when the data reaches the ground. Poorly designed or executed plans and processes for handling the huge volumes of drone data that are stored, processed, and distributed on the ground pose as much of a security vulnerability as unencrypted control/payload links and unconstrained data sharing do. Everyone involved in drone operations must understand that data is currency and that lost data is like lost money; not good. In addition to “new aviators,” agency UAS programs will find themselves dealing with people who are new to data management (certainly on the scale drones are capable

of collecting) and data security. It is critical to include training and policy on “terrestrial” data security in your agency’s drone program. It is also important to engage your OCIO early in the program. They can assist you in understanding and applying the requirements for data security on government systems and help you safely navigate toward the use of things like cloud services (e.g. like understanding [FEDRAMP](#) compliance).



- Partnering to Stay Current:** The UAS/drone space is a fast-paced technology and business space. The most successful and secure programs collaborate with government, industry, and academia partners to stay current with technology, policy, and best practices, while conserving precious time and resources by leveraging each other’s expertise.

In the area of drone airworthiness for public aircraft operations, Interior has partnered with NASA, where we leverage their established airworthiness expertise and long practiced vehicle review structure to



provide an added level of assurance for all fleet and contract drones Interior employs. Likewise, Interior has partnered with NASA, DOD, DHS, and private industry on UAS data management assurance issues and verification of potential solutions. Agencies need to invest time, resources, and a commitment to share with others if they want to be considered valued partners in this nascent ecosystem. This includes regular attendance and participation in trade shows, discussions with UAS

trade groups and connecting with individual companies to share your mission specifics and current and future requirements and learn about their products, services, and research activities. Only through this deliberate practice can you ensure industry will build you the products and services that meet your mission, safety, and security needs.