United States Department of the Interior
Office of Aviation Services
300 E Mallard Drive, Suite 200
Boise, Idaho 83706-3991

DOI OPERATIONAL PROCEDURES MEMORANDUM (OPM) - 11

Subject: DOI Use of Uncrewed Aircraft Systems (UAS)

Effective Date: January 1, 2023

Last Updated: December 2, 2022

Expiration: December 31, 2023

1. Summary of Changes.

Added language to include provisions of Deputy Assistant Secretary for Public Safety, Resource Protection, and Emergency Services Memorandum "Updated Uncrewed Aircraft Systems (UAS) operations and procurement policy" dated 10/21/2022, changed terms from Emergency Certificate of Authorization (ECOA) to Special Governmental Interest Certificate of Authorization (SGI COA) to reflect the change to Federal Aviation Administration (FAA) procedures, changed the term "unmanned aircraft system" to "uncrewed aircraft system', and changed periodic UAS inspection period to 12 months instead of 24 months. Added requirement for a functional flight test of systems during the annual inspection and clarified flight use reporting procedures for DOI remote pilots operating United States Forest Service (USFS) UAS. Added length of assignment limitations of 14 or 21 days for remote pilots, reduced the number of possible endorsements on the OAS-30U, and added the ability for a UAS evaluator pilot to work with expired remote pilots to regain currency. Added a section delineating training roles for UAS inspectors, instructors, and evaluators, included including updated Department of Homeland Security (DHS) best practices for commercial UAS operations and updated links to various documents in the appendix.

2. Purpose.

The purpose of this OPM is to provide DOI with a policy on the operations and management of Uncrewed Aircraft Systems (UAS) within the Department of the Interior and on Department of Interior-managed lands and waters.

3. Authority.

This policy is established by the Director, Department of the Interior (DOI or Department), Office of Aviation Services (OAS) in accordance with the provisions of Departmental Manual 112 DM 12, 350 DM 1; Secretarial Order 3322, dated August 23, 2012; Presidential Memorandum on Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems, dated February 15, 2015; Executive Order 13981, Protecting the United States from Certain Unmanned Aircraft Systems; Secretarial Order 3374 Implementation of the John D. Dingell, Jr. Conservation, Management and Recreation Act; and Executive Order 13855 Promoting Active Management of America's Forests, Rangelands, and Other Federal Lands to Improve Conditions and Reduce Wildfire Risk.

4. Scope.

This policy covers the acquisition and use of all UAS under the operational control of DOI bureaus and offices as well as operations under departmental contracts, grants, and cooperative agreements relying on UAS for achieving objectives.

5. Policy.

Policy for the use of all aircraft within DOI is contained in Departmental Manuals 350-353 (DMs) and the associated Operational Procedures Memoranda (OPMs).

A. Bureau-specific UAS policy pertaining to the use of UAS can be found in each bureau's national aviation management plan.

B. Current Federal Aviation Administration (FAA) policy is provided in 14 CFR Parts 91,107,135,137.

C. For all DOI UAS operations the following fundamental provisions apply:

1) 14 CFR 1.1 defines "aircraft" as a device that is used or intended to be used for flight in the air. UAS are considered aircraft and must comply with applicable regulations, policies, and procedures required by FAA and DOI and its bureaus and offices.

2) A DOI Remote Pilot is an individual who holds a both a current FAA Part 107 remote pilot certificate and a current OAS-30U DOI remote pilot qualification card.

3) A Remote Pilot in Command;

a) Has final authority and responsibility for the operation and safety of the flight;

b) Has been designated as a remote pilot in command before or during the flight; and

c) Holds the appropriate category, class, and type rating, if appropriate, for the conduct of the flight.

4) Aircraft and pilots must maintain compliance with OPM-11 and with applicable sections of Title 14 CFR to operate in the National Airspace System (NAS). The FAA retains the sole authority to approve UAS operations within the NAS. The controlling agency has the authority to approve UAS operations in active Prohibited and Restricted Areas, Special Flight Rules Areas, and the Washington DC Flight Restricted Zone.

5) UAS is defined as an aircraft and the associated elements (including communication links and the components that control the unmanned aircraft) that are required for safe and efficient operation.

6) Per 351 DM 1.2 B, DOI employees are not authorized to manipulate the controls of DOI UAS unless they possess a current DOI Remote Pilot card, are receiving a flight evaluation from an OAS-designated UAS pilot inspector, or are attending an approved DOI UAS training course.

7) Cooperator/Affiliate and vendor pilots and aircraft operating under DOI operational control must have an approval letter issued from OAS.

8) DOI remote pilots may not operate non-DOI UAS without authorization from OAS and notification to the Bureau UAS program manager.

9) When operating in Class A, B, C, D, E, and G airspace, DOI UAS must be operated in accordance with 14 CFR Parts 91 and 107, FAA Certificate of Waiver or Authorization (COA), Special Governmental Interest Waiver and any terms and conditions outlined in agreements between DOI/FAA.

10) UAS operations in Restricted, Prohibited, or Warning airspace will be regulated and approved by the controlling authority.

6. Roles and Responsibilities.

A. OAS (https://www.doi.gov/aviation/uas):

1) Coordinates fleet management, acquisition, and disposal of DOI-owned UAS.

2) Issues Department-wide policies, procedures, and training requirements.

3) Establishes UAS specifications and standards to ensure aviation safety and individual privacy, civil rights, and civil liberties protections in compliance with applicable laws, regulations, and policies.

4) Coordinates with internal and external agencies, partners, and organizations on UAS policy, acquisition, inspections, audits, compliance reviews, and proposed rulemaking.

5) Evaluating bureau cooperator approval requests. If approved, OAS will issue a letter of authorization to the requesting bureau. Joint cooperator approval letters with OAS/USFS will be signed by the OAS Division Chief, UAS and the Regional Aviation Manager from the requesting region of the USFS.

B. Office of the Chief Information Officer:

1) Promulgates and provides oversight of Department-wide information management policies, guidelines, and procedures to bureaus and offices for their implementation to ensure compliance with relevant Federal laws, regulations, and policies. Such policies, guidelines, and procedures include, but are not limited to, addressing requirements associated with privacy, IT security, and records management.

2) Publishes privacy policy, provides guidance, and collaborates with bureaus, offices, and program officials to evaluate program activities to ensure privacy considerations are addressed for the collection, use, retention, and dissemination of personally identifiable information and appropriate safeguards are implemented to protect individual privacy, civil rights, and civil liberties.

C. Office of Civil Rights:

1) Develops policy and guidelines to assure proper implementation of laws, Executive Orders, regulations, and Departmental initiatives relating to affirmative employment, equal opportunity, civil rights, and educational partnerships.

2) Oversees the management and evaluation of programs, activities, and services receiving Federal financial assistance, and ensures expedient processing and resolution of complaints of discrimination, prevention of discriminatory practices, and equal access to Federal financial assistance and federally conducted programs for all persons regardless of race, color, age, religion, sex, national origin, disability, and sexual orientation.

D. Bureau or Office:

1) Implements departmental and bureau or office UAS-specific policies, procedures, and protections consistent with applicable Federal laws, executive orders, regulations, policies, and standards.

2) Bureaus are responsible for contributing to the development, organization, and delivery of training required and authorized by DOI OAS.

7. UAS Acquisition.

A. Unless otherwise authorized, acquisition of UAS for DOI shall be limited to "non-covered" systems. All acquisitions of available approved systems by DOI personnel shall be routed through OAS and the Interior Business Center, Acquisitions Services Directorate (IBC- AQD). Specifications for UAS used by DOI will be developed collaboratively between the bureaus and OAS. Acquisition activities including requests for information, quotation, or proposal will be coordinated through the Bureau National Aviation Manager's office.

The term "covered UAS" as defined in EO 13981, and adopted for official use by the Department moving forward, means any UAS that:

1) Is manufactured, in whole or in part, by an entity domiciled in an adversary country.

2) Uses critical electronic components installed in flight controllers, ground control system processors, radios, digital transmission devices, cameras, or gimbals manufactured, in whole or in part, in an adversary country (As defined in Executive Order 13981.)

3) Uses operating software (including cellphone or tablet applications, but not cell phone or a tablet operating systems) developed, in whole or in part, by an entity domiciled in an adversary country.

4) Uses network connectivity or data storage located outside the United States, or administered by any entity domiciled in an adversary country; or

5) Contains hardware and software components used for transmitting photographs, videos, location information, flight paths, or any other data collected by the UAS manufactured by an entity domiciled in an adversary country.

The term "critical electronic component" means any electronic device that stores manipulate or transfers digital data. The term critical electronic component does not include, for example, passive electronics such as resistors, and non-data transmitting motors, batteries, and wiring.

B. Procurement Methods:

1) For UAS acquisitions the bureau shall complete the DOI UAS Acquisition Request Form (OAS-13U).

2) UAS purchases above the capital asset threshold of $25,000 will require an Aviation Business Case as described in OPM-08 as required by DOI-OIG Survey Report "recovery of costs of the working capital fund, Office of Aviation Services, Office of the Secretary" dated March 1997.

8. UAS Flight Services.

Contractor provided UAS Flight Services must follow the processes outlined in 353 DM 1 and OPM-35.

9. UAS Airworthiness Certification.

A. All UAS operated under DOI operational control, including cooperator aircraft, must have a current OAS-36U DOI UAS Data Card or letter of authorization issued by OAS.

B. Any modification to a DOI UAS, such as adding a new sensor may affect airworthiness and requires approval from the DOI UAS Fleet Management (OAS).

C. For UAS without a DOD, FAA, or NASA airworthiness review, OAS will conduct an airworthiness review and issue an airworthiness statement for the specific make/model/configuration of the UAS.

10. Periodic Inspections.

A. The DOI UAS Fleet Manager, in collaboration with the bureaus, determines the appropriate method of inspection and re-inspection of DOI UAS.

B. DOI Remote Pilots assigned a small UAS shall inspect the aircraft prior to the expiration of the OAS-36U and submit the inspection form online:

Link to Small UAS Inspection Form (Microsoft).

C. OAS-36U Aircraft Data Cards for small UAS, will be issued every 12 months, upon receipt of the inspection form. The Remote Pilot Operator must submit the inspection form no later than 30 days prior to the expiration of the OAS-36U.

D. If a UAS inspection is expired a new inspection must be completed and a current OAS-36U must be issued prior to the operation of that UAS.

E. The OAS Fleet Administrator will be responsible for updating all FAA registrations for DOI UAS and communicating new expiration dates for FAA registrations. The Fleet Administrator will not renew registrations for DOI UAS unless the annual inspection has been completed.

F. Large UAS (>55lbs) will be inspected annually, or as required by a contract, by an OAS-approved inspector or designee.

G. All periodic inspections for UAS and inspections following repair, and before return to service, shall accomplish the following tasks:

1) Confirm aircraft configuration conforms to the original manufacturer's design or OAS-approved modification.

2) Inspect the airframe of general condition and serviceability.

3) Note the serial numbers of the airframe and ground control station (GCS).

4) Perform preflight checklist.

5) Run systems diagnostics to confirm all test results are normal.

6) Check the battery charger and other peripherals for proper operation.

7) Ensure the system is operating on the OAS-approved firmware.

8) Confirm DOI UAS are registered and marked in accordance with FAA and DOI requirements.

9) Perform a functional flight test of the system.

11. DOI Remote Pilot Responsibilities.

A. DOI Remote Pilots shall possess a Part 107 FAA Remote Pilot Certificate prior to attending A-450 DOI UAS Training course. DOI Remote Pilots must maintain their Remote Pilot certificate as required by FAA.

B. The Remote Pilot In Command (RPIC) is responsible for and is the final authority as to the operation of the aircraft.

C. Remote Pilots are responsible for performing a preflight inspection of the UAS in accordance with the manufacturer's recommendations and assuring the aircraft is in an airworthy condition.

D. DOI Remote Pilots shall fly in accordance with the manufacturer's specifications and established DOI policy/training standards. Proposed deviations from established operational procedures (checklists, etc.), which may affect the safety of flight, shall be discussed with the NAMs, UAS Program Managers, and OAS prior to the deployment of such operations to minimize programmatic/operational risk.

1) If a procedure is required for a specific mission and was not instructed during A-450, then it is the responsibility of the PIC to contact their NAM/OAS to vet the process as described in paragraph 2. Examples of operations or procedures not taught in A-450 include, but are not limited to, launch and recovery methods other than those taught or described during approved training (i.e., launch and recovery involving hand catching or any method that increases the risk of human contact, launch and recovery from a vessel, or launch and recovery procedures from a moving vehicle not taught/endorsed by the manufacturer). DOI Remote Pilots must utilize the Non-Standard Operational Procedure form when requesting approval.

Link to DOI UAS Non-Standard Operational Procedure form (Microsoft).

2) Process for obtaining approval of a new procedure:

a) Bureau identifies a need that is outside of how the remote pilot was trained.

b) The DOI remote pilot who identified the need must contact the bureau NAM or designee to make a request for evaluation of the procedure.

c) If NAM or designee concurs then the bureau national aviation office and OAS will collaboratively work to create training and certification standards for the identified procedure.

d) Upon meeting the certification standards, the remote pilot will receive an endorsement on their OAS-30U for that procedure from an OAS-approved UAS inspector.

E. The RPIC must discontinue any flight in which the airworthiness of the aircraft or system is in question or there are discrepancies with the aircraft that have not been corrected or the cause of the discrepancy is not understood.

F. DOI Remote Pilots are responsible for ensuring they are qualified and current for any mission they intend to fly. This includes tracking expiration dates of their FAA and DOI pilot certificates.

G. Remote Pilots are responsible for ensuring their equipment has been inspected within the timeframe specified on the aircraft data card (OAS-36U).

12. UAS Use Reporting.

A. Fleet aircraft:

1) DOI remote pilots shall report all flights under DOI operational control (OPCON) in the OAS-2U system. DOI remote pilots utilizing USFS UAS under USFS OPCON shall report flights in both the USFS and DOI flight use reporting systems.

2) The DOI remote pilot shall record UAS flight time using the OAS-2U form. Updates shall be submitted at least monthly or at the conclusion of the project, whichever occurs first.

3) DOI Remote Pilots must record malfunctions, damage or repairs to UAS, and component replacement on the OAS-2U form. Repair of damage beyond normal wear shall be coordinated with the DOI UAS Fleet Manager.

B. Flight service contract flight use reporting will follow the reporting process outlined in the contract.

13. Flight Time and Duty Day.

A. Remote Pilots are limited to 8 hours of flight time during any duty day.

B. When conducting UAS operations, DOI UAS flight crewmembers are limited to a 16-hour duty day.

C. DOI Remote pilots conducting flight operations are limited to a 14-day assignment with two days off at the end of the assignment. Remote pilots may work up to a 21-day assignment with two days off at the end of the assignment with prior supervisor approval.

14. Visual Observer (VO) Requirements.

A. DOI Remote Pilots conducting operations under 14 CFR Part 107 must maintain visual contact with the UAS, or utilize a VO. The use of VOs must comply with the provisions of Part 107.

B. If operating under COA, MOA, or SGI Waiver the VO requirement of those authorizations must be complied with.

C. VO Training: Certain certificates of authorization/waiver (COAs) require that observers must have completed the required training to communicate to the pilot any instructions required to remain clear of conflicting traffic. DOI Remote pilots shall ensure that VO training requirements have been met. Refer to 14 CFR part 107 or COA/SGI as applicable.

15. Visual Observer Responsibilities.

VOs must:

A. Have a clear view of the area of operation.

B. Be in communication with the Remote Pilot either within speaking distance or with a portable radio/cell phone equipped for immediate communication.

C. Keep the Remote Pilot advised of any possible hazards such as power lines, birds, other aircraft, terrain, and hazardous weather conditions.

D. VOs may not act as Remote Pilots unless they possess a valid FAA Remote Pilot certificate and a current OAS-30U qualification card.

E. Dedicated VO's shall not have collateral duties during flight operations.

16. UAS Inspectors.

OAS is responsible for designating UAS pilots and aircraft inspectors. Requests for use of approved bureau inspectors will be evaluated and approved on a case-by-case basis by the director of OAS.

OAS requests for the use/designation of bureau inspectors must be routed through the NAM. The list of approved DOI inspectors will be kept on the OAS website.

17. Initial UAS Training.

A. DOI Remote Pilot candidates and supervisors must meet the following prerequisites before a candidate may attend the A-450 Basic Remote Pilot training:

1) Candidate must possess a current Part 107 FAA Remote Pilot certificate.

2) Candidate must meet the training requirements for Aircrew Member as outlined in OPM-04, DOI Aviation User Training Program. Current DOI crewed aircraft pilots are not required to retake A-100.

3) DOI Supervisors of Remote Pilots and crewmembers shall be current in the training requirements outlined in OPM-04. Details can be found in the Interagency Aviation Training Guide (https://www.iat.gov/).

4) Candidates will be nominated by the Bureau NAM or designee via the nomination form.

B. DOI Remote Pilots must complete the A-450 Basic Remote Pilot course. Specific training for additional makes/models of aircraft may be required.

C. All DOI UAS personnel must pass an initial evaluation administered by an OAS UAS Pilot Inspector or OAS-designated bureau UAS pilot inspector. In the situation of a candidate not meeting the evaluation standards, but who may become proficient with additional training and practice under the supervision of a qualified DOI instructor. Upon completion of additional training, the remote pilot candidate can request re-inspection from OAS in coordination with the bureau program manager.

D. DOI UAS Remote Pilots and crewmembers, apart from current DOI crewed aircraft pilots, are required to maintain currency as DOI Remote Pilots and Aircrew Members per OPM-04. A UAS crewmember is defined as any person directly involved in the setup, launch, recovery, or manipulation of the controls of the UAS. Only qualified DOI remote pilots should take part in the setup, launch, recovery, or manipulation of the controls of the UAS.

18. Additional UAS Training.

A. Pilots wishing to fly additional make/model of UAS must attend an A-454 add-on course provided by a qualified UAS instructor, evaluator, or inspector.

B. A-454 Add-On training including additional GCS software or applications to operate DOI UAS, DOI Remote Pilots must obtain training with another DOI-approved A-454 Instructor with experience in the specific software/application. The GCS shall be documented on the OAS-2U. OAS will maintain and post a list of approved GCS software/applications for each approved UAS. Remote Pilots wishing to utilize unapproved GCS software/applications shall coordinate with their NAM or Designee to facilitate approval.

C. A signed endorsement from an OAS-approved DOI inspector is required on the OAS-30U for the following type of missions:

1) Extended line of sight (EVLOS)/ Beyond visual line of sight (BVLOS endorsement includes night flights)

2) Aerial Ignition

3) Test/Evaluation Pilot

D. Incident UAS Operations

1) Pilots participating in fire operations shall be qualified for those missions in accordance with the NWCG Standards for Wildland Fire Position Qualifications, PMS 310-1.

2) DOI Remote Pilots participating in all-hazard incidents are encouraged to coordinate with the Bureau National Program Manager to ensure that airspace coordination, communication, and deconfliction are established.

An Incident is defined as an occurrence either a human-caused or natural phenomenon, that requires action or support by emergency service personnel to prevent or minimize loss of life or damage to property and/or natural resources. (Source: NWCG Glossary).

19. Flight Proficiency and Currency.

A. Flight proficiency: Remote Pilots must demonstrate, at a minimum, three takeoffs (launch) and landings (recovery) with the UAS they are approved to operate within the preceding 90 days. If proficiency is lost prior to a mission, the Remote Pilot must regain proficiency by performing the flight maneuvers and emergency procedures for the specific make and model, during a proficiency flight prior to an operational mission or conduct their mission flight under the observation of a current UAS pilot.

B. Flight Currency: Remote Pilots are required to fly each of the aircraft for which they are carded at least once every 12 months or the interval specified on their OAS-30U. Remote Pilots failing to meet this requirement shall fly under the supervision of a carded and current Remote Pilot and perform the flight maneuvers and emergency procedures for that aircraft.

20. UAS Refresher Training.

A. DOI Remote Pilots must complete UAS refresher training (A-452R) every 24 months following the issuance of their OAS-30U. Current DOI Remote Pilots participating in either A-450 or A-452R, as a student or instructors, will receive credit for refresher training. This training can be completed in advance or within 30-days after the date of expiration on the OAS-30U and shall be documented on the iat.gov website. Remote Pilots operating low-complexity UAS will be able to complete this requirement via distance learning opportunities. Remote Pilots operating more complex aircraft may be required to attend a refresher in person.

B. Required Refresher Training Elements:

1) Program and policy updates

2) Mishaps, SAFECOMs, and trends

3) Airspace authorization

4) Risk management and crew resource management review

5) Lessons learned

6) Aircraft/Sensor updates

7) Identified special emphasis items

C. Recommended Refresher Training Elements:

1) Industry trends

2) Emerging technology discussion

3) Hardware/software/apps

4) Lessons learned/case studies

5) Training review/curriculum updates

6) Flight exercises

D. If a DOI Remote Pilot is more than 90 days past the end of the expiration indicated on their OAS-30U they must, at a minimum, complete the following in order to regain certification:

1) Attend the A-452R refresher course and,

2) Complete a flight evaluation provided by an OAS-approved pilot inspector or evaluator. Evaluators shall send documentation to OAS at the conclusion of the training (OAS-69U).

21. DOI UAS Training Roles- Instructor/ Instructor Pilot Qualifications.

Interagency UAS Training roles titles and qualifications are utilized by DOI and USFS. The most current language can be found in the current Interagency Aviation Training Guide (IAT).

https://www.iat.gov/docs/Interagency_UAS_Training_Roles.pdf

22. DOI UAS Operations in the National Airspace System (NAS).

DOI has the authority to conduct operations in the NAS under the following authorities:

A. Following the provisions of 14 CFR Part 107 and OPM-11.

B. Authorizations granted using the FAA's Low Altitude Authorization and Notification Capability system (LAANC). Waiver requests outside of the LAANC systems shall be reviewed by the NAM or designee and OAS prior to submittal to the FAA.

C. Utilizing the DOI/FAA Memorandum of Agreement Regarding Operation of Small Unmanned Aircraft Systems in Class G Airspace.

D. Utilizing the MOA Regarding Beyond Visual Line of Sight Operations of Unmanned Aircraft Systems in Support of Emergency Assistance within an Active Temporary Flight Restriction Under the terms of the DOI/FAA Agreement.

E. Following the provisions outlined in the DOI Blanket Certificate of Authorization for operating in Class G airspace.

F. Under a standalone COA for a specific mission.

G. COAs will be coordinated with the Bureau/Office NAM or designee and OAS.

H. Under a special governmental interest (SGI) or emergency COA (ECOA) requested through the NAM or designee in coordination with OAS UAS Division to the FAA.

I. UAS operations within restricted, prohibited and warning areas must be authorized by the controlling authority. DOI UAS operators must comply with any restrictions placed on the operation by the controlling authority.

23. UAS Operations General Provisions:

A. Bureaus should follow the DHS Best Practices for Commercial UAS Operations to minimize the risk of loss of data when utilizing UAS.

B. A Project Aviation Safety Plan (PASP) will be developed for all UAS missions. For UAS missions on a recurring or routine basis, the required PASP can be rolled into a station/unit aviation plan that shall be reviewed by the NAM or designee at least annually.

C. Coordination:

1) Bureaus and Offices are responsible for coordinating with each other for UAS operations over lands owned or managed by DOI.

2) For operations taking off and landing on Federal, State, Tribal and municipal lands, Bureaus and Offices will receive authorization from the appropriate authority prior to operations. This coordination shall include anticipated periods of operation, the purpose of the flights, and contact information for the responsible unit when questions or issues arise.

3) For flights over private land, DOI UAS pilots shall make every effort to notify landowners of the anticipated periods of operation, the purpose of the flights, and contact information for the responsible unit if questions or issues arise.

4) For flights under the DOI/FAA MOAs or blanket COA (see Appendix 3) may require landowner notification. Refer to provisions of the COA.

D. Flights will be planned to avoid sustained/repeated overflight of heavily trafficked roads or highways but may briefly cross over active roads as necessary.

E. Flights over people: Currently none of the aircraft in the DOI fleet meet the criteria for flights over non-participating people under Part 107 and should be avoided. For flights conducted under authorizations other than Part 107 flights over people should be avoided to the extent possible.

F. Cooperator/Affiliate Missions (DOI Operational Control): Requests for approval of cooperator/affiliate UAS under the operational control of DOI must follow the process outlined in 351 DM 4. UAS Cooperator approval letters will be issued by the OAS UAS Division Chief.

G. Notice to Air Missions (NOTAM)

1) Flights conducted under 14 CFR Part 107 do not require a NOTAM.

2) Flights conducted under DOI/FAA MOAs/COAs will adhere to the terms of the MOAs or COAs for filing of NOTAMs (may be filed online): https://www.1800wxbrief.com/

H. Beyond Visual Line of Sight (BVLOS) must be conducted with an FAA Part 91 waiver or under the terms of the DOI/FAA MOA for flights within a Temporary Flight Restriction (TFR).

I. Flights within a TFR must be conducted under the direction of the official in charge of the on-scene activity.

J. Night flights must follow the language of the Agency flight authorization the operation is being conducted:

1) FAA Part 107: 107.29

2) FAA Certificate of Waiver or Authorization (COA): Agency "Blanket" COA, SGI or mission-specific waiver.

3) Permission from the controlling agency if in restricted airspace.

4) Be advised that some authorizations require documentation that the RPIC and VO be trained to recognize and overcome visual illusions and physiological conditions.

K. Flights above 400 feet AGL must be conducted with an FAA Part 107 waiver, under the DOI/FAA MOA or blanket COA, or with permission from the controlling agency when flying in Restricted airspace.

24. UAS Mishap Reporting.

A. Submit SAFECOM reports for any conditions, acts, observations, circumstances or maintenance problems that led to, or could have led to, an aircraft mishap (https://www.safecom.gov). This includes any damage to an aircraft that renders it un-airworthy, even temporarily.

B. Immediately report the following by calling the Aircraft Accident Reporting Hotline at 1-888-4MISHAP prior to continuing operations:

1) Any missing aircraft.

2) Injury to any person or any loss of consciousness.

3) Damage to any property other than the small Uncrewed aircraft.

C. The same reporting requirements for manned aircraft apply to any incident involving a UAS that exceeds the small category. Please reference 352 DM 3 for details.

25. Privacy, Civil Rights, and Civil Liberties Protections.

A. The use of UAS significantly expands DOI's ability to obtain remotely sensed data critical to fulfilling diverse mission objectives. However, this use raises distinct privacy, civil rights, and civil liberties concerns that must be addressed in order to promote the responsible use of UAS and protections for individual privacy, civil rights, and civil liberties in accordance with the Constitution, Federal law, and applicable regulations and policies.

B. Privacy Protections. In light of the advancements in UAS technologies and diverse potential uses of UAS across Departments, Bureaus, and Offices missions, it is imperative that DOI take appropriate steps to implement UAS policies that address privacy protections, procedures, and standards to ensure compliance with the Privacy Act of 1974, DOI Privacy Act regulations, Departmental privacy policies, and other applicable laws, regulations and policies. Accordingly, DOI Bureaus and Offices utilizing UAS or UAS-collected information shall meet the following privacy requirements:

1) DOI bureaus and offices shall only collect information using UAS, or use UAS-collected information, to the extent that such collection or use is consistent with and relevant to an authorized purpose and DOI privacy policy.

2) Information collected by or on behalf of DOI bureaus and offices using UAS that may contain personally identifiable information (PII) shall not be retained for more than 180 days unless retention of the information is determined to be necessary to an authorized mission, is maintained in a system of records covered by the Privacy Act, or is required to be retained for a longer period by any other applicable law or regulation.

3) DOI bureaus and offices shall take appropriate steps to ensure that UAS- collected information that is not maintained in a system of records covered by the Privacy Act is not disseminated outside of the agency unless dissemination is required by law, or fulfills an authorized purpose and complies with the bureau's and office's mission.

C. Civil Right and Civil Liberties Protections. To protect civil rights and civil liberties, DOI bureaus and offices shall:

1) Ensure that policies are in place to prohibit the collection, use, retention, or dissemination of data in any manner that would violate the First Amendment or in any manner that would discriminate against persons based upon their ethnicity, race, gender, national origin, religion, sexual orientation, or gender identity, in violation of the law.

2) Ensure that UAS activities are performed in a manner consistent with the Constitution and applicable laws, Executive Orders, and other Presidential directives.

3) Ensure that adequate procedures are in place to receive, investigate, and address, as appropriate, privacy, civil rights, and civil liberties complaints.

D. Accountability. To provide for effective accountability, OAS, in conjunction with the Office of the Chief Information Officer and the Office of Civil Rights, will provide collaborative oversight of the DOI UAS program within their respective areas of expertise and responsibility. DOI bureaus and offices employing UAS or UAS- collected information shall comply with Departmental oversight activities, and take additional appropriate steps to ensure effective oversight and accountability for their respective UAS programs. Accordingly, bureaus and offices shall ensure:

1) Oversight procedures are implemented for UAS use, including audits or assessments, in compliance with Departmental policies and regulations.

2) Bureau and office personnel and contractors comply with UAS program training requirements, rules of behavior, and procedures for reporting suspected cases of misuse or abuse of UAS technologies.

3) Policies and procedures are implemented that provide meaningful oversight of individuals who have access to sensitive information (including any PII) collected using UAS consistent with applicable Federal laws, regulations, and policies, as well as Departmental policy guidance.

4) Any data-sharing agreements or policies, data use policies and records management policies applicable to UAS conform to applicable laws, regulations, and policies.

5) Policies and procedures are implemented to authorize the use of UAS in response to a request for UAS assistance in support of Federal, State, local, tribal, or territorial government operations. Any authorized use, letter of authorization, or memorandum of understanding must include the requirements of this policy and appropriate safeguards to protect privacy, civil rights, and civil liberties.

6) State, local, tribal, and territorial government recipients of Federal grant funding for the purchase or use of UAS for their own operations have in place policies and procedures to safeguard individuals' privacy, civil rights, and civil liberties prior to expending such funds.

E. Transparency. OAS will complete the following activities, in collaboration with bureau and office UAS programs, to promote transparency about DOI UAS activities within the NAS, while not revealing information that could reasonably be expected to compromise law enforcement or national security.

1) Provide notice to the public regarding where DOI's UAS are authorized to operate in the NAS.

2) Keep the public informed about the DOI UAS program as well as changes that would significantly affect privacy, civil rights, or civil liberties.

3) Make available to the public, on an annual basis, a general summary of DOI UAS operations during the previous fiscal year, to include a brief description of types or categories of missions flown, and the number of times the agency provided assistance to other agencies, or to State, local, tribal, or territorial governments.

26. Oceanic and International Operations.

DOI UAS operations over international waters typically do not lend themselves to compliance with International Civil Aviation Organization (ICAO) procedures due the low altitudes flown and lack of required avionics. For UAS flights in Oceanic Flight Information Regions (FIR) where the FAA is the air traffic provider, DOI owned and operated UAS shall be considered "State Aircraft." The following conditions are designed to provide a level of safety equivalent to that normally given by ICAO Air Traffic Control agencies and fulfill United States Government obligations under Article 3 of the Chicago Convention of 1944 which stipulates there must be "due regard for the safety of navigation of civil aircraft" when the flight is not being conducted under ICAO flight procedures.

A. These conditions apply only to small UAS weighing 55 pounds or less.

B. The Ground Control Station (GCS) and UAS shall remain within uncontrolled airspace at all times.

C. The GCS shall remain greater than 12 NM (international waters) from the U.S. coastline during all phases of flight.

D. Operations will be limited to below 1200 feet AGL provided the UAS remains within ICAO Class G airspace at all times.

E. The UAS shall remain within 5NM of the GCS at all times.

F. All UAS flights will be flown in Visual Meteorological Conditions (VMC) only. If Instrument Meteorological Conditions (IMC) conditions are unintentionally encountered, the pilot will return the UAS to VMC conditions by the safest and most expeditious means possible.

G. Day or night operations are permitted, and associated risks and mitigation measures shall be addressed in each project-specific Operational Risk Management (ORM) document.

H. UAS operating areas shall be selected so as not to interfere with established air routes and ocean shipping lanes.

I. The operating agency will request the FAA publishes a NOTAM for the affected airspace to alert non-participating aircraft of the operation and advise them of the VHF-AM frequency which will be monitored while operations are being conducted. The Remote Pilot and team must be equipped with an operable VHF-AM radio capable of transmitting and receiving on the monitored frequency and VHF guard frequency (121.5).

J. For launches conducted from ships equipped with search radar, the launch vessel shall conduct a surface search using its radar within (no later than) 10 minutes of the launch in order to identify other vessels within the operational area. A qualified radar operator should monitor the ship's radar display at all times the UAS is airborne. If another vessel is identified within a 5 NM operational radius of the GCS, the pilot shall take action to keep the UAS at least 2 NM from that vessel at all times unless identification of vessels is a requirement of the mission flight.

K. For UAS flights in Oceanic FIRs, where the air traffic service provider is a foreign government, coordination, and approval with that government is required prior to commencing flight operations. Additional diplomatic clearances may also be required.

L. International UAS Flights: Any proposed international flights of DOI-owned or operated UAS will be approved on a case-by-case basis by the Bureau or Office NAM and OAS. Proposals for international UAS activities must be forwarded in writing to the Bureau or Office NAM and OAS UAS Division Chief 60 days in advance of the proposed mission.

WALKER CRAIG Digitally signed by WALKER CRAIG
Date: 2022.12.29 09:34:42 -07'00'

Walker Craig
Acting Director, Office of Aviation Services

Attachments:
Appendix 1: Definitions
Appendix 2: Guidance for End-Product Contracting
Appendix 3: CISA: Cybersecurity Best Practices for Operating Commercial Uncrewed Aircraft Systems Fact Sheet
Appendix 4: Useful Web Links

Appendix 1

Definitions

Operational Control: Per 14 CFR 1.1 Operational control, with respect to a flight, means the exercise of authority over initiating, conducting or terminating a flight.

COA: Certificate of Authorization issued by the Air Traffic Organization to an operator for a specific UAS activity not covered under a Federal Aviation Regulation, such as 14 CFR Part 107.

ECOA: An Emergency COA (ECOA) is an authorization issued by the Air Traffic Organization to an operator for a specific emergency UAS activity. ECOAs are requested through OAS to the FAA.

MOA: A Memorandum of Agreement (MOA) is a written document describing a cooperative relationship between DOI and another party working together on a project or to meet an agreed upon objective. An MOA serves as a legal document and describes the terms and details of the partnership agreement.

NOTAM: A Notice To Airmen or NOTAM is a notice containing information (not known sufficiently in advance to publicize by other means) concerning the establishment, condition, or change in any component (facility, service, or procedure of, or hazard in the National Airspace System) the timely knowledge of which is essential to personnel concerned with flight operations.

TFR: A Temporary Flight Restriction (TFR) is a limitation on aviation activity applied to an area of airspace (defined both laterally and vertically) that has been temporarily or partially closed to non-participatory aircraft for a specified period of time due to a hazardous condition, a special event, or to provide a safe environment for operation of disaster relief aircraft. A NOTAM is issued containing information on the reason for the TFR, contact information and fine points of the restriction.

UAS Crewmember: Person directly involved in the setup, launch, recovery or manipulating the controls of the UAS.

Appendix 2

Guidance for End-Product Contracting

End Product Contracts are not aircraft flight service contracts. They are used to acquire a product for the Department (i.e., per-acre, per-unit or per-area, or per head basis). The intent of this type of procurement is for the contractor to supply all personnel and equipment in order to provide a "service" or "end-result." Many contractors utilize aircraft (including UAS) to meet the performance objectives of End Product contracts for activities such as: animal capture, seeding, spraying, survey, photography, etc. Since these are not flight services contracts, the AQD does not perform any acquisition service. End Product contracts are administered by the bureau procurement units.

These contracts must be conducted in accordance with OPM-35. OPM-35 aids in determining whether an operation is being conducted as either "end-product" or "flight service" and supplements existing DOI policy regarding End Product contracts found in 353 DM 1.2A (3). If the provisions of 353 DM 1.2A (3) and OPM-35 are met, the aircraft will be operated as a civil aircraft and the aviation management principles normally required for aircraft under DOI operational control do not apply.

End Product Contract Specifications

Specifications in the contract must only describe the desired quantity or quality of the service or contracted end-result. Contracting officers, procurement specialists, and aviation managers at all levels must be aware of these requirements. DOI contracting officers and resource specialists must consult with their bureau aviation managers if the acceptable language guidelines do not address a specific project requirement or the contract solicitation does not follow the guidelines in OPM-35. End Product contracts where contractors could conceivably utilize aircraft must be reviewed by the bureau aviation manager to ensure that specifications and language do not unintentionally imply or determine aircraft operational control.

The following list describes acceptable contract language for end-product contracts.

- No contract language describing aircraft or pilot capabilities, standards, requirements or aircraft specific payment provisions.
- The area of work must be described in terms of: location, scale of area, general topography, elevation, slope, vegetation, and accessibility by roads or off-road vehicles, land use restrictions for mechanized equipment, etc.
- Aviation Regulations - Acceptable Language: "The Contractor must comply with all applicable federal, state and local regulations and land-use permitting procedures."
- Airspace Coordination - In areas of military airspace it is acceptable to describe coordination agreements with military airspace scheduling or range control authorities and that it is the contractors' responsibility to coordinate their activities with the scheduling office or Range Control. Close coordination is necessary to ensure compliance with applicable airspace coordination agreements that states have with military authorities.

- Aircraft Equipment Specifications - Acceptable Language: Delete all reference to aircraft/equipment. Suggested example clause: "...Contractor is required to demonstrate to the government that the equipment can capture the imagery and/or data as specified in the project description."
- Radio/Communication Requirements - Acceptable Language: "Contractor must provide a communication system so that contractor personnel engaged in the project at different locations can communicate at all times with each other, and so that government Project Inspectors may communicate with the contractor at any time to discuss performance matters." (The government VHF-FM radio system may have to be described.)
- Transporting, Passengers and Equipment - Acceptable Language: "Only approved contractor personnel, contractor equipment and government-provided equipment required for performance ... will be transported by contractor vehicles, trailers, animals or equipment."
- Safety Hazards - Acceptable Language: "Any ground or aerial hazards that would pose a danger to Contractor's personnel or operating equipment must be identified and mitigated by the Contractor prior to commencing operations".
- Aircraft Use Reporting - Acceptable Language: Do not mention or require flight hour/aircraft usage reports.

Covered Uncrewed Aircraft Systems: For end-product contracts where the vendor might possibly utilize UAS to fulfill the contract, the following language should be included in the specifications to ensure that no covered UAS are utilized in the performance of the contract.

1.Condition all Department contracts, grants, and cooperative agreements relying on UAS for achieving approved objectives on the requirement that funds will not be expended on covered UAS.

2. Condition all parties' operations pursuant to a department contract, grant or cooperative agreement on the requirement that covered UAS will not be operated on Department managed lands.

The term "covered UAS" as defined in EO 13981, and adopted for official use by the Department moving forward, means any UAS that:

i. is manufactured, in whole or in part, by an entity domiciled in an adversary country.

ii. uses critical electronic components installed in flight controllers, ground control system processors, radios, digital transmission devices, cameras, or gimbals manufactured, in whole or in part, in an adversary country (as defined by the Department of Commerce and referenced in OPM-11.)

iii. uses operating software (including a cell phone or tablet applications, but not a cell phone or tablet operating systems) developed, in whole or in part, by an entity domiciled in an adversary country.

iv. uses network connectivity or data storage located outside the United States, or administered by any entity domiciled in an adversary country; or

v. contains hardware and software components used for transmitting photographs, videos, location information, flight paths, or any other data collected by the UAS manufactured by an entity domiciled in an adversary country.

vi. The term “critical electronic component” means any electronic device that stores, manipulates, or transfers digital data. The term critical electronic component does not include, for example, passive electronics such as resistors, and non-data transmitting motors, batteries, and wiring.

Operational Control: During the performance of End Product contracts, DOI will not exercise operational control of the aircraft in any way. DOI will not direct the contractor as to flight profiles, flight following, landing areas (except for areas that are off limits due to land management restrictions), use of personal protective equipment, etc. DOI personnel assigned to administer End Product contracts will have no aviation management responsibility or authority. Any directions to the contractor must be in terms of the service or end-result being specified; e.g., desired imagery quality, number and disposition of animals surveyed, etc. It is acceptable to inform military airspace scheduling authorities or range control that the contractor plans on performing work during specified time periods and provide the military authorities the contractor contact information. DOI dispatchers will not perform the airspace scheduling service for the contractor. DOI personnel must not become involved in any way with aircraft ground operations such as takeoff and landing areas, loading, fueling, etc. They can, however, be on site for other support activities such as setting ground control, scale bars, etc. or collection of in-situ type data for ground truthing to aid in the overall data collection aspects.

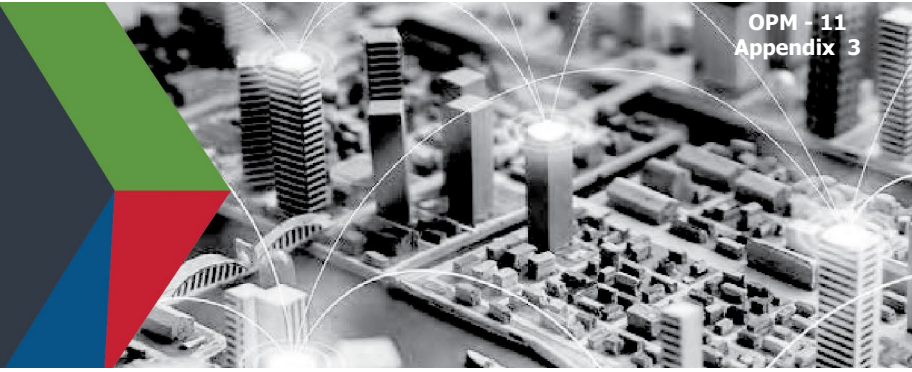
Aircraft Use Reporting: Since aircraft utilized by the contractor under DOI end product contracts are operating entirely within the applicable 14 CFR as a civil aircraft, and procurement is not through AQD, the Bureau will not submit any billing invoice to AQD in conjunction with End Product contracts. Any flight time incurred by the contractor will not be recorded or reported as DOI or Bureau aviation statistics.

Aircraft Incidents and Accidents: Although aircraft utilized by the contractor under End Product contracts are operating entirely within the applicable 14 CFR as a civil aircraft, mishaps should be reports as per FAA - to continue to promote aviation safety the Bureau will report aviation incidents or accidents incurred by these contractors through the FAA. These events should be noted in the Contract Daily Diary and reported through channels as normally required for End Product contracts.

Reconnaissance/Observation Flights: Before, during or after the performance of an End Product contract it may be necessary for Bureau employees to aerially survey or inspect the project area.

When flights transporting DOI personnel are required, an AQD aviation "flight service" procurement (completely separate from the End Product contract) is required. Aircraft and pilots must have current OAS approvals for the intended mission and a current DOI contract or Aircraft Rental Agreement must be in place. When a DOI procurement is utilized all DOI and Bureau aviation management policy, procedures and requirements must be applied.

Operations within Military Airspace: If an "End Product" contract project using aircraft is being conducted within Military Airspace (MOA, RA, MTR) it is the responsibility of the contractor to coordinate with the Military Airspace Scheduling Office. DOI Contracting Officers and CORs should inform the contractor of any DOI agreements with the Military organizations regarding airspace. The Bureau may contact the Scheduling Office to alert them of the project and general time frames and provide contractor contact information.



DEFEND TODAY, SECURE TOMORROW

CYBERSECURITY BEST PRACTICES FOR OPERATING COMMERCIAL UNMANNED AIRCRAFT SYSTEMS (UASs)

UASs provide innovative solutions for tasks that are dangerous, time consuming, and costly. Critical infrastructure operators, law enforcement, and all levels of government are increasingly incorporating UASs into their operational functions and will likely continue to do so. Although UASs offer benefits to their operators, they can also pose cybersecurity risks, and operators should exercise caution when using them.

To help UAS users protect their networks, information, and personnel, the Department of Homeland Security (DHS)/Cybersecurity and Infrastructure Security Agency (CISA) identified cybersecurity best practices for UASs. This product, a companion piece to CISA's Foreign Manufactured UASs Industry Alert, can assist in standing up a new UAS program or securing an existing UAS program, and is intended for information technology managers and personnel involved in UAS operations. Similar to other cybersecurity guidelines and best practices, the identified best practices can aid critical infrastructure operators to lower the cybersecurity risks associated with the use of UAS, but do not eliminate all risk.

INSTALLATION AND USE OF UAS SOFTWARE AND FIRMWARE

An important part of managing risk when employing UASs is to understand the steps involved and potential vulnerabilities introduced during the installation and use of UAS software and firmware. UAS operators should strongly consider and evaluate the following cybersecurity best practices when dealing with software and firmware associated with UAS:

- Ensure that the devices used for the download and installation of UAS software and firmware do not access the enterprise network.
- Properly verify and securely conduct all interactions with UAS vendor and third-party websites. Take extra precaution to download software from properly authenticated and secured websites and ensure app store hosts verify mobile applications.
    - Access these websites or app stores from a computer not associated with, or at least not connected to, the enterprise network or architecture.
    - Ensure the management of security for mobile devices that will be directly or wirelessly connected to the UAS.[1] Review additional information for enhancing security on mobile devices.[2,3]

[1] For more information, see: National Institute of Standards and Technology (NIST). (2013). "Guidelines for Managing the Security of Mobile Devices in the Enterprise." https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf. Accessed May 16, 2019.
[2] For mobile security guidance from Apple, visit www.apple.com/privacy/manage-your-privacy.
[3] For mobile security guidance from Android, visit www.android.com/play-protect.

- Ensure file integrity monitoring processes are in place before downloading or installing files. Check to see if individual downloads or installation files have a hash value or checksum.[4] After downloading an installation file, compare the hash value or checksum of the installation file against the value listed on the vendor's download page to ensure they match.
- Run all downloaded files through an up-to-date antivirus platform before installation and ensure the platform remains enabled throughout installation.
- Verify a firewall on the computer or mobile device is enabled to check for potentially malicious inbound and outbound traffic caused by the recently installed software. External network communications could be part of the installation process and could potentially expose your system to unknown data privacy risks.
- During installation, do not follow "default" install options. Instead, go through each screen manually and consider installing software on a removable device (external HDD or USB drive).
    - Deselect any additional features or freeware bundled into the default install package.
    - Disable automatic software updates. Necessary updates should follow the same process outlined for download and installation.
    - Thoroughly review any license agreements prior to approval. Consider involving a legal team in the process to ensure organizations do not unknowingly agree to unsafe or hazardous practices on the part of the vendor.

SECURING UAS OPERATIONS

An important part of operating UASs is to ensure that communications are secure during all aspects of usage. There are multiple publicly accessible sites that indicate and detail how to intercept UAS communications and hijack UASs during flight operations. UAS operators should consider and evaluate the following cybersecurity best practices when conducting UAS operations:

- If a UAS data link is through Wi-Fi connections between the UAS and the controller.[5]
    - Ensure the data link supports an encryption algorithm for securing Wi-Fi communications.
        - Use WPA2-AES security standards or the most secure encryption standards available.
        - Use highly complicated encryption keys that are changed on a frequent basis. Ensure that encryption keys are not easily guessable, and do not identify the make or model of the UAS or the operating organization.
    - Use complicated Service Set Identifiers (SSIDs) that do not identify UAS operations on the network. Avoid using the specific make or model of the UAS or the operating organization in the SSID.
    - Set the UAS to not broadcast the SSID or network name of the connection.
    - Change encryption keys in a secure location to avoid eavesdropping either visually or from wireless monitoring.
- If the UAS supports the Transport Layer Security (TLS) protocol, ensure that it is enabled to the highest standard that the UAS supports.

[4] A checksum is a value derived from a segment of computer data calculated before and after transmission to assure data is free from tampering and errors. A hash value is a fixed-length numeric value that results from the calculation of a hashing algorithm. A hash value uniquely identifies data and is often used for verifying data integrity.
[5] For more information on securing a wireless network, see: DHS Cybersecurity Engineering. (2017). "A Guide to Securing Networks for Wi-Fi (IEEE 802.11 Family)." www.us-cert.gov/sites/default/files/publications/A_Guide_to_Securing_Networks_for_Wi-Fi.pdf. Accessed March 18, 2019.

- Have the data links for UAS control, telemetry, payload transmission, video transmission, and audio transmission encrypted with different keys. Make sure the UAS is able to encrypt the data stored onboard.
- Use standalone UAS-associated mobile devices with no external connections or disable all connections between the Internet and the UAS and UAS-associated mobile devices during operations. Consider running wireless traffic analyzers during selected UAS operations to understand and monitor UAS communications traffic while in use.
- Run mobile device applications in a secure virtual sand-box configuration that allows operation while securely protecting the device and the operating system.

DATA STORAGE AND TRANSFER

Ensuring the security and privacy of UAS data, while at rest or in transit, is essential to managing UAS cybersecurity risks. UAS operators should consider and evaluate the following cybersecurity best practices for UAS data storage and transfer:

- When connecting the UAS or UAS-associated removable storage device to a computer:
  - Use a standalone computer to connect to the UAS or removable storage device to ensure no access to the Internet or enterprise network.
  - Verify a firewall on the computer or mobile device is enabled to check for potentially malicious inbound and outbound traffic caused from the connection of the UAS or removable storage device. Verify and ensure that the computer has up-to-date antivirus installed.
- Data should be encrypted both at rest and in transit to ensure confidentiality and integrity.[6]
- Authentication mechanisms should be in place for UASs with access to private or confidential data. Use Multi-Factor Authentication (MFA) whenever possible for accounts associated with UAS operations.[7]
- Follow data management policies for data at rest, data in transit, and any sensitive data.
- Erase all data from the UAS and any removable storage devices after each use.

INFORMATION SHARING AND VULNERABILITY REPORTING

By participating in information-sharing programs and reporting non-public, newly-identified vulnerabilities, users will have access to timely information to mitigate cybersecurity threats. These programs can also serve as a forum for UAS operators to share security vulnerabilities that could potentially impact the Nation's critical infrastructure or pose a threat to public health and safety. The following are three information sharing programs:

- Cyber Information Sharing and Collaboration Program (CISCP):
  - CISCP enables actionable, relevant, and timely information exchange through trusted, public-private partnerships across all critical infrastructure (CI) sectors by leveraging the depth and breadth of DHS cybersecurity capabilities within a focused, operational context.

[6] For more information on encrypting stored data, see: National Institute of Standards and Technology (NIST). (2007). "Guide to Storage Encryption Technologies for End User Devices." NIST Special Publication 800-111. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-111.pdf. Accessed March 15, 2019.
[7] For more information on security controls, see: National Institute of Standards and Technology (NIST). (2013). "Security and Privacy Controls for Federal Information Systems and Organizations." NIST Special Publication 800-53, Revision 4. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf. Accessed March 15, 2019.

- For more information on the CISCP program, visit www.dhs.gov/ciscp or email CISCP_Coordination@hq.dhs.gov.

- Automated Indicator Sharing (AIS) Program:
  - The AIS program enables the quick exchange of cyber threat indicators between the Federal Government and the private sector through CISA. Companies that share indicators through AIS are granted liability protection and other protections through the Cybersecurity Information Sharing Act of 2015.
  - For more information on CISA services, call 1-888-282-0870 or email Central@cisa.gov. For more information on AIS and how to join, go to www.cisa.gov/automated-indicator-sharing-ais.
- Information Sharing and Analysis Centers (ISACs):
  - Information Sharing and Analysis Centers (ISACs) are non-profit, member-driven organizations formed by critical infrastructure owners and operators to share information between government and industry. CISA, through the NCCIC, works in close coordination with all of the ISACs.
  - For more information about ISACs, go to www.nationalisacs.org/.

If an organization discovers a UAS software or hardware vulnerability, or a suspicious or confirmed UAS cybersecurity incident occurs, CISA recommends reporting the vulnerability or incident through the following channels:

- DHS CISA:
  - Email Central@cisa.dhs.gov or call 1-888-282-0870. When sending sensitive information to DHS CISA via email, we recommend encryption of messages. For more information, visit us-cert.cisa.gov/report.
- CERT Coordination Center:
  - To report a vulnerability, go to www.kb.cert.org/vuls/report.

The UAS Cybersecurity Best Practices document is a collaborative product written by CISA's National Risk Management Center and Cybersecurity Division. This product was coordinated with the DHS/CISA/Infrastructure Security Division, DHS/Federal Protective Service, U.S. Army/Combat Capabilities Development Command, and Federal Bureau of Investigation/Cyber Division.

The National Risk Management Center (NRMC), Cybersecurity and Infrastructure Security Agency (CISA), is the planning, analysis, and collaboration center working in close coordination with the critical infrastructure community to Identify; Analyze; Prioritize; and Manage the most strategic risks to National Critical Functions. These are the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating impact on security, national economic security, national public health or safety, or any combination thereof. NRMC products are visible to authorized users at HSIN-CI and Intelink. For more information, contact NRMC@hq.dhs.gov or visit www.cisa.gov/national-risk-management.

June 11, 2019

Appendix 4

Useful Web Links

DOI UAS Website (Link to public DOI Website)

DOI's Interagency UAS Site (access permission required) Link to the Interagency UAS SharePoint.

DOI Small UAS Annual Inspection Form
Link to Small UAS Inspection Form

DOI Small Uncrewed Aircraft Systems Acquisition Request Form (OAS-13U) Link to OAS-13U Form

DOI FAA MOA for Class G operations
https://www.doi.gov/sites/doi.gov/files/uploads/DOI_FAA_MOA_Class_G_0911201 5.pdf

DOI/FAA MOA for BVLOS flights within TFRs
https://www.doi.gov/sites/doi.gov/files/uploads/FAA_DOI_UAS_TFR_MOA_8-13- 15.pdf

DOI Blanket COA
Link to Certificate of Waiver or Authorization between FAA and DOI (6 Sept. 2018; current).

Presidential Memo for Protecting Privacy, Civil Rights and Civil Liberties
Link to 2015 "Presidential Memo".

DOI UAS Privacy Impact Assessment
Link to DOI UAS Privacy Impact Assessment

Online NOTAM filing service 1800wxbrief.com
https://www.1800wxbrief.com/

Sky Vector flight planning tools
https://skyvector.com/

Interagency Fire UAS Operations Guide
https://www.nwcg.gov/sites/default/files/publications/pms515.pdf