



DEPARTMENT OF THE ARMY
UNITED STATES ARMY GARRISON BAVARIA
UNIT 28130
APO AE 09114-8130

JUL 30 2019

IMBA-PL

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: USAG Bavaria Policy Memorandum #19, Small Unmanned Aircraft Systems (SUAS)

1. References:

- a. Deputy Secretary Of Defense (DSD) Policy Memorandum, Subject: Unmanned Aerial Systems Cyber Security Vulnerabilities
- b. Office of the Secretary Of Defense (OSD) Policy Memorandum, Subject: Commercial off the Shelf (COTS) UAS Implementation Guidance
- c. OSD Policy Memorandum, Subject: Commercial off the Shelf (COTS) Unmanned Aircraft Systems Implementation Guidance
- d. Army Policy Memorandum, Army Policy for Unmanned Aircraft Systems on Army Installations
- e. ALARACT 029-2019, Consolidated DoD-Army Cots UAS Cyber Security Waiver Business Rules
- f. USAREUR OPORD 0006-19 (FY19-FY20 USAREUR SUAS Policy), dated 10 December 2018
- g. "Drone-Regulation" - German Regulation on the Operation of Unmanned Aerial Vehicles ("Drohnenverordnung" - Verordnung zur Regelung des Betriebs von unbemannten Fluggeräten)
- h. German Air Traffic Regulation (Luftverkehrs-Ordnung - LuftVO)
- i. German Air Traffic Licensing Regulation (Luftverkehrs-Zulassungs-Ordnung - LuftVZO)

2. This memorandum establishes policy on operating SUAS on USAG Bavaria controlled installations. This policy applies to all military members, DoD Civilian employees, contractors, dependents, sponsored guests, and Host Nation Employees.

IMBA-PL

SUBJECT: USAG Bavaria Policy Memorandum #19, Small Unmanned Aircraft Systems (SUAS)

3. For the purposes of this policy, unless specified, SUAS refers to all systems that are operated remotely or with programmed GPS flight plans, including radio controlled (RC) aircraft, unmanned aerial vehicles, drones (all rotary and fixed winged), model airplanes, model helicopters, quadcopters, and balloons.

4. This policy does not apply to SUAS that are managed by a formal program of record under a service level program office or have the authority to operate with a cyber vulnerability assessment.

5. The operation of any recreational SUAS on any USAG Bavaria installation is strictly prohibited; there are no exceptions.

6. SUAS usage for operational reasons not belonging to a formal program of record requires a waiver request endorsed by the first General Officer or Senior Executive Service (SES) civilian in the requestor's chain of command IAW reference (e), to the Army Acquisition Executive (AAE) and Army Chief Information Officer (CIO/G-6). Both will review each request on a case-by-case basis, track waivers, and certify that all specified mitigation procedures required are agreed to by the requestor. SUAS waivers or exceptions to policy will be processed IAW enclosure 2.

7. German Law Regarding SUAS.

a. The following rules do not apply to model aircraft training areas. The only rule for such areas is that the SUAS have a tag with the name and address of its owner.

b. SUAS must only be operated in the range of vision (i.e., no camera-based flights).

c. Weight-based rules for SUAS (see enclosure 1).

1) More than 250 grams: device must have a non-removable label with the owner's name and address.

2) More than 2 kilograms: operator must present proof of knowledge and device must have a non-removable label with the owner's name and address. Proof of knowledge may include pilot's license or certificate from an approved air sports association.

3) More than 5 kilograms: same requirements as 2+ kg class plus permission of the aeronautical authority to operate the SUAS.

IMBA-PL

SUBJECT: USAG Bavaria Policy Memorandum #19, Small Unmanned Aircraft Systems (SUAS)

d. Altitude-based rules for SUAS.

1) Below 100m: see weight-based rules for SUAS.

2) Above 100m: generally banned (exception can be requested from the aeronautical authority) or mandatory proof of knowledge. Proof of knowledge may include pilot's license or certificate from an approved air sports association.

e. Prohibitions.

1) Operating SUAS heavier than 250 grams over a housing area.

2) Operating SUAS with a camera, microphone, radio wave receiver, transmitter, or similar equipment over a housing area.

3) Operating SUAS at or over sensitive areas like airports, locations of a police or emergency services' action, arterial roads or gatherings of people.

8. Personnel should immediately report any SUAS operated on or near a USAG Bavaria installation to the MP station at DSN 476-3398/3397, CIV 09662-83- 3398/3397 (Vilseck and Grafenwoehr), DSN 466-2812/2713, CIV 09472-83-2812/2713 (Hohenfels) or DSN 440-3801/3827, CIV 08821-750-3801/3827 (Garmisch).

9. POC for this policy memorandum is the USAG Bavaria S3/5 Antiterrorism Officer, DSN 526-3007/3008, CIV 09641-70-526-3007/3008.

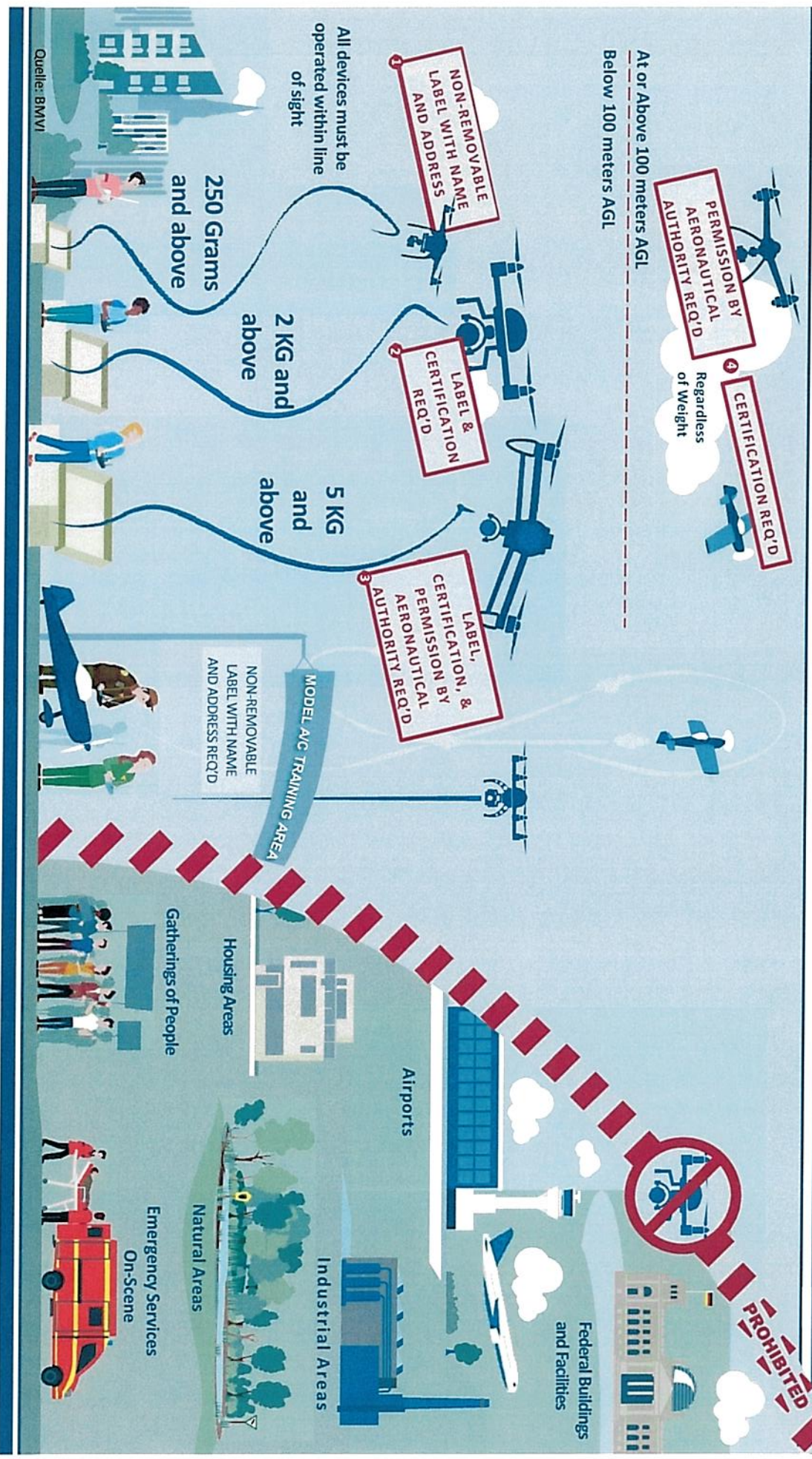


CHRISTOPHER R. DANBECK
COL, AR
Commanding

Encl

1. Drone Infographic
2. SUAS COTS Event Approval Procedures

New Drone/RC Aircraft Regulations in Germany



For further information, see: www.bmvi.de/drohen

- 1 250 Grams and above require the owner's name and address to be attached on a non-removable label.
- 2 2 KG and above further require the owner to be able to demonstrate special knowledge.
- 3 5 KG and above further require a special permit from the national air traffic authority.
- 4 From 100 meters AGL and above, regardless of weight, drones may only fly if officially authorized and RC aircraft may only fly if the operator can demonstrate special knowledge.

Enclosure 2 to USAG-Bavaria SUAS Commercial-Off-The-Shelf (COTS) Event Approval Procedures

1. This enclosure applies to all military members, DoD Civilian employees, contractors, dependents, sponsored guests, and Host Nation Employees.

2. Definitions.

a. COTS systems are defined as:

(1) All UAS systems sold in substantial quantity in the marketplace and offered to the government in the same form in which it is sold to non-government consumers. UAS systems are commercially available to the public from both domestic and foreign manufacturers.

(2) All UAS that were commercially available in original form, but have been modified with different hardware, software, or payloads.

(3) All UAS ground command and control elements to include smart phone or tablet with associated software and hardware.

b. Exempt systems are defined as UAS systems that are assigned to a formal "Program of Record" and managed by an Army Program Executive Office (PEO); have an Authority to Operate (ATO), complying with DODi 8510.01 and have a completed cyber vulnerability assessment for the system.

c. Submissions will be considered on a case-by-case basis for the following six (6) activities:

(1) Critical operations with no alternative solutions.

(2) Counter-UAS surrogate testing/training

(3) Intelligence and Information Warfare testing, analysis and training.

(4) Analysis and training.

(5) Research and Development (R&D).

(6) Demonstrations for COTS UAS.

d. Approval authority for all uncontrolled environments remains with USD/Acquisition & sustainment (A&S) and the Army Chief Information Officer (CIO/J6).

e. USAG Bavaria policy memorandum #19 also applies to COTS UAS used for recreational (hobby or personal use) purposes on Army installations and contractor-owned COTS UAS operated by or in support of (ISO) government operations or testing.

3. Procedures for Requesting Exceptions to Policy.

a. Waiver requests will be endorsed in writing by the first General Officer or Senior Executive Service (SES) civilian in the requestors chain of command and notifying the Senior Mission Commander/Senior Responsible Officer (SRO).

b. The Army authorizing officials, are co-defined as the Army Acquisition Executive (AAE) and CIO/G-6. Both will review each request on a case-by-case basis, track waivers, and certify that all specified mitigation procedures are agreed to by the requestor.

c. For risk assumption purposes, the Army Secretary (ARSEC) staff requires each request submitted to the SIPRNET SharePoint include a Senior Commander memo or letter endorsing the waiver on all installations.

d. All Army COTS UAS exception requests, with cover letter, will be forwarded to the Headquarters, Department of the Army (HQDA) SIPRNET SharePoint (<https://intelshare.intelink.sgov.gov/sites/cotsuasetsp>), 45 days prior to the start of the scheduled event.

e. Exception requests will be specific to the requesting unit, the COTS UAS model/version, mitigation procedures, locations(s), date, and type of event. Please be advised, HQDA is not allowed to approve a blanket waiver.

f. The following information is mandatory in order to process future requests in accordance with (IAW) HQDA EXORD 193-18, Army Purchase , Use, and Accountability of COTS UAS, dated 20 Jun 2018:

(1) Army/Unit requesting name and address.

(2) Type of request (Exception or Renewal).

(3) Point of Contact (POC) name(s), contact information (include SIPR email). POC must be prepared to defend requests via secure video teleconference (SVTC) or in person to OSD/HQDA review boards.

(4) Rationale for the need and justification for urgency.

(5) Concept of Operations (brief description only).

(6) Dates/Times/Event Status.

(7) Specific operating location(s) (include range maps and target area pictures with latitude and longitude coordinates to the center of the operations area.

(8) Categorization and short description of the intended operating environment (e.g. benign vs. controlled/uncontrolled, sensitive facilities/activities potentially impacted, what radio frequencies work within the environment, presence of any unauthorized sensors, potential for inadvertent observation by third parties, including other friendly audiences. Also include information in the organizational request if a covered facility is being used per Title 10 US Code, Section 130I and has been approved by DCS/G-3/5/7.

(9) Name all COTS UAS storage location(s) home and deployed.

(10) Brief description of COTS UAS equipment must include: 1) Make, 2) Quantity, 3) Manufacturer, 4) Command and Control (C2) application and device), 5) C2 Flight Mode, 6) C2 Firmware/Software, 7) C2 Link Encryption, 8) Camera Link Encryption, 9) Camera Link Data, 10) Camera Data Control, 11) Payload Link Encryption, 12) Sensor Payload Control, 13) Sensor Payload Mode, 14) Did you conduct a Cybe Vulnerability Assessment? If so, date of assessment, 15) Type of Radios/Frequencies, 16) What are you using as your Ground Control System (GCS)?, 17) Airworthiness Certification and if there is an ATO Date, and 18) UAS Maximum Operational Altitude.

g. Short description of your pre-mission and post-mission cyber security procedure(s). Identify all mitigating measures you will be taking during the case event(s); additional information may be included as required and will be labeled as annex(es).

h. Requests will also state and validate that all COTS UAS in the possession of the requestor are accurately recorded on an approved Army Property System of Record (APSR) as required.

6. POC for this enclosure is the USAG Bavaria S3/5 Antiterrorism Officer, DSN 526-3007/3008, CIV 09641-70-526-3007/3008.