Position Paper

Confederation of European Security Services

# Position Paper on the future Commission Regulations on UAs

November 2018

The Confederation of European Security Services (CoESS) welcomes the opportunity to comment on the 2 proposals for Commission Regulations on UA's and herewith would like to submit its comments and suggestions.

CoESS has commented on several occasions on earlier Commission and EASA documents and wishes to reiterate its interest for UAs, as useful addition to the range of technological means and equipment in use in private security services. As also highlighted in previous position papers, CoESS sees opportunities in **three types of activities** with unmanned aircraft:

- **Supporting guards in their missions**, making them less dangerous and more efficient, using fully automated drones to carry out security missions;
- **Tracking, tracing, monitoring and responding to alerts related to drones**, in the same way as the industry already tracks land vehicles, in coordination and cooperation with air control agencies;
- **Detecting and preventing the ill use of UA's**, whether unintentional, intentional or malicious – subject to rules and regulations creating a legal basis for this type of response and the ensuing liability as a result of the latter.

## General comments

- Further to its earlier comments regarding the lack of attention to security in the future legislation, the answer from the Commission has been that security would be addressed by Member States. CoESS is concerned at this approach, as it will create divergences between the national approaches, in turn possibly leaving gaps. As the saying goes "a security chain is as strong as its weakest link" and CoESS therefore believes that in the absence of an EU common approach to security, there should at the very least be a regular exchange of views and information on security risk assessments between Member States, as well as between them and the neighbouring countries.
- CoESS also has concerns on **cybersecurity and IoT security**. In particular, it wonders if there is sufficient security embedded both in the hardware and software or if manufacturers and developers need to step up current security measures and technologies.

**Catherine PIANA**, Director General
**CoESS | Confederation of European Security Services**
Jan Bogemansstraat | rue Jan Bogemans 249 | B-1780 Wemmel Belgium
Mobile : +32 472 180 107 | **catherine@coess.eu** | **coess.org**

- Security is not included in any of the flight aspects, i.e. the pilot training, the flight risk analysis, the reasons why a flight should be prohibited or interrupted.
- CoESS issued a position paper in March 2017 entitled **"The Use of UA in Private Security"**, which includes a number of standard scenarios for the use of UAs in the industry it represents. It would welcome some feedback on these scenarios.

**Detailed comments**

**On PART-2018-221929V3 on unmanned aircraft intended for use in the 'open' category, and on third country operators of unmanned aircraft systems**

**Article 6 – Obligations of Manufacturers** (in relation with Annex points 1 to 6): there is no mention of the obligation to ensure robust cyber security of both the hardware and the software, so as to protect the UAs against unlawful or criminal interference. As highlighted above, as well as in our previous documents, CoESS has mentioned the current and future use of drones as security threats. As part of the IoT ecosystem, UAs have been used in criminal and terrorist activities before, and will be used again. All measures should be taken to prevent this from happening and making systems as robust against cyber attacks as is possible.

Rules for C1, C2, and C3 classes of UAVs are welcomed, in particular provisions (11), (12) and (13) for class C1 and similar provisions for C2 and C3.

Similarly we welcome (in Part 6) the requirement for a remote identification system add-on.

**On PART-2018-221538V4 on the rules and procedures for the operation of unmanned aircraft**

**Article 2**

In the definition of VLOS and BVLOS (definitions (g) and (h)), how should night flights be considered?

Definition (p) defines autonomous operations and mentions that the remote pilot cannot intervene. However, the concept of "autonomous" generally implies not only that *the pilot cannot intervene*, but that *there is no pilot*. We would welcome clarification on this point.

**Catherine PIANA**, Director General
**CoESS | Confederation of European Security Services**
Jan Bogemansstraat | rue Jan Bogemans 249 | B-1780 Wemmel Belgium
Mobile : +32 472 180 107 | **catherine@coess.eu** | **coess.org**

**Article 11 section 3**

5 (h): It should be considered that the cyber security of the UAs is an element to be considered for establishing the risk assessment.

**Article 12 – Authorizing operations in the 'specific' category**

4 (b) mentions technical features. Cyber-security aspects should also be taken into account (both hardware and software).

**Article 14**

We welcome the fact that there should be a registration system for UAS operators whose operations may present a risk to safety, security, privacy and protection of personal data or the environment. There is, however, no mention of what the methodology should be regarding the security risk assessment. It might be useful to look if ISO 31000 on risk assessment could be used as a common reference to this end.

For security operations, such as guarding, remote surveillance, etc, UA pilots should be licensed security guards, and these operations should therefore fall under the national legislation governing private security.

**Article 16 – Model aircraft clubs and associations**

The fact that the competent authority may (or not) issue a model aircraft club or association with an operational authorisation in accordance with relevant national rules, and may (or not) specify the conditions under which they may continue their activities is a concern. Has this been decided further to a security risk assessment? If these clubs and associations may function without rules and under the radar, they may become a point of attraction for the ill-intentioned people (as small aviation clubs attracted the 9/11 terrorists for undetected aviation training). As far-fetched as this may seem, it is worth examining this provision with a security mindset.

**ANNEX**

**Transition period**: has this provision been examined from a security mindset, and a risk assessment been carried out?

**Catherine PIANA**, Director General
**CoESS | Confederation of European Security Services**
Jan Bogemansstraat | rue Jan Bogemans 249 | B-1780 Wemmel Belgium
Mobile : +32 472 180 107 | **catherine@coess.eu** | **coess.org**

**PART A (1) (c) ii UAS operators in subcategory A1:** CoESS would recommend adding general safety to the list (not just air safety).

**UAS.OPEN.70 Responsibilities of the remote pilot:** there may be a mistake and point (4) should actually read "For the purposes of point (f) (not (e)) of paragraph 2…" (rest of the sentence unchanged).

**UAS.LUC.030 Safety Management System**

As observed above in the general comments, CoESS has repeatedly drawn the attention to the fact that security aspects should be integrated within the document. There are many synergies between safety and security and it would make sense that this section would refer to Safety and Security Management System. For example, the risk of Insider Threats should be looked at more closely, as this too has been identified by the Commission as an increasing threat.

**Closing statement**

In conclusion, CoESS holds the view that the future legislation is still lacking the security aspect, which is crucial, as only one security incident may jeopardise or even halt the development of UAs in the future.

Practical elements are also needed to ensure that the legislation is fully operational and ready for implementation. CoESS welcomes information on concrete aspects of implementation, such as registration, geo-awareness, how to obtain an LUC certificate, how the U-space will actually work, for example.

CoESS looks forward to an exciting future and to the opportunities that UAs hold, with the caveats expressed above. The CoESS experts are at the Commission's and EASA's disposal for further and more detailed information.

Thank you for your attention.

Catherine PIANA
Director General

**Catherine PIANA**, Director General
**CoESS | Confederation of European Security Services**
Jan Bogemansstraat | rue Jan Bogemans 249 | B-1780 Wemmel Belgium
Mobile : +32 472 180 107 | **catherine@coess.eu** | **coess.org**