



FPV UK response to
CAA CAP2610: Consultation: Review of UK Unmanned Aircraft
Systems (UAS) Regulations

Version 1.0

30/11/2023

Purpose of this document

On 22nd November 2023 the CAA published a consultation document and response form on its website: <https://consultations.caa.co.uk/rpas/review-of-uk-uas-regulations-consultation/>

The CAA have launched a consultation on proposals to make it easier for drone users to fly safely and meet regulatory requirements.

The proposals are based on feedback from the drone community in a previous Call for Input. Proposals include introduction of product requirements for drones, extension of Flyer ID training to users of drones under 250g, introduction of Remote ID and extension of time period to adopt class-marked drones by 2 years.

The consultation closes on 10th January 2024.

This represents an important opportunity for you, and the drone community as a whole, to have a say in the future of UAS regulations in the UK.

Please read the CAA document and respond, using the web based form, with your thoughts on each topic.

The following pages contain FPV UK's response which you may be interested to read before you submit your own reply to the CAA. However, it is important that you complete the CAA response in your own words. Identical copy and pasted responses are normally ignored by the CAA.

Format

In the following pages you will find the CAA preamble in black italics, the associated questions in non-italic black, followed by FPV UK's response in blue.

Where the CAA's response form requires a response from a bullet point list, our selection is included first. Followed by the rationale for our answer.

CAA Preamble:

Operational Requirements

- 2.1 *At present, operational requirements are structured through a system of categories (i.e. Open, Specific and Certified) and sub-categories (i.e. Open A1, A2 and A3), reflecting the characteristics of the operation. The Call for Input presented opportunities to simplify operational requirements in the Open category.*
- 2.2 *Responses to the Call for Input raised concerns with the proposals to simplify how operational requirements are categorised (Question 5). Overall, 33.3% of responses were positive, and 59.7% were negative. Respondents generally favoured maintaining the system of categories and sub-categories, although there was some recognition of the complexity of existing regulation, and the benefits of making regulations simpler.*
- 2.3 *We agree with stakeholders who submitted that the framework of operational categories and sub-categories remains broadly appropriate and who challenged the costs of changing. However, we also consider there to be opportunities to make targeted improvements to operational requirements that UAS users could find confusing. Specifically:*
- (i) Currently, all flights in the A1 sub-category cannot take place over groups of uninvolved people, but UAS <250g and C0 UAS can fly over uninvolved individuals. C1 UAS (<900g) must reduce, as much as possible, flights over uninvolved persons. Our view is that this complexity could make it harder for UAS remote pilots to understand and comply with this requirement. We are proposing to allow C1 UAS to overfly uninvolved people, whilst maintaining the requirement not to overfly groups of uninvolved people. This would, in effect, harmonise requirements for flying over uninvolved persons in the A1 subcategory for different types of UAS. Over the coming months, we will assess the safety implications of this approach.*
- (ii) At present, the regulation only explicitly allows C0 and C1 UAS to fly in the A1 sub-category. We are proposing to explicitly allow C0 and C1 UAS to fly in the A3 sub-category. Whilst this will not impact the actual operational privileges for these UAS, it will clarify that C0 and C1 can be used in these sub-categories, and help CAA communicate how class-marks relate to operational requirements.*
- (iii) The current operational requirements for flights in the A3 sub-category do not specifically define a minimum distance a UAS must fly from an uninvolved person. However, guidance material (e.g. CAP2012 and AMC/GM) sets out that a minimum distance of 50m should be maintained from uninvolved persons. We are proposing to introduce a regulatory requirement in the A3 sub-category for UAS to fly a minimum*

of 50m from uninvolved persons. This aims to avoid confusion for users by aligning regulation with current guidance.

(iv) At present, the operational requirements for flights in the A3 sub-category limit distances to residential, commercial, industrial or recreational areas to 150m. The CAA interpretation of this requirement, published within guidance material, sets out that this also includes distance to individual buildings. The difference between the guidance material and the regulatory requirements may create confusion for operators flying near individual buildings. We are proposing to change the regulatory requirement for flights in the A3 sub-category to be at least 150m away from residential, commercial, industrial, recreational areas and buildings. Flights taking place closer than 150m to individual buildings in the Open category will continue to be subject to A1 or A2 subcategory requirements.

Question 1: Do you agree or disagree with our proposal to allow C1 UAS to fly over uninvolved people in the A1 sub-category, aligning to regulations for C0 and <250g UAS? Please explain your answer.

Agree.

It is simpler to understand and more permissive, so we agree with this proposal.

Question 2: Do you agree or disagree with our proposal to explicitly allow C0 and C1 UAS to fly in the A3 sub-category? Please explain your answer.

Agree.

It stands to reason that a C0 and C1 UAS which is permitted to fly close to and over uninvolved people (A1), should also be permitted to fly far away from people too.

This is clearly an unintended anomaly and it should be corrected.

Question 3: Do you agree or disagree with our proposal to align regulatory requirements in the A3 sub-category to current guidance to fly UAS a minimum of 50m from uninvolved persons? Please explain your answer.

Agree.

If the intent is for UAS to always be at least 50 metres from uninvolved people in A3 then this should be specified in the regulation, not secondary guidance material.

However, we would challenge the rationale for the 50m number. What evidence is there that 50m separation is required? Is this proposed to be 50m horizontal, or 'not-within 50m'?

Question 4: Do you agree or disagree with our proposal to align regulatory requirements in the A3 sub-category to current guidance to fly a minimum of 150m from residential, commercial, industrial, recreational areas or buildings? Please explain your answer.

Disagree.

An individual building - e.g. a standalone home - is not the same as a commercial, industrial or recreational area.

Operational Category Names

- 2.4 *The Call for Input set out that the names of operational categories (Open, Specific, Certified) and sub-categories (A1, A2, A3) are perceived as confusing and unintuitive for some users. We asked whether it would be beneficial to re-name operational categories, to make them easier for users to understand (Question 4).*
- 2.5 *Responses to this question were mixed, as 45.6% were positive and 44.1% were negative. Some responses provided limited support for changing category names (e.g. Open, Specific), but greater support for changing sub-category names (e.g. A1, A2, A3). Many stakeholders specifically recommended changing the sub-category names to 'Over', 'Near' and 'Far'.*
- 2.6 *Our view is that changing the operational sub-category names to be more intuitive and meaningful will help users understand and recall UAS regulations, resulting in increased compliance. **We are proposing to change the names of UAS subcategories from A1, A2, and A3, to 'Over', 'Near' and 'Far'.** These revised names aim to reflect the key operational differences between each sub-category – i.e. the distance to uninvolved persons.*
- 2.7 *We have also considered alternative names for sub-categories, reflecting potential risk-profile (e.g. Low, Medium, High Risk) or complexity of operation (e.g. Basic, Advanced). Our view is that these alternatives do not appropriately convey the key parameters of each operational sub-category and may lead to further confusion. However, we welcome feedback from stakeholders on any alternative names we should consider.*
- 2.8 *We agree with respondents who submitted that Open, Specific and Certified are well embedded in the sector. We therefore do not propose to change the name of operational categories.*

Question 5: Do you agree or disagree with our proposal to re-name the A1, A2, A3 operational sub-categories to ‘Over’, ‘Near’ and ‘Far’? Please explain your answer, including any other names you would suggest.

Agree.

This is certainly easier to understand and remember.

Question 6: Do you agree or disagree with our proposal to maintain existing names for Open, Specific and Certified operational categories? Please explain your answer.

Agree.

These three categories are fairly well understood and relatively easy for a newcomer to understand.

Operational Exclusions

- 2.9 *At present, some UAS - such as toys or UAS <250g - benefit from exclusions from some operational requirements, including registration, remote pilot competency and safety requirements. The Call for Input considered whether to simplify operational requirements by removing some of these exclusions.*
- 2.10 *Feedback to this question (Question 7) was moderately supportive, as 54.3% of responses were positive, and 36.7% of responses were negative. Changes to exclusions for ‘toy’ UAS received more positive feedback due to the ambiguity of the definition of ‘toy’. However, changes to exclusions for <250g UAS were received less favourably, due to a perceived lack of risk from these UAS, despite their widespread adoption.*
- 2.11 *Our view is that the exclusion for ‘toy’ UAS from registration and remote pilot competency requirements is confusing for users and enforcement bodies. This is due to the lack of standard marking for ‘toy’ UAS, and the ambiguous criteria for what is considered a ‘toy’ – such as whether it was advertised or packaged to attract children. For some users, this could result in non-compliance and the unsafe and insecure operation of their UAS. In the future, this will likely be exacerbated further when both toy and non-toy UAS will be required to meet C0 class-marking requirements, making it even harder for UAS users to differentiate between what is and isn’t a ‘toy’.*

- 2.12 *We also recognise that UAS technology is evolving, to become smaller, cheaper and more capable. Consequently, the risks associated to some 'toy' UAS are also changing. We aim to ensure our regulatory framework is fit for the future, as technology evolves.*
- 2.13 *We are proposing to remove the exclusions from registration and remote pilot competency requirements for 'toy' UAS operations – instead, relying wholly on weight and/or class-mark to determine the scope of requirements. This change will result in operators of UAS <250g with cameras needing an Operator ID, irrespective of whether it is a 'toy' or not. As is the case today, operators of UAS <250g without cameras will not require an Operator ID. Proposals relating to Flyer ID are discussed in Chapter 3*

Question 7: Do you agree or disagree with our proposal to remove exclusions for 'toy' UAS from registration and pilot competency requirements? Please explain your answer.

Disagree.

Children's toys, designed to be used in back gardens and parks, should be excluded from the regulations. These will frequently include cameras, which are now very small and very cheap and will only get smaller and cheaper.

Question 8: Are there other opportunities to simplify operational regulation that we should be considering? If yes, please describe them in full.

N/A.

Flyer Education

- 3.1 *At present, remote pilots flying a UAS which is 250g or more must obtain a Flyer ID and take an online theory test. This test, provided free of charge by the CAA, ensures that beginner UAS flyers have a foundational understanding of UAS regulations.*
- 3.2 *The Call for Input highlighted that remote pilots of UAS less than 250g are currently exempt from some operational requirements, including the Flyer ID test. It noted the increasing capability and availability of <250g UAS and the risks from these UAS – such as entering restricted airspace, flying dangerously close to uninvolved persons, buildings or objects, or unlawfully collecting personal and sensitive data. In response to the Call for Input, some respondents proposed that the Flyer ID test should also be required for pilots of a wider range of UAS.*

- 3.3 *Our view is that greater education would help UAS pilots know how to comply with the regulations, and would improve the safety, security and compliance of UAS operations. Surveys completed for the CAA show that understanding of some regulatory requirements is below where we would hope. For example, 62% of drone users knew about legal registration requirements, and only 56% of drone users knew that operators of <250g UAS with cameras should be registered with the CAA. In addition, only 21% of drone users had awareness of the 400 ft height restriction, without being prompted.*
- 3.4 *Our view is that requiring a foundational understanding of how to use a UAS safely and lawfully is a proportionate measure, given the risks posed and the wider benefits of a safe, secure airspace. Through encouraging more responsible UAS use by recreational users, we aim to help improve the reputation and acceptance of UAS in wider society, assisting the sector to grow.*
- 3.5 *We also recognise that the technical capabilities of lightweight UAS have increased significantly over time and are likely to increase further. This changes the safety and security mitigations required.*
- 3.6 *We are proposing to extend the requirement for a remote pilot to take the Flyer ID test for UAS operations in the 'Open' category, to include when flying a UAS less than 250g with and without a camera. As is described in Chapter 2, we also propose to remove exclusions for 'toy' UAS from these requirements.*
- 3.7 *We recognise that miniature UAS (e.g. <100g) without cameras pose negligible safety and security risks, and previously would have been considered 'toys' in most cases. We welcome views on whether we should introduce a minimum weight threshold, in the region of 50g to 100g, to exclude miniature UAS from these requirements.*
- 3.8 *Beyond the Flyer ID test, we have also published a consultation on changes to the pilot competence framework in the Specific category. These proposals aim to create a comprehensive competency framework for advanced UAS operations, enabling Beyond-Visual-Line-of-Sight (BVLOS).*

Question 9: Do you agree or disagree with our proposal to require remote pilots of <250g UAS to take the online Flyer ID test? Please explain your answer.

Disagree.

<250g aircraft are 'harmless'* ('pose a negligible safety and security risk') and as a result the regulations permit them to fly virtually anywhere.

Also, there is no evidence to suggest that the risk posed by sub-250g has changed / become unacceptable. I.e. there have not been widespread injuries to the public or mid-air-collisions involving sub-250g drones.

There is therefore no requirement to alter the competency requirements for <250g drones.

* This study defines sub-250g drones as 'harmless' - <https://journals.sagepub.com/doi/pdf/10.1177/1756829317691991>).

Question 10: Should the CAA introduce a minimum weight threshold, in the region of 50g – 100g, that aims to exclude miniature UAS from Flyer ID requirements? Please explain your answer.

Disagree.

This limit should be 250g as previously defined based on the internationally-aligned logic* which dictated that sub-250g aircraft posed a negligible/acceptably low level of risk to aviation and people on the ground* is still sound and no extra restrictions should be imposed on sub-250g aircraft.

* Such as this study which defines sub-250g drones as 'harmless' - <https://journals.sagepub.com/doi/pdf/10.1177/1756829317691991>).

Furthermore, there is no evidence to suggest that the risk posed by sub-250g has changed / become unacceptable. I.e. there have not been widespread injuries to the public or mid-air-collisions involving sub-250g drones.

If an even lower limit really is required, for an even *more harmless* group of aircraft, we would suggest 150g.

Product Guidance

- 3.9 *Under the UK Regulation (EU) 2019/94518, manufacturers must provide an information notice to users, alongside the UAS. In practice, this could be a leaflet included in the product packaging that describes the safety and security mitigations users should carry out when operating a UAS.*
- 3.10 *The Call for Input presented an opportunity to improve how user guidance is communicated, by requiring manufacturers to convey regulatory information during product set-up via the controller app or other user interface. Responses to the Call for Input (Question 16) were largely in support of this proposal, as 78.4% were positive and 13.4% were negative. Some negative responses submitted that introducing mandatory information notices for every flight, without the option to skip the notification, would be burdensome for experienced flyers.*
- 3.11 *Our view is that users are likely to be more responsive to information displayed via the user interface or controller app, compared to a physical leaflet. Providing this information digitally could also have wider benefits, such as enabling accessibility*

features to help those with disabilities and updates to reflect any changes in guidance.

- 3.12 *We are proposing to require C0, C1, C2 and C3 UAS to display important regulatory information, via a digital information notice, on the user interface or controller app during the product set-up. However, we also agree with Call for Input respondents, who argued that more frequent displays of this information would inconvenience experienced fliers. As such, we do not propose to require manufacturers to display the digital information notice more frequently.*
- 3.13 *The digital information notice could include key messages on the registration processes, safety mitigations, flyer competency requirements, airspace restrictions and data privacy. We would expect to prescribe the guidance text to UAS manufacturers, with a supporting requirement for UAS to present the information in a user-friendly and accessible way. This aims to encourage manufacturers to present the information impactfully, without being overly prescriptive in terms of the format.*
- 3.14 *If the UAS does not have a digital user interface or controller app, manufacturers could continue to provide user guidance as a physical information notice that is included in the box. This aims to prevent imposing a disproportionate burden on UAS manufacturers that do not have the capability to provide digital information notices.*
- 3.15 *There may be scenarios where the CAA wishes to update the digital information notice, or to communicate safety information to UAS flyers through the user interface or controller app. For example, this could be to communicate changes to regulation, or to issue guidance based on new safety risks. We are considering how to futureproof this proposal, including whether to require manufacturers to keep the digital information notice up-to-date, or to issue information to flyers at the request of the CAA*

Question 11: Do you agree or disagree with our proposal to require manufacturers to present important regulatory information on the user interface or controller app to C0-C3 UAS users at product set-up? Please explain your answer, and consider whether manufacturers should update the digital information notice or communicate safety information to UAS flyers at the request of CAA. Please explain your answer.

[Agree - in the case of commercial-off-the-shelf drones.](#)

[This must not affect other types of unmanned aircraft, such as RTF \(Ready to Fly\) radio controlled aeroplanes, etc which do not have a 'product set-up' process or 'user interface' in the same way.](#)

Policy and Guidance Documentation

- 3.16 *Regulations should be organised, presented and communicated clearly to users, to ensure requirements are understood. Today, regulatory requirements contained primarily in UK Regulation (EU) 2019/945, UK Regulation (EU) 2019/94719 and the Air Navigation Order 2016 are supported by other sources of information including the CAA website, the Drone and Model Aircraft Code, the CAP 722 series and supporting Acceptable Means of Compliance (AMC) and Guidance Material (GM).*
- 3.17 *The Call for Input recognised that the complexity of the current document structure could make it harder for some users to understand how to comply. Responses to the Call for Input (Question 18) largely supported the opportunity to simplify the policy and guidance document structure, with 90.7% providing a positive view.*
- 3.18 *We recognise the challenges raised by stakeholders on the CAP 722 document series, and the potential duplication with the AMC and GM. This can make it difficult for users to know which documentation to consult, how the documents inter-relate, and the legal status of guidance. In addition, the regulatory changes proposed in this consultation and the implementation of SORA in the Specific category will result in significant changes to the CAP 722 guidance material. Therefore, we are proposing to phase out the CAP 722 series over time.*
- 3.19 *However, we understand that phasing out the CAP 722 series will create a gap in the supplementary guidance available in the Open and Specific categories. Subject to ongoing analysis, we are proposing to absorb relevant information from the CAP 722 series into AMC/GM and to create new, digital guidance material. The purpose of this new guidance will be to provide information using non-technical language, that is easy to understand and navigate.*

Question 12: Do you agree or disagree with our proposal to phase out the CAP 722 series and introduce new, user-friendly guidance material? Please explain your answer.

Agree.

CAP722 is far too complex.

Question 13: Are there other opportunities to improve education and understanding that we should be considering? If yes, please describe them in full.

Yes.

Publish information about consultations such as this one, and other important regulatory and safety information, to all registered drone operators and flyers.

The CAA has email addresses for all drone operators and flyers - this mailing list should be used to disseminate useful information.

Class Marking and Product Standards

- 4.1 *The framework for Open category product standards is referred to as 'class marking' and is based on retained EU law. Whilst the regulation exists in UK Regulation (EU) 2019/945, compliance is not yet possible due to a lack of product standards and oversight regime. As such, no UAS-specific product requirements have been implemented in the UK yet.*
- 4.2 *The Call for Input highlighted the important role of product standards in mitigating safety and security risks from UAS. Through placing technical mitigations within UAS, it will make it easier for users to comply and help prevent misuse. Responses to the Call for Input were strongly supportive of our proposal to implement manufacturer standards (Question 7), with 78% of respondents supporting the proposal. In addition, many respondents proposed that our approach should align with EU legislation. There was minimal support for implementing significantly different approaches to those used in the EU, due to the impacts of international divergence.*
- 4.3 *Our view is that product standards will be essential to deliver our policy objectives, ensuring that UAS meet a minimum level of safety, security and performance. In turn, we would expect that this would reduce the safety and security incidents from UAS and help build confidence in the UAS sector. **We are proposing to implement class-marking and product standards from 1st January 2026 for UAS intended to be used in the Open category.** In effect, manufacturers and other economic operators placing UAS on the market for use in the Open category would need to meet class-marking requirements from this point.*
- 4.4 *We recognise the benefits of international alignment. However, we also consider there to be areas where divergence is in the UK's interests. **We are proposing to align to EU regulations for class-marking and product standards, unless there is a safety, security or user benefit that requires divergence.** Chapters 3 and 5 describe specific proposals that diverge from EU regulations, relating to Remote ID, geo-fencing, and user guidance. In addition, we are proposing to:*
- ***Update requirements for tethered UAS**, to improve product safety and harmonise requirements across tethered UAS. Specifically, we propose to align requirements across C1, C2 and C3 UAS to exempt tethered UAS from command-and-control link protection and link recovery requirements. We also propose to require tethered UAS to have Remote ID.*
 - ***Require C0 and C4 UAS to have a unique serial number**, to enable the CAA and other bodies to identify and manage conformity of these UAS.*

- **Remove requirements for C5 and C6 UAS intended for use in the Specific category**, given that these will not be used in future regulation.

4.5 *To deliver this regulation in practice, the Secretary of State will need to designate technical standards that have been adopted by the British Standards Institute (BSI). Manufacturers who adopt these designated standards would have a presumption of conformity against regulatory requirements. The CAA and BSI will work with the Department for Transport to identify the technical standards that could be used by manufacturers to demonstrate compliance. Appendix B provides a table of the standards we intend on assessing.*

Question 14: Do you agree or disagree with our proposal to implement class-marking and product standards? Please explain your answer, and provide any further feedback on the technical standards we intend on assessing, if possible.

Agree.

The UK class marking standards should align with international standards as much as possible to ensure that manufacturers sell their products in the UK.

The removal of C5 and C6, updates to tethered UAS requirements, etc seem sensible. Except requiring remote ID on a tethered UAS. Surely it is pretty simple to identify the operator of a tethered UAS?

Question 15: To what extent should the UK align to the EU regulatory framework for product requirements? Please explain your answer.

The UK class marking standards should align with international standards as much as possible to ensure that manufacturers sell their products in the UK.

Question 16: Do you agree or disagree with our proposed changes to product requirements, as set out in paragraph 4.4? Please explain your answer.

Cautiously agree.

Generally speaking, it is clearly in the UK's interest for the UK class marking standards to align with the EU. UK rules should only diverge in minor ways, where it is in the UK's interest to do so.

Product Labelling and Identification

- 4.6 *The Call for Input considered whether to introduce a product labelling scheme for class-marked UAS, over and above the class identification label requirements (e.g. C0, C1 etc.) currently in the regulation for class-marking. Most respondents were supportive of product labelling, with 78% responding positively. However, some respondents advocated for use of the class identification label retained in legislation and used in the EU. Some respondents questioned whether an additional labelling scheme, as well as EU class identification label, would be confusing.*
- 4.7 *We agree with the stakeholders who submitted that an additional labelling scheme may create confusion. We recognise that the intended benefits could be delivered through improving how the current labelling scheme and class marking requirements are communicated*
- 4.8 *However, as is described in the above section, we do not expect to fully align to EU product requirements in all cases, and the UK and EU may diverge further over time. Consequently, EU class identification labels cannot be an enduring solution to physically identify compliant products under the UK jurisdiction. Using the same label as the EU would introduce practical challenges for stakeholders to understand whether the product is compliant under the UK or EU jurisdictions, or both.*
- 4.9 ***We are proposing to replace the EU class identification label with a UK-specific identification label. We expect that replacing the letter 'C' with 'UK' provides the simplest solution (i.e. replacing C1 with UK1). We believe this proposal is necessary to ensure class identification labels can be used to demonstrate compliance with the regulations under the UK and/or EU jurisdictions.***

Question 17: Do you agree or disagree with our proposal to use UK-specific class identification labels on class-marked UAS, to differentiate between UAS compliant under UK and EU legislation? Please explain your answer.

Agree.

If the UK has slightly different class marking standards to the EU then it will require a different label. In the same way that consumer electronics are now labelled CE and UKCA.

Market Surveillance

- 4.10 *To implement class-marking and product standards, new capabilities will be required to manage conformance and compliance. This includes the creation of a Market Surveillance Authority (MSA). The MSA is a key role defined in UK Regulation (EU) 2019/945, responsible for overseeing compliance with product*

standards and acting when there is non-compliance. The Secretary of State is responsible for appointing a MSA. The CAA is working with the Department for Transport to consider whether the CAA or an alternative organisation should take this role.

4.11 *We are also considering which organisation is most appropriate to approve and manage the organisations responsible for providing conformity assessment against product standards ('Conformity Assessment Bodies'). Whilst the regulation currently requires the Secretary of State to approve and manage Conformity Assessment Bodies, we consider other organisations may be more appropriate – such as the CAA, or the organisation acting as the MSA. This would require regulatory change.*

4.12 ***We are proposing to introduce a requirement on manufacturers to provide information to the MSA on UAS product codes, make, model, and relationship to serial numbers, when products are placed on the market. This will allow the MSA to identify the make and model of UAS from their Remote ID message. It will enable the MSA to identify specific models of drones that may be involved in potential incidents and take appropriate mitigating action.***

Question 18: Do you agree or disagree with our proposed approach to enable the implementation of a MSA? Please explain your answer.

Agree.

It seems reasonable for the CAA to approve and manage Conformity Assessment Bodies for UAS. It is the CAA which effectively creates and manages the regulations. Having a direct relationship between the regulator and the CABs makes sense.

Question 19: Are there other opportunities to improve UAS product safety and security that we should be considering? If yes, please describe them in full.

N/A.

Remote ID

5.1. *Remote ID is the ability of a UAS to communicate identification and location information during flight. The requirement for Remote ID already exists in UK Regulation (EU) 2019/945 and 2019/947 but is yet to be implemented. The Call for Input described the important role of Remote ID in improving the ability to*

identify individuals misusing UAS and in enabling enforcement. In addition, it discussed how Remote ID could be implemented in practice and potential changes to the regulation.

- 5.2. *60.7% of responses to the Call for Input were negative, and 15.3% responses were positive. Respondents raised concerns regarding data privacy implications, and Remote ID's effectiveness in delivering improved security. Respondents with positive views recognised the benefits from identifying unlawful operators.*
- 5.3. *Data available to the CAA, government and police provides conclusive evidence of the severity and scale of safety and security risks posed by the misuse of UAS. Since November 2020, police have received 18,290 reports of drone flights involving a legal, nuisance, criminal or safety concern. In the first 9 months of 2023, reports are 10% higher than the same time last year.*
- 5.4. *The CAA, Home Office, Department for Transport and Police maintain the view that the security benefits of Remote ID will be important in preventing unlawful UAS operations and enabling UAS regulations to be enforced. Specifically, Remote ID will:*
 - *Support the police and other relevant authorities to identify malicious UAS operators and take appropriate action.*
 - *Enable the police to differentiate between malicious and negligent UAS operations, and focus resources on those that pose the greatest threat.*
 - *Promote increased compliance, by increasing accountability from UAS users.*
- 5.5. *Our view is that Remote ID is a proportionate intervention, due to the scale of security risks presented by UAS misuse and the low impact of Remote ID to operators who fly UAS safely and securely. Remote ID is an established technical solution implemented by several international governments and national aviation authorities, including in the EU, USA, Switzerland and Japan, demonstrating the important role Remote ID has in protecting airspace globally.*
- 5.6. *Remote ID could also provide safety benefits, through promoting increased compliance with safety requirements. Data collected by Remote ID will also provide valuable safety and operational information to the CAA, allowing us to develop policy based on actual UAS operational data.*
- 5.7. *Several respondents to the Call for Input submitted that geo-awareness and/or geofencing would provide a more effective mitigation against misuse of UAS. Whilst we recognise the significant benefits of these mitigations, we also consider that they will not be effective in all cases – for example, for malicious UAS operations taking place in un-restricted airspace.*
- 5.8. **We are proposing to implement Remote ID through product and operational requirements.** *The key parts of our proposal are as follows:*

- (i) **Technical approach:** Remote ID requires UAS to transmit the operator's registration number, serial number, position, altitude, route, speed and position of the pilot or take-off point. This data could be readable through a mobile phone near to the UAS (e.g. via Wi-Fi/Bluetooth, referred to as 'direct' Remote ID). Data could also be passed to a database over a network (referred to as 'network' Remote ID), providing real-time and historical visibility.

Our view is that Hybrid Remote ID (i.e. network and direct) offers the optimal solution for the UK. The Network Remote ID would be the default approach, and would enable the remote tracking of UAS and historic investigations when a connection to the network is possible. The direct element would provide a 'backup' in areas of poor connectivity or in situations where the network is down.

More specifically, UAS operators would register themselves on DMARES and receive their Operator ID (and a 'secret key' used for validation). UAS operators would set up their UAS, inputting their Operator ID and secret key and ensure the required form of Remote ID is enabled based on their location for their UAS to be able to take off. For Network Remote ID, the UAS (or Ground Control Station) would transmit a standard set of data on the UAS position and the remote pilot position to a Network Remote ID Service Provider. The Remote ID Service Providers would push the UAS flight data to the Master Data Hub. UAS flight data would be ingested and stored in the Master Data Hub and made available to Authorised Users where access controls permit. Where Direct Remote ID only is permitted, the UAS would first attempt to connect to the Network, and should this not be possible, would be able to take off with Direct Remote ID enabled.

Appendix B also sets out the technical standards we are considering for manufacturers to demonstrate compliance with this requirement.

- (ii) **UAS in scope:** Remote ID is proposed to be mandated for all UAS with a maximum take-off mass of 250g or more, or under 250g with a camera, in both the Open and Specific category. This recognises the safety and security risks from these UAS, and the increasing technical capabilities of light-weight UAS with cameras in particular. C0 UAS without cameras and C4 UAS would not be in scope of product requirements.
- (iii) **Operational requirements:** UAS operators and remote pilots would also be subject to operational requirements to ensure UAS in scope are operated with active Remote ID. This aims to provide an additional layer of assurance that Remote ID is being used. Operators of privately-built UAS weighing 250g or more, or with a camera, would be required to have active Remote ID, delivered via an add-on module, unless a Model Aircraft exemption has been granted, as described below in paragraph 5.8.viii.
- (iv) **On-device enforcement:** We propose to implement technical mitigations that ensure Remote ID is active before a UAS takes flight. This aims to prevent unlawful UAS users from disabling UAS before operations and undermining the

security benefits of Remote ID. We recognise concerns raised around how Network Remote ID would work in areas of poor connectivity. A proposal we are considering is to define Remote ID zones, where the UAS would require active Network Remote ID to fly in certain geographic areas. In other areas, where security risks are lower and mobile connectivity may be poor, operations would be allowed with Direct Remote ID enabled, provided that the UAS must first attempt to enable Network Remote ID.

(v) **Legislative enforcement:** *To promote compliance with these requirements, it is necessary for the police to have the ability to take action against operators who do not comply with Remote ID, or who attempt to tamper with or spoof a Remote ID transmission. To enable legislative enforcement of Remote ID requirements, we expect to create new offences in legislation for non-compliance with these requirements.*

(vi) **Data privacy, security and access:** *The Call for Input highlighted concerns from UAS users regarding the impact of Remote ID on data privacy. Our approach to data privacy would be compliant with the Data Protection Act 2018 and therefore GDPR principles. More specifically, we will ensure that personally identifiable information, such as Operator ID, is not made available to the general public, and is protected by robust security controls. Under Network Remote ID, service providers would not display the pilot or ground control station's location - this would be viewable by authorised persons only, such as the police. The pilot or ground control station location data would be visible to those able to receive and interpret Direct Remote ID data, as it is not technically possible to encrypt this data to only be viewable by certain user groups. The pilot's location will therefore only be available publicly if Network Remote ID is not enabled.*

It is proposed that authorised organisations such as the police and prisons would have access to the Remote ID data, with the police having access to operator details when necessary.

To address data privacy concerns raised in the Call for Input, we are proposing to work with stakeholders to develop and publish a data privacy, security and access policy. We expect this to include details on what information is shared with who, how data is communicated, the security mitigations used to prevent unauthorised access to data, and the requirements to protect the storage of personal data.

(vii) **Legacy UAS:** *The current operational requirements allow legacy (i.e. non-class marked) UAS to be operated in the A1 and A3 sub-category indefinitely. Our view is that these regulations for legacy UAS would undermine the benefits of Remote ID, by allowing malicious operators to operate lawfully without Remote ID indefinitely, and by reducing the ability for police to differentiate between lawful, negligent and criminal operations. We are therefore proposing to require legacy UAS to be operated with active Remote ID from 1st January 2028 onwards (excluding UAS <250g without cameras). This requirement could be met through either remotely upgrading a UAS with inactive Remote ID capabilities, or through users attaching a compliant*

Remote ID add-on module to their device.

- (viii) **Model Aircraft:** *We recognise the good safety record of Model Aircraft flying in the UK, and the importance of Model Aircraft to many hobbyists. However, our view is that a blanket, unconstrained Remote ID exemption for all Model Aircraft flying would make UAS regulations challenging to enforce and create inconsistent security outcomes, due to the wide range of locations and aircraft currently used for Model Aircraft flying. Our aim is therefore to find a proportionate approach that supports the Model Aircraft community to fly safely and securely, without undermining the security benefits we aim to achieve through Remote ID.*

We are proposing for safe and secure Model Aircraft flights to be exempt from Remote ID requirements. Under our proposed approach, Model Aircraft flights would be exempt from Remote ID requirements, if:

- a. *The aircraft meets the CAA's definition and specification for exempt Model Aircraft;*
- b. *The pilot and UAS remain within the bounds of a designated Model Aircraft flying site, authorised by the CAA based on proximity to urban, sensitive or restricted sites; and*
- c. *The flight takes place within a Model Aircraft club, with an authorisation granted under Article 16 of UK Regulation(EU) 2019/947.*

This approach is similar to that taken by the Federal Aviation Authority (FAA) in the USA. In practice, the detailed definition of Model Aircraft and criteria for designated flying zones would need to be established in parallel to this consultation, in collaboration with Model Aircraft stakeholders. These would be developed to ensure that flights taking place without Remote ID are limited to locations and aircraft that pose a sufficiently low security risk.

Where these conditions are not met, Model Aircraft flights would be expected to meet the same regulatory requirements as legacy UAS – i.e. to have active Remote ID, delivered via a Remote ID add-on module (unless the aircraft is less than 250g without a camera).

Under these proposals, Model Aircraft that fly at low-risk club or association sites and meet the definition of an exempt Model Aircraft would not be impacted by Remote ID. We expect for this approach to be implemented from 1st January 2028 onwards, aligning to our proposals for legacy UAS.

- 5.9. *The CAA has developed these proposals with significant input from the Department for Transport, Home Office and the Police. We will continue to work with our government stakeholders to progress these proposals.*

Question 20: Do you agree or disagree with our proposed technical approach to implementing Remote ID? Please explain your answer, and consider our proposed approach of Hybrid Remote ID and on-device enforcement.

Disagree.

Remote ID would require huge investment in infrastructure and systems in the UK. This cost would no doubt be passed on to UAS Operators in one way or another (perhaps through the registration fee).

It would also require significant investment from drone manufacturers. And finally it would involve very significant, and disproportionate, cost to operators of legacy drones and potentially model aircraft flyers too.

The fact is that those intent on using a drone for nefarious purposes will not activate remote ID, and they certainly will not retrofit a remote ID module to a legacy drone. It is almost inevitable that any remote ID functionality will be defeated/disabled by 'hackers' (those who like to 'tinker' with how electronic products work).

Spoofing could also be employed by those intent on using their drone without being traced. Or, they could simply build a drone from components.

Furthermore, the Police already successfully track and trace criminals who use drones using existing detection systems. Likewise, the CAA already has access to this data which allows it to *understand the sector*, etc.

The proposed network and direct approach is overkill and puts an even greater burden on UAS operators. For example, retrofit Remote ID modules, such as those available in the US, work for direct Remote ID, but not network. Adding a mobile data connection system, and a direct radio system, to an existing UAS (for example a legacy radio controlled aeroplane, or helicopter, etc) is complex and disproportionate..

Question 21: Do you agree or disagree with our proposed policy approach to Remote ID? Please explain your answer, and consider our proposed approach to product and operational requirements, legislative enforcement and data privacy, access and security.

Disagree.

Remote ID would require huge investment in infrastructure and systems in the UK. This cost would no doubt be passed on to UAS Operators in one way or another (perhaps through the registration fee).

It would also require significant investment from drone manufacturers. And finally it would involve very significant, and disproportionate, cost to operators of legacy drones and potentially model aircraft flyers too.

The fact is that those intent on using a drone for nefarious purposes will not activate remote ID, and they certainly will not retrofit a remote ID module to a legacy drone. It is almost inevitable that any remote ID functionality will be defeated/disabled by 'hackers' (those who like to 'tinker' with how electronic products work).

Spoofing could also be employed by those intent on using their drone without being traced. Or, they could simply build a drone from components.

Furthermore, the Police already successfully track and trace criminals who use drones using existing detection systems. Likewise, the CAA already has access to this data which allows it to *understand the sector*, etc.

The proposed network and direct approach is overkill and puts an even greater burden on UAS operators. For example, retrofit Remote ID modules, such as those available in the US, work for direct Remote ID, but not network. Adding a mobile data connection system, and a direct radio system, to an existing UAS (for example a legacy radio controlled aeroplane, or helicopter, etc) is complex and disproportionate.

Question 22: Do you agree or disagree with our proposed scope of Remote ID requirements? Please explain your answer, and consider our proposed approach to UAS in scope, legacy UAS and Model Aircraft.

Disagree.

If there is an exemption for model aircraft it should apply to all association members/ people who fly under an Article 16 Operational Authorisation, wherever they are flying. Not just on limited sites.

Perhaps the exemption could include a stipulation that the flying location must not be within a certain distance of a prison or nuclear power station, etc.

If the CAA does require a list of approved locations (perhaps those locations confirmed to be not near prisons and nuclear sites, etc) then the associations should handle the approval of these suitable locations.

As per the EASA regulations, a model aircraft should be defined by how it is used. I.e. for the purposes of recreational model flying under the auspices of a model flying association, as against any specific attribute of the aircraft itself.

Geo-awareness and Geo-fencing

- 5.10. *The Call for Input described two technical mitigations to protect against UAS entering restricted airspace – geo-awareness and geo-fencing. Geo-awareness functionality would alert remote pilots when a UAS is approaching restricted airspace. Geo-fencing functionality provides a stronger mitigation, by preventing the UAS from entering restricted airspace at all. At present, geo-awareness functionality is part of retained product regulations in UK Regulation (EU) 2019/947, due to be implemented as part of class marking requirements from 1st January 2026, whereas geo-fencing is only optional. In addition, UAS remote pilots and operators are also subject to operational requirements to not fly in restricted airspace without the required permission.*
- 5.11. *Call for Input responses were supportive of using geo-awareness to protect against UAS flying in restricted airspace. Of those who provided a view, 51.7% of responses were positive, whereas 19.7% of responses were negative. However, there were some specific questions and concerns around how geo-awareness would be implemented in practice, including the UAS in scope, the approach for managing permissions to fly in restricted airspace, and how airspace data would be communicated.*
- 5.12. *Data available to the CAA provides conclusive evidence that there is a real and growing risk to safety and security from UAS operating in restricted airspace. In the 6 weeks following 23rd September 2023, the CAA received 558 notifications of a UAS operating within a Flight Restriction Zone or outside a Flight Restriction Zone but over 400ft. In 2023 so far, 9 UAS have been reported operating between 6,000 and 13,000 feet. Real-world incidents include UAS flying within restricted areas near to airports or particularly busy airspace, UAS capturing images of sensitive sites, and UAS used for trafficking illegal substances in to restricted sites, such as prisons.*
- 5.13. *Our view is that geo-awareness and geo-fencing will be crucial in enabling UAS to operate in UK airspace safely and securely, particularly as our airspace becomes busier with UAS and non-UAS. Without further mitigation, we would expect the number and severity of airspace incidents to increase, as UAS become more advanced and widely available. Whilst requirements placed on UAS remote pilots and operators to not fly in restricted airspace provide some mitigation, our view is that stronger technical mitigations will be required to prevent individuals from negligently or deliberately breaching regulations. We also note that several UAS manufacturers already have implemented geo-awareness and geo-fencing systems, demonstrating the maturity of this technology.*
- 5.14. **We are proposing to implement geo-awareness and geo-fencing for UAS.** *The key parts of our proposal are as follows:*

- (i) **UAS in scope:** We are proposing for C1-C3 UAS and C0 UAS with cameras to be in scope of product requirements, reflecting the safety and security impacts from these UAS entering restricted airspace. UAS used in the Specific category may be subject to similar or other adequate mitigations if required as part of the operational authorisation. We do not expect the requirements to apply to Model Aircraft (including C4 UAS), privately built UAS or C0 UAS without cameras, given the technical challenges of applying this requirement in practice.
- (ii) **Operational requirements:** We are also proposing to place a requirement on UAS operators and remote pilots in the Open category to have an active geofencing function during UAS operations of C1-C3 UAS and C0 UAS with cameras, in addition to existing regulatory requirements for geo-awareness to be used. This will provide an additional layer of assurance that UAS operators do not attempt to disable or override this capability during operations.
- (iii) **Legacy UAS:** We do not propose to apply this requirement to legacy UAS operations, given the challenges in applying this retrospectively. (iv) **Technical solution:** Our view is that existing technical standards for geoawareness and geo-fencing can provide an appropriate and harmonised solution for manufacturers to be compliant with these regulatory requirements. Appendix B provides a summary of the technical standards we propose to evaluate.
- (v) **Airspace data:** Current regulation requires operators and remote pilots to ensure geo-awareness data is updated in the UAS, in accordance with Geographical Zones made under Article 15 of UK Regulation (EU) 2019/947. This is supported by requirements for UAS to be able to load and update airspace data. To ensure that geo-awareness and geo-fencing systems are implemented accurately, UAS operators, pilots and manufacturers should be using appropriate sources of airspace data that meet required levels of accuracy, resolution, integrity, traceability, timeliness, completeness, and format. We are proposing to extend these requirements to include any airspace restriction applicable to UAS, and are considering whether additional regulatory requirements, AMC or GM are needed to ensure that appropriate data sources are used.
- (vi) **Scope of airspace restrictions:** To implement geo-awareness and geo-fencing, UAS will be required to receive and maintain airspace data. At present, data regarding permanent airspace restrictions is fully standardised and machine readable via the Aeronautical Information Service. Data regarding temporary airspace restrictions (e.g. NOTAMs and AICs) is not. We would expect geoawareness and geo-fencing functionality to also apply to temporary airspace restriction data. The CAA will continue to work with airspace data stakeholders to standardise how dynamic data is communicated to UAS. We will consider whether changes to flyer education and guidance is needed to ensure UAS operators and remote pilots account for temporary airspace restrictions appropriately.
- (vii) **Airspace access permissions:** Legitimate UAS operations within restricted

airspace will require a method to obtain permission. This requires a process for airspace owners to provide permission for UAS flights to take place in restricted airspace, and for this permission to enable geo-fencing functionality to be overridden temporarily or permanently. Whilst some UAS manufacturers have already implemented bespoke processes for managing permissions to restricted airspace, we expect that greater coordination and standardisation will be needed to execute these processes at scale. Furthermore, we expect that UAS in scope of this proposal should be required to have an airspace access permissions function. Subject to the outcome of this consultation, we will consider in more detail how this permissions function could work in practice further into the future.

(viii) **Enforcement:** To support the implementation of these proposals, relevant authorities would need the ability to enforce against non-compliance. We are continuing to consider how these requirements could be enforced effectively

Question 23: Do you agree or disagree with our proposal to implement geo-awareness for UAS? Please explain your answer.

Agree.

Geofencing has been a part of COTS (consumer-off-the-shelf) drones for many years and some pilots (incorrectly) rely on the geofencing/geo-awareness built into their drone to keep them from flying in unsuitable locations.

In some cases, this geofencing is incorrect. The 'no fly zones' on the drone/app, don't match the actual UK FRZs, etc. Therefore in some cases the drone will allow flight in an area that it shouldn't, and the operator may be unaware that they are contravening the rules.

The CAA should require that geofencing data be accurate - and provide suitable data to the manufacturers to facilitate this.

Furthermore, there must be a provision to allow geofencing to be overridden where the remote pilot has permission to operate in that area. Permission to fly in an FRZ should not be unreasonably withheld by the ATSU (air traffic services unit) in question. Perhaps ATC could provide a code to the permitted drone pilot, which would then disable geofencing for that drone for that FRZ for the permitted period. (DJI does have an override system for their drones, perhaps this could be finessed as above).

It is very important that model aircraft, including home built drones, should be excluded from any geofencing requirement. Such aircraft don't usually have GPS onboard and therefore could not meet a geo-awareness requirement without a very significant burden being added.

Question 24: Do you agree or disagree with our proposal to implement geo-fencing for UAS? Please explain your answer.

Agree.

Geofencing has been a part of COTS (consumer-off-the-shelf) drones for many years and some pilots (incorrectly) rely on the geofencing/geo-awareness built into their drone to keep them from flying in unsuitable locations.

In some cases, this geofencing is incorrect. The 'no fly zones' on the drone/app, don't match the actual UK FRZs, etc. Therefore in some cases the drone will allow flight in an area that it shouldn't, and the operator may be unaware that they are contravening the rules.

The CAA should require that geofencing data be accurate - and provide suitable data to the manufacturers to facilitate this.

Furthermore, there must be a provision to allow geofencing to be overridden where the remote pilot has permission to operate in that area. Permission to fly in an FRZ should not be unreasonably withheld by the ATSU (air traffic services unit) in question. Perhaps ATC could provide a code to the permitted drone pilot, which would then disable geofencing for that drone for that FRZ for the permitted period. (DJI does have an override system for their drones, perhaps this could be finessed as above).

It is very important that model aircraft, including home built drones, should be excluded from any geofencing requirement. Such aircraft don't usually have GPS onboard and therefore could not meet a geo-awareness requirement without a very significant burden being added.

Flashing Light

5.15. We have identified safety and security concerns from UAS flying at night without a light. Whilst there are requirements on C1-C3 UAS to be manufactured with a flashing light, there is no requirement on remote pilots to have this active during flights at night. The requirement to use the flashing light at night was not retained from EU law, due to the timing of EU Exit, and the date that requirement was due to become applicable.

5.16. To improve the conspicuity of Open category UAS at night, **we are proposing to require UAS remote pilots to have an active flashing light on their UAS for operations taking place** at night. This would apply to all UAS, irrespective of weight or class.

5.17. In practice, UAS operations using C1-C3 UAS would be able to meet this requirement through using functionality in-built within these UAS. UAS manufactured without flashing lights would be able to meet this requirement through using an add-on flashing light, but would otherwise not be permitted to fly in the dark.

Question 25: Do you agree or disagree with our proposal to require remote pilots to have an active flashing light on their UAS for operations at night? Please explain your answer.

Agree.

Night time lighting makes sense for conspicuity. Most consumer drones include LED lighting as standard and very bright standalone LED lights are readily available.

Transition Period and Legacy UAS

- 6.1. *Article 22 of UK Regulation (EU) 2019/947 states that, until 1st January 2026:*
- (i) *Legacy UAS weighing less than 500g can be operated in the A1 sub-category (over people) if the pilot has an A2 Certificate of Competency.*
 - (ii) *Legacy UAS weighing less than 2kg can be operated a minimum horizontal distance of 50m from people, if the pilot has an A2 Certificate of Competency.*
 - (iii) *Legacy UAS weighing less than 25kg can be operated in the A3 sub-category (far from people), if the pilot has a Flyer ID.*
- 6.2. *In addition, Article 20 sets out that UAS weighing less than 250g can be used in the A1 sub-category indefinitely, and UAS weighing less than 25kg can be used in A3 sub-category indefinitely. These requirements reflect regulatory changes made by the government, following our consultation and recommendation provided in 2022.*
- 6.3. *In the Call for Input, we asked whether the CAA should change the transitional arrangements for legacy UAS (Question 8). Of those who provided a view, 74.8% of responses were positive, citing the impacts of the current transitional arrangements, such as the costs to UAS operators of needing to replace legacy UAS with new models.*
- 6.4. *Our view is also that the current transition period set out in Article 22, due to end on 1st January 2026, could create some challenging impacts for the UAS sector. For example, these arrangements could result in some UAS operators needing to replace their aircraft in a short timeframe. It could also have undesirable environmental impacts from many UAS being disposed of earlier than necessary and/or incorrectly, undermining the sustainability of the UAS sector.*
- 6.5. *However, we also consider that an indefinite transition period for all legacy UAS may delay the safety and security benefits of class-marked UAS. We expect this to become more important over time, as the UAS sector grows.*
- 6.6. ***We are proposing to extend the transitional arrangements set out in Article 22 of UK Regulation (EU) 2019/947 to 2 years after the introduction of classmarking requirements on UAS manufacturers – 1st January 2028. This aims to mitigate some of the impacts on the UAS sector of the current arrangements, whilst also ensuring we transition to using safe and secure UAS in a***

timely manner. It aims to reduce the regulatory burden for UAS users, where possible.

6.7. As is described in Chapter 5, we are also proposing to continue to allow the use of legacy UAS under the arrangements of Article 20 (as described in paragraph 6.2), provided that the UAS is flown with active Remote ID from 1st January 2028 onwards (excluding UAS <250g without cameras). These proposals are summarised in the below table.

Legacy UAS: Maximum Take-Off Mass	Up to 31 st December 2027			1 st January 2028 onwards		
	A1 (Over)	A2 (Near)	A3 (Far)	A1 (Over)	A2 (Near)	A3 (Far)
249g or less	✓	✓ ^b	✓	✓ ^c	✗	✓ ^c
250g – 499g	✓ ^a	✓ ^b	✓	✗	✗	✓ ^d
500g – 1.99kg	✗	✓ ^b	✓	✗	✗	✓ ^d
2kg – 24.99kg	✗	✗	✓	✗	✗	✓ ^d

a = Remote pilot requires A2 Certificate of Competency

b = Remote pilot requires A2 Certificate of Competency; UAS must be minimum horizontal distance of 50m from people

c = UAS with cameras must be operated with active Remote ID

d = UAS must be operated with active Remote ID

6.8. We propose to maintain current regulations that, in effect, prevent legacy UAS operations in the A2 sub-category after the transition period. Our view is that this approach remains appropriate, given the increased risks of UAS operations in the A2 sub-category. We also consider that the proposed 2-year transition period provides a reasonable amount of time for UAS operators to replace their legacy UAS.

Question 26: Are there other opportunities to promote safe and secure airspace that we should be considering? If yes, please describe them in full.

CAA should use the mailing list of all registered UAS operators and flyers to communicate safety information and invite responses to consultations, etc.

Question 27: Do you agree or disagree with our proposal to extend the transition period for UAS operators to adopt class marked UAS from 1st January 2026 to 1st January 2028? Please explain your answer.

UAS purchased before the 2026 deadline should be allowed to continue with the same operational limitations indefinitely. I.e. to the end of their lives.

This is inline with road vehicle regulations. E.g. vehicles that were purchased before the legal requirement for seat belts came into force, do not require seat belts to drive on the public road today. There are numerous other examples, such as front number plates on motorcycles, black and white number plates, etc.

Question 28: How many years should the CAA extend the transition period for operation of non-class marked UAS by? Please explain your answer.

Indefinitely - to the end of the natural life of those non-class marked drones.

Question 29: Do you agree or disagree with our proposal to maintain regulation that, in effect, prevents the use of legacy UAS in the A2 sub-category after the transition period has completed? Please explain your answer.

Disagree.

UAS purchased before the 2026 deadline should be allowed to continue with the same operational limitations indefinitely. I.e. to the end of their lives.

This is inline with road vehicle regulations. E.g. vehicles that were purchased before the legal requirement for seat belts came into force, do not require seat belts to drive on the public road today. There are numerous other examples, such as front number plates on motorcycles, black and white number plates, etc.

Conformity Assessment

- 6.9. *The current regulations for class-marked UAS propose three approaches to conformity assessment: internal production control, type examination, and conformity based on full quality assurance. The first type (internal production control) relies on self-assessment and declaration, and is currently allowed only for C0 and C4 UAS.*
- 6.10. *The current approach to conformity assessment will provide high degrees of confidence that products meet regulatory requirements. However, we also recognise that requiring C1-C3 UAS to undertake third-party type examination and conformity based on full quality assessment before 1st January 2026 may be challenging in practice. This may result in disruption to manufacturers placing products on the market, and to UAS operators obtaining class-marked UAS.*

- 6.11. *We are considering options to introduce more flexibility into conformity assessment requirements for class-marked UAS. The options we are considering include:*
- (i) *Allowing C1 to C3 UAS to meet conformity assessment requirements using internal production control, for a temporary period – subject to the UAS undergoing type examination or full quality assurance in the future.*
 - (ii) *Allowing C1 to C3 UAS to meet conformity assessment requirements using internal production control, for requirements that have undergone type examination by conformity assessment bodies under other jurisdictions.*
- 6.12. *We welcome feedback from UAS manufacturers and Conformity Assessment Bodies on how we could improve the implementation of conformity assessment for classmarked UAS.*

Question 30: What changes should we make to the approach to conformity assessment of class-marked UAS? Please explain your answer.

C1 to C3 UAS should be allowed to meet conformity assessment requirements using internal production control, in a similar way to how CE and UKCA is done. I.e. the manufacturer confirms that their product complies with all of the relevant requirements.

It can then be sold on the market.

If there is some complaint that a particular product isn't actually compliant, the MSA can then investigate and take the appropriate action.

Model Aircraft

- 6.13. *The Call for Input asked what changes we could make to the regulatory framework for Model Aircraft, to support the Model Aircraft community. Potential changes include creating a separate operational sub-category for Model Aircraft and creating a clearer definition for Model Aircraft to differentiate between other UAS.*
- 6.14. *Of those Model Aircraft flyers who provided a response, 50.6% respondents were neutral, 30.9% were in favour of the proposal and 17.5% were against it. Whilst some Model Aircraft flyers requested significant changes to the regulatory framework (such as removing Model Aircraft from the regulations altogether), others cautioned against the cost, complexity and impact of making substantial changes.*

- 6.15. *Our view is that, on balance, the costs of change to government, the CAA and the Model Aircraft community outweigh the potential benefits from creating an entirely new regulatory framework. As such, we intend to maintain the foundations of the current regulatory framework and continue to collaborate with the Model Aircraft community to improve how regulations are applied.*
- 6.16. *As is described in the Remote ID section, we have worked closely with our security stakeholders to consider how to balance security objectives without over-burdening the Model Aircraft community. Our proposed approach to Remote ID exemptions is set out in full in Chapter 5. This should ensure that low-risk Model Aircraft flights can continue, without being impacted by Remote ID requirements. If this proposal is taken forward, we expect to work closely with the Model Aircraft community to define an appropriate definition for exempt Model Aircraft and approach to locational exemptions.*

Question 31: Do you agree or disagree with our proposal to maintain the existing regulatory approach for Model Aircraft?
Please explain your answer

Agree.

The current regulatory approach is appropriate.

Question 32: Are there other opportunities to support the UAS sector that we should be considering? If yes, please describe them in full.

As above, better communication with operators and flyers, using the mailing list of registered operators and flyers.

Next Steps and How To Respond

- 7.1 *The consultation process is an integral part of our policy development approach, allowing us to understand the impact of proposed policy changes on our stakeholders. Responses to this consultation will be essential for the CAA to form policy that meets our objectives and can be adopted by stakeholders effectively. We welcome responses to the consultation from any stakeholder impacted by these proposals, including recreational and commercial UAS pilots/operators, UAS manufacturers, UAS service providers, amongst others.*
- 7.2. *The consultation is open until 23:59 10th January 2024. Responses can be provided via Citizen Space.*

7.3. *Once the consultation has closed and we have considered your responses, we will publish our consultation reply document. If legislative change is required to deliver any of the proposals which we consider should be implemented, we will submit our formal opinion to the Department for Transport, who will in turn consider whether to implement our proposed changes in a Statutory Instrument.*

Question A1: Do you agree or disagree with our qualitative categories for costs and benefits across the user and stakeholder groups, set out in Appendix A? Please elaborate if there are other costs and/or benefits we haven't identified.

There is no actual benefit to UAS operators - compared with the current regulations.

Evidently the cost to implement remote ID, etc is not even known by the CAA. Whatever it is, it is likely to be passed on to the UAS operator to some degree, in one form or another.

As an organisation, FPV UK will incur costs updating and creating guidance and training materials and training mentors and examiners, etc.

Question A2: What are your current costs across these categories, particularly training/certification, product/service development, and other compliance? Please provide an estimate of costs (£) where possible or qualitative explanations.

Training is provided by RAEs at around £50 for our members to do the A2 CofC course.

Our own Certificate of Competency: Practical course is free of charge - provided by our national network of mentors and examiners.

Registration costs £10.33 per annum (rising to £11.19 in April 2024).

Question A3: What additional up front or ongoing costs do you expect to incur, in order to comply with these proposals? Please provide an estimate of costs (£) where possible or qualitative explanations.

It is possible that some consumer off the shelf UAS can be retrofitted with remote ID capabilities by firmware update. Direct remote ID could be transmitted using the onboard software defined radio, and network ID could be transmitted by connecting through the pilot's mobile device (which is already connected as part of the system).

This is not yet clear, since the specific requirements for remote ID remain vague, and the manufacturer's capabilities, and willingness, remain unclear.

However, in older/less sophisticated drone models, and in the case of other types of UAS - such as radio controlled aeroplanes and helicopters - retrofitting these elements will be complex and costly. Potentially this could cost in excess of £150 per UAS - and for legacy systems which do not have a 'smart' controller, connected to an existing mobile device, or where the operator does not have an existing data plan, the cost for a cellular data plan could add £10 per month in fees.

There is also the existing (annually increasing) registration fee of £10.33 (rising to £11.19 in April 2024).

An estimate would be £150 upfront per UAS (and members usually have several UAS), plus a maximum of £131.19 annually.

This will unfairly burden those members who operate the more simple/traditional UAS - and particularly those who don't already have a smartphone.