Department for Transport consultation on

TAKING FLIGHT: THE FUTURE OF DRONES IN THE UK

Written submission by the Security Institute

15 September 2018

Introduction to the Security Institute

1. The Security Institute is the UK's largest professional membership body for security professionals. Established in 1999 and with a growing membership of over 2,700, our mission is to inspire, inform and influence professional excellence for the benefit of our members, the security community and wider society.

2. The authors of this submission are Jeremy Fitton, John Wood, Andy Blackwell, Chris Barratt, Paige Kenningdale and Alison Wakefield.

Summary

3. The consultation focuses on the localised safety threat posed by drone flying: errors and offences in the piloting of drones, and in countermeasures to such flying. In our experience, government policy and law-making could be more targeted to the type of flying. When answering the questions, we often found that our answers would be different for different types of flight.

4. We note that the questions do not explicitly consider the threats presented by drones in the areas of civil aviation safety, privacy, terrorism (aviation/civil/critical national infrastructure), smuggling (cross-border/prisons), or other crime. A key question that needs to be answered concerns which of those threats this additional legislation is intended to address. In our view, the existing legislation does not adequately address those threats, at least in the areas of privacy and aviation terrorism.

5. With respect to regulation, the New Zealand approach using Airshare seems more in keeping with the existing Civil Aviation regulatory approach. We believe it would be a more effective solution than the proposed FINS and its infrastructure, and we would have liked to have seen this option included in the impact assessment. In addition, we note that the drone countermeasures focus on electronic effectors. There are also physical drone countermeasures on the market and, if the electronic countermeasures are considered to need legislation, we would expect the physical countermeasures to be addressed too.

Submission

6. The Security Institute welcomes the consultation and the opportunity to submit a response. The consultation focuses on the localised safety threat posed by drone flying: errors and offences in the piloting of drones, and in countermeasures to such flying. We note that the questions do not explicitly consider the threats presented by drones. In this submission we address the consultation questions, with many of our responses varying according to different types of drone flying and different stakeholder perspectives, and our responses to the survey questions are provided in the Appendix. We provide some additional comments on the government's approach to the threats presented by drones, and an alternative regulatory framework that the government might consider, which comprise the basis of our answer to the final, open question in the questionnaire.

Considerations by type of flight

7. In our experience, government policy and law-making could be more targeted to the type of flying. When answering the questions, we often found that our answers would be different for different types of flight: recreational vs commercial, and flying line-of-sight under 100 metre altitude vs flying beyond visual line of sight (BVLOS) or over 100 metre altitude.

8. To this end, we created the table below to summarise our responses as they relate to the type of flight. At a high level, we separated line-of-sight flying from beyond-line-of-sight flying; VLOS-v-BVLOS. We believe that the safety delta between the two modes of flight is sufficiently large as to create separate yet symbiotic policies for both modes. For example, in our experience, the vast majority of current (and future) civilian drone flying – both for leisure and commercially – is when the pilot is within line-of-sight of their drone and below 100 metres of altitude. In this case, the pilot can engage in low-risk flying by visually avoiding collisions and not flying in airspace used by manned aircraft – hence simpler rules for operating and a light-touch from government. Conversely, flying risk is considerably higher when flying BVLOS and/or at higher altitudes – hence more relevance to insurance, a FINS mechanism and (police) enforcement of safety protocols.

9. Thus, the answers to the questions are dependent upon the level of risk of the flying. The table summarises the main topics of the document and our general responses.

Flying type	**Flying line-of-sight and under 100 metre altitude**		**Flying BVLOS or over 100 metre altitude**
Operational intent	**Recreational**	**Commercial**	**Any**
Age of Operator	Agree	Agree	Agree
Aerodrome proximity	Regulation should be risk based		
Mandate Apps like FINS	No	No	Yes
Police powers	No change (with some reservations)		
Fines for non-compliance (FPN)	To enforce existing ANO		
Counter Drone – Detect/Effect	Maintenance of civil aviation safety and security should be identified explicitly as one of the purposes of drone detection technology		
Growth of Industry	Agree		

Threats presented by drones

10. The questionnaire does not explicitly address the drone threat in the areas of civil aviation safety, privacy, terrorism (aviation/civil/critical national infrastructure), smuggling (cross-border/prisons), or other crime. A key question that needs to be answered concerns which of those threats this additional legislation is intended to address. In our view, the existing legislation does not adequately address those threats, at least in the areas of privacy and aviation terrorism. In some of our answers to the questionnaire we have suggested explicit reference be made in the legislation to aviation safety or security measures, and to empowering individuals to protect themselves from privacy invasion.

11. Constrained as it is by the structure of this consultation, our consideration of aviation security in our answers has been limited. We believe that the government should take a more comprehensive approach to the threats posed by drones in the areas we listed above. Taking one of these as an example, in civil aviation the government and the Civil Aviation Authority (CAA) have done much work on risk-based management by operators and oversight by the regulator. They have strongly promoted PBR (performance based regulation) in safety and the government also promised OFRB (outcome-focused risk-based regulation) in security (for which the CAA uses the same term as safety – PBR). Both of these are yielding considerable benefits to the commercial aviation industry and the regulator alike, in terms of assurance and efficiency. None of this figures in the existing or proposed drone legislation, suggesting a possible lack of co-ordination across different policy areas.

12. It can be noted that the security sector tends to be reactive, learning from past events, mistakes or omissions, often losing precious time against developing technology and methodologies. This is true of drone capability and use, in part due to the fact that no significant attack has been executed on UK soil. However, global patterns have seen an increase in the use of small unmanned aircraft as an attack platform on a tactical (local) level as well as their use for hostile reconnaissance.

13. The regulatory environment provides limited scope in dealing with this problem for many reasons, not least because those with criminal intent do not seek training, registration or operational process. Parallels can be drawn with many different areas of security concern, such as legal versus illegally held firearms, with few crimes committed by those who follow home office governance.

14. Drones are available at no more than the cost of a smart-phone that can sense and avoid, fly autonomously, maintain flight for 28 minutes, gather TV quality imagery and reach extended ranges of 5km. All of this can be deployed from a small briefcase that would not look out of the ordinary to a security officer. Such a small drone is covert prior to flight and, due to the small size, remains so when airborne. The Air Navigation Order regulates drones but its efficacy depends on security officers being able to see the drones and having the wherewithal to deal with those not adhering to the regulations.

15. The progress made by the DfT and the CAA with SMS (Safety Management Systems) and PBR (performance based regulation) in safety and SeMS (Security Management Systems) and PBR in security shows that such challenges are best tackled proactively by the operators since they

incur and understand the risks, supported by the government and the regulator providing guidance and a framework within which to work. Yet none of this has been considered in existing drone legislation or in the legislation considered in this consultation.

Options for regulation

16. The New Zealand approach using Airshare[1] seems more in keeping with the existing Civil Aviation regulatory approach. We believe it would be a more effective solution than the proposed FINS and its infrastructure, and we would have liked to have seen this option included in the impact assessment. Specifically, it appears to us to offer the following benefits:

    - Simpler, cheaper quicker to implement;
    - Proven technology and methodology;
    - Much more cost-effective than an optional FINS;
    - Much more 'better regulation" oriented than a mandatory FINS; and
    - More in keeping with DfT's approach to aviation safety and security regulation which puts the onus on the operator.

17. Presumably New Zealand has other laws that operators/pilots must obey, but this gives them crowd-sourced information to fulfil their obligations. In the UK context as in New Zealand, they are required to abide by the law, and this is a tool to help them. FINS seems more oriented towards an auditing tool to provide prosecuting authorities with evidence.

18. Finally, we note that the drone countermeasures focus on electronic effectors. There are also physical drone countermeasures on the market and, if the electronic countermeasures are considered to need legislation, we would expect the physical countermeasures to be addressed too.

1 The Courtyard
Caldecote
Warwickshire
CV10 0AS
Tel: 02476 346 464
Email: info@security-institute.org
Web: www.security-institute.org

[1] International Airport Review, '10,000 drone pilots register to fly in New Zealand airspace via Airshare' (14 September 2018), date retrieved 14 September 2018: https://www.internationalairportreview.com/news/75468/drone-pilots-register-fly/.

Appendix

Department for Transport

Taking flight: the future of drones in the UK

1. Introduction

Thank you for taking the time to read the consultation document and to respond to the questions. Your views will help contribute to the design of future drones policy.

Confidentiality and data protection

The Department for Transport (DfT) is carrying out this consultation on drone legislation in the UK. The consultation is being carried out in the public interest to inform the development of policy. DfT is the data controller for your personal information.

As part of this consultation we're asking for your name and email address. This is in case we need to ask you follow-up questions about any of your responses. You do not have to give us this personal information. If you do provide it, you consent to DfT using it only for the purpose of asking follow-up questions.

This consultation document has been developed in collaboration with other government departments and partner agencies. Consultation responses may be shared with these other bodies, but will not include personal details on respondents. This will aid in the facilitation of future government policy development and legislation.

You can withdraw your consent to be contacted at any time by emailing dronesconsultation@dft.gov.uk.

DfT's privacy policy has more information about your rights in relation to your personal data, how to complain and how to contact the Data Protection Officer.

To receive this information by telephone or post contact us on 0300 330 3000 or write to Data Protection Officer, Department for Transport, Ashdown House, Sedlescombe Road North, St Leonards-on-Sea, TN37 7GA.

Your personal information will be kept securely on a secure IT system within DfT and destroyed within 12 months after the consultation has been completed.

Filling in the questionnaire:

All questions are singular choice unless stated as multiple choice.

Guidance about which questions to complete, based on your choices, is included.

Sending your completed return

You can either attach the form to an email, sending it dronesconsultation@dft.gov.uk or post a printed copy to:

The Drones Policy Team
Technology & International Aviation (TIA) Division
Aviation Directorate
Department for Transport
33 Horseferry Road
London
SW1P 4DR

2. Personal details

Your:

name? Dr Alison Wakefield FSyI

email? alison@security-institute.org

Are you responding: *

X	on behalf of an organisation? (Go to 6.Organisational details)
	as an individual? (Go to 3.Individual details)

3. Individual details

Are you currently a drone user?

Yes (Got to 4. Individual details: drone use)
No (Go to 5. Individual details)

4. Individual details: drone use

You are: (multiple choice option)

a leisure drone flyer?
a model aircraft flyer?
a General Aviation Pilot?
a commercial drone flyer?
other?

If you selected more than one option, which option is your primary option?

5. Individual details

How many drones do you think you will operate in:

the next 1 year?
2023?
2028?
the longer term?

(After answering individual details go to 7

6. Organisation details

What describes your organisation best?

	A business that uses drones
	A business considering using drones
	Drone manufacturer
	A drone vendor
	A test centre
	An insurance company
	An airline
	A research institution or university
	An airport
	An airport consultative committee
X	A membership or representative organisation
	A devolved government
	A local authority
	A statutory body
	Another type of organisation:

How many drones do you think your organisation will operate in:

the next 1 year?	0
2023?	0
2028?	0
the longer term?	0

Your:

organisation name?	Security Institute
organisation does?	UK professional association for security practitioners.
organisation interest in drones is?	Our main interests are the drone threat in the areas of civil aviation safety, privacy, terrorism, smuggling and other crimes, and the use of drone and counter drone technology in a security context.

7. Minimum age for an operator

An SUA (small drone) operator is the person who has the management of the small unmanned aircraft.

An SUA (small drone) remote pilot is an individual who operates the flight controls of the small unmanned aircraft by manual use of the controls, or when the small unmanned aircraft is flying automatically, monitors its course and is able to intervene and change its course by operating its flight controls.

The government is proposing that 18 is the minimum age requirement to be a SUA operator.

The government is not proposing to introduce a minimum age requirement to be a remote pilot of a SUA.

Do you see any advantages to the introduction of a minimum age for SUA (small drone) operators?

X Yes (Go to 8.Minimum age for an operator)
No (Go to 9.Minimum age for an operator)
Don't know (Go to 9.Minimum age for an operator)

8. Minimum age for an operator: advantages

What advantages?

Legally able to enter into contracts.

Regulation of flying BVLOS or over 100 metre altitude.

9. Minimum age for an operator

Do you see any disadvantages to the introduction of a minimum age for SUA (small drone) operators?

x Yes (Go to 10.Minimum age for an operator)
No (Go to 11.Minimum age for an operator)
Don't know (Go to 11.Minimum age for an operator)

10. Minimum age for an operator: disadvantages

What disadvantages?

This should only apply to commercial operators, not leisure operating.

It should be noted that, at 16 years, a person may fly a microlight aircraft that, arguably, could have greater consequences in the event of an accident or intentional misuse. Whilst it may be argued that the microlight can be flown only after tuition, training could be considered for small drone pilots if that was the government's view.

11. Minimum age for an operator

Do you agree with the government's proposal that a minimum age of 18 should be introduced for SUA (small drone) operators?

X Yes (Go to 13.Minimum age for an operator)
No (Go to 12.Minimum age for an operator)

12. Minimum age for an operator: reasons against

Why not?

13. Minimum age for an operator

Do you believe that the introduction of a minimum age of 18 for SUA (small drone) operators will have:

	a positive impact?
	a negative impact?
X	no impact?

14. Minimum age for an operator: effects

Why?

The impacts, positive and negative, to be assessed should include:

- The potential extent of the reduction in airspace conflicts and other offences;
- Effect on sales, and therefore retailers, manufacturers and prices;
- Curtailment of freedoms of would-be operators under the minimum age; and
- Benefits to other air-space users by reducing conflicts.

15. Aerodrome restriction

The review into the aerodrome restriction will consider questions such as:

- what the minimal acceptable vertical separation between a drone and an aircraft should be
- how the geography surrounding airports could impact on this restriction
- areas where drones are likely to be used (such as public parks) which are near aerodromes, and could be issued with a permanent exemption
- whether additional categories should be added to the list of protected aerodromes
- whether the restriction has had any impact on the number of drone sightings and Airprox reports near aerodromes
- the number of permission requests generated, and what percentage were accepted or rejected
- whether a different kind of restriction should be considered - such as radius circles near the runway thresholds

What other areas do you feel the review should cover?

Prevention of incursion into the aerodrome restricted area and the sensitivity of any adjacent areas (freight operators, fuel depots, carparks, etc.).

"Restriction" here means drone restriction not the "security restricted area" definition used in aviation security. The government should use other terminology.

16. Aerodrome restriction

Do you believe that the 1km restriction zone around a protected aerodrome is sufficient?

Yes (Go to 19. Aerodrome restriction: shape agreement)
X No (Go to 17. Aerodrome restriction: shape agreement)
Don't know (Go to 19. Aerodrome restriction: shape agreement)

17. Aerodrome restriction: shape agreement

Do you feel that a restriction zone of a different shape would be more appropriate?

x Yes (Go to 18. Aerodrome restriction: alternative shaped)
No (Go to 19. Model aircraft flying associations after "If no, why not?" comment box)
Don't know (Go to 19. Model aircraft flying associations)

If no, why not?

See response to next question

18. Aerodrome restriction: alternative shaped

State the shape, its dimensions and why?

Shape should be determined by geography and local risks. 1km could perhaps be the default restriction, but there are several issues with that:

- A blanket regulation is not good practice – it should be risk-based as in aviation safety and aviation security.
- Clarity is needed on the meaning of "1km round a protected aerodrome". Round the restricted area, the perimeter, or the perimeter plus outlying operational areas?
- Depending on geographic considerations and local risks 1km might be unnecessarily restrictive, or be inadequate. For example it would be hard to have a blanket restriction to protect "operational areas" which is not a defined term, but in some aerodromes it may be desirable to provide protection for fuel depots, cargo/freight operations outside but adjacent to the aerodrome.
- In addition, the workable dimensions will depend on the aerodrome and the terminal manoeuvring area. Circuits for general aviation (GA) aerodromes are flown at distances greater than 1km from the aerodrome boundary. In inclement weather, the circuit height is reduced to maintain visual flight rules. If a collision occurs whilst a low level circuit is being flown, there may be insufficient time for recovery before impacting the ground.

19. Model aircraft flying associations

In its response to the previous drone policy consultation, the government made a commitment to work with model aircraft flying associations to examine ways in which it may be possible to exempt members of model aircraft flying associations with adequate safety cultures and practices from certain elements of registration and other educational requirements, or where their club could be permitted to undertake regulatory requirements on their behalf.

Do you have any other proposals for solutions to minimise the impacts on safe model aircraft flying that we could consider?

No

20. Mandating and/or regulating a Flight Information and Notification System(s) (FINS)

The government is considering whether to legislate that for certain drone activity, certain users will be required to use an approved Flight Information and Notification System (FINS) to:

- view local airspace information
- check it is permitted to use the surrounding airspace
- create a notification that a drone is going to be flown at a particular location at a given time

It is proposed the FINS(s) could be digital, interactive and real time and a means of two-way communication between the user, other users around them, and relevant government authorities. We envisage the delivery mechanism could take the form of an electronic application (an 'app'), and may be used on a phone, tablet or web browser for example, but could equally be delivered via other equipment. Any solution would be built on open standards, to avoid lock in to a specific vendor and to encourage continued innovation for drone pilots and the sector.

The aim of this proposed policy is to increase drone user accountability, to ensure a flight can be made safely, without compromising the security or privacy of others. The real-time data and records made by a FINS could also be useful for enforcement.

Do current drone information apps provide enough support to ensure the safe and appropriate use of drones?

Yes
No
x Don't know

Why?

From the aviation safety perspective, “for certain activity, certain users” is too unspecific for us to be able to comment.

Even for a small number of users and locations, the suggestion of real-time communication with government authorities seems impracticable. Is it proposed to establish a drone “Air Traffic Control” authority managing airspace?

Current air traffic management (ATM) service providers are equipped, trained and resourced for real-time interaction with large, radio and transponder-equipped aircraft and well-trained aircrew, and usually in a different airspace.

They are not well positioned to provide drone ATM but if a new authority is created what co-ordination between them will be necessary? Will the additional communication load for aircraft ATM and aircrews be sustainable?

If the airspace for which a FINS would be mandatory is selective, who will determine which locations? For safety that may be straightforward, but for privacy it is difficult to envisage anything but ubiquitous coverage.

Do you think there is a need to mandate the use of a FINS(s) for certain types of drone activity?

- [ ] Yes
- [x] No
- [ ] Don't know

Why?

FINS is an aid for BVLOS but responsibility should ultimately lie with the operator/pilot.

Should the government explore options to achieve similar policy aims, but without mandating the use of a FINS(s)?

- [X] Yes
- [ ] No
- [ ] Don't know

Why?

OK to explore options, but maybe review the policy aims first.

Do you agree with the requirement to use a FINS as outlined by the government?

- [ ] Yes
- [X] No

Why?

See previous answer

21. The Flight Information and Notification System(s)

What do you think should be the maximum mass of a drone for which its user should have to use a FINS(s), if such a requirement were to be introduced?

- [ ] 20kg
- [ ] 50kg
- [ ] 100kg
- [ ] Over 100kg

Why?

We have left all options blank. From an aviation security and safety perspective, if there is to be a FINS requirement it should apply to all but the smallest drones (250g) in relevant locations. As technology and miniaturisation improves, even 20kg could carry a significant threat payload, and the drone itself is a threat in locations such as an aerodrome runway.

Mass implies a specific flight task (concept of operations). Therefore mass should not be a criteria for FINS and no minimum mass should be considered if FINS is implemented for BVLOS.

Should there be a requirement to file a pre-flight notification on the FINS(s) before flying a drone?

- [X] Yes
- [X] No

Why?

Yes for BVLOS if FINS is (a) developed and (b) not a voluntary information system. No for everything else.

What do you think should be the minimum allowed time, prior to take-off, for filing a pre-flight notification on the FINS(s)?

- [ ] File the notification at point of take-off
- [ ] File the notification no less than 5 minutes before take-off
- [ ] File the notification no less than 30 minutes before take-off
- [ ] File the notification no less than 1 hour before take-off
- [ ] File the notification no less than 3 hours before take-off
- [X] Other:

Why?

FINS is for de-conflicting the flying space to avoid collisions. Hence the pre-flight filing time relates to the concept of operations, which is yet to be defined.

What do you think should be the maximum allowed time, prior to take-off, for filing a pre-flight notification on the FINS(s)?

- [ ] File the notification at point of take-off

File the notification no more than 5 minutes before take-off
File the notification no more than 30 minutes before take-off
File the notification no more than 1 hour before take-off
File the notification no more than 3 hours before take-off
File the notification no more than 24 hours before take-off
File the notification no more than a week before take-off
x Other:

Why?

As per previous answer.

It is proposed that drone pilots should not have sole responsibility in relation to the use of a FINS. Do you agree?

Yes
x No

Why?

Pilot in command of aircraft during (BVLOS) flight should hold the responsibility.

Should there be a duty on FINS providers to display accurate information?

Yes
No
x Don't know

Why?

What information and displayed to whom? The data could be commercially sensitive, showing competitors the flight data and customer lists.

Should it be an offence for a FINS provider to display inaccurate data to drone users?

X Yes
No
Don't know

Why?

Yes, if FINS is mandatory, then the data needs to be accurate.

What do you believe should be approved for the public to use?

A single FINS?
X Multiple
FINSs?

Why?

Needs to be competitive.

In your opinion what should the FINS(s) cover?

X All of the UK
Select regional information, but together the multiple FINSs would provide full UK coverage?
Other:

Why?

Only for BVLOS.

22. Access to the Flight Information and Notification System(s)

Besides poor signal, no battery on the electronic device, maintenance or crashing do you think there are other scenarios which could restrict access to the FINS(s)?

X Yes (Go to 23. Access to the Flight Information and Notification System(s))
No (Go to 24. Access to the Flight Information and Notification System(s))
Don't know (Go to 24. Access to the Flight Information and Notification System(s))

23. Access to the Flight Information and Notification System(s)

What scenarios?

In addition to poor signal, any inadequacies in FINS server capacity or communication bandwidth could result in slow system response to the point that the system is unusable for real-time flight communication.

24. Access to the Flight Information and Notification System(s)

If real time access to the FINS(s) cannot be gained do you believe the drone flight should be allowed?

x Yes (Go to 25. Access to the Flight Information and Notification System(s))
No (Go to 26. Managing system providers for the Flight Information and Notification System(s))

25. Access to the Flight Information and Notification System(s)

Do you think there should be an exception from using real time data on the FINS(s) if access is restricted by: (Multiple choice)

poor signal?

no battery on device?
the FINS crashing?
the FINS being offline for maintenance?
x other?

Why?

If FINS is to be made mandatory, in the first rollout, FINS should not be used to ‘authorise’ or allow/deny a flight.

Conceptually, FINS is an option to notify one BVLOS flight of another BVLOS flight.

Flight responsibility lies with the operator/pilot.

If real time access to the FINS cannot be gained, how should this be managed? (Multiple choice)

Allow drone flight in certain scenarios
Allow drone flight using offline maps and data from FINS(s)
Allow drone flight in designated geographically zoned low risk areas, but not in higher risk areas
X Other:

Allow all flights for non-BVLOS that comply with the ANO (Air Navigation Order). A FINS-type mechanism should be required for BVLOS.

For manned aircraft, flight plans can be submitted by telephone or radio to flight information service units. Whilst there is a cost that would need to be addressed somewhere. Could a similar facility be available in the absence of real time FINS access if it is mandated?

26. Managing system providers for the Flight Information and Notification System(s)

Which organisation do you believe is best suited to manage and regulate the FINS(s)?

Civil Aviation Authority
NATS (the UK air navigation service provider)
Department for Transport
X Other:

Different organisations should manage or regulate different aspects of the FINS.

Why?

The CAA mandate is responsible for regulation of aviation safety and security in accordance with government policy and regulations set by the DfT. Similarly for drones, we envisage DfT would create/manage the policy with advice from the CAA, and the CAA would regulate compliance with the rules. Aviation security equipment certification is a DfT responsibility, and we envisage the FINS would be specified and certified by the DfT.

NATS publishes the UK Aeronautical Information Publication (AIP) and Notices to Airmen (NOTAMs) and is responsible for deconfliction. The information will likely need to be shared with operators of other aircraft if airspace is shared and they plan on the UK AIP and NOTAMS.

In line with government strategy should anonymised drone data from the FINS(s) be shared with the industry to drive technological development?

x Yes
No
Don't know

Why?

For the purposes of carrying out their function, to which organisation or organisations should a FINS provider have to provide data if requested? (Multiple choice)

Department for Transport
Police
Intelligence and Security Services
Border Force
National Crime Agency
HM Prisons and Probation Service
x None of the above
Other:

Why?

For anonymised data, all of the above can have access.

For non-anonymised data, we believe there are already legal mechanisms in place for these organisations to request data from other organisations.

The DfT and CAA would require data about the FINS operational performance, the DfT for certification, the CAA for operational monitoring.

For regulating operators, the CAA might require flight data.

There would be a duty on any FINS(s) provider(s) to provide information to a list of organisations specified in legislation. The specified organisation(s) may only request information in order for them to carry out their function. Potential specified organisations may include, but are not limited to:

- the Civil Aviation Authority
- the Department for Transport
- UK police
- Intelligence and Security Services

Do you agree it should be an offence for a FINS system provider to withhold information from a specified organisation if a valid request for data is made?

Yes
No
X Don't know

Why?

If DfT and CAA are to be given new regulatory responsibilities they will need the data indicated in the preceding answer, and this may require new powers to deal with FINS providers withholding such information.

Do you believe certain organisations should have some level of instant, or near instant, access to all data on the FINS(s)?

Yes
X No
Don't know

Why?

Current data protection laws are applicable.

27. Managing system providers for the Flight Information and Notification System(s)

Which organisation do you believe should have some level of instant, or near instant, access to all data on the FINS(s)? (Multiple choice)

Police
Intelligence and Security Services
Border Force
National Crime Agency
HM Prisons and Probation Service
Other:

Why?

For flying compliant with ANO, there is no need for FINS.

For BVLOS flights, current data protection laws are applicable.

In general we would urge caution on giving such powers without really understanding why they are needed and how they would improve safety or security. It runs counter to previous government policy on better regulation and there should be an evidenced justification for it.
If the mandatory use of FINS is considered as a safety measure it should not be seen as an enforcement tool. For it to be so, may lead to mistrust of the system and avoidance thereby defeating the object.

Do you believe there should be a charge to the drone user in order to use a FINS?

Yes
x No

Why?

Cost will reduce compliance. And if not mandatory, will disincentivise adoption.

28. Future development for the Flight Information and Notification System(s)

If a FINS provider decided to charge for using the system, should the government maintain the ability to control the maximum cost that could be charged?

- [ ] Yes
- [X] No
- [ ] Don't know

Why?

Pricing should be driven competitively.

Do you think there is a need to have a Special Administration Regime to manage the risk of insolvency for FINS providers?

- [ ] Yes
- [X] No
- [ ] Don't know

Why?

FINS should either be a government owned mechanism or FINS services should operate in a free-market with the usual company-house safeguards (however, the question can be raised that if the argument is that it is mandated and necessary for safety, if the service provider went bust, do we ground all flights until a new provider is found?). At the time of writing, any FINS service is not Critical National Infrastructure.

Are you a technology provider or company considering being involved in the development of a FINS? *

- [ ] Yes (Go to 29. Future development for the Flight Information and Notification System(s))
- [x] No (Go to 32. Model aircraft flying associations and the Flight Information and Notification System(s))

29. Future development for the Flight Information and Notification System(s)

If an approach is chosen that uses multiple FINSs, in your opinion would it be better to have:

- [ ] all FINSs transfer information to a single back end system?
- [ ] multiple FINSs transferring information between each other directly?

Why?

How would you consider funding a FINS? (Multiple choice)

- [ ] Charge the drone user
- [ ] Charge the industry
- [ ] Use adverts
- [ ] Have additional add-ons that can be purchased
- [ ] Other:

Why?

Would you anticipate a yearly subscription fee for users of the FINS(s)?

- [ ] Yes (Go to 30. Yearly cost)
- [ ] No (Go to 31. Future development for the Flight Information and Notification System(s))
- [ ] Don't know (31. Future development for the Flight Information and Notification System(s))

30. Yearly cost

How much?

31. Future development for the Flight Information and Notification System(s)

Would you consider bidding for the work to provide a FINS?

- [ ] Yes
- [ ] No

Why?

Would you be interested in attending a government focus group session with other potential sector technology providers?

- [ ] Yes

☐ No

32. Model aircraft flying associations and the Flight Information and Notification System(s)

Should the government work with model aircraft flying associations to consider ways in which the policy could be shaped to minimise the impact of any new legislation relating to FINS(s) for this group?

X Yes
No

Why?

Clubs are good ways to engage with users and often self-regulate. Gliding is managed and to a degree regulated by the British Gliding Association and microlights by the British Microlight association and similar can apply to the model fraternity.

33. Police powers and Fixed Penalty Notices

The government proposes new police powers of:

1. require the production of evidence in specified circumstances (such as where there is a reasonable suspicion of the commission of an offence) for:

- drone operator registration
- remote pilot acknowledgement of competency
- the use of a mandated and/or regulated Flight Information and Notification System by the remote pilot and/or drone operator, should the decision be taken to mandate their use
- other evidence relevant to legal flying requirements, including commercial permissions or exemptions from the CAA to adhere to any Air Navigation Order 2016 articles

2. obtain information such as the names and addresses of the registered drone operator and/or remote pilot believed to be in charge of the drone in specified circumstances (such as where there is a reasonable suspicion of the commission of an offence). If the identity of the drone operator is not provided, the name and address of who made the drone available for use by the remote pilot

3. require a remote pilot to land a drone in specified circumstances.

4. enter and/or search premises, with a warrant, where there is reasonable suspicion that there is a drone and/or its associated components which a constable reasonably suspects of having been involved in the commission of an offence

5. seize and retain a drone and/or its associated components which a constable reasonably believes of having been involved in the commission of an offence on entering and/or searching premises

6. access information stored electronically on a seized drone and/or its associated components which a constable reasonably suspects:

- is evidence in relation to an offence; or
- has been obtained in consequence of the commission of an offence; and
- that it is necessary to do so in order to prevent it being concealed, lost, tampered with or destroyed

7. require any information stored in electronic form on a drone to be produced in a form in which it can be taken away and in which it is visible and legible. The power can only be exercised if a constable has reasonable grounds for believing that:

- it is evidence in relation to an offence; or
- it has been obtained in consequence of the commission of an offence; and
- that it is necessary to do so in order to prevent it being concealed, lost, tampered with or destroyed

8. stop and search powers. The Home Office intends to consult on extending stop and search to cover the possession of corrosive substances in a public place without good reason. We are working with the Home Office to consider the possibility of including within that a similar power for the possession of drones in certain circumstances

Do you agree that the police require new powers in relation to the misuse of drones?

Yes (Go to 35. Police powers and Fixed Penalty Notices)
x No (Go to 34. Enforcement)
Don't know (Go to 35. Police powers and Fixed Penalty Notices)

Why?

Drones are simply a 'tool' used by non-compliant people. Police already have powers to manage non-compliant people. In the same way that police can seize assets if they are misused, drones are simply another asset.

We would urge caution about unintended consequences before extending powers in such a specific manner. It is unclear why current powers are inadequate and any extension should be subject to an assessment of the impact on the regulatory burden, public amenity and civil liberties.

#3 might be a necessary power but this is covered in Q36.

#4 – obtaining a warrant can take a considerable time and if such a power is necessary, the government should consider other options.

Are police now trained in the provisions of the Air Navigation Order?

34. Enforcement

58. As you are against greater police powers in relation to drones misuse you can either:

x continue answering questions about police powers? (Go to 35. Police powers and Fixed Penalty notices)
skip to the next section on counter drone technology? (Go to 41. Counter drone technology)

35. Police powers and Fixed Penalty Notices

Do you agree that the police should be able to require the production of evidence from drone users where:

	Yes	No	Don't know
there is a reasonable suspicion of an offence being perpetrated?	☐	x	☐
compliance with a legal requirement is being checked?	☐	X	☐

Why?

Burden of proof lies with the accuser.

The government proposes to allow drone users such as operators and/or remote pilots a 7 day grace period within which to produce evidence at a police station, that they have complied with the law. This will minimise the burden on magistrates courts as well as allow those who may not have the necessary documentation on them, to demonstrate their compliance. If a person does not produce this evidence, they will be liable to paying a Fixed Penalty Notice fine (more details on this in the next section). This process is similar to that of certain road traffic offences as contained in the Road Traffic Act 1988.

Do you agree with the proposal to grant a 7 day grace period to produce this evidence?

Yes
x No
Don't know

Why?

No was answered in the previous question.

36. Police powers and Fixed Penalty Notices

Do you agree that the police should be able to obtain information to check that the following have complied with the law?

	Yes	No	Don't know
A drone user			X
A drone operator			X
A remote pilot			X
The person who made the drone available for use			X

Why?

This question needs context.

Obviously the police need to gather evidence of an alleged offence after it has been committed. In this case the answers are obviously, Yes.

Should a police bot trawl through data proactively looking for infringements? Do we want this?

Do you agree that the police require powers to instruct a remote pilot to land a drone, if there is a reasonable suspicion of the commission of an offence?

X Yes
No
Don't know

Why?

However, the police are not drone pilots and cannot be expected to know about the 'safe' operation of drones. Therefore, if police over-ride the pilot in command they must assume the safety responsibility.

If the drone pilot considers it unsafe or impossible to obey the police instruction, it is not safe to argue or sanction the pilot while the drone is still airborne. In such a case the pilot should be required to obey 'as soon as safely possible' and explain the circumstances of the delay.

A more useful and practical power would be to require the pilot to return the drone to its base. From the aviation safety and security perspective this is far preferable to simply landing it at a distant location, which may incur safety or security risks.

Do you agree that the police require powers to instruct a remote pilot to land a drone, if a constable believes that:

	Yes	No	Don't know
it will protect persons from harm, harassment, alarm or distress?	☐	☐	x
it will protect persons occupying any premises from nuisance?	☐	☐	X
it is causing an annoyance relating to the occupation of a premise?	☐	☐	X
it will protect public order?	☐	☐	X
it will protect property from damage?	☐	☐	X
it would assist in exercising the functions of a police constable?	☐	☐	x

Why?

As per previous answer.

Do you agree the police should have the power, when a drone and/or its components are suspected of being involved in the commission of an offence, to enter and search premises with a warrant?

x Yes

No
Don't know

Why?

No new power is required. A misused drone is just like a misused knife or other tool of crime.

Do you agree the police should have the power, when a drone and/or its components are believed of being involved in the commission of an offense, to seize and retain the drone or its associated components?

Yes
No
x Don't know

Why?

The ability to seize assets should be in relation to the seriousness of the offense

Do you agree the police should have the power to access electronically stored information from the drone or its components if a constable reasonably suspects that it is:

1. evidence in relation to an offence or has been obtained in consequence of the commission of an offence and
2. necessary to do so in order to prevent it being concealed, lost, tampered with or destroyed?

x Yes
No
Don't know

Why?

Yes, but only like the power they already have to access data.

Do you agree the police should have the power to require any information stored on the drone or its associated components to be duplicated in a legible form that can be taken away if a constable believes that it is:

1. evidence in relation to an offence or it has been obtained through committing an offence and
2. necessary to prevent concealment, loss, tampering or destruction of the data?

x Yes
No
Don't know

Why?

Yes, but only like the power they already have to access data.

These proposed powers are only being considered for police constables. Do you believe any of the proposed powers should also be extended to: (Multiple choice)

- prison officers?
- police community support officers?
- civil enforcement officers?
- x other?

There are current legal powers for data collection. These are sufficient for other data sources (mobile phones, cars, CCTV, etc.) and we cannot see a need for special attention regarding drones.

Prison Officers while acting in their role already have all the powers of a constable (Prison Act 1952).

Are there other powers you feel the police should have in relation to drone misuse?

- Yes (Go to 37. Additional police powers)
- No (Go to 38. Police Powers and Fixed Penalty Notices)
- x Don't know (Go to 38. Police Powers and Fixed Penalty Notices)

37. Additional police powers

What powers and why?

38. Police powers and Fixed Penalty Notices

We propose to attach FPNs to the following offences of:

- not producing registration documentation, and/or proof of registration for drones between 250g and up to and including 20kg, at the request of a police constable
- not producing evidence that a flight plan was submitted before flying, or that an appropriate FINS is being used, should the decision be taken to mandate the use of FINS
- not producing evidence of any other relevant permissions required by legislation, for example if you are a commercial drone operator or when flying a drone 20kg and above
- not complying with a police officer when instructed to land a drone
- flying a drone without a valid acknowledgement of competency, or failure to provide evidence of meeting this competency requirement when requested
- other offences under the Air Navigation Order 2016, such as flying a small drone (small unmanned aircraft - SUA) with a camera or other data collection device within 50 metres of people, vehicles or buildings

Looking to the Road Traffic Offenders Act 1988 for comparable penalty levels, we would look to set the penalty range from £100 to £300. The exact penalty amount for the different offences will not be specified in the Bill.

Do you agree that Fixed Penalty Notices (FPN) are a suitable alternative to prosecution for certain drone-related offences?

Yes (Go to 40. Police powers and Fixed Penalty Notices)
X No (Go to 39. Against FPN's)
Don't know (Go to 40. Police powers and Fixed Penalty Notices)

39. Against FPNs

Why not?

A blanket imposition of FPNs for these offences would create disproportionate powers. There should be more consideration of the proportionality of the regulations as well as the FPNs.

As you are against using Fixed Penalty Notices you can either:

☐ continue answering Fixed Penalty Notice questions? (Go to 40. Police powers and Fixed Penalty Notices)
☐ skip to the counter drone technology section? (Go to 41. Counter drone technology)

40. Police powers and Fixed Penalty Notices

Do you agree that if a person is unable to produce the required evidence within 7 days of a police constable's request they should receive an FPN?

Yes
No
X Don't know

Why?
The question is too broad. What evidence does this relate to? If it is the information required by drone legislation, yes. This power should not be usable for fishing.

Do you agree that drone users not complying with a police officer's instruction to land a drone should receive a FPN?

Yes
x No
Don't know

Why?
Will the police officer be a certified drone pilot? If not, then how will the officer know if landing is safer than flying? See answer to Q36.

Do you agree that the FPN cost should be between £100 and £300 pounds?

Yes
No
x Don't know

The power to issue FPNs is only being considered for police constables. Do you believe the power to issue a FPN should also be given to: (Multiple choice)

Police community support officers?
Council enforcement officers?
x Other:

The ability to issue an FPN should be no different for drone offences than it is for FPN offences

41. Counter drone technology

The UK government assesses that the use of drone detection technology should be only where it is necessary and proportionate for one or more of the following operational purposes:

- in the interests of national security
- for the purpose of preventing or detecting crime
- for the purpose of safeguarding the economic well-being of the UK
- in the interests of public safety
- for the purpose of preventing death or injury to a person; or
- for the purpose of preventing damage to property
- for the purpose of maintaining prison security or good order and discipline

Do you think the operational purposes identified for the use of drone detection technology are appropriate?

Yes (Go to 43. Counter drone technology)
X No (Go to 42. Drone detection technology principles)
Don't know (Go to 43. Counter drone technology)

42. Drone detection technology principles

Why not?

The maintenance of civil aviation safety and security should be identified explicitly as one of the purposes of drone detection technology.

43. Counter drone technology

The government recognises that to ensure the appropriate use of drone detection technology, a number of safeguards must be put in place. It is considered that the following types of safeguards could be appropriate when any drone detection technology is operational:

- drone detection technology is limited to use by trained and/or licensed operators
- there is a clear purpose and scope for use of the technology, and operational policy specific to each site which is in line with appropriate legislation (for example, a defined code of practice)

- where applicable, a full risk assessment is conducted in line with Health and Safety legislation
- a Memorandum of Understanding with the relevant regulatory bodies could be put in place where appropriate, covering dispute resolution mechanisms and resolving difficulties arising from malfunctioning or misuse of the technology
- any data captured from drone detection technology is managed (including storage and transference) in accordance with the appropriate
- the technology is only deployed in line with an operational requirement where its use is deemed necessary and proportionate in line with appropriate legislation
- the technology has undergone fit for purpose testing and testing to minimise incidental interference
- regulatory bodies with responsibility for oversight of the technology deployed are informed when the drone technology is installed and where possible, prior to its installation
- depending on the nature of the site or event, organisations warn the public that unauthorised drone use will be monitored and enforcement action may be taken; and/or
- there is appropriate insurance in place

Do you think the safeguards identified for the use of drone detection technology are appropriate?

Yes (Go to 45. Counter drone technology)
X No (Go to 44. Drone detection technology safeguards)
Don't know (Go to 45. Counter drone technology)

44. Drone detection technology safeguards

Why not?

The safeguards are broadly appropriate, but licensing and training of operators should be open to members of the public, and private deployment and use for personal privacy and safety should be specified as a permitted purpose/requirement (refers also to Q45 and Q46).

Are there other safeguards for the use of drone detection technology you think we should consider?

45. Counter drone technology

The government plans to develop a clear policy framework governing the use of drone detection technology, and set minimum operator training standards. It will also publish guidance on drone detection technology and guidelines for the development of a clear purpose and scope for use of the technology, and operational policy.

Do you think there is anything else that should be done to assist organisations in meeting the defined safeguards?

Yes (Go to 46. Assisting organisations in meeting safeguards)
X No (Go to 47. Counter drone technology)
Don't know (Go to 47. Counter drone technology)

46. Assisting organisations in meeting safeguards

What should be done to assist organisations in meeting the safeguards?

47. Counter drone technology

The government recognises that in order for organisations to defer authority to trained security personnel to make an assessment of threat, a number of safeguards must be put in place. Trained security personnel will include military personnel, the police, prison staff, private security managers and commercial guard forces. It is proposed that the following types of safeguards ought to be considered:

- a minimum training requirement; and
- a site specific operational policy informed by the government guidance on how to assess a drone threat

Do you think the safeguards identified to enable deferred authority are appropriate?

Yes (Go to 49. Counter drone technology)
X No (Go to 48. Deferred authority)
Don't know (Go to 49. Counter drone technology)

48. Deferred authority

Why not?

Organisations should be buyer-aware and make their own security assessments.

Qualifications and training for threat assessment of other categories of aviation risk such as physical safety, security and cyber are not mandated and there should not be different qualification requirements for the assessment of different threat categories.

Whilst threat-assessment expertise is important, experience should be recognised as an alternative to training if there is to be a qualification requirement.

What other safeguards would you like to be considered to enable deferred authority?

49. Counter drone technology

The UK government assesses that the use of drone electronic effector technology should be only where it is necessary and proportionate for one or more of the following possible specified operational purposes:

- in the interests of national security
- for the purpose of preventing or detecting crime
- for the purpose of safeguarding the economic well-being of the UK
- in the interests of public safety
- for the purpose of preventing death or injury to a person; and/or
- for the purpose of preventing damage to property
- for the purpose of maintaining prison security or good order and discipline

Do you think the operational purposes identified for the use of drone electronic effectors are appropriate?

- Yes (Go to 51. Counter drone technology)
x No (Go to 50. Drone electronic effector principles)
Don't know (Go to 51. Counter drone technology)

50. Drone electronic effector principles

Why not?

The maintenance of civil aviation safety and security should be identified explicitly as one of the purposes of electronic effector technology.

Private deployment and use for personal privacy and safety should be specified as a permitted purpose/requirement.

51. Counter drone technology

The government is undertaking work to evidence the potential for collateral damage when electronic effector drone technology is used, and to seek to identify appropriate mitigations, which may include government advice on where to situate, and when to operate, such effectors. The government is also working to understand, and standardise if needed, what happens to the drone once this drone electronic effector technology is activated, e.g. the drone returns to home or lands safely. The results of this will also be used to develop safety mitigations.

Should any other studies be conducted to minimise the safety risks associated with deploying electronic effectors in the UK?

Yes (Go to 52. Electronic effector studies)
X No (Go to 53. Counter drone technology)
Don't know (Go to 53. Counter drone technology)

52. Electronic effector studies

What should the studies focus on?

53. Counter drone technology

The government recognises that to ensure the appropriate use of this technology a number of safeguards must be put in place, and is giving consideration to the following types of possible safeguards when drone electronic effectors are in place:

- drone electronic effectors are limited to use by trained, and approved and/or licensed operators
- there is a clear purpose and scope for use of the technology, and operational policy specific to each site, which is in line with appropriate legislation (for example, a defined code of practice)
- where applicable, a full risk assessment is conducted in line with Health and Safety legislation
- a Memorandum of Understanding with the relevant regulatory bodies is put in place where appropriate, covering dispute resolution mechanisms and resolving difficulties arising from the malfunctioning or misuse of the technology
- any data captured from drone electronic effectors is managed (including storage and transference) in accordance with the appropriate legislation, e.g. the Data Protection Act
- the technology is only deployed in line with an operational requirement where its use is deemed necessary and proportionate, in line with appropriate legislation, e.g. Article 8 of the European Convention on Human Rights
- the technology has undergone fit for purpose testing and testing to minimise incidental interference
- regulatory bodies with responsibility for oversight of the technology deployed are informed prior to installation of any drone electronic effectors
- depending on the nature of the site or event, organisations warn the public (use of public communications, community engagement and signage) that unauthorised drone use will be monitored and enforced; and/or
- there is appropriate insurance in place

Do you think the safeguards proposed for the use of drone electronic effectors are appropriate?

	Yes (Go to 55. Counter drone technology)
x	No (Go to 54. Electronic effector safeguards)
	Don't know (Go to 55. Counter drone technology)

54. Electronic effector safeguards

Why not?

The maintenance of civil aviation safety and security should be identified explicitly as one of the purposes of drone detection technology.

Private deployment and use for personal privacy and safety should be specified as a permitted purpose/requirement.

What other safeguards should be considered for the use of drone electronic effectors?

Licensing and training of operators, which should include members of the public for private use.

55. Counter drone technology

The government is considering the development of a clear policy framework governing the use of drone electronic effectors, and set minimum operator training standards. This could include publishing guidance on drone technology and the importance of a layered response, in a way which is proportionate to the threat. It could also include guidelines on the development of a concept of operations for using drone electronic effectors, including rules of engagement and guidance on the collateral damage study caused by certain types of electronic effectors to assist organisations in determining the most appropriate technology to choose and in developing their concept of operations.

Do you think anything else should be done to assist organisations in meeting the defined safeguards?

- [ ] Yes (Go to 56. Assisting organisations in meeting safeguards)
- [X] No (Go to 57. Counter drone technology)
- [ ] Don't know (Go to 57. Counter drone technology)

56. Assisting organisations in meeting safeguards

What else do you think should be done?

57. Counter drone technology

Testing drone detection technology and drone electronic effectors is required to enable current or further activities for one or more of the following purposes:

- in the interests of national security
- for the purpose of preventing or detecting crime
- for the purpose of safeguarding the economic well-being of the UK
- in the interests of public safety
- for the purpose of preventing death or injury to a person
- for the purpose of preventing damage to property
- for the purpose of maintaining prison security or good order and discipline

Do you think the requirements identified for both the testing of drone detection technology and drone electronic effectors are appropriate?

Yes (Go to 59. Counter drone technology)
x No (Go to 58. Requirements for drone detection technology and effectors)
Don't know (Go to 59. Counter drone technology)

58. Requirements for drone detection technology and effectors

Why not?

The purposes should be the same as in Q53 and our answer corresponds, namely:

The maintenance of civil aviation safety and security should be identified explicitly as one of the purposes of drone detection technology.

Private deployment and use for personal privacy and safety should be specified as a permitted purpose/requirement.

59. Counter drone technology

The government recognises that to minimise the risks of testing these technologies a number of safeguards must be put in place. It is proposed that the following possible safeguards could be enforced when testing counter drone technology:

- there is a clear purpose and scope for the testing of drone detection technology and drone electronic effectors
- testing is only permitted on government authority
- where applicable, a full risk assessment is conducted in line with Health and Safety legislation
- a Memorandum of Understanding with the relevant regulatory bodies is put in place where appropriate, covering dispute resolution mechanisms and resolving difficulties arising from the malfunctioning of technology during testing

- any data captured during the testing of drone detection technology or drone electronic effectors is managed in accordance with the appropriate legislation, e.g. the Data Protection Act
- depending on the nature of the testing, organisations warn the public (use of public communications, community engagement and signage) that testing is taking place
- there is appropriate insurance in place
- for drone electronic effectors, testing only takes place in a government defined controlled environment
- for drone electronic effectors, appropriate equipment is used to monitor the collateral damage

Do you think the safeguards identified for both the testing of drone detection technology and drone electronic effectors are appropriate?

	Yes (Go to 61. Counter drone technology)
x	No (Go to 60. Safeguards of technology and effectors)
	Don't know (Go to 61. Counter drone technology)

60. Safeguards of technology and effectors

Why not?

Using only Government controlled environment will restrict the innovation and development of technologies.

There is no need for further legislation beyond that for use of drone detection and drone effector technologies, which are dealt with in earlier questions.

61. Counter drone technology

Would you like any other safeguards to be considered to enable the testing of:

	Yes	No
drone detection technology?		x
drone electronic effectors?		X

If yes, explain what you would like these safeguards to be? If no, why not?

The list safeguards are sufficient. See answer to Q60.

62. Drone scenario modelling

To inform the impact assessments accompanying this consultation we have produced some potential scenarios of future drone use. The emerging nature of the market, and short period for which we have data means we are unable to produce robust forecasts or targets, however these scenarios give us an idea of the possible extent of UK drone use if historical trends in drone registration continue. We have included this section to provide

respondents with the opportunity to provide feedback on our methodology, rather than as a publication of official estimates.

Do you have forecasts of the number of drone or drone users (commercial or non-commercial) you are willing to share?

- [ ] Yes (Go to 63. Forecasts of use)
- [x] No (Go to 64. Drone scenario modelling)

63. Forecasts of use

Add details.

64. Drone scenario modelling

To reflect the widely observed s-curve in technology adoption, we fit a simple quadratic trend to the historical commercial drone operator permission data that shows growth at an increasing rate. To reflect the eventual slowdown in growth, we identify a point in the future at which we expect market saturation to occur after which we reduce the growth rate to one tenth of what continuing the trend would predict. The low and high scenarios show uncertainty by varying saturation points from December 2024 to December 2035 compared to June 2030 in the central case.

Are the scenarios for the number of commercial users:

- [X] realistic?
- [ ] overestimates?
- [ ] underestimates?

Why?

No data to suggest otherwise.

The low to high spread of options may be wide enough but we cannot answer this question with any authority. The market saturation point (in terms of volume) of any technology has proved historically to be very difficult to predict, and is further conditioned by economic climate. We do not understand and cannot assess the assumptions leading to a steady state rate of growth of 10% “of the continuing trend”.

To create scenarios for the number of commercial drones we scale the user scenarios by assumed numbers of drones per commercial user taken from responses to the January 2017 Drone Consultation. These begin at 5.6 drones per business in 2017 rising to 10.4 in 2028.

Are the scenarios for the number of commercial drones:

- [x] realistic?
- [ ] overestimates?
- [ ] underestimates?

Why?

No data to suggest otherwise

How do you rate the assumptions that:

	Accurate	Weak	Unknown
growth in commercial drone users will continue according to the quadratic trend that best fits historical data?			x
market saturation will most likely occur in 2030, with 2024 and 2035 representing low and high estimates respectively?			X
the average commercial user currently has 5.6 drones and this will rise to 10 in 2037?			X

Why?

For the reasons given in Q64 we cannot answer this.

What do you estimate the average number of drones per commercial user to be in:

the next year?	
2023?	
2028?	
the long run?	

How many drones do you estimate the average non-commercial user owns?

For the reasons given in Q64 we cannot answer this.

65. Final comments

Any other comments?

In our experience, government policy and law-making could be more targeted to the type of flying. When answering the questions, we often found that our answers would be different for different types of flight recreational vs commercial, and flying line-of-sight under 100 metre altitude vs flying BVLOS or over 100 metre altitude.

The questionnaire does not explicitly address the drone threat in the areas of civil aviation safety, privacy, terrorism (aviation/civil/critical national infrastructure), smuggling (cross-border/prisons), or other crime. A key question that needs to be answered concerns which of those threats this additional legislation is intended to address. In our view, the existing legislation does not adequately

address those threats, at least in the areas of privacy and aviation terrorism. In some of our answers to the questionnaire we have suggested explicit reference be made in the legislation to aviation safety or security measures, and to empowering individuals to protect themselves from privacy invasion.

Constrained as it is by the structure of this consultation, our consideration of aviation security in our answers has been limited. We believe that the government should take a more comprehensive approach to the threats posed by drones in the areas we listed above. Taking one of these as an example, in civil aviation the government and the Civil Aviation Authority (CAA) have done much work on risk-based management by operators and oversight by the regulator. They have strongly promoted PBR (performance based regulation) in safety and the government also promised OFRB (outcome-focused risk-based regulation) in security (for which the CAA uses the same term as safety – PBR). Both of these are yielding considerable benefits to the commercial aviation industry and the regulator alike, in terms of assurance and efficiency. None of this figures in the existing or proposed drone legislation, suggesting a possible lack of co-ordination across different policy areas.

It can be noted that the security sector tends to be reactive, learning from past events, mistakes or omissions, often losing precious time against developing technology and methodologies. This is true of drone capability and use, in part due to the fact that no significant attack has been executed on UK soil. However, global patterns have seen an increase in the use of small unmanned aircraft as an attack platform on a tactical (local) level as well as their use for hostile reconnaissance.

The regulatory environment provides limited scope in dealing with this problem for many reasons, not least because those with criminal intent do not seek training, registration or operational process. Parallels can be drawn with many different areas of security concern, such as legal versus illegally held firearms, with few crimes committed by those who follow home office governance.

Drones are available at no more than the cost of a smart-phone that can sense and avoid, fly autonomously, maintain flight for 28 minutes, gather TV quality imagery and reach extended ranges of 5km. All of this can be deployed from a small briefcase that would not look out of the ordinary to a security officer. Such a small drone is covert prior to flight and, due to the small size, remains so when airborne. The Air Navigation Order regulates drones but its efficacy depends on security officers being able to see the drones and having the wherewithal to deal with those not adhering to the regulations.

The progress made by the DfT and the CAA with SMS (Safety Management Systems) and PBR (performance based regulation) in safety and SeMS (Security Management Systems) and PBR in security shows that such challenges are best tackled proactively by the operators since they incur and understand the risks, supported by the government and the regulator providing guidance and a framework within which to work. Yet none of this has been considered in existing drone legislation or in the legislation considered in this consultation.

The New Zealand approach using Airshare[2] seems more in keeping with the existing Civil Aviation regulatory approach. We believe it would be a more effective solution than the proposed FINS and its infrastructure, and we would have liked to have seen this option included in the impact assessment. Specifically, it appears to us to offer the following benefits:

- Simpler, cheaper quicker to implement;
- Proven technology and methodology;
- Much more cost-effective than an optional FINS;
- Much more 'better regulation" oriented than a mandatory FINS; and
- More in keeping with DfT's approach to aviation safety and security regulation which puts the onus on the operator.

Presumably New Zealand has other laws that operators/pilots must obey, but this gives them crowd-sourced information to fulfil their obligations. In the UK context as in New Zealand, they are required to abide by the law, and this is a tool to help them. FINS seems more oriented towards an auditing tool to provide prosecuting authorities with evidence.

Finally, we note that the drone countermeasures focus on electronic effectors. There are also physical drone countermeasures on the market and, if the electronic countermeasures are considered to need legislation, we would expect the physical countermeasures to be addressed too.

[2] International Airport Review, '10,000 drone pilots register to fly in New Zealand airspace via Airshare' (14 September 2018), date retrieved 14 September 2018: https://www.internationalairportreview.com/news/75468/drone-pilots-register-fly/.