Communications Department
External Information Services

[redacted]

12 July 2018
Reference: F0003756

Dear [redacted]

Thank you for your request of 8 June 2018 for the release of information held by the Civil Aviation Authority (CAA). We have considered your request in line with the provisions of the Freedom of Information Act 2000 (FOIA).

Your request:

Could you send the most recent evaluation of the risk to UK aviation from cyber incidents and the suggested ways to mitigate them as part of your safety plan.

Our response:

The CAA is the UK's aviation regulator, and our role is to provide effective oversight of how the UK aviation industry is managing its cyber security risks to achieve safety and economic resilience. The UK aviation industry itself is responsible for managing their cyber risks in accordance with the requirements of both the European Aviation Safety Agency (EASA) and the Network and Information Services Directive.

While we do hold information relevant to your request, we are unable to provide it to you for the reasons set out below.

Critical infrastructure, such as the aviation industry, is a target for individuals or groups that seek to disrupt the UK through cyber attacks. Reflecting this, certain UK airlines, airports and air traffic control providers are designated as an "essential service" under the Network and Information Services Directive, meaning a service which is essential for the maintenance of critical societal or economic activities.

The disclosure of information on specific cyber risks to UK aviation would highlight vulnerabilities to potential attackers, helping them to target attacks at areas of weakness and increasing the likelihood of a successful attack. Similarly, the disclosure of information on suggested mitigations would provide information on measures likely to be in place to protect against attacks, helping potential attackers to develop methods to circumvent those mitigations.

The CAA considers that the following exemptions to the duty to disclose apply to the information you have requested.

Section 31

Section 31(1)(a) provides that information is exempt information if its disclosure would, or would be likely to, prejudice the prevention or detection of crime. As outlined above, the information requested could be used to identify vulnerabilities and help potential attackers to develop methods to circumvent mitigations, leaving the UK aviation industry more vulnerable to cyber attacks. Therefore, in the CAA's view, disclosure of the information requested would prejudice the prevention of crime.

As section 31 is a qualified exemption, we have also considered whether or not it is in the public interest to disclose the information. The public interest in disclosure includes the general principles of transparency and open government and the accountability of the CAA for the way it oversees how the UK aviation industry is managing its cyber security risks. However, disclosure of the information requested could assist criminal activity and increase the chances of a successful cyber attack against the UK's aviation infrastructure. A successful cyber attack against the UK's aviation industry has the potential to cause significant disruption and economic harm to the UK, as well as significant risks to aviation safety. The potential consequences are such that there is a very strong public interest in withholding information that would increase the chances of a successful cyber attack.

Having considered the public interest factors on both sides, we have concluded that, in all the circumstances of the case, the public interest in withholding the information outweighs the public interest in disclosure.

Section 24

Section 24(1) of the FOIA provides that information is exempt if exemption from the duty to disclose is required for the purposes of safeguarding national security, and the CAA believes that this applies to the information you have requested.

In the CAA's view, the national security of the UK includes not only the protection of UK citizens and their assets against acts of terrorism and violence, but also the protection of the UK's economic well-being. The aviation industry makes a substantial contribution to the UK economy, and the information you have requested relates to the security of critical parts of the aviation infrastructure. A successful cyber attack against the UK's aviation industry has the potential to cause significant disruption and economic harm to the UK. Beyond that, a successful cyber attack also poses significant risks to aviation safety.

As section 24 is a qualified exemption, we have also considered whether or not it is in the public interest to disclose the information. The public interest in disclosure includes the general principles of transparency and open government and the accountability of the CAA for the way it oversees how the UK aviation industry is managing its cyber security risks. However, the potential consequences of a successful cyber attack are such that there is a very strong public interest in withholding information that would be of value to potential attackers.

Having considered the public interest factors on both sides, we have concluded that, in all the circumstances of the case, the public interest in withholding the information outweighs the public interest in disclosure.

Section 23

In addition, under section 23(5) of the FOIA (information supplied by, or concerning, certain security bodies) the CAA neither confirms nor denies whether it holds any information in scope of your request, which would be exempt under section 23. Section 23 is an absolute exemption and not subject to a public interest test.

A copy of these exemptions can be found below.

If you are not satisfied with how we have dealt with your request in the first instance you should approach the CAA in writing at:-

Caroline Chalk
Head of External Information Services
Civil Aviation Authority
Aviation House
Gatwick Airport South
Gatwick
RH6 0YR

caroline.chalk@caa.co.uk

The CAA has a formal internal review process for dealing with appeals or complaints in connection with Freedom of Information requests. The key steps in this process are set in the attachment.

Should you remain dissatisfied with the outcome you have a right under Section 50 of the FOIA to appeal against the decision by contacting the Information Commissioner at:-

Information Commissioner's Office
FOI/EIR Complaints Resolution
Wycliffe House
Water Lane
Wilmslow
SK9 5AF
https://ico.org.uk/concerns/

If you wish to request further information from the CAA, please use the form on the CAA website at http://publicapps.caa.co.uk/modalapplication.aspx?appid=24.

Yours sincerely

Mark Stevens
External Response Manager

CAA INTERNAL REVIEW & COMPLAINTS PROCEDURE

- The original case to which the appeal or complaint relates is identified and the case file is made available;
- The appeal or complaint is allocated to an Appeal Manager, the appeal is acknowledged and the details of the Appeal Manager are provided to the applicant;
- The Appeal Manager reviews the case to understand the nature of the appeal or complaint, reviews the actions and decisions taken in connection with the original case and takes account of any new information that may have been received. This will typically require contact with those persons involved in the original case and consultation with the CAA Legal Department;
- The Appeal Manager concludes the review and, after consultation with those involved with the case, and with the CAA Legal Department, agrees on the course of action to be taken;
- The Appeal Manager prepares the necessary response and collates any information to be provided to the applicant;
- The response and any necessary information is sent to the applicant, together with information about further rights of appeal to the Information Commissioners Office, including full contact details.

Freedom of Information Act – Section 23

(1) Information held by a public authority is exempt information if it was directly or indirectly supplied to the public authority by, or relates to, any of the bodies specified in subsection (3).

(2) A certificate signed by a Minister of the Crown certifying that the information to which it applies was directly or indirectly supplied by, or relates to, any of the bodies specified in subsection (3) shall, subject to section 60, be conclusive evidence of that fact.

(3) The bodies referred to in subsections (1) and (2) are—

(a) the Security Service,
(b) the Secret Intelligence Service,
(c) the Government Communications Headquarters,
(d) the special forces,
(e) the Tribunal established under section 65 of the Regulation of Investigatory Powers Act 2000,
(f) the Tribunal established under section 7 of the Interception of Communications Act 1985,
(g) the Tribunal established under section 5 of the Security Service Act 1989,
(h) the Tribunal established under section 9 of the Intelligence Services Act 1994,
(i) the Security Vetting Appeals Panel,
(j) the Security Commission,
(k) the National Criminal Intelligence Service,
(l) the Service Authority for the National Criminal Intelligence Service.
(m) the Serious Organised Crime Agency.
(n) the National Crime Agency.
(o) the Intelligence and Security Committee of Parliament.

(4) In subsection (3)(c) “the Government Communications Headquarters” includes any unit or part of a unit of the armed forces of the Crown which is for the time being required by the Secretary of State to assist the Government Communications Headquarters in carrying out its functions.

(5) The duty to confirm or deny does not arise if, or to the extent that, compliance with section 1(1)(a) would involve the disclosure of any information (whether or not already recorded) which was directly or indirectly supplied to the public authority by, or relates to, any of the bodies specified in subsection (3).

Freedom of Information Act – Section 24

(1) Information which does not fall within section 23(1) is exempt information if exemption from section 1(1)(b) is required for the purpose of safeguarding national security.

(2) The duty to confirm or deny does not arise if, or to the extent that, exemption from section 1(1)(a) is required for the purpose of safeguarding national security.

(3) A certificate signed by a Minister of the Crown certifying that exemption from section 1(1)(b), or from section 1(1)(a) and (b), is, or at any time was, required for the purpose of safeguarding national security shall, subject to section 60, be conclusive evidence of that fact.

(4) A certificate under subsection (3) may identify the information to which it applies by means of a general description and may be expressed to have prospective effect.

Freedom of Information Act : Section 31

(1) Information which is not exempt information by virtue of section 30 is exempt information if its disclosure under this Act would, or would be likely to, prejudice-

(a) the prevention or detection of crime,
(b) the apprehension or prosecution of offenders,
(c) the administration of justice,
(d) the assessment or collection of any tax or duty or of any imposition of a similar nature,
(e) the operation of the immigration controls,
(f) the maintenance of security and good order in prisons or in other institutions where persons are lawfully detained,
(g) the exercise by any public authority of its functions for any of the purposes specified in subsection (2),
(h) any civil proceedings which are brought by or on behalf of a public authority and arise out of an investigation conducted, for any of the purposes specified in subsection (2), by or on behalf of the authority by virtue of Her Majesty's prerogative or by virtue of powers conferred by or under an enactment, or
(i) any inquiry held under the Fatal Accidents and Sudden Deaths enquiries (Scotland) Act 1976 to the extent that the inquiry arises out of an investigation conducted, for any of the purposes specified in subsection (2), by or on behalf of the authority by virtue of Her Majesty's prerogative or by virtue of powers conferred by or under an enactment.

(2) The purposes referred to in subsection (1)(g) to (i) are-

(a) the purpose of ascertaining whether any person has failed to comply with the law,
(b) the purpose of ascertaining whether any person is responsible for any conduct which is improper,
(c) the purpose of ascertaining whether circumstances which would justify regulatory action in pursuance of any enactment exist or may arise,
(d) the purpose of ascertaining a person's fitness or competence in relation to the management of bodies corporate or in relation to any profession or other activity which he is, or seeks to become, authorised to carry on,
(e) the purpose of ascertaining the cause of an accident,
(f) the purpose of protecting charities against misconduct or mismanagement (whether by trustees or other persons) in their administration,
(g) the purpose of protecting the property of charities from loss or misapplication,
(h) the purpose of recovering the property of charities,
(i) the purpose of securing the health, safety and welfare of persons at work, and
(j) the purpose of protecting persons other than persons at work against risk to health or safety arising out of or in connection with the actions of persons at work.

(3) The duty to confirm or deny does not arise if, or to the extent that, compliance with section 1(1)(a) would, or would be likely to, prejudice any of the matters mentioned in subsection (1).