Freedom of Information Act 2000 (FOIA)

Decision notice

Date:	**21 November 2024**
Public Authority:	**Department for Transport**
Address:	**33 Horseferry Road London SW1P 4DR**

Decision (including any steps ordered)

1. The complainant has requested information about reported network and information system incidents. The Department for Transport ('the DfT') provided some of the requested information but relied on section 24 of FOIA (national security) and section 31 of FOIA (law enforcement) to withhold the remainder of the requested information.

2. The Commissioner's decision is that the DfT was not entitled to rely on section 24 nor section 31 of FOIA to withhold the remainder of the requested information.

3. The Commissioner requires the DfT to take the following steps to ensure compliance with the legislation.

   - Disclose, to the complainant, the information it has relied on exemptions to withhold.

4. The public authority must take these steps within 30 calendar days of the date of this decision notice. Failure to comply may result in the Commissioner making written certification of this fact to the High Court pursuant to section 54 of the Act and may be dealt with as a contempt of court.

Request and response

5. On 14 March 2024, the complainant wrote to the DfT and requested information in the following terms:

"For each of the last three calendar years (i.e. 2023, 2022 & 2021) please could you let me know:

a. The total number of network and information systems incidents notified to your department by relevant OESs/RDSPs under the NIS Regs.

b. For each such notification please provide:

(i) the year of the notification, e.g. 2023/2022/2021; and

(ii) where you regulate more than one sector, the sub-sector of the entity making the notification (e.g. Electricity/Gas);

(iii) whether the notification was made within the 72 hour reporting window; and

(iv) whether formal enforcement action was taken.

For each instance in which formal enforcement action was taken, as set out above, please you could you let me know:

(a) The power exercised, e.g. information notice, use of powers of inspection, service of an enforcement notice or issue of a penalty.

(b) If the power exercised was a fine, the amount of the fine."

6. The DfT responded on 15 April 2024. It provided information about the total number of incident notifications and whether the notifications were made within 72 hours. It withheld the remainder of the requested information and relied on sections 24 and 31 of FOIA to do so.

7. Following an internal review, the DfT wrote to the complainant on 13 June 2024. It maintained its position.

Scope of the case

8. The complainant contacted the Commissioner on 20 June 2024 to complain about the way their request for information had been handled.

9. The Commissioner considers that the scope of his investigation is to determine whether the DfT was entitled to rely on sections 24 and 31 to withhold some of the requested information.

Reasons for decision

Section 24 – national security

10. Section 24(1) states that:

> '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'.

11. FOIA does not define the term 'national security'. However, in Norman Baker v the Information Commissioner and the Cabinet Office (EA/2006/0045 4 April 2007) the Information Tribunal was guided by a House of Lords case, Secretary of State for the Home Department v Rehman [2001] UKHL 47, concerning whether the risk posed by a foreign national provided grounds for his deportation. The Information Tribunal summarised the Lords' observations as follows:

- 'national security' means the security of the United Kingdom and its people;
- the interests of national security are not limited to actions by an individual which are targeted at the UK, its system of government or its people;
- the protection of democracy and the legal and constitutional systems of the state are part of national security as well as military defence;
- action against a foreign state may be capable indirectly of affecting the security of the UK; and,
- reciprocal co-operation between the UK and other states in combating international terrorism is capable of promoting the United Kingdom's national security.

12. Furthermore, in this context the Commissioner interprets 'required for the purpose of' to mean 'reasonably necessary'. Although there has to be a real possibility that the disclosure of requested information would undermine national security, the impact does not need to be direct or immediate.

The complainant's position

13. The complainant has argued that the requested information is very high level and limited in nature. They stated that it could not plausibly affect national security or expose any organisation to a cyber threat.

14. In their request for internal review, the complainant explained that their request did not ask for any details of the nature of the breach, the affected operator or any technical information. They therefore didn't accept the suggestion that the requested information could be used for a cyber-attack.

15. The complainant added that they had submitted the same request to other organisations and had been provided with the requested information.

The DfT's position

16. The DfT has disagreed that the information requested is only high-level and unlikely to be a threat to national security. It stated that the requested information in its current level of detail and specificity is a genuine risk to the UK's transport sector.

17. The DfT has explained that the cyber threat to the UK is as high now as it has ever been and that this is particularly the case in areas of Critical National Infrastructure, like transport. There have recently been numerous high-profile cyber-attacks in various sectors, including transport, in the UK.

18. It explained that cyber criminals, like ransomware-for-hire groups, or nation state backed cyber criminals, are constantly increasing in their sophistication and abilities.

19. The DfT stated that when looking for organisations to attack, malicious actors will use a variety of information to acquire targets that have an increased chance of successful penetration. It explained that this information will be from numerous sources, including the dark web, from open-source information and any other areas that can help develop a picture of targets at increased risk.

20. The DfT expressed concern that by providing more information than it already has in response to the request, it risks adding to the information ecosystem available to malicious actors. By providing the requested information in the specified detail, the DfT considers that it could improve the targeting ability of cyber criminals and draw their attention to transport entities.

21. The DfT has acknowledged that, in isolation, the requested information is unlikely to prove critical to helping cyber criminals target the transport sector. However, it considers that the information is not provided in isolation. When taken in conjunction with other information in the public domain, and information available from other sources, the DFT considers that the threat to targeting of the transport sector is increased, posing a threat to national security.

22. The DfT considers that revealing the year of each of the incidents could highlight patterns or trends in a subsector's approach to cyber security. These patterns, when combined with other information (including open-source data) could be exploited for malicious actions or future targeted attacks. The DfT considers that this could potentially make UK citizens more vulnerable to cyber-attacks. It explained that as the focus in this case would be within the transport sector, this information can be used to narrow down or identify which subsectors to target when considering these patterns of potential weakness.

23. The DfT has explained that disclosing information on whether formal enforcement action was taken could draw attention to the impacted transport subsector, making it more likely to be targeted. The DfT acknowledged that the complainant did not ask for details of specific Operators of Essential Services ('OES'). However, it considers that, if a subsector has received multiple enforcement actions against it, it would be sensible for a cyber actor to target organisations in that sub sector, particularly if they are a subsector which may enable lateral movement into other sectors or are large operators that are able to cause significant disruption.

24. The DfT provided further arguments in respect of its application of section 24 but advised that it wished them to remain confidential. The Commissioner has considered these arguments but has not included them in this notice for this reason.

The Commissioner's view

25. The Commissioner acknowledges that the transport sector forms an integral part of national infrastructure, and that any threats to, or attacks on, that infrastructure could cause serious harm.

26. However, the Commissioner is mindful that he has recently issued a decision[1] on a complaint case concerning the same information. He found that while the potential harm was apparent, the causal link between the disclosure of the withheld information itself and that harm could not be clearly identified. He considers that the same applies in this case.

27. As in IC-299337-B4V1, the Commissioner finds that while the withheld information could be used to indicate the success of a cyber-attack, he

[1] ic-299337-b4v1.pdf

is not convinced that it reveals considerably more than a motivated individual could already gather from open source material.

28. Disruption and issues with different transport networks, including those due to cyber-attacks, are widely reported in the media and online with most networks operating a live service monitoring system that advises the public of any problems. While the general public may not link information on disruptions to cyber-attacks, any individual motivated to carry out such activity could easily monitor media stories service information to determine the impact of previous attacks.

29. Disclosure of the withheld information would identify the number of incidents reported by a transport sub-sector and could make the public aware that certain transport disruptions were due to a cyber-attack. However, it would not give any detail of the attack method or the perpetrator of the attack. As explained in IC-299337-B4V1, the usefulness of the withheld information is limited as a result.

30. Indeed, it may be possible for a motivated individual to use the withheld information and open source data to piece together details of a particular incident. However, the Commissioner considers that cyber attackers would be more likely to focus their efforts on recent incidents rather than historical ones. This reasoning being that any organisation that has been subject to a particular attack will have since had time to address any vulnerabilities and the DfT will have had the opportunity to warn other organisations to check their own vulnerabilities.

31. Having reviewed the withheld information and considered his previous decision on a very similar complaint case, the Commissioner is not convinced that withholding such information is required for the purposes of safeguarding national security. He therefore finds that section 24 is not engaged.

32. The Commissioner will go on to consider the DfT's application of section 31 of FOIA.

Section 31 – law enforcement

33. Section 31(1)(a) of FOIA says that:

> "Information …. is exempt information if its disclosure under this Act would, or would be likely to, prejudice- (a) the prevention or detection of crime…."

34. The exemption in section 31(1)(a) covers all aspects of the prevention and detection of crime. It could apply to information on general policies and methods adopted by law enforcement agencies.

35. The exemption also covers information held by public authorities without any specific law enforcement responsibilities. It could be used by a public authority to withhold information that would make anyone, including the public authority itself, more vulnerable to crime.

The DfT's position

36. The DfT has explained that disclosing the requested information could potentially aid cyber attackers in planning an attack on the UK's Critical and National Infrastructure. This is because releasing this information would be likely to help malicious actors to identify vulnerabilities in the cyber security systems of OES.

37. As with its submission for section 24, the DfT acknowledged that, in isolation, the requested information is unlikely to prove critical to helping cyber criminals target the transport sector but could be used with other available information to target the transport sector. It considers that this increases the risk of crime.

38. The DfT explained that its Cyber Compliance Team can take enforcement action against OES that are not compliant with the NIS Regulations. It considers that providing the detail of its enforcement action(s) would be likely to undermine them, whilst also exposing OES to additional cyber risk.

39. The DfT considers that disclosing further information about its enforcement activities may increase the chances of cyber attackers being successful in attacks. Disclosure of the withheld information could provide them with data that, when combined with information from other sources, will enable them to build a picture about enforcement capability or areas of vulnerability. The DfT stated that this will reduce its ability to prevent or detect crime, generate a lower trust environment with its OES, and reduce the likelihood of information being freely shared.

40. The DfT provided further arguments in respect of its application of section 31 but advised that it wished them to remain confidential. The Commissioner has considered these arguments but has not included them in this notice for this reason.

The Commissioner's view

41. The Commissioner acknowledges that if a particular OES was subject to a number of enforcement activities by DfT then a prospective cyber attacker may consider that OES as a good target. However, the request does not ask for the name of the OES and is not requesting a level of detail that would necessarily reveal the OES subject to the enforcement activity. As with his view of the DfT's application of section 24, the

Commissioner considers that an OES in receipt of enforcement action a year or more ago would have had ample opportunity to rectify any issues.

42. The Commissioner notes the DfT's argument about a lower trust environment with its OES, and a reduction in information being shared freely. He also notes however that OES are required by law to report incidents that meet the NIS threshold, and that the DfT has its own powers to compel the provision of information.

43. The Commissioner is not convinced that the DfT has demonstrated the causal link between disclosure of the information and the prejudice to the prevention or detection of a crime. In its submission concerning section 31, the DfT stated that it was no longer relying on section 31(1)(g), however the Commissioner finds that the majority of its arguments relate to this sub-section of section 31.

44. OES are required to report incidents to the DfT and will likely share more specific detail with the DfT about the nature of the incident, breach of security system and impact. This detail would undoubtably assist potential attackers in planning future attacks, and the Commissioner can understand why OES would not want this disclosed. However, the complainant has not asked for this detail and has requested high-level figures for incidents from 2023 and earlier.

45. In terms of enforcement action, the Commissioner does not accept the DfT's argument that requested information would undermine this. While the free and informal flow of information helps regulatory activity, it is not essential for the DfT to be able to carry out its functions.

46. The Commissioner accepts that disclosure of the withheld information could reveal the level of enforcement action carried out by the DfT. As stated in IC-299337-B4V1: "If the public authority was not using its formal powers regularly, that may well provoke a public debate about the extent to which the regulator is taking its responsibilities seriously. In such a scenario, may well be good reasons why the public authority had chosen to take the approach it had, but there would still be a legitimate debate."

47. Given the limited nature of the information being requested and the availability, to the DfT, of formal powers to compel the provision of such information, the Commissioner is not persuaded that disclosure of the information would harm law enforcement or regulatory activity. He therefore finds that section 31 of FOIA is not engaged, and that the information must be disclosed.

Right of appeal

48. Either party has the right to appeal against this decision notice to the First-tier Tribunal (Information Rights). Information about the appeals process may be obtained from:

    First-tier Tribunal (Information Rights)
    GRC & GRP Tribunals,
    PO Box 9300,
    LEICESTER,
    LE1 8DJ

    Tel: 0203 936 8963
    Fax: 0870 739 5836
    Email: grc@justice.gov.uk
    Website: www.justice.gov.uk/tribunals/general-regulatory-chamber

49. If you wish to appeal against a decision notice, you can obtain information on how to appeal along with the relevant forms from the Information Tribunal website.

50. Any Notice of Appeal should be served on the Tribunal within 28 (calendar) days of the date on which this decision notice is sent.

Keeley Christine
Senior Case Officer
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF