Freedom of Information Act 2000 (FOIA)

Decision notice

Date:	**28 August 2024**
Public Authority:	**Office of Gas and Electricity Markets**
Address:	**10 South Colonnade** **Canary Wharf** **London** **E14 4PU**

Decision (including any steps ordered)

1. The complainant has requested information about reportable incidents. The above public authority ("the public authority") relied on section 24 (national security) and 31 (law enforcement) of FOIA to withhold the information.

2. The Commissioner's decision is that neither section 24 nor 31 is engaged.

3. The Commissioner requires the public authority 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 30 January 2024, the complainant requested information of the following description

> "[1] 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.
>
> "[2] 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 public authority responded on 26 February 2024. It refused to provide the requested information. It relied on sections 24 and 31 of FOIA as its basis for doing so. It upheld this stance following an internal review.

Scope of the case

7. At the outset of his investigation, the Commissioner asked the complainant whether there might be scope to resolve the matter informally. However the complainant asked for their request to be complied with in full.

8. The public authority also offered to provide the information within the scope of parts 1(a) and 1(b)(iii) of the letter – though the

Commissioner's understanding is that it was only willing to provide totals for the overall three year period, not each individual year.

9. The Commissioner considers that the scope of his investigation is to determine whether sections 24 or 31 apply.

Reasons for decision

10. Section 24 of FOIA allows a public authority to withhold information if that is required for the purposes of safeguarding national security.

11. The Commissioner recognises that the withheld information relates to incidents involving disruption to the supply of gas and electricity. The supply networks for these utilities comprise critical national infrastructure. Any harm to them could have a widespread and significant effect on the public. He is therefore satisfied that disclosure of information that would increase the risk of such harm would present a risk to national security.

12. The public authority noted that it was designated as the competent authority for gas and electricity suppliers for the purposes of the Network and Information Systems Regulations 2018 (NIS). NIS requires suppliers of essential services to notify their competent authority of any incident which has a "significant" impact on their ability to supply that service. Whether an incident meets the reporting threshold will depend on how many people are affected and for how long.

13. The public authority explained that, if it were to disclose the requested information it could reveal vulnerabilities within critical national infrastructure, or demonstrate which types of cyber attack were likely to have the widest impact, or both.

14. It pointed out to the Commissioner that a disruption to power supplies can have severe consequences for those affected – regardless of how the disruption was caused. For example it noted that in 2021, Storm Arwen had knocked out power to over 100,000 people which, in some cases actually caused fatalities.

15. The public authority also noted to the Commissioner that cyber-attackers have been known to research potential targets for months or even years, gathering intelligence from open source material in order to design sophisticated attacks they think are likely to succeed. It argued that even seemingly-bland information could form part of a wider jigsaw that enables a cyber attacker to refine their next attack.

16. More particularly, the public authority noted in this case that the information requested was sufficiently granular as to allow the identity of each supplier that had reported an incident to be revealed. For example, a motivated individual could research reported power outages to link a specific incident to a specific outage in a specific location and thereby deduce the supplier for that location.

The Commissioner's view

17. The Commissioner recognises that energy supply forms part of critical national infrastructure. The public authority has demonstrated that key information about such infrastructure could, if it fell into the wrong hands, put that infrastructure at risk. He also accepts that the harm that could result from a major attack, if it did occur, would be severe and, in some cases, possibly fatal.

18. However, for the exemption to apply, there needs to be a causal link between disclosure and harm. In this case, the Commissioner has struggled to identify one.

19. To the extent that the withheld information gives an indication of the success of a cyber-attack, the Commissioner is not convinced that it reveals considerably more than a motivated individual could already gather from open source material.

20. If a particular attacker had just launched an attack, they could monitor the success of that attack by checking for any reports on local or even national news. They would also be able to scour social media to judge how widespread any effects had been. The Commissioner also notes that UK Power Networks operates a live listing of power outages across the country.

21. Whilst it would get harder to carry out such research the longer ago the incident occurred, it would still be far from impossible – even for incidents that occurred several years ago.

22. Someone unconnected to the original attack would be alerted, by the withheld information, to the fact that a particular outage had been caused by a cyber attack. They could then identify the suppliers involved based on the geographical extent of the reporting of outages. In the Commissioner's view, someone with the skills and motivation to carry out a cyber attack would have the skills and motivation required to carry out such research.

23. However, the usefulness of such information would be very limited. It would not reveal who the attacker had been or the methods they used to carry out their attack.

24. Cyber attackers have been known to share information amongst themselves. It may not be impossible for a person, alerted to the fact of a successful cyber attack, to establish the method used and replicate it themselves. However, that work would take time.

25. In the Commissioner's view a cyber attacker is more likely to invest time in trying to research a recent cyber attack, thereby aiming to replicate it before their target has had a chance to address its vulnerability. Logic would suggest that cyber attackers are less likely to spend time researching older attacks, where the supplier involved will have had time to address any vulnerabilities and where the public authority has had the opportunity to warn other suppliers to check their own vulnerabilities.

26. Having reviewed the withheld information, the Commissioner is satisfied that, at the point the request was responded, any supplier that could be identified would have had sufficient time to take appropriate remedial action and the public authority would have had ample to time to take any enforcement action it deemed necessary to protect the public. The Commissioner is therefore of the view that withholding such information is not required for the purposes of safeguarding national security and so section 24 is not engaged.

Section 31 – law enforcement

27. The Commissioner has next considered whether section 31 applies.

28. Section 31 allows a public authority to withhold information whose disclosure would make it more difficult for various law enforcement bodies to enforce the law.

29. In this case the public authority has argued that disclosing this information would harm its ability to regulate effectively. The Commissioner accepts that the public authority has relevant regulatory functions capable of being harmed.

30. The public authority explained to the Commissioner that its ability to regulate effectively relied upon the free flow of information to and from the suppliers it regulated. The suppliers must feel free to be candid with the regulator and to co-operate with any investigations.

31. The public authority accepted that suppliers are required by law to report incidents that meet the NIS threshold and that it has its own powers to compel the provision of information. However it argued that the process was much more effective where suppliers co-operated and where it did not need to resort to formal powers.

32. The public authority also argued that:

> "any organisation regulated under NIS could request such information on a regular basis about their peers to gain a commercial advantage by identifying vulnerabilities about their economic competitors. This could lead to significant issues and undermine our ability to carry out our role."

The Commissioner's view

33. In the Commissioner's view, the public authority has failed to demonstrate a causal link between disclosure and harm.

34. Suppliers are required by law to report incidents that meet a particular threshold to the public authority – regardless of what the public authority may then choose to disclose.

35. The Commissioner accepts that, when reporting an incident, suppliers will share much more detailed information about the incident. For example NIS also requires suppliers to disclose details about the "nature and impact" of the incident as well as "any other information that might be helpful to the competent authority." Suppliers are very unlikely to want this information to be widely known and they have a certain amount of discretion as to the level of detail they provide.

36. However, whilst the Commissioner appreciates that suppliers will want to keep detailed information about the nature of the incident and any counter-measures deployed during or after, confidential, that is not what the complainant has asked for.

37. The Commissioner is not persuaded that a supplier would fail to comply its legal obligations simply because the public authority might, more than a year after the incident has taken place, disclose information which might lead to its identification – whilst keeping more detailed information confidential.

38. Nor is the Commissioner convinced that disclosing when formal powers have been used (more than a year after the incident) is likely to harm the public authority's ability to regulate.

39. If suppliers see that the regulator is using its formal powers regularly to deal with companies that fail to take their security seriously, this is likely to have a deterrent effect. Suppliers will want to be more pro-active to prevent regulatory attention – particularly if the fact of regulatory attention may become known in future.

40. 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, there

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.

41. Given the limited nature of the information being requested and the availability, to the public authority, of formal powers to compel the provision of such information, the Commissioner is not persuaded that disclosure of the information would harm regulatory activity. Consequently section 31 of FOIA is not engaged and therefore the information must be disclosed.

Right of appeal

42. 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

43. 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.

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

Signed

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