Freedom of Information Act 2000 (FOIA)

Decision notice

Date: **28 March 2018**

Public Authority: UK Export Finance

Decision (including any steps ordered)

1. The complainant has requested information in relation to the number, nature, and effects of cyber attacks. The public authority refused to disclose the information held within the scope of the request on the basis of the exemption at section 31(1)(a) FOIA.

2. The Commissioner's decision is that the public authority was entitled to rely on the exemption at section 31(1)(a) as the basis for withholding the information held within the scope of the request

3. No steps are required.

Request and response

4. On 3 November 2016, the complainant wrote to the public authority and requested information in the following terms:

   "I write with a request for information about cyber attacks on the department….

   Please disclose the number of recorded cyber attacks in 2015;

   Please disclose the number of recorded cyber attacks to date in 2016;

   For 2016, please provide:

   A month-by-month breakdown;

   The number of successful attacks – i.e. where there was a breach;

   In the cases of a breach, please disclose:

   the nature of the attack (DDOS, phishing etc),

   the nature of the breach,

   how many individuals' information were affected,

   whether any classified information was affected,

   what organisations or individual/s are suspected to known to have made the attack."

5. The public authority responded in the following terms on 1 December 2016:

   "I can neither confirm nor deny whether UK Export Finance (UKEF) holds the information that you have requested on the grounds that doing so would prejudice the prevention or detection of crime in a real and substantial way (see the exemption provided under section 31(3) of the FOIA).

   Even if the exemption in section 31(3) of the FOIA did not apply, UKEF would be unable to disclose the requested information on the grounds that communicating the information requested would prejudice the prevention or detection of crime in a real and substantial way (see the exemption provided under section 31(1)(a) of the FOIA)."

6. It also concluded that the public interest in neither confirming nor denying whether the information requested was held outweighed the

public interest in doing so. It added that the public interest in "withholding such information" would be weightier "even [if] it could confirm or deny whether or not it holds the requested information…."

7. The complainant requested an internal review of the public authority's decision on 1 December 2016.

8. The public authority wrote back with details of the outcome of the internal review on 31 January 2017. It responded in the following terms:

"The reviewer considered that the Response correctly withheld the information requested by you, but that the 'neither confirm nor deny' ("NCND") response under Section 31(3) of the Freedom of Information Act 2000 ("FOIA") while correctly applied to the Information Request, should not have been combined with (and indeed was negated by) the subsequent application of Section 31(1)(a).

The reviewer also considered whether the information was correctly withheld under Section 31(1)(a) of the FOIA. The reviewer agreed that the public interest in withholding this information would, or would be likely to, prejudice the prevention or detection of crime which outweighs the public interest benefits in disclosing such information….

In view of this, the internal reviewer upheld the original decision to withhold the information requested by you under Section 31(1)(a) FOIA."

Scope of the case

9. The complainant contacted the Commissioner on 1 February 2017 to complain about the way his request for information had been handled. The Commissioner has referred to his submissions at the relevant parts of her analysis below.

10. The scope of the investigation therefore was to determine whether the public authority was entitled to rely on the exemption at section exemption at section 31(1)(a).

11. In the circumstances of this case, the Commissioner would like to place on record that during the course of the investigation, she commented that the internal review had overturned the original decision by the public authority to rely on NCND. The public authority however disagreed with her observation and provided the following explanation:

"The internal reviewer……did not revise the original decision as stated in the ICO Letter. The Information Request Response held that section

31(3) of the FOIA was engaged and that section 31(1)(a) of the FOIA would otherwise be engaged if section 31(3) of the FOIA did not apply.

The Internal Review Request Response held that the 'neither confirm nor deny' ("NCND") response under Section 31(3) of the FOIA, while correctly applied to the Information Request, should not have been combined with (and indeed was negated by) the subsequent application of Section 31(1)(a) of the FOIA.

The citing of Section 31(1)(a) of the FOIA in the Information Request Response therefore undermined the NCND response (as the complainant would be able to ascertain that [it] did indeed hold the information requested. In view of this, the internal reviewer considered and upheld that the information was correctly withheld under Section 31(1)(a) of the FOIA."

12. The Commissioner considers that the internal review response clearly revised the original response which was that the public authority could neither confirm nor deny whether it held the information requested.

Reasons for decision

Section 31(1)(a)

13. The Commissioner has considered whether the public authority was entitled to engage this exemption which was applied to the information held within the scope of the request.

14. Section 31(1)(a) states:

"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."

Complainant's submissions

15. The complainant has submitted the following arguments in support of his view that the requested information ought to be disclosed.

16. "There is a compelling public interest in disclosure of information capable of informing people how many attacks there have been and how many have been successful or not. Transparency allows the public to scrutinise whether the millions of pounds of public money being spent on secure systems is adequate and provides sufficiently robust protection for data held by the UKEF. Only recently the Government

announced that £1.9 billion of public money is being spent on cyber security. This alone provides a compelling justification for transparency surrounding this issue."

17. "It must also be pointed out that transparency will increase public confidence in Government security."

18. "None of the information requested would help hackers. It doesn't reveal the hacks they used to penetrate the systems. It simply reveals how many attacks have been successful and how many people were affected etc."

19. "There is a compelling and legitimate public interest in knowing how secure the UKEF's systems are. Information concerning Britons relies on UKEF having resilient systems and it is paramount that the public is able to obtain basic information about how secure those systems are. It must be pointed out that the numbers are capable of demonstrating how many attacks have failed. This shows that public money UKEF has spent on secure systems has been well spent and, as mentioned, improves confidence in the UKEF."

Public authority's submissions

20. The public authority's submission in support of reliance on this exemption is summarised below.

21. It clarified that its position is that disclosing the withheld information would be likely to prejudice the prevention or detection of crime.

22. It explained that in considering the request, it had consulted its security team and guidance issued by the Cabinet Office on responding to requests about cyber attacks.

23. It explained that cyber attacks represent a real threat to its IT systems, the information it holds and its ability to carry out its functions as a public authority. The risk of cyber attacks succeeding remains despite the anti-malware software it has in place.

24. The public authority therefore argued that releasing the withheld information would pose a real and significant risk that it could be used by malicious actors to conduct cyber attacks against the authority and assist in criminal activity. It submitted that malicious actors would be able to determine the effectiveness of detecting such attacks which could compromise measures to protect government IT systems. An additional consequence of disclosure it argued, may be to encourage further attacks if it is known that one type of attack is more successful than another.

25. It further argued that the withheld information could be combined along with existing information already in the public domain to gain a wider understanding of the security of government IT systems which would be useful to malicious actors.

26. In addition, a precedent could be set whereby complying with one request would make it more difficult to refuse requests for similar information. Over time, this information could be combined to form a pattern which could enable criminals to conduct further attacks and assist criminal activity.

27. Finally, it explained that it provided the withheld information to the Police following a successful cyber attack against the public authority. Disclosure could be prejudicial to the ongoing police investigation.

28. The public authority also considered whether the public interest in maintaining the exemption outweighs the public interest in disclosing the information in scope. Its submission on the balance of the public interest is summarised below

29. It argued that there is a stronger public interest in protecting its IT systems, information it holds, and its ability to carry out its duties as a public authority. It explained that it provides significant financial support to UK businesses and exporters and that if its systems were to be compromised, this would present a real and significant risk to the public authority, the businesses it supports and the UK's economy more generally. In addition, disclosure of information likely to weaken its cyber security would also diminish the effectiveness of its expenditure of public funds on cyber security, undermining the public interest in obtaining value for money.

Is the exemption engaged?

30. The Commissioner has first considered whether the exemption at section 31(1)(a) was engaged.

31. In order for a prejudice based exemption such as that contained within section 31(1)(a) to be engaged, the Commissioner considers that three criteria must be met.

- Firstly, the actual harm which the public authority alleges would, or would be likely, to occur if the withheld information was disclosed has to relate to the applicable interests within the relevant exemption;

- Secondly, the public authority must be able to demonstrate that some causal relationship exists between the potential disclosure of the information being withheld and the prejudice which the exemption is

designed to protect. Furthermore, the resultant prejudice which is alleged must be real, actual or of substance; and

- Thirdly, it is necessary to establish whether the level of likelihood of prejudice being relied upon by the public authority is met – ie, disclosure 'would be likely' to result in prejudice or disclosure 'would' result in prejudice. In relation to the lower threshold the Commissioner considers that the chance of prejudice occurring must be more than a hypothetical possibility; rather there must be a real and significant risk. With regard to the higher threshold, in the Commissioner's view this places a stronger evidential burden on the public authority. The anticipated prejudice must be more likely than not.

32. With regard to the first criterion of the three limb test described above, the Commissioner accepts that the potential prejudice described by the public authority generally relates to the interests which the exemption contained at section 31(1)(a) is designed to protect. Specifically, in terms of the likely prejudice to the ongoing police investigation, the consequent likely effect of impeding the investigation would be; prejudice to the prevention or detection of crime, both of which are interests relevant to the exemption.

33. The Commissioner is satisfied that the prejudice alleged by the public authority is real and of substance, and there is a causal relationship between the disclosure of the requested information and the prejudice which the exemption is designed to protect. She must however establish whether disclosure would be likely to result in the prejudice alleged (ie the third criterion).

34. The Commissioner has examined the withheld information and she accepts it would give a useful indication of the robustness of the public authority's defences against cyber attacks. She is satisfied that malicious actors could easily deduce from the information whether an attack they had initiated has been successful. They would also have a perception of the success rate for a specific type of attack they might want to initiate in future which could increase the frequency of certain attacks and consequently the likelihood of success. She also accepts that the information would be useful to malicious actors when combined with other intelligence, gathered lawfully or not. The information in conjunction with other intelligence could provide a malicious actor with valuable insight into the public authority's security posture, its level of resilience and its perceived strengths and weaknesses.

35. The Commissioner accepts that it would at least make it difficult in principle to refuse to disclose information pursuant to a similar request in future. Such an outcome is therefore also likely to increase the

intelligence available to malicious actors and enable them to establish whether there certain types of attacks have a greater chance of success.

36. Consequently, she has concluded that disclosing the withheld information would pose a real and significant risk of prejudice to the prevention or detection of cyber related offences/infringements in particular, and crimes more generally.

37. Therefore, the public authority was entitled to engage the exemption at section 31(1)(a).

Balance of the public interest

38. The exemption at section 31(1)(a) is qualified by the public interest test set out in section 2(2)(b) FOIA. Therefore, the Commissioner must determine whether in all the circumstances of the case, the public interest in maintaining the exemption outweighs the public interest in disclosure.

39. The Commissioner considers that the complainant has made a strong case for releasing the information in the public interest. She accepts that there is a public interest in being able to assess the extent to which the significant sums of money spent and budgeted on cyber security is having an impact. However, she does not consider that it is possible to extrapolate anything conclusive in this regard from the limited amount of information in scope. Nevertheless, she considers that the information held by the public authority would provide a snapshot (albeit limited in relation to this specific public interest) of the robustness or otherwise of the public authority's defences against cyber attacks.

40. However, in the circumstances, she considers that there is a significant public interest in maintaining the exemption. There is a significant public interest in her view in withholding information that would pose a real and significant risk to the integrity of the public authority's IT system and consequently the information that it holds. There is also a strong public interest in withholding information that would otherwise prejudice the prevention or detection of crime.

41. She has therefore concluded that in all the circumstances of the case the public interest in maintaining the exemption outweighs the public interest in disclosing the withheld information. The public authority was entitled to rely on the exemption at section 31(1)(a).

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: 0300 1234504
    Fax: 0870 739 5836
    Email: GRC@hmcts.gsi.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 .....

Gerrard Tracey
Principal Adviser
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF