

**Reference: 2024-032**

Thank you for your email in which you requested the following information under the Freedom of Information Act 2000 (FOIA):

1. **How regularly do you perform Disaster Recover exercises based on a Cyber Breach use case, which involves recovery of data and servers from backups, and are these exercises performed manually or automated?**
  - a. **Quarterly**
  - b. **Bi-annually**
  - c. **Annually**
  - d. **Other – please specify**
  
2. **Within the last twelve months, have you proven that your current data and server backup and recovery solution can recover all your critical business services' (typically 30-40% of all infrastructure) within your organisations Recovery Time Objectives and Recovery Point Objectives?**
  
3. **What is your level of confidence that your backups are protected sufficiently such that, as part of a sophisticated cyber breach which initially targets backups prior to compromising production data, you can fully recover?**
  - a. **Extremely confident**
  - b. **Somewhat confident**
  - c. **Neither confident nor unconfident**
  - d. **Somewhat unconfident**
  - e. **Extremely unconfident**
  
4. **Is your department actively using any software which is no longer supported by the developer of that software? (Software which no longer receives updates or patches from the developer.) For example, an old version of Windows.**

**Response**

Please see below our response to your questions in the order asked.

**Questions 1, 2 & 3**

The information you have requested is exempt from release under section 31(1) of the FOIA.

Section 31(1)(a)(b) and (c) provides that:

*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:*

**How the exemption is engaged**

As a law enforcement agency, the SFO holds highly sensitive information which is of interest to others, including those we investigate. Releasing detailed information about the SFO's IT systems and tools could therefore compromise our ability to protect SFO investigative material and information systems, thereby prejudicing the interests at (a), (b), and (c) above.

**The public interest test**

Section 31(1) is a qualified exemption and requires consideration of whether, in all the circumstances of the case, the public interest in exempting this data outweighs the public interest in disclosing it. More information about exemptions in general and the public interest test is available on the ICO's website at [www.ico.org.uk](http://www.ico.org.uk).

It is recognised that there is a general public interest in publicising information about the SFO, so that the public knows that serious fraud, bribery, and corruption are being investigated and prosecuted effectively, and so that the public can be reassured about the general conduct of our organisation and how public money is spent.

However, following our consideration of the public interest in releasing this information, we consider that the stronger interest lies in maintaining the exemption at section 31(1) of the FOIA. Primarily, the risk that this information could pose to the SFO's security systems against which it is essential to safeguard given the highly sensitive nature of the information held as a law enforcement agency. Releasing sensitive information regarding IT software risks compromising the SFO's ability to provide and maintain data security for the cases at pre-investigation, investigation, prosecution stages and beyond.

Having considered the opposing arguments, I believe that the stronger public interest lies in exempting the information from release.

#### **Question 4**

The Serious Fraud Office (SFO) neither confirms nor denies whether it holds information falling within the description specified in your request. The duty in Section 1(1)(a) of the FOIA does not apply, by virtue of sections 30(3) and 31(3) of that Act. Nothing in my reply should be taken as an indication that the information you requested is or is not held by the SFO.

*Section 30 (3) provides that:*

*The duty to confirm or deny does not arise in relation to information which is (or if it were held by the public authority would be) exempt information by virtue of subsection (1) or (2).*

*Section 30 (1) provides that:*

*(1) Information held by a public authority is exempt information if it has at any time been held by the authority for the purposes of—*

*(a) any investigation which the public authority has a duty to conduct with a view to it being ascertained—*

*(i) whether a person should be charged with an offence, or*

*(ii) whether a person charged with an offence is guilty of it,*

*(b) any investigation which is conducted by the authority and in the circumstances may lead to a decision by the authority to institute criminal proceedings which the authority has power to conduct, or*

*(c) any criminal proceedings which the authority has power to conduct.*

*Section 31(3) provides that:*

*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).*

*Section 31(1)(a)-(c) provides that:*

*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.*

### How the exemptions are engaged

#### Section 30(3)

Section 30(1) exempts any information held by a public authority if it has at any time been held by the authority for the purposes of (b) any investigation which is conducted by the authority, and in the circumstances may lead to a decision by the authority to institute criminal proceedings which the authority has power to conduct.

Section 30(3) allows the respondent to “neither confirm nor deny” whether any information is held in relation to the question where the requested information, if held, is described by section 30(1).

It is clear that your questions relate to information that you believe may be held by the SFO for the purposes of criminal investigations, as set out in section 30(1)(b), meaning the SFO must neither confirm nor deny whether the information is held in accordance with section 30 of the FOIA (2000).

#### Section 31(3)

Section 31 permits the exemption of information from release when the “disclosure of which would, or would be likely to, prejudice certain specified law enforcement matters”. This exemption is engaged in this response because of the prejudice or likely prejudice caused by the cumulative effect of disclosing information in response to a series of requests of a similar nature (the ‘precedent effect’).

The SFO investigates and prosecutes only the most serious or complex fraud, bribery and corruption. We have a relatively small caseload and routinely disclosing information about our cases risks creating an increasingly detailed picture of how the SFO decides to deploy its resources within and between cases. The SFO routinely publishes its Annual Report and Accounts, and appropriate information regarding active cases and new investigations can be found there. To release details that go beyond this already disclosed information would set a precedent that could risk our operational integrity.

#### The public interest test

Sections 30(3) and 31(3) are qualified exemptions and require consideration of whether, in all the circumstances of the case, the public interest in maintaining the exclusion of the duty to confirm or deny outweighs the public interest in disclosing whether the public authority holds the information. More information about exemptions in general and the public interest test is available on the ICO’s website at [www.ico.org.uk](http://www.ico.org.uk).

It is recognised that there is a general public interest in publicising the work of the SFO, so that the public knows that serious fraud, bribery and corruption are being investigated and prosecuted effectively and so that the public can be reassured about the general conduct of our organisation and how public money is spent.

However, it is also recognised that it is in the public interest to safeguard the investigatory process and that investigating bodies should be afforded the space to determine the course of an investigation. On some occasions, releasing information about what is held or not held by law enforcement bodies would be detrimental to that process. To confirm or deny whether the information you have requested is held would, for reasons outlined earlier, be likely to prejudice the SFO’s conduct of an ongoing criminal investigation/ability to tackle and prevent serious crime. This would not be in the public interest as the right of access to information should not undermine the investigation and prosecution of criminal matters.

Having considered the opposing arguments, I am of the view that the benefits of confirming whether or not the information is held are outweighed by the disbenefits and thus the public interest favours maintaining the exclusion of the duty to confirm or deny whether information is held.