Freedom of Information Act 2000 (FOIA)

Decision notice

Date:	**11 November 2025**
Public Authority:	**Department for Science, Innovation & Technology**
Address:	**100 Parliament Street** **London** **SW1A 2BQ**

Decision (including any steps ordered)

1. The complainant made a three-part request for specific information associated with the 2024 General Election. The Department for Science, Innovation & Technology ('DSIT') said it did not hold the requested information for **part 1** of the request. For **parts 2 and 3**, DSIT refused to provide the information, citing section 24(1) of FOIA – the exemption for national security. The complainant was only concerned with DSIT's application of section 24(1) of FOIA.

2. During the course of the Commissioner's investigation, DSIT revised its position and provided the information at **part 3** of the request. For **part 2** of the request, DSIT disclosed the previously withheld report with redactions under section 24(1) of FOIA. The complainant remained dissatisfied with the redacted material within the disclosed report.

3. The Commissioner's decision is that DSIT has properly relied on section 24(1) of FOIA to withhold the redacted information within the disclosed report.

4. No steps are required as a result of this notice.

Background

5. DSIT's role is described here as being to:

> "Accelerate innovation, investment and productivity through world-class science, ensure that new and existing technologies

> are safely developed and deployed across the UK and drive forward a modern digital government for the benefit of its citizens."

6. DSIT is a ministerial department, supported by various agencies and public bodies.

7. The NSOIT (National Security Online Information Team) sits within DSIT and:

> "leads the UK government's operational response to information threats online, and ensures the government takes necessary steps to identify and respond to acute misinformation (ie incorrect or misleading information) and disinformation (ie information which is deliberately created to cause harm) that pose risks to UK national security and public safety". (National Security Online Information Team: privacy notice - GOV.UK)

Request and response

8. On 15 January 2025, the complainant wrote to DSIT and requested information in the following terms (numbers added for ease of reference):

> "I am writing to request the following information relating to NSOIT:
>
> 1. A copy of all NSOIT reports related to the General Election produced by the unit in-house in the week commencing June 24, 2024
>
> 2. A copy of all reports related to the General Election produced in the week commencing June 24, 2024 produced by Crisp Thinking for NSOIT
>
> 3. The number of referrals to social media companies for potential terms of service breaches made in June 2024 I would like all document [sic] sent electronically please.
>
> Under Section 16 of the Act I also ask that if this request cannot be fulfilled under the legislation, that you offer advice and assistance to help the request comply with the act. I look forward to your response within 20 working days."

9. DSIT responded on 30 January 2025. For **part 1** of the request, DSIT said no information was held, explaining that NSOIT had not produced any reporting during this period as it was supporting the cross-government election. For **part 2**, DSIT explained that all but one report

had been deleted in line with NSOIT's document retention policy. It refused to provide the remaining report, citing section 24(1) of FOIA – the national security exemption. For **part 3** of the request, DSIT provided the figure of 180 referrals for the whole of 2024, but withheld the specific number for June 2024, citing section 24(1) of FOIA.

10. The complainant requested an internal review on 3 February 2025, in relation only to **parts 2 and 3** of his request, raising a number of points.

11. Following its internal review, DSIT wrote to the complainant, late, on 1 April 2025. It maintained its original position, and responded to the points raised by the complainant.

Scope of the case

12. The complainant contacted the Commissioner on 3 April 2025 to complain about the way his request for information had been handled.

13. The Commissioner relayed the complainant's grounds of complaint to DSIT as part of his investigation.

14. During the course of the Commissioner's investigation, DSIT revised its position. On 24 October 2025, DSIT disclosed the requested Crisp Thinking Report with redactions under section 24(1) of FOIA (**part 2** of the request). For **part 3** of the request, DSIT now provided the figure of ten for June 2024, previously withheld under section 24(1) of FOIA.

15. The Commissioner sought the complainant's view of DSIT's revised position, which was provided on 30 October 2025. He remained dissatisfied with what he described as DSIT's "overzealous application" of section 24(1) to the redactions within the disclosed Crisp Thinking report (ie **part 2** of his request).

16. Having secured consent, the Commissioner relayed the complainant's view to DSIT on 4 November 2025. DSIT told the Commissioner it considered it had already addressed these points and did not wish to submit any further comments.

17. The Commissioner has taken the complainant's comments, including those about specific redactions, into account in reaching his decision.

18. In this case, the Commissioner has considered whether DSIT was entitled to rely on section 24(1) of FOIA to withhold the redacted information within the disclosed Crisp Thinking report (at **part 2** of the request). He has viewed the unredacted report in full.

Reasons for decision

Section 24 – national security

19. Section 24(1) of FOIA 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."

20. 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.

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

22. At internal review, DSIT responded to each of the complainant's concerns. It also acknowledged it had not sufficiently demonstrated how the release of the Crisp Thinking report (as was the case at that point), would prejudice national security. As a result, DSIT said it had re-evaluated the public interest test and set out those arguments (see paragraph 35 below for further details).

23. The Commissioner has reproduced some of the rationale for DSIT relying on section 24(1), albeit that at that point, the entire report had been withheld. DSIT told the complainant that:

> "The [then fully] withheld report relates to suspected foreign state interference. Disclosing its contents would provide hostile states with insights into the topics and narratives NSOIT is monitoring, allowing them to adapt their tactics to avoid detection. This would significantly weaken the UK's ability to identify and counter disinformation and safeguard national security, including the UK's democratic processes. The report contains sensitive information that cannot be redacted in a way that would allow partial disclosure without compromising national security."

And

> "In this case, the [then fully] withheld report includes information on suspected foreign interference and specific narratives targeted at the UK. If released, this could help foreign adversaries refine their tactics and increase the effectiveness of their disinformation campaigns targeting the UK, with the aim of causing harm to its institutions and the public."

24. In its submissions to the Commissioner, DSIT explained 'in confidence' about how the redactions had been applied and marked up. The Commissioner has respected DSIT's position and has not reproduced this explanation in this notice. DSIT also, again in confidence, set out its rationale for applying the redactions and citing section 24(1) of FOIA.

25. DSIT requested that parts of its submissions were not reproduced in this notice due to the risk to national security, a position which the Commissioner has respected. He has taken those confidential arguments into consideration.

26. DSIT explained that the redacted material falls into the definition of of section 24(1) of FOIA, a position the Commissioner agrees with. DSIT also said it was relying on the lower threshold of 'would be likely' to prejudice national security, should the redacted material within the report be disclosed.

27. Having considered the rationale, the Commissioner is satisfied that DSIT's arguments show that withholding the redacted information within the disclosed report is reasonably necessary for the purposes of safeguarding national security.

28. It follows that the Commissioner is therefore satisfied that section 24(1) of FOIA is engaged.

Public interest test

29. Section 24(1) is subject to a public interest test, meaning that even though the exemption is engaged, the information can only be withheld if the public interest in maintaining the exemption outweighs the public interest in disclosure.

Public interest arguments in favour of disclosing the information

30. The complainant submitted the following arguments in favour of disclosure, summarised below:

    - DSIT's public interest arguments were too broad and generic, imcluding those on the mosaic effect.
    - DSIT had relied on arguments it had put forward in relation to other complaints, such that it appeared to the complainant that DSIT had not given individual consideration to the current case.
    - Disclosure of the entire Crisp Thinking report would reassure and inform the public about disinformation and the steps taken to protect the democratic process in the UK.
    - There is also a specific public interest in this information that is very strong, relating to transparency around NSOIT contractor activities during elections.

31. Following partial disclosure of the redacted Crisp Thinking report, DSIT recognised the following in favour of disclosing the remaining redacted material, and advised the complainant accordingly:

    - **Promotes government transparency**: The department recognise that the release of this information would promote government transparency which would allow the public to scrutinise the decisions and operations taken by the department. This would help form trust between the department and the public and allow the public to satisfy themselves that decisions are being taken with the best information available.
    - **Enhances public understanding**: The department recognises that the release of this information would provide an enhanced understanding of inner government workings. If the public are aware of policy discussions it can lead to more informed and effective policies, as it allows for diverse perspectives and expertise to be considered.
    - **Facilitate public debate**: The department recognise that releasing this information would help with actively supporting public debate by equipping individuals and organisations with

authoritative data to inform their perspectives. Transparent access enables robust discussion, encourages diverse viewpoints, and allows the public to engage meaningfully with departmental decisions. This would likely strengthen democratic engagement and empowers citizens to contribute constructively to policy development and government accountability.

32. At internal review, DSIT revisited its public interest arguments in light of the complainant's comments, (set out in his internal review request), and acknowledged the following in favour of disclosing the redacted material:

- The department recognises that there may be public interest in the release of this type of information, as it would increase transparency and openness within government, which increases public trust in government.

- The release of this information could help to increase public trust in government activities, especially concerning online mis/disinformation. It would provide insight into how the government is addressing these issues, fostering greater public confidence in the decision-making process and the actions taken to safeguard national security and protect the public.

- Public interest in disinformation and its impact on democracy has been growing. Disclosure of this information would offer the public confidence that the government is taking necessary steps to mitigate the risks associated with online mis/disinformation.

33. In its submissions to the Commissioner, DSIT added the following argument:

> **Deters misuse of power**: Making information available to the public is a crucial safeguard against the misuse or abuse of governmental powers, especially in sensitive areas like surveillance, intelligence, and counter-disinformation. Transparency ensures that government actions are open to scrutiny by Parliament, oversight bodies, and the public, making it harder for individuals or institutions to act outside legal or ethical boundaries. This openness encourages careful, proportionate use of authority and reassures the public that robust checks and balances are in place. Ultimately, the possibility of disclosure acts as a powerful deterrent, reinforcing accountability and upholding the integrity of government operations.

Public interest arguments in favour of maintaining the exemption

34. Against disclosure of the redacted material within the report, DSIT advised the complainant as follows:

- **Protecting intelligence sources**: The department recognises that safeguarding the identities and operational details of intelligence sources is paramount for the ongoing effectiveness of national security. Disclosure of information under section 24(1) would likely inadvertently reveal sensitive information that might be used to identify individuals or organisations working with security services. Even seemingly benign details could, when pieced together, compromise the anonymity and safety of operatives and informants. The risk of exposing such sources not only endangers their personal safety but also jeopardises the ability of security agencies to recruit future assets. If adversaries detect vulnerabilities or patterns in operational approach, it would likely render critical intelligence efforts ineffective. The resulting damage to intelligence gathering capabilities would have a direct impact on the nation's ability to pre-empt security threats. Therefore, withholding information under section 24(1) is essential to protect intelligence sources and, by extension, maintain the integrity of national security operations.

- **Preventing hostile exploitation**: The department recognises that disclosure of information exempts under section 24(1) risks providing hostile actors—whether foreign governments, organised criminals, or terrorist groups—with valuable insights into national security operations and strategies. Even limited releases could enable adversaries to deduce operational methods, security weaknesses, or defensive priorities. Such knowledge might be exploited to mount attacks, evade surveillance, or disrupt national security measures. The rapid evolution of digital analysis tools means that adversaries can quickly process and correlate seemingly disparate data points. The consequences of such exploitation would likely not only threaten the immediate objectives of national security services but could also undermine public confidence in the government's ability to safeguard its citizens. Withholding information is therefore a necessary precaution to prevent hostile entities from gaining any advantage that could endanger national interests and the safety of the population.

- **Maintaining operational effectiveness**: The department recognises that national security agencies must be able to operate flexibly and adapt to evolving threats without the risk of their methods, plans, or capabilities being exposed. Releasing information under section 24(1) would likely hinder operational

versatility by revealing patterns of activity, resource deployment, or technological limitations. Adversaries could exploit this knowledge to circumvent protective measures, neutralise surveillance, or disrupt investigations. Additionally, the perception that sensitive operational details might be disclosed could deter cooperation from other agencies or allied nations, weakening the overall security network. Effective security strategy relies on the element of unpredictability and the assurance that operational information remains confidential. Therefore, withholding information is necessary to preserve the effectiveness and adaptability of national security operations in a constantly changing threat landscape.

- **Implications for national infrastructure**: The department recognise that the security and resilience of national infrastructure are linked to the confidentiality of information relating to its operation and protection. Disclosure of details concerning digital services, structural assets, or operational protocols would likely expose potential weaknesses. Such vulnerabilities, once identified, might be exploited to cause disruption, affect essential services, or undermine public safety. Maintaining confidentiality helps to prevent widespread interruptions or disruptions that could impact daily life or lead to broader risks for citizens. When information is withheld, it contributes to the safeguarding of crucial networks and the reliability of services that underpin the well-being and security of the population. Ultimately, the initiative-taking protection of infrastructure-related details is an essential component of effective risk management and is integral to DSIT's approach to ensuring robust, uninterrupted service provision across all areas of national infrastructure.

- **The mosaic effect and security considerations**: The department recognises that the aggregation of multiple, individually innocuous pieces of information would likely result in the unintended exposure of sensitive details, a phenomenon often referred to as the "mosaic effect." Even if each separate data point appears harmless, when pieced together, they can provide a comprehensive view of operational capabilities, vulnerabilities, or protective strategies. This unintended synthesis of data can be exploited by those seeking to circumvent security measures, disrupt operations, or gain illicit advantages. Withholding specific types of information reduces the risk of such aggregation, ensuring that critical operational details remain protected from misuse. The departments cautious approach to disclosure supports the long-term interests of both security and public safety, by reducing the likelihood of exploitation through information synthesis.

35. Having revisited the public interest considerations in light of the complainant's arguments raised at internal review, DSIT provided the following arguments against disclosure:

- The requested information provides operational insights into the UK government's counter-disinformation efforts, including sensitive details of the work undertaken by NSOIT. Releasing this information could aid hostile actors in understanding the UK's methods and strategies, allowing them to identify and exploit potential operational vulnerabilities which could harm national security.

- There is a risk that foreign states or other malign actors could use this information to better target mis and disinformation campaigns aimed at UK audiences. This could increase the effectiveness of such campaigns, amplifying risks to national security and potentially harming UK institutions and citizens.

- Specific details related to the UK's capabilities in identifying and analysing mis and disinformation are highly sensitive. If disclosed, this information would give hostile actors an understanding of the UK's strategies and response mechanisms, allowing them to better understand how they could counteract those measures. This could potentially exacerbate the spread of harmful disinformation to UK audiences.

- By withholding information related to the volume of referrals or other specific operational details, the department prevents hostile states or malign actors from gaining intelligence that could be used to disrupt efforts to protect the UK from online threats. Disclosure of this data could weaken the government's ability to identify and respond to future disinformation incidents effectively.

- The department recognises that hostile actors often go to great lengths when planning potential attacks and that seemingly harmless information when compiled together with other information obtained from different sources could result in individuals gathering substantial information to execute attacks on the department or country. This would not be in the public interest.

- The release of granular data, such as specific referrals to social media platforms, would provide hostile states or actors with the ability to gauge the UK's priorities and resources, revealing tactical and strategic decisions about how the government responds to threats. This could compromise government's ability to protect the UK from future disinformation campaigns.

36. In its submissions to the Commissioner, DSIT provided the following arguments against disclosing the remaining redacted information:

> **Reveals monitoring capabilities and methods**: The Crisp Thinking report outlines the tools and techniques NSOIT uses to monitor social media platforms for mis- and disinformation. These include keyword tracking, behavioural analytics, and platform specific strategies. Revealing such capabilities would likely allow hostile actors to understand how monitoring is conducted and adapt their tactics to avoid detection. They could alter language, shift platforms, or mimic benign behaviours, making it harder to identify threats. This would reduce the effectiveness of current systems and force NSOIT to overhaul its methods, delaying responses during critical periods such as local and general elections. Disclosure could also expose the limitations of existing tools, encouraging adversaries to exploit gaps. Additionally, vendors may be discouraged from future collaboration if proprietary technologies are publicly revealed, fearing reputational damage or misuse. The confidentiality of these capabilities is essential to maintaining strategic advantage. Once adversaries understand how monitoring works, they can engineer content to bypass detection. This would likely compromise the United Kingdom's ability to respond to disinformation threats, weakening national security and undermining public confidence in protective measures.
>
> **Discloses threat identification criteria**: The report contains examples of flagged posts or accounts, revealing the criteria NSOIT uses to identify harmful content. The criteria includes specific keywords, behavioural patterns, or network indicators. If disclosed, hostile actors could reverse engineer these thresholds to craft disinformation that avoids detection. This would likely enable more sophisticated and evasive influence operations, particularly during democratic events such as general elections. Adversaries could exploit this knowledge to spread harmful content that appears legitimate, undermining public trust and electoral integrity. Disinformation campaigns are increasingly tailored to exploit known weaknesses in detection systems. Revealing identification criteria would force NSOIT to recalibrate its methods, diverting resources and potentially leaving gaps during the transition. It would create a reactive posture, where adversaries continuously adapt faster than defences can evolve. The criteria used to flag threats are a cornerstone of NSOIT's operational effectiveness. Protecting them is essential to maintaining a proactive stance against disinformation. Disclosure would likely compromise this posture and increase the risk of undetected threats and weakening the United Kingdom's ability to safeguard national security.

Compromises live operational efforts: The Crisp Thinking report focuses on the week of the general election, a period when NSOIT was engaged in actively identifying and responding to information threats to the UK during the 2024 general election. Disclosure of the report would likely reveal real time response strategies, including how threats were identified, prioritised, and addressed. It would further expose coordination mechanisms and the speed of operational decision making. Hostile actors could use this information to time their campaigns for maximum impact, exploiting known response delays or procedural steps. This would likely disrupt the integrity of future electoral process and embolden adversaries. Revealing operational details during or shortly after a critical democratic event would compromise the United Kingdom's ability to respond effectively to future threats of a similar nature. It could also signal to adversaries that the government's defences are transparent and vulnerable to manipulation. Disclosure would likely undermine NSOIT's agility and effectiveness, forcing changes to operational protocols and reducing confidence in future response capabilities. Maintaining confidentiality around live operations is essential to preserving national security and ensuring the resilience of democratic institutions.

Enables hostile intelligence mapping: The Crisp Thinking report contains detailed insights into NSOIT's operational priorities, resource allocation, and strategic focus. If disclosed, hostile intelligence services could use this information to map the United Kingdom's counter disinformation infrastructure. They could identify which platforms are monitored most closely, which behaviours trigger intervention, and where gaps may exist. This would likely enable adversaries to design campaigns that exploit under resourced areas or avoid detection altogether. Additionally, patterns in response strategies could be reverse engineered to anticipate government actions, allowing adversaries to stay one step ahead. Intelligence mapping is a known tactic used by hostile states to undermine national security. The report could serve as a valuable asset in this effort, providing a comprehensive view of the United Kingdom's defences. Once adversaries understand how NSOIT operates, they can tailor their influence operations to bypass scrutiny and maximise disruption. Protecting the confidentiality of strategic and operational data is essential to maintaining a resilient national security posture. Disclosure would likely assist adversaries in planning future campaigns, increasing the risk of successful disinformation and weakening the United Kingdom's defences.

Damages platform cooperation and trust: NSOIT's success in countering disinformation depends on strong cooperation with

social media platforms. These relationships rely on discretion and mutual trust. As the Crisp Thinking report includes internal assessments of content on social media platforms its disclosure could damage these partnerships. Platforms may fear reputational harm or public backlash, leading to reduced willingness to collaborate. This would likely result in slower responses to harmful content, limited data sharing, and weakened joint operations. During high-risk periods such as elections, delays in platform cooperation could allow disinformation to spread unchecked. Furthermore, platforms may question the government's ability to protect sensitive information, potentially withdrawing from voluntary arrangements. This would leave NSOIT with fewer tools to counter threats effectively. Damaging these relationships would erode a critical component of the United Kingdom's disinformation response strategy. The long-term impact could include diminished operational capacity and reduced agility in responding to emerging threats. Withholding elements of the report is necessary to preserve trust and ensure continued cooperation. Disclosure would likely compromise these partnerships, undermining national security and the government's ability to protect democratic processes.

Suppresses future reporting and oversight: Disclosure of sensitive content from the Crisp Thinking report could discourage NSOIT staff from documenting operational insights in future reports. Fear of public exposure may lead to self-censorship, where teams avoid recording detailed observations or assessments. This would likely erode institutional memory and hinder the ability to learn from past operations. Effective counter disinformation work depends on honest reporting and continuous improvement. If staff sanitise or omit critical information, oversight mechanisms such as audits and reviews become less effective. This weakens accountability and allows operational blind spots to persist. The long-term consequence is a decline in strategic adaptability, as lessons are lost and errors repeated. Protecting the confidentiality of internal reporting is essential to maintaining a resilient and responsive national security posture. Disclosure would likely suppress the quality and depth of future documentation, reducing NSOIT's ability to evolve and respond to emerging threats. Withholding some parts of the report ensures that teams can continue to report candidly, supporting robust oversight and effective counter disinformation operations that protect the United Kingdom's democratic institutions.

Enables mosaic intelligence gathering: Even if the Crisp Thinking report appears benign on its own, it could contribute to a mosaic of intelligence when combined with other public or

leaked information. Hostile actors often use open-source techniques to assemble fragmented data into a coherent picture of government operations. The report contains information highlighting operational timelines, platform focus areas, or examples of flagged content. When aggregated with other sources, this could reveal NSOIT's strategic priorities, response patterns, and vulnerabilities. The mosaic effect is particularly dangerous because it allows adversaries to infer sensitive information without accessing any single classified document. Intelligence agencies routinely warn against piecemeal disclosures that, when combined, expose more than intended. In this case, the report could serve as a critical puzzle piece in adversarial efforts to understand and exploit the United Kingdom's counter disinformation infrastructure. The risk is cumulative and difficult to reverse. Once adversaries gain a clearer picture of operations, they can tailor campaigns to avoid detection and maximise disruption. Withholding the remainder of the report is necessary to prevent strategic exploitation and preserve the confidentiality of national security operations.

37. DSIT also provided a further argument against disclosure in confidence, which the Commissioner has taken into account.

Balance of the public interest

38. DSIT provided the following balance test arguments:

> "In considering the public interest, the department fully acknowledges the vital role of transparency, accountability, and open debate in upholding democratic values. Public access to government information strengthens scrutiny, deters misuse of power, and fosters public trust in institutions. However, this must be carefully balanced against the significant risks posed by releasing sensitive operational details.
>
> Disclosing such information would likely negatively impact the UKs national security by revealing the monitoring capabilities, criteria for threat identification, and real-time response strategies. These disclosures would aid hostile actors in evading detection, adapting their tactics, or mapping the government's defences, thereby increasing the risk of sophisticated disinformation campaigns and weakening the nation's ability to protect itself. Furthermore, releasing confidential details could damage essential cooperation with external partners, undermine internal reporting candour, and erode public confidence in the government's ability to protect both civil liberties and democratic processes.

> After weighing these considerations, the department finds that the risks and potential harms associated with disclosure are immediate and substantial. The imperative to maintain an effective, adaptable, and secure counter-disinformation strategy outweighs the benefits of further transparency in this instance. Therefore, withholding the information is considered the most responsible course of action to safeguard the nation and uphold public confidence."

39. The Commissioner appreciates that there is a clear and valid public interest in the disclosure of **all** the information within the Crisp Thnking report. There is a legitimate public interest in the disclosure of information which can inform the public about the measures DSIT is taking to counteract disinformation and to protect the UK's democratic process and national security.

40. However, the Commissioner is also mindful that the very existence of DSIT and NSOIT and their activities go partway to reassuring the public that measures are being taken to protect the election process and national security.

41. The Commissioner also notes that DSIT has now disclosed the requested report, minus the parts that have been identified as being a risk to the UK's national security. He considers that this goes some way towards meeting the transparency and openness requirements, and also informs the public about the hoax video with the UK Foreign Secretary.

42. The Commissioner recognises the very strong and weighty public interest in protecting the UK's national security. Whilst disclosure of the remaining requested information could further inform the public about the specific steps and activities taken to maintain national security, disclosure of such details also risk undermining the UK's national security.

43. The Commissioner considers that the benefit that would flow from disclosure would not justify the potential harm to the UK's national security. In view of this the Commissioner agrees with DSIT that the public interest favours maintaining the exemption at section 24(1) of FOIA.

Right of appeal

44. 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)
    General Regulatory Chamber
    PO Box 11230
    Leicester
    LE1 8FQ

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

45. 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.

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

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