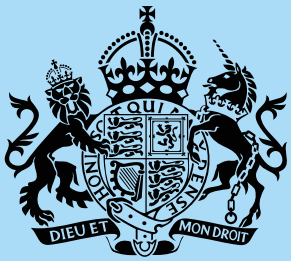


# Intelligence and Security Committee of Parliament

## Annual Report 2023–2025

Chairman:
The Rt Hon. the Lord Beamish PC

HC 1544


# Intelligence and Security Committee of Parliament

# Annual Report 2023–2025

Chairman:
The Rt Hon. the Lord Beamish PC

Presented to Parliament pursuant to sections 2 and 3 of the Justice and Security Act 2013

Ordered by the House of Commons to be printed on 15 December 2025

HC 1544



Any enquiries regarding this publication should be sent to us via our webform at isc.independent.gov.uk/contact

This publication is also available on our website at: isc.independent.gov.uk

ISBN 978-1-5286-6092-1

E03492825 12/25

Printed on paper containing 40% recycled fibre content minimum

Printed in the UK by HH Associates Ltd. on behalf of the Controller of His Majesty's Stationery Office

# THE INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT

*The Rt Hon. the Lord Beamish PC (Chairman)*

| | |
|---|---|
| *The Baroness Brown of Cambridge DBE FREng FRS* | *Jessica Morden MP* |
| *Peter Dowd MP* | *Derek Twigg MP* |
| *Richard Foord MP* | *Admiral The Rt Hon. the Lord West of Spithead GCB DSC PC* |
| *The Rt Hon. Sir John Hayes CBE MP* | *The Rt Hon. Sir Jeremy Wright KC MP* |

This Report summarises the work of the Intelligence and Security Committee of Parliament (ISC) for the period from April 2023 to March 2025 and therefore also covers work carried out by the previous Committee, which sat from July 2020 to May 2024.*

The Intelligence and Security Committee of Parliament (ISC) is a statutory committee of Parliament that has responsibility for oversight of the UK Intelligence Community. The Committee was originally established by the Intelligence Services Act 1994 and was reformed, and its powers reinforced, by the Justice and Security Act 2013.

The Committee oversees the intelligence and security activities of the Agencies,† including the policies, expenditure, administration and operations of MI5 (the Security Service), MI6 (the Secret Intelligence Service or SIS) and GCHQ (the Government Communications Headquarters). The Committee also scrutinises the work of other parts of the Intelligence Community, including: the Joint Intelligence Organisation (JIO) and the National Security Secretariat (NSS) in the Cabinet Office; Defence Intelligence (DI) in the Ministry of Defence (MoD); and Homeland Security Group (HSG) in the Home Office.

The Committee consists of nine Members drawn from both Houses of Parliament. Members are appointed by the Houses of Parliament, having been nominated by the Prime Minister in consultation with the Leader of the Opposition. The Chair of the Committee is elected by its Members.

* The membership of the previous Committee during the period covered by this Report was: The Rt Hon. Sir Julian Lewis MP (Chairman), Dame Angela Eagle MP (from 15 January 2024), The Rt Hon. Maria Eagle MP (until 8 September 2023), The Rt Hon. Sir John Hayes CBE MP, The Rt Hon. Kevan Jones MP, Colonel The Rt Hon. Bob Stewart DSO MP, The Rt Hon. Owen Thompson MP, The Rt Hon. Theresa Villiers MP, Admiral The Rt Hon. the Lord West of Spithead GCB DSC PC, and The Rt Hon. Sir Jeremy Wright KC MP.

† Throughout the Report, the term 'Intelligence Community' is used to refer to the seven organisations that the Committee oversees. The term 'Agencies' (or, on occasion, 'the intelligence Agencies') refers to MI5, SIS and GCHQ as a collective; and the term 'Departments' refers to the intelligence and security parts of the Ministry of Defence, Cabinet Office and the Home Office (DI, JIO, NSS and HSG) as a collective, unless specified otherwise.

The Members of the Committee are subject to section 1(1)(b) of the Official Secrets Act 1989 and are routinely given access to highly classified material in carrying out their duties. The Committee sets its own agenda and work programme, taking evidence from Government Ministers, the Heads of the intelligence and security Agencies, senior officials, experts and academics as required. Its Inquiries tend to concentrate on current events and issues of concern, and therefore focus on operational[‡] and policy matters, while its Annual Reports address administration and finance.

ISC Reports can contain highly classified material, which would damage the operational capabilities of the intelligence Agencies if it were published. There is therefore a well-established and lengthy process to prepare the Committee's Reports ready for publication. The Report is checked to ensure that it is factually correct (i.e. that the facts and figures are up to date in what can be a fast-changing environment). The Intelligence Community may then, on behalf of the Prime Minister, request redaction of material in the Report if they consider that its publication would damage their work – for example, by revealing their targets, methods, sources or operational capabilities. The Committee requires the Intelligence Community to demonstrate clearly how publication of the material in question would be damaging since the Committee aims to ensure that only the minimum of text is redacted from a Report. Where the Committee rejects a request for material to be redacted, if the organisation considers that the material would cause serious damage to national security if published, then the Head of that organisation must appear before the Committee to argue the case. Once these stages have been completed, the Report is sent to the Prime Minister to consider. Under the Justice and Security Act 2013, the Committee can only lay its Reports before Parliament once the Prime Minister has confirmed that there is no material in them which would prejudice the discharge of the functions of the Agencies or – where the Prime Minister considers that there is such material in the report – once the Prime Minister has consulted the Committee and it has then excluded the relevant material from the Report.

The Committee believes that it is important that Parliament and the public should be able to see where information had to be redacted: redactions are clearly indicated in the Report by ***. This means that the published Report is the same as the classified version sent to the Prime Minister (albeit with redactions).

[‡] The Committee oversees operations subject to the criteria set out in section 2 of the Justice and Security Act 2013.

# CONTENTS

# THE WORK OF THE COMMITTEE

**The Intelligence and Security Committee of Parliament (ISC) is the only body that has regular access to protectively marked information that is sensitive for national security reasons, such that it is in a position to scrutinise effectively the work of the security and intelligence Agencies and of those parts of Departments whose work is directly concerned with intelligence and security matters.[1] The ISC is therefore an essential part of the UK democratic system, providing a vital check and balance to ensure that secret organisations and their activities are accountable to Parliament and the public for the action being taken in their name.**

1. This Report summarises the work of the Intelligence and Security Committee of Parliament (ISC) for the period from April 2023 to March 2025 in carrying out its oversight of the Intelligence Community.[2] (The Report is therefore historical in nature, and does not cover those developments since March 2025, including in relation to the Committee's resources, governance and remit. The Committee will update on these separately.)

2. The Report covers a two-year period (and spans two Committees) as the Committee was not able to issue an Annual Report in 2024, due to the dissolution of the previous Committee on 30 May 2024 ahead of the General Election, with the Committee not being reconstituted until 16 December 2024. The new Committee did issue a short public summary on 1 May 2025, to provide an update on the work the previous Committee had conducted before it was dissolved in May 2024.

3. **In our last Annual Report, we addressed the worrying lack of oversight of parts of other policy departments engaged in security and intelligence activities – and the impact on the assurances that can currently be provided to Parliament and the public regarding those activities. The impact of these matters has become more serious since then and, in conjunction with acute resourcing and governance issues in relation to the Committee's Office, has, together, at times left the Committee unable to perform its statutory functions. We address these issues later in this Report.**

## *Committee membership during the period covered by this Report*

4. The Rt Hon. Maria Eagle MP notified the Chairman on 8 September 2023 of her intent to step down from her role on the Committee. Following a consultation process, as set out in the Justice and Security Act 2013, Dame Angela Eagle MP was nominated for membership of the Committee by the Prime Minister, and was appointed as a Member of the Committee by the House of Commons on 15 January 2024.

5. On 30 May 2024, in accordance with the Justice and Security Act 2013, Members of the Committee vacated their posts upon the dissolution of Parliament prior to the July 2024 General Election.

[1] Other bodies such as the Investigatory Powers Commissioner's Office (IPCO) and the National Audit Office (NAO) have regular access to protectively marked information within their specific scrutiny and oversight functions.

[2] The term 'Intelligence Community' currently refers to the three intelligence Agencies (MI5, SIS and GCHQ) and the parts of those policy departments which deal with intelligence and security matters (the Ministry of Defence, Cabinet Office and Home Office).

6. The Committee was reconstituted on 16 December 2024. It held its inaugural meeting on 18 December 2024, at which Members elected the Rt Hon. the Lord Beamish PC as Chairman, under the Justice and Security Act 2013.

## *Work programme*

7. In carrying out its work during the period covered by this Report, the Committee:

- held 35 full Committee meetings, including evidence sessions with Government Ministers and senior officials from across the Intelligence Community;
- conducted one visit to the Intelligence Community;
- held bilateral discussions with its counterparts from the Parliament of Australia and the United States Congress, and with Ministers and legislators from Canada, New Zealand and the United States; and
- held two other meetings.

## *Reports*

### *China*

8. The Committee began an Inquiry into national security issues relating to China in March 2019. At the outset of this Inquiry, the Committee considered whether Huawei should be allowed to supply equipment for the UK's 5G telecommunications network, given the UK's over-reliance on Chinese technology, and released a statement urging that action be taken to address this. The Committee continued to take evidence for the Inquiry up to 2021,[3] considering the nature of the threat across a number of thematic areas.

9. The Report was published on 13 July 2023.[4] It considers the nature of the national security threat from China broadly, as well as in relation to three specific areas – Academia, Industry and Technology, and Civil Nuclear energy – together with an analysis of China's response to, and use of, the Covid-19 pandemic.

10. The Committee found that the UK is of significant interest to China when it comes to espionage and interference, given our close relationship with the United States, our membership of international bodies and the perception of the UK as an opinion-former. This would appear to place the UK just below China's top priority targets, as it seeks to build support for its current 'core interests' – to mute international criticism and gain economically. It is therefore China's global ambition to become a technological and economic superpower, on which other countries are reliant, that represents the greatest risk to the UK.

[3] The Committee began the Inquiry in 2019. Shortly afterwards followed: the dissolution of the Intelligence and Security Committee in November 2019 ahead of the General Election; a series of national lockdowns in 2020 and 2021 in the wake of the global Covid-19 pandemic; and the excessive delay in appointing a new Committee from December 2019 to July 2020. These events impeded the conclusion of the Inquiry and the publication of the final Report.

[4] *China*, HC 1605, 13 July 2023 (https://isc.independent.gov.uk/wp-content/uploads/2023/07/ISC-China.pdf).

11. China's state intelligence apparatus – almost certainly the largest in the world – targets the UK and its interests prolifically and aggressively, presenting a challenge for our Agencies to cover. The problem is further compounded by China's 'whole-of-state' approach, as Chinese state-owned and non-state-owned companies – as well as academic and cultural establishments and ordinary Chinese citizens – are liable to be willingly or unwillingly co-opted into Chinese espionage and interference operations overseas. Furthermore, much of the impact that China has on the UK's national security is overt – through its economic might, its takeovers and mergers, and its interaction with Academia and Industry – and its size, ambition and capability have enabled it to successfully penetrate every sector of the UK's economy.

12. The Government told the Committee that its response to this threat is "*robust*" and "*clear-eyed*".[5] However, the External Experts we spoke to were rather less complimentary, concluding that the Government has no strategy on China, let alone an effective one, and that it was singularly failing to deploy a 'whole-of-state' approach. Similarly, the Committee found that the level of resource dedicated to tackling the threat posed by China's 'whole-of-state' approach has been completely inadequate, and the slow speed at which strategies and policies are developed and implemented leaves a lot to be desired.

13. The Committee made a number of observations and recommendations in relation to the Government's approach to China – both generally, and specifically in relation to the Academia, Civil Nuclear, and Industry and Technology sectors. However, overall, the Committee noted that, until recently, the Agencies did not even recognise that they had any responsibility for countering Chinese interference activity in the UK, instead focusing their efforts on China's 'covert' activity. Moreover, responsibility for addressing the more overt aspects of the threat seems to rest with Whitehall policy departments; however, there is no evidence that those departments have the necessary resources, expertise or knowledge of the threat to counter China's approach. The UK is instead playing catch-up and the whole of the Government has its work cut out to understand and counter the threat from China.

14. On 14 September 2023, the Government published its Response to the *China* Report. In acknowledging the Response, the then Chairman said:

> "*I welcome this substantial attempt to respond to our Report. However, it is misleading repeatedly to imply – as the Government does – that our findings are outdated. Until two months before publication, we monitored all relevant developments and noted them throughout the Report. This was not difficult to do given the glacial pace at which the Government's China policy developed.*"[6]

## *International Partnerships*

15. On 5 December 2023, the Committee published its Report, *International Partnerships*.[7] The Committee began this Inquiry in October 2019; however, the Agencies' approach to it resulted in counterproductive and entirely unnecessary delays. Indeed, even after the Committee completed taking evidence, there was a lengthy delay by the Government – meaning that it took over two years to publish the Report.

[5] Written evidence – HMG, 18 April 2019.
[6] ISC website, 14 September 2023 (https://isc.independent.gov.uk/statements/#previous-parliaments).
[7] *International Partnerships*, HC 288, 5 December 2023 (https://isc.independent.gov.uk/wp-content/uploads/2023/12/ISC-International-Partnerships.pdf).

16. Nevertheless, the breadth of evidence taken during the Inquiry reflects the reality of modern intelligence: that almost every aspect of intelligence work relies upon, or benefits from, international co-operation. Strong international partnerships act as a vital 'force multiplier', enhancing the ability of the intelligence Agencies, the wider Intelligence Community and the Government to make sense of, and act in, an increasingly complex world. The Committee therefore fully supports the positive approach the Intelligence Community take towards intelligence partnerships, seeking actively to develop them beyond the merely transactional. Making full use of the UK's relative strength in intelligence terms to build partnerships is an effective use of resources that can help keep the UK safe in times of crisis.

17. However, the potential pitfalls cannot be ignored. In many cases, the partners with whom the Agencies work operate under different legal and ethical constraints to the UK and may not necessarily share the UK's values – a fact to which the Intelligence Community have not always been sufficiently alert, as this Committee has previously reported. With no choice but to work with other countries, the legal and compliance framework under which our Agencies engage is therefore of the utmost importance, and it must be embedded into the operational culture and decision-making of the Agencies. From the evidence provided to this Inquiry, it is clear that lessons have been learnt. There has been a significant improvement in processes and procedures, there is a far greater understanding of the issues that must be taken into account, and there is a genuine recognition of the broader impact of these relationships and the need for continued monitoring of their appropriateness.

18. On 22 February 2024, the Government published its public Response to the *International Partnerships* Report. The Committee received a further update on 18 December 2024 regarding the redacted Recommendations and Conclusions in this Report, and continues to monitor the progress being made in this area.

## *Annual Report 2022–2023*

19. The Committee published its Annual Report for 2022–2023 on 5 December 2023, summarising the work of the Committee from April 2022 to March 2023.[8] This work included the publication of two Reports, and contributions to five pieces of legislation.

20. The Report reiterated the Committee's concerns over the erosion of Parliamentary oversight as a result of the Committee's current Memorandum of Understanding (MoU) not being updated to cover all intelligence and security activities across Government. This is due to such issues increasingly being devolved to units within policy departments, and runs counter to a clear undertaking by the Government to Parliament during the passage of the Justice and Security Act 2013, that "*the ISC should have oversight of substantively all of central Government's intelligence and security activities*".[9] It also fails adequately to reflect the recognition in the MoU itself, agreed with the Prime Minister in 2013, that "*only the ISC is in a position to scrutinise effectively the work of the Agencies and of those parts of Departments whose work is directly concerned with intelligence and security matters*". This issue is also addressed later in the Report, in the chapter on Other Matters.

[8] *Annual Report 2022–2023*, HC 287, 5 December 2023 (https://isc.independent.gov.uk/wp-content/uploads/2023/12/ISC-Annual-Report-2022-2023.pdf).
[9] Justice and Security Bill [Hansard – HL Deb (9 July 2012), vol. 738, col. 1005].

## *Legislation*

21. During the period covered by this Report, there have been two pieces of legislation before Parliament with which the Intelligence and Security Committee has been heavily engaged.

### *Investigatory Powers (Amendment) Act 2024*

22. The original Investigatory Powers Act 2016 (the 2016 Act) was introduced partly as a result of the ISC's 2015 *Privacy and Security* Report: the Committee had recommended that a new Act of Parliament should clearly set out the intrusive powers available to the Agencies, the purposes for which they may be used and the authorisations required.

23. In February 2023, the Government published a post-legislative report on the operation of the 2016 Act – as required by statute. It reviewed the effectiveness of the Act and considered potential reforms that could be made. The Home Secretary also appointed Lord Anderson of Ipswich KBE KC to carry out an independent review of several areas within the legislation which the Government had identified as priority areas for reform. Lord Anderson published his report on 30 June 2023, setting out a number of recommendations for updating the 2016 Act to reflect the rapidly evolving threat and technology landscape.[10] For the most part, the Government accepted Lord Anderson's recommendations – and these, together with the post-legislative report, formed the basis for the Investigatory Powers (Amendment) Bill, which was introduced to Parliament on 8 November 2023.

24. The Committee sought to engage closely with this important legislation as it progressed through Parliament. We commissioned classified written evidence from the Intelligence Community and the Government on the need for the changes, before holding a number of oral evidence sessions with those involved in the legislation.

25. The Committee recognised the need for reform, to enable the Intelligence Community to tackle evolving national security threats to the UK, and to keep up with the pace of technological advances. We therefore broadly supported the Government's stated aim, which was to make a number of "*targeted changes*"[11] to key aspects of the 2016 Act. Nevertheless, given that the Bill addressed fundamental matters which bear on individuals' rights to privacy, the Committee sought to rigorously test the detail of the legislation, and to ensure that all measures proposed were both necessary and proportionate.

26. During the passage of the Bill through Parliament, the Committee tabled a number of amendments to ensure that there were robust safeguards in place. As a result of the Committee's advocacy, improvements to the regime were secured in three key areas.

#### *(i) The triple lock*

27. The Committee proposed changes in relation to the so-called 'triple lock'. The triple lock is the requirement that the Prime Minister, the relevant Secretary of State and a Judicial Commissioner[12] approve (a) any warrant that involves the interception of communications sent by, or intended for, a Member of a Relevant Legislature (for example, a Member of Parliament

[10] *Independent Review of the Investigatory Powers Act 2016*, Lord Anderson of Ipswich KBE KC, June 2023.
[11] Investigatory Powers Amendment Bill [Hansard – HL Deb (20 November 2023), vol. 834, col. 621].
[12] Judicial Commissioners are serving or retired members of the senior judiciary in the UK, who support the Investigatory Powers Commissioner in their oversight duties by providing independent authorisation of warrants for the use of certain investigatory powers.

or a Member of the House of Lords),[13] or (b) targeted equipment interference warrants, where the purpose of the warrant is to obtain communications sent by, or intended for, a person who is a Member of a Relevant Legislature, or to obtain a Member of a Relevant Legislature's private information. The Bill initially sought to allow the Prime Minister to designate any Secretary of State to approve such a warrant in his or her place, where there is an urgent need for a decision and the Prime Minister is "*unavailable*" to take the decision.

28. When taking evidence from the intelligence Agencies in November 2023, the Committee was told that there had been times when a Prime Minister had not been available due to ill health or international travel ***. The Committee recognised the need for greater resilience in the system, where the warrant in question is particularly time-sensitive. We therefore supported a change to ensure that, in truly exceptional circumstances, a Secretary of State who has knowledge of the warrantry process should be able to deputise for the Prime Minister and authorise such urgent triple-lock warrants.

29. However, the Committee considered that the Bill as introduced went too far – both in allowing any Secretary of State to deputise (even if they had no knowledge or experience of national security or warrantry), and in allowing that to happen when the Prime Minister was simply "*unavailable*" and it was considered that an urgent warrant decision had to be made. The latter in particular opened up a wide number of scenarios in which the Prime Minister might delegate this power to a Secretary of State, risking use of this power becoming routine rather than truly exceptional.

30. The draft Codes of Practice published alongside the Bill stated that "*the Prime Minister should have due regard as to whether a designee would have the necessary operational awareness of the warrantry process in order to carry out the role*".[14] However, the Committee was firmly of the opinion that matters as important as this must always be defined on the face of a Bill, where they cannot be amended or diluted by future administrations without first returning to Parliament – an issue the Committee itself has faced as Parliamentary commitments in relation to updating its MoU have been ignored by a number of administrations over the past ten years.

31. To address these concerns, the Committee proposed several amendments focusing on three key areas:

(i) that decisions would only be delegated in the most exceptional circumstances;

(ii) that decisions would only be delegated to the limited number of Secretaries of State who are already responsible for authorising relevant warrantry; and

(iii) that the Prime Minister would retain oversight of all warrants that have been authorised in their name, through retrospective review.

[13] This extra layer of approval applies to:
1) targeted interception warrants – for example, warrants which authorise the interception of a specific individual's communications;
2) targeted examination warrants – for example, warrants which authorise the selection and examination of specific content obtained through a bulk interception warrant; and
3) targeted equipment interference warrants – for example, warrants which authorise the gathering of information by interfering with electronic equipment (for example, phones or computers).

[14] Investigatory Powers (Amendment) Bill [HL] [Hansard – HL Deb (13 December 2023), vol. 834, col. 1912].

32. The Government accepted the first of these amendments: this mechanism will now only be used when the Prime Minister is "*unable*"[15] to decide whether to give the necessary approvals – due to incapacity or inability to access secure communications – rather than simply being "*unavailable*".

33. The Government made concessions on the remaining two points:

(i) designees are limited to no more than five Secretaries of State who have the "*necessary operational awareness to decide whether to give approvals*"; and

(ii) the Security Minister gave a commitment that the Codes of Practice associated with the Bill would include that "*the Prime Minister will be required*" to be retrospectively notified of any warrants signed in their name.

The draft Codes of Practice published by the Government in March 2025 reflected these changes.

34. **The Committee recognised that the existing 'triple lock' regime needed greater resilience. The Government went too far in its initial drafting, and the Committee sought amendments to ensure that the power to authorise such warrants remained tightly constrained. We are content that the right balance was struck eventually.**

*(ii) Monitoring the exploitation of Bulk Personal Datasets*

35. Part 7A of the 2024 Bill sought to introduce a lighter-touch regime for the examination of lawfully acquired Bulk Personal Datasets,[16] where the subject of the data is deemed to have "*low or no*" reasonable expectation of privacy[17] (an example would be a dataset available on the internet containing published news articles). The Bill allowed the Agencies to apply to retain and examine such datasets under either a 'category authorisation' – which authorises the use of a number of datasets which have similar content – or an 'individual authorisation' – which authorises the use of a single dataset, where the content does not naturally fall into a category authorisation or is more contentious.

36. While the Committee recognised the principle behind these changes, it considered that it was not necessarily clear-cut as to whether an individual would have "*low or no*" reasonable expectation of privacy in each instance. The Committee therefore sought to ensure that there was sufficient oversight of these decisions. The Bill initially included only limited provision for oversight: category authorisations in particular were intended to be approved internally by the Agencies and then by a Judicial Commissioner, with an annual report to the Secretary of State setting out the detail of all of the individual datasets authorised under Part 7A (both within individual and category authorisations).

37. The Committee sought to amend the Bill to provide that that annual report would also be given to both the ISC and the Investigatory Powers Commissioner, in order to reinforce

[15] Investigatory Powers (Amendment) Act 2024, section 23.

[16] A Bulk Personal Dataset is a set of information that is retained electronically by an intelligence Agency for the purpose of the exercise of its functions, and which includes personal data relating to a number of individuals, where the majority of the individuals are unlikely to be, or to become, of intelligence interest. ('Personal data' refers to information that relates to an individual who can be identified from either that data alone, or from that data in combination with other information that the data controller possesses, or is likely to come into possession of.)

[17] Investigatory Powers (Amendment) Act 2024, Part 7A *(*https://www.legislation.gov.uk/ukpga/2024/9/part/1/crossheading/low-or-no-reasonable-expectation-of-privacy).

Parliamentary and judicial oversight of the new regime, but adding no additional burden for the Intelligence Community (as the amendment would simply require sending an existing report to two additional bodies).

38. The Government rejected this amendment. Instead, it provided for a separate annual report – and for it to be sent to the ISC alone. This report will cover new and renewed category authorisations only (no detail is to be provided on individual authorisations). While the Committee welcomed this as a step in the right direction, it remains unclear to the Committee why the Government did not accept the original ISC amendment, which would have represented less of a burden on the Agencies and provided greater reassurance that the new regime was subject to independent Parliamentary and judicial scrutiny.

39. **We will scrutinise the annual report on category authorisations, which is to be provided to the Committee under the 2024 Act, to ensure that it provides sufficient detail to assure Parliament and the public that these expanded powers are not being misused.**

*(iii) The power to compel disclosure of Communications Data*

40. The Bill sought to remove the requirements on public authorities to take a number of additional procedural steps before they could compel a Telecommunications Operator to release specific Communications Data (CD).[18]

41. During the passage of the 2016 Act, Parliament recognised that the ability to access CD was a potentially intrusive power, and had therefore restricted the ability of most public sector organisations to access this type of data. For example, organisations such as the Environment Agency or the Health and Safety Executive were obliged to obtain one of the following in order to access CD:

(i) an authorisation under the 2016 Act (only available for criminal investigations);

(ii) a court order or other judicial authorisation;

(iii) specific 'regulatory powers' in relation to the regulation of Telecommunications Operators or postal authorities; or

(iv) an interception or equipment interference warrant (through which they may be permitted to obtain CD as secondary data).

42. However, since 2016 the technological landscape has evolved significantly. A broader array of communications now fall into the category of CD, and an increasing number of organisations have taken on the responsibility of Telecommunications Operators. In his review of the 2016 Act, Lord Anderson noted that "*the concept of a telecommunications operator, once restricted to providers of telephony services, is now used to embrace bodies as various as vehicle manufacturers and hotel chains*", and that "*the category of communications data, once explicable as akin to 'the writing on the envelope' ... now embraces location data generated automatically by a mobile phone when its owner is asleep – something closer to the product of intrusive or directed surveillance*".[19]

43. The Government argued that, as a result of this broadening of both the bodies covered and the data being captured, public authorities are now far more reliant on CD to carry out their

[18] Communications Data (CD) encompasses the details about a particular communication – the 'who, when and where' – but not the content of what is said or written.

[19] *Independent Review of the Investigatory Powers Act 2016*, Lord Anderson of Ipswich KBE KC, June 2023.

functions, rather than being primarily able to rely on their own statutory information-gathering powers. In the worst-case scenario, public authorities are prevented from accessing information necessary to fully discharge their functions. (This could happen where, for instance, the existing regime only permitted access to certain data for the purpose of preventing serious crime, and the public authority is not able to meet this requirement.)

44. The Government therefore sought to remove the restrictions entirely so that:

> "*bodies with recognised regulatory and supervisory functions, and who utilise civil proceedings as a means of enforcement …* [can] *continue to perform the roles required of them by Parliament in permitting them to acquire CD using their own information gathering powers as previously was the case*".[20]

45. The Committee asked which bodies this would apply to; we were deeply concerned that the Government was not able to offer a comprehensive list of those bodies that would have this power returned to them. The Committee considered it essential that no organisation should be given these powers back by default without Parliamentary approval, and pressed the Government to amend the Bill.

46. The Committee was therefore pleased when – after several interventions by its Members during the passage of the Bill – the Government finally tabled an amendment specifying that only those bodies listed in Schedule 4 of the 2016 Act, as well as HM Treasury and local authorities, would have their powers restored, and that any additional or new bodies must be added by regulation.[21]

47. The Investigatory Powers (Amendment) Act received Royal Assent on 25 April 2024. The Committee will continue to engage with its operation, including those parts of it relating to the Codes of Practice and Communications Data which are given later effect by Statutory Instrument.

48. **The amendments made demonstrate the value of the Committee, as the only body that can effectively scrutinise the classified information behind national security legislation on behalf of Parliament. The ISC provides the authoritative oversight needed to ensure that such important legislation strikes the right balance between privacy and security.**

## *National Security Act 2023*

49. The Committee had strongly welcomed the introduction of the National Security Bill in May 2022: the Committee had been calling for such legislation for many years. In our last Annual Report, we detailed our engagement with the Bill from its introduction through to its consideration by the House of Lords in the first quarter of 2023. Between April 2023 and July 2023, the Bill passed through the final stages of Parliamentary scrutiny.

50. One area that the Committee particularly scrutinised was the suggested amendment to the Serious Crime Act 2007, to create an automatic 'exemption' for the intelligence services (and the Armed Forces) in relation to offences overseas (specifically, "*encouraging or assisting the commission of an offence*"),[22] where these actions were necessary for the proper exercise of

[20] Explanatory Notes: Investigatory Powers (Amendment) Act 2024, HMG, no date.
[21] Regulations amending the list in Schedule 4 were laid on 3 April 2025, after the timeframe covered by this Report.
[22] As set out in Part 2 and Schedule 4 of the Serious Crime Act 2007.

their functions. The Committee noted in its Annual Report 2022–2023 that it had instead recommended a more limited 'defence', which the Government had accepted. This change was strengthened further by a number of critical assurances at Report Stage in the House of Lords.

51. The Committee can now report that the amendment was agreed by both Houses of Parliament. This 'defence' provides a better balance between protecting intelligence officers and also maintaining a sufficient level of accountability. This is an example of the Committee's constructive engagement with the Intelligence Community, to find the right balance when it comes to the powers of the intelligence services, and of the value that the Committee provides in scrutinising classified information on behalf of Parliament.

52. However, there are four other areas where there are unresolved issues – about which the Committee is concerned – over the provisions of the legislation as enacted.

*(i) Foreign Influence Registration Scheme*

53. The Committee had welcomed the introduction of the Foreign Influence Registration Scheme (FIRS) as part of the National Security Bill: we had been calling for such a scheme as far back as the 2020 *Russia* Report.[23] The benefits were clear, in terms of increasing the transparency around state threats and making the UK a more difficult operating environment for foreign intelligence services.

54. However, the Committee continues to be concerned by several aspects of the scheme as introduced.[24] This includes: the complexity and lack of flexibility of the two-tiered scheme; the narrow nature of the scheme; the potential lack of transparency; and the practical difficulties relating to fully resourcing the FIRS.

55. **The Committee's concerns on the general operation of the FIRS remain. We repeat the recommendation from our Annual Report 2022–2023 that the Government should keep the effectiveness of the scheme under review and report to Parliament on its operation within the next two years.**

56. As the scheme comes into operation, the key question is which countries will be placed under the Enhanced Tier of the FIRS. (Whilst the primary Political Influence Tier requires the registration of political influencing activities directed by a foreign power, the secondary Enhanced Tier requires the registration of a broader range of foreign influencing activity.)

57. The Committee was pleased when the Government announced in March 2025 that the whole of the Iranian state, including Iran's intelligence services, would be placed into the Enhanced Tier.[25] However, during the period covered by this Annual Report, the Government had still not made a decision as to which other countries would be added to the Enhanced Tier of the FIRS.[26]

58. Given the extent of the threat posed by China (as identified in the Committee's 2023 *China* Report), and particularly that of its interference operations, we are concerned to see the Government dragging its heels on this decision. MI5 has previously told the Committee that a "*Foreign Agent Registration* [Act]-*type power, which the Australians and Americans enjoy …*

[23] *Russia*, HC 632, 21 July 2020.
[24] We explored these concerns in detail in our previous Annual Report: *Annual Report 2022–2023*, HC 287, 5 December 2023.
[25] Iranian State Threats [Hansard – HC Deb (4 March 2025), vol. 763, col. 195].
[26] The Government announced that Russia would be added to the Enhanced Tier on 1 April 2025.

[would] *have proportionately more effect against … Chinese activity*".[27] We acknowledge that balancing the tension between security and prosperity requires dexterity and that there are a number of difficult trade-offs involved. However, we have previously found that the Government has been reluctant to prioritise security considerations when it comes to China.

59. **The Government should swiftly come to a decision on whether to add China to the Enhanced Tier of the FIRS. This Committee should be provided with a full account of how that decision was arrived at, including the factors that were considered, to ensure that security concerns have not been overlooked in favour of economic considerations.**

*(ii) Reform of the Official Secrets Acts*

60. The Committee has long called for the reform of the entire Official Secrets Acts (OSA) regime. However – as noted in the Committee's Annual Report 2022–2023 – the National Security Bill only sought to reform the Official Secrets Acts 'espionage' regime; it did not seek to reform the Official Secrets Act 1989, as recommended by the Committee and by the Law Commission.[28] Given that the Government's 2021 public consultation had committed to reform of the Official Secrets Act 1989 "*at a minimum*",[29] this is disappointing.

61. During the Bill's Second Reading in the House of Commons, Members of the Committee sought assurances that reform of the Official Secrets Act 1989 would be brought forward with "*some urgency*".[30] Whilst the Government did not commit to a timeline, the then Home Secretary stated: "*I can assure the House that as soon as we can, when we find the right moment, we will come back to this.*"[31] We therefore understood that the Government still intended to bring forward reforms.

62. Whilst taking evidence for our *Iran* Report, Homeland Security Group told us: "*we very much heard the concerns around OSA 1989* [Official Secrets Act 1989] *as the National Security Bill went through, including from this Committee … it is something that we will continue to look at …* [we are] *committed to continuing to look at it*".[32] However, when we pushed the then Home Secretary on timelines, she gave quite a different answer: "*we don't repeal the 1989 Act. It is something that we haven't, we don't have plans to do … we haven't identified a need to go further, as of yet.*"[33] This discrepancy appears to represent a worrying change in the Government's position, given the assurances previously given to this Committee and to Parliament.

63. The failure to include this reform as part of the National Security Act means that the current problems with the Official Secrets Act 1989 will persist, including the requirement to prove damage for certain unauthorised disclosures – which acts as a significant barrier to prosecutions – and the two-year maximum sentence, which is clearly insufficient to deter or respond to the most serious unauthorised disclosures.

64. **We repeat our longstanding call for reform of the Official Secrets Act 1989. The Government should act on the assurances provided in the previous Parliament and pursue these reforms.**

---

[27] *China*, HC 1605, 13 July 2023.
[28] *Protection of Official Data*, Law Commission, HC 716, September 2020.
[29] *Legislation to Counter State Threats (Hostile State Activity): Government Consultation*, Home Office, May 2021.
[30] National Security Bill [Hansard – HC Deb (6 June 2022), vol. 715, col. 572].
[31] National Security Bill [Hansard – HC Deb (6 June 2022), vol. 715, col. 572].
[32] Oral evidence to the Iran Inquiry – HSG, 6 July 2023.
[33] Oral evidence to the Iran Inquiry – Home Secretary, 6 July 2023.

*(iii) Foreign interference in elections – duties on political parties*

65. During the Bill's stages in the House of Lords, Lord Carlile of Berriew proposed several versions of an amendment that would require UK political parties to publish a policy statement to ensure that any donations from a foreign power (whether direct or through an intermediary) could be identified. The amendment also required political parties to provide the Electoral Commission with an annual statement of risk management that identified how risks relating to donations from a foreign power have been managed and mitigated.

66. The Committee strongly supported Lord Carlile's amendment. Current protections within electoral financing law are not adequate: there are many gaps which could be exploited by a foreign adversary to covertly channel money to political parties. In addition, the law only requires UK political parties to check the status of donors. They are not required to examine the source of the funds that they receive and there is no form of enhanced due diligence even when a donor is operating from a high-risk country listed in terrorist-financing or money-laundering guidance.

67. Lord Carlile's amendment would therefore have had clear benefits: helping to make foreign donations within the UK's political system more transparent, and increasing the accountability of UK political parties. The Committee was therefore disappointed that the Government refused to accept this modest amendment – despite the widespread support it received across both Houses.

68. At a very late stage in Parliament's consideration of the Bill, the Government did at least commit to consult on improving information sharing between relevant public bodies (for example, Companies House and the Electoral Commission) to help identify and mitigate the risks of foreign influence in political donations. The Government committed to start this consultation within a year of the Bill coming into force, and to table a report in the House.[34] At the time of writing, this report had not been laid in Parliament. It is as yet unclear whether the new Government will maintain this commitment following the General Election.[35]

*(iv) Updating the Memorandum of Understanding between the Committee and the Prime Minister*

69. During consideration of the Bill by the House of Lords, an amendment was proposed by the then Opposition to require the Government to update the Memorandum of Understanding (MoU) between the Committee and the Prime Minister if the Bill led to the creation of any new teams outside the organisations already subject to the Committee's scrutiny. This update would ensure that the Committee oversaw the entirety of the new national security regime being implemented by the Bill.

70. The Government initially attempted to oppose this amendment in both Houses. However, at a very late stage, it proposed its own version of the amendment which was subsequently accepted by Parliament. Whilst the Committee – and many other Parliamentarians – questioned the Government's resistance to the original amendment, we were pleased to see the Government recognise the strength of Parliamentary feeling on this issue and bring forward its own version, albeit a weaker one.

---

[34] National Security Bill [Hansard – HL Deb (4 July 2023), vol. 831, col. 1125].

[35] In response to a question in the House of Lords on 9 June 2025 on the previous Government's commitment on information-sharing powers relating to political donations, the Minister said that information sharing will "*play a key role*" in the forthcoming Elections Strategy, which is due to be published in Summer 2025 [Hansard – HL Deb (9 June 2025), vol. 846, col. 1064].

71. The Government amendment only stipulates that there must be "*consideration*"[36] of whether to revise the MoU: it does not directly require the Government to revise the MoU if new teams are formed as a result of the Act. As enacted,[37] the provision states that consideration as to whether the MoU should be altered or replaced must begin within six months of the legislation coming into force. The relevant part of the Act was brought into force in December 2023. The Deputy National Security Adviser wrote to the Committee on 28 May 2024 to say that the Government had begun this statutory consideration and that it would "*welcome the Committee's views in due course*". As this letter was received four days after Parliament had been prorogued and two days before Parliament was dissolved ahead of the General Election, the Committee was in no position to respond. At the time of writing, the Committee is still to receive an update on the status of the statutory consultation.

72. Although the consultation relates only to matters within the scope of the Act – i.e. it will only consider whether bodies created directly by the legislation should be added to the Committee's MoU – it has a bearing on the wider problem we have raised consistently in several previous Annual Reports: that the Committee's MoU is woefully out of date. This means that there is intelligence and security activity being undertaken by the Government that is outside the remit of the Committee and therefore does not receive effective Parliamentary scrutiny. We return to this issue in more detail in the next chapter on Other Matters.

73. The National Security Act received Royal Assent on 11 July 2023. It had been much improved since its introduction and the Committee was reassured that many of its recommendations had been accepted. The Act will provide new tools to help both the UK Intelligence Community and law enforcement to tackle the complex, varied and wide-ranging state threats facing the UK.

## *Areas of inquiry*

### *Iran*

74. The Committee began its Inquiry into the threat posed by Iran in August 2021. During the period covered by this Annual Report, the Committee received written evidence and held oral evidence sessions with Ministers and officials from the Intelligence Community, completing its evidence gathering in August 2023. The Committee completed its Report in November 2023. Pre-publication checks – including the process of factual amendment and redaction requests – were being conducted at the point that the Election was called in May 2024. When the Committee was reconstituted it resumed these checks, which were still being finalised as at March 2025. The Committee is prioritising this work – and urging the Government to do so too – such that the Report can be published before the summer recess.

### *Cloud Technologies*

75. In May 2021, the Committee commenced an Inquiry into Cloud Technologies. During the period covered by this Annual Report, the Committee has received further written evidence from the Intelligence Community.

[36] National Security Act 2023, section 93.
[37] This Government amendment became section 93 of the National Security Act 2023.

## *Areas of scrutiny*

76. In accordance with its broader oversight function, the Committee has continued to monitor the expenditure, administration and policy of the seven organisations it oversees through the Quarterly Reports it receives from them[38] and the end-of-year information covering the 2022/23 and 2023/24 financial years. The threat assessment is summarised in Annex A, and the key facts and major developments for each organisation in 2022/23 and 2023/24 are summarised in Annexes B and C.

[38] The National Cyber Force is covered in the Quarterly Reports provided by GCHQ and DI.

# OTHER MATTERS

77. The Intelligence and Security Committee (ISC) has for some years highlighted the lack of sufficient resources for its Office and the need for its staff to be independent from the Executive: in our last Annual Report, we noted that the situation "*raised significant concerns as to whether there is now a concerted effort being made to undermine the democratic scrutiny of the UK Intelligence Community*".[39] During the period covered by this Report, the situation became critical.

## *The independence of the ISC*

78. The ISC has a small team of staff (the Office of the ISC), who are civil servants employed by the Cabinet Office but working directly to the Committee, and they support all of the Committee's work. The ISC Staff have been employed by the Cabinet Office for administrative purposes since the Committee was first formed in 1994. At that time, the Committee's oversight was limited to the three Agencies – MI5, SIS and GCHQ.

79. However, in 2013, two Cabinet Office units (NSS and JIO) were added to the Committee's remit. This raised a serious constitutional issue: an oversight body should not sit within (and be beholden to) a body that it oversees. The Committee and the Government agreed that the situation was untenable, and that the Committee and its staff would move out of the Cabinet Office.

80. At that time the solution was thought to be for the Committee to move to Parliament. However, after discussions with Parliament it became clear that, for a number of reasons, this was not possible. The Government and the Committee agreed that an alternative solution would need to be found. In the meantime, undertakings were given to the Committee that appropriate safeguards would be put in place within the Cabinet Office to ensure that the ISC Staff could not be influenced by those they oversee.

81. These undertakings have been completely ignored in recent years. ISC Staff have been subject to exceptional pressure, jeopardising the functioning of both the Office and the Committee. On 19 March 2024, the Committee therefore unanimously determined that the solution was for the Committee to establish an independent Office – a body corporate – linked to Parliament through the establishment of a new Board.

82. On 8 May 2024, the then Chairman and the current Deputy Chair both met the then Deputy Prime Minister to set out this decision, following up in writing on 15 May. The Deputy Prime Minister asked Cabinet Office officials to take work forward to assist in establishing the new Office; however, no progress had been made before the announcement of the General Election. Having initiated discussions with the previous Government, once the Committee was reconstituted in December 2024 it reopened discussions with Cabinet Office officials to explore how the necessary constitutional changes can be made.

83. **The Committee in the last Parliament became very seriously concerned that the vital scrutiny that the ISC provides was being undermined by continued interference by**

[39] *Annual Report 2022–2023*, HC 287, 5 December 2023.

**the Cabinet Office in the Committee's Office. Whilst this may appear to be an administrative matter, it goes to the very heart of Parliament's ability to hold the Government to account for those actions being taken in secret, behind closed doors, funded by the public purse.**

84. **The root of the problem lies in the control exerted over the Committee's staff and resourcing by the Cabinet Office – despite the Committee having oversight over substantial parts of the Cabinet Office. That, self-evidently, should not be the case.**

85. **The Committee is encouraged that Ministers recognise the importance of the Committee having an independent Office. Efforts continue to be made to find a workable solution: at the time of writing this Report, it appears likely that it will require amendment to the Justice and Security Act 2013 if the Committee's Office is to be established as a separate entity.**

## *Committee resources*

86. During the passage of the Justice and Security Act 2013, which gave the Committee an expanded remit, the headcount of the Committee's independent Office was set at 15.1 full-time equivalent (FTE), and the budget at £1.84 million: an allocation that was agreed at the time between the Committee and the Secretary of State.

87. That headcount has not increased since 2013, despite the vast increases in the number of bodies that the Committee oversees. In the Committee's Annual Report 2022–2023, we noted that the final budget granted to the ISC for the 2022/23 financial year had been reduced to £1.635 million – despite assurances in the years after the Covid-19 pandemic that the Committee's full budget would be reinstated. Then, for the financial year 2024/25, the Cabinet Office cut both the ISC's budget and the headcount further, to just £1.425 million and 9 FTE staff.[40]

### *(i) Keeping pace with the Intelligence Community's expansion*

88. The resourcing arrangements for the ISC put in place at the time of the Justice and Security Act 2013 – including the headcount and budget agreed by the Committee and the Secretary of State – have now been in place for 12 years. Over that time, not only has the Committee had no increase in capacity – unlike every other part of the Executive – but its staffing has been cut by over 40% and its budget by 23%.

89. To provide a comparison, over the same period, those organisations that the Committee oversees that are also within the Cabinet Office have grown at an extraordinary rate:

- JIO has grown from just over 50 staff to 116.
- NSS has grown from just over 100 staff to more than 233.

90. Other organisations that we oversee, which are outside the Cabinet Office, have also doubled in size: HSG has grown from just over 500 staff to 1,229. We are not able to publish specific details for all of the organisations that the Committee oversees, but suffice to say all

[40] In April 2025, the delegation for the financial year 2025/26 had just been received, and the Committee's budget had been cut again – this time to just £1.363 million.

have grown considerably. As a result, the Committee is now overseeing something that is of a fundamentally different order than what was envisaged in 2013 – but is being expected to do so with even fewer resources itself.

91. There are also now more organisations within the Intelligence Community (such as the National Cyber Force), and the Community is pursuing bigger projects under a broader remit (for example, MI5 has led on Extreme Right-Wing Terrorism since 2020). If the Committee is to meet the requisite increase in statutory oversight obligations, then it requires greater resources. **In budgetary terms, there is now an additional £3 billion being spent each year by the organisations we oversee, compared with 2014.**

92. The threat landscape itself has also changed almost beyond recognition in that time. The nature of the threat is substantively different, and the rate of technological change has brought new issues, which requires different expertise to support scrutiny. The Committee now needs to be able to bring in subject matter experts for certain issues, which is not possible with the current headcount. The 2013 arrangements are simply no longer fit for the world in which we find ourselves 12 years later.

93. The Committee needs to establish a headcount that redresses the historic failure to keep pace with the organisations that the Committee oversees, with sufficient capacity to be able to offer jobs on more competitive terms, and which enables recruitment from a wider pool of staff – which would provide greater access to skills and talent including subject matter experts.

### *(ii) An immediate crisis*

94. Since the pandemic, the Committee has faced sharp challenges in recruiting and retaining the staff it requires: external events have elevated what was already a deep-seated problem. Working arrangements for ISC Staff (around restrictions on leave, mandatory office attendance and lack of flexible working patterns) are far less flexible than those in the wider Civil Service and, as a result, the Committee's very small Office sank to the lowest level of staffing in over 20 years, with only a fraction of its actual allocated headcount.

95. The Committee therefore requested a short-term uplift in headcount of 15 staff, in addition to the 15.1 headcount previously agreed with Ministers. The then Deputy Prime Minister personally confirmed to the Committee that he had agreed this uplift shortly before the 2024 General Election, but unfortunately this was not acted upon by officials before the dissolution of Parliament. The Committee returned this issue to Ministers in January 2025, seeking that uplift now be actioned.[41]

96. **Over a period of several years, the ability of this Committee to exercise independent scrutiny over the Intelligence Community has been increasingly constrained. This Committee was less able to provide assurance to the public that the activities of the intelligence Agencies and the wider Community are properly scrutinised and overseen because its governance, resources and remit are inadequate.**

97. **The Heads of the organisations within the Intelligence Community frequently cite the importance of the ISC in providing their 'licence to operate'. Without sufficiently robust and empowered Parliamentary oversight, this 'licence to operate' is inhibited.**

[41] Written confirmation of that uplift was provided at official level on 13 May 2025. At the time of writing, the Committee awaits a revised delegation letter from the Cabinet Office.

98. **At the time of writing, we welcome the progress that has been made on this issue, and the Government's commitment to increase the ISC's headcount and budget. Once that is received, the Committee will begin recruitment of new staff to rectify both the short- and long-term issues that have resulted in the acute understaffing of the ISC's Office, and allow the Committee to fulfil its statutory responsibilities going forwards.**

## *Remit*

99. For the past four years, the Committee has highlighted the erosion of effective Parliamentary oversight of intelligence and security matters, which has resulted from the Government's failure to update the Memorandum of Understanding (MoU) between the ISC and the Prime Minister. This runs counter to the clear undertaking given by the Government to Parliament during the passage of the Justice and Security Act 2013 that "*the ISC should have oversight of substantively all of central Government's intelligence and security activities to be realised now and … in the future*".[42] This also fails adequately to reflect the recognition in the MoU itself, agreed by the Prime Minister, that "*the ISC is the only Committee of Parliament that has regular access to protectively marked information that is sensitive for national security reasons*" and that "*only the ISC is in a position to scrutinise effectively the work of the Agencies and of those parts of Departments whose work is directly concerned with intelligence and security matters*".[43]

100. During the passage of the Justice and Security Act 2013, the then Security Minister made clear that the MoU was designed to be a living document: "*Things change over time. Departments reorganise. The functions undertaken by a Department one year may be undertaken by another the following year … An MoU is flexible: it can be changed much more easily than primary legislation*".[44] Yet the MoU has not been updated at all since it was first published 12 years ago.

101. The failure by successive Governments to adhere to these undertakings since the introduction of the Fusion Doctrine in 2018, which led to the dispersal of national security responsibilities beyond the Intelligence Community, has resulted in a significant gap in Parliamentary oversight of UK intelligence and security activities. The Committee was established by Parliament in order to scrutinise secret matters that could not be considered by Parliament itself. Unlike Select Committees, it has appropriate IT systems, storage facilities and vetted staff to allow it to handle and scrutinise classified material on a routine basis. It is therefore the only Parliamentary body that can effectively scrutinise the Government's national security apparatus.

102. In 2013, seven intelligence and security organisations were listed in the ISC's MoU as those bodies that the ISC would oversee on behalf of Parliament.[45] However, the Government then adopted the Fusion Doctrine as its approach to national security in 2018. This resulted in the increasing devolution of intelligence and security matters to teams within Government departments that have not traditionally held significant national security responsibilities (for example, the Department for Business and Trade and the Department for Education).

[42] Justice and Security Bill [Hansard – HL Deb (9 July 2012), vol. 738, col. 1005].
[43] Memorandum of Understanding under the Justice and Security Act 2013, paragraph 8.
[44] Justice and Security Bill [HL] [Hansard – Public Bill Committees (31 January 2013), col. 98].
[45] The National Cyber Force was added to the Committee's remit in April 2020, by way of a letter from the Foreign and Defence Secretaries.

103. These teams have not been added to the ISC's MoU and therefore do not currently sit within the Committee's remit. As a result, there is now a significant – and widening – gap in oversight of national security work because the relevant departmental Select Committees, within whose remit these teams fall, are not equipped to scrutinise the work of these teams fully. We have previously highlighted the example of the Investment Security Unit (ISU), created by the National Security and Investment Act 2021 to work with the Intelligence Community in order to advise on national security risks to the UK from foreign investments, acquisitions or transactions. Despite the ISU being moved from the then Department for Business, Energy and Industrial Strategy to the NSS in the Cabinet Office – which we oversee – scrutiny of the ISU has remained with the House of Commons Business and Trade Select Committee. There is still no adequate explanation as to how the Select Committee is expected to scrutinise the ISU's work effectively without the ability to routinely access and handle classified information.

104. As mentioned in the previous chapter on The Work of the Committee, an amendment was accepted into the National Security Bill to require the Government to consider whether the ISC's MoU should be altered or replaced to reflect any changes arising out of the Act.[46] The Government wrote to the Committee in May 2024 confirming that it had begun this consideration, but the Committee is still to receive an update on progress. We expect a substantive discussion between the Government and the Committee to take place as the next step.

105. **The Committee was deeply disappointed that the previous Government did not consider itself bound by the undertakings to keep the Committee's remit up to date that were given to Parliament in the course of the passage of the Justice and Security Act 2013.**

106. **The Committee's position is that its remit is to oversee all intelligence and security activities across Government, and that this is not limited to those organisations currently listed in the MoU. The MoU should be revised to make clear that the bodies that it lists are not exhaustive. Without an update to the MoU, a growing proportion of national security work is left without fully effective Parliamentary oversight. We hope that the new Government will ensure that the commitments made to Parliament about oversight of secret matters are respected.**

## *Meeting with the Prime Minister*

107. Since its establishment in 1994, and for 20 years thereafter, the Committee met annually with the Prime Minister to discuss its work, report on key issues and raise any concerns. However, the Committee last had a meeting with a Prime Minister in December 2014 – over ten years ago.

108. This was the subject of discussion in Parliament during the passage of the Investigatory Powers (Amendment) Act 2024. Dan Jarvis MP (now Security Minister) said: "*as the years pass, there is now a risk of a new convention being created of the Prime Minister not appearing before the ISC*"[47] and "*I do not think it unreasonable to expect that once a year the Prime Minister should seek to meet what is a very important cross-party Committee of this House*".[48]

[46] This provision became section 93 of the National Security Act.
[47] Investigatory Powers (Amendment) Bill [HL] (Second sitting) [Hansard – Public Bill Committees (7 March 2024), col. 64].
[48] Investigatory Powers (Amendment) Bill [HL] [Hansard – HC Deb (25 March 2024), vol. 747, col. 1307].

Lord Coaker (now Minister of State at the Ministry of Defence) introduced an amendment to the Investigatory Powers (Amendment) Bill, which would have required the Government to publish a report on engagement between the Prime Minister and the ISC in relation to investigatory powers. Although this amendment was subsequently withdrawn, Lord Coaker said: "*I cannot believe ... that it has been 10 years since a Prime Minister has gone to the body which has been set up by Parliament to ensure there is liaison between Parliament and the intelligence and security services ... Could the Minister explain what on earth is going on?*"[49]

109. Following the 2024 General Election, the Committee has been reassured that the Prime Minister recognises the importance of the ISC's work. The Prime Minister wrote immediately to the Chairman upon his election on 18 December 2024, inviting the Committee to meet him and those Ministers responsible for the organisations the ISC scrutinises.

110. **The Committee welcomes the Prime Minister's positive engagement and offer of a meeting. We look forward to re-establishing a regular cycle of annual meetings.**

[49] Investigatory Powers (Amendment) Bill [HL] [Hansard – HL Deb (23 January 2024), vol. 835, col. 689].

# LIST OF WITNESSES

### *Ministers*

The Rt Hon. Suella Braverman KC MP – then Secretary of State for the Home Department

The Rt Hon. James Cleverly TD VR MP – then Secretary of State for Foreign, Commonwealth and Development Affairs

The Rt Hon. Tom Tugendhat MBE VR MP – then Minister of State for Security

### *Officials*

CABINET OFFICE

Sir Simon Gass KCMG CVO – then Chair, Joint Intelligence Committee

Dame Madeleine Alessandri DCB CMG – Chair, Joint Intelligence Committee

Mr Matthew Collins CBE – Deputy National Security Adviser, National Security Secretariat

Other officials

GOVERNMENT COMMUNICATIONS HEADQUARTERS (GCHQ)

Sir Jeremy Fleming KCMG CB – then Director

Ms Anne Keast-Butler – Director

Dr Richard Horne – CEO, National Cyber Security Centre

Other officials

HOME OFFICE

Ms Chloe Squires – Director General, Homeland Security Group

Other officials

MINISTRY OF DEFENCE

Mr Adrian Bird CB – Chief of Defence Intelligence

Other officials

SECRET INTELLIGENCE SERVICE (SIS)

Sir Richard Moore KCMG – Chief

Other officials

SECURITY SERVICE (MI5)

Sir Ken McCallum KCB – Director General

Other officials

# ANNEX A: THREAT ASSESSMENT

The threat to the UK and its interests overseas comes from a number of different sources, as outlined in previous Annual Reports, including Islamist terrorism, Extreme Right-Wing Terrorism (ERWT), Left-wing, Anarchist and Single-Issue Terrorism (LASIT) and Northern Ireland-related terrorism (NIRT), State Threats, the Cyber Threat and Proliferation of Weapons of Mass Destruction. The Intelligence Community work to counter these threats. The following is a summary of the Intelligence Community's threat assessment for the period 1 April 2023 to 31 March 2025.

## *The threat picture*

### *The threat to the UK from hostile activity by states*

The threat to the UK from hostile activity by Russian, Iranian and Chinese State-linked actors is multi-faceted and complex. The threat of state-sponsored assassination, attacks and abductions of those perceived as dissidents has remained at a higher level than we have seen in previous years. In December 2023, a Chechnya-born Austrian national was sentenced under the Terrorism Act for collecting information regarding Iran International, a Farsi-language media organisation that has been under persistent threat from the Iranian regime. In addition, as part of its efforts to destabilise Western support to Ukraine, Russia has engaged in sabotage campaigns across Europe. In May 2024, the UK Government expelled the Russian defence attaché – an undeclared military intelligence officer – and removed diplomatic protections from several Russian properties in the UK in response to an increasing pattern of malign activity over the previous year.

The methodologies used by state actors have also continued to develop, with proxy actors increasingly conducting activity on behalf of states. In March 2025, three UK-based Bulgarian nationals, members of a 'Russian spy ring' who carried out espionage activity in the UK – including gathering information on individuals of interest to the Russian State – were successfully prosecuted, with three other members of the network having previously pleaded guilty. Further, in April 2025, the UK Government announced the sanctioning of criminal group the Foxtrot Network, which has carried out violence against Jewish and Israeli targets in Europe on behalf of the Iranian regime.

Attempts by foreign intelligence services to conduct espionage to obtain UK Government and defence-sector secrets continue. In March 2024, the UK attributed a multi-year cyber campaign against the UK and other countries to a Chinese intrusion set (APT31); this included the attempted targeting of UK MPs and a hack of the UK Electoral Commission. Similarly, in February 2025 Daniel Khalife was sentenced to 14 years and 3 months in prison, having been found guilty of charges under the Official Secrets Act, for spying for Iran. Espionage is similarly conducted to access economic information, including intellectual property, research and development, and scientific academic research.

The threat to the UK also includes the efforts of foreign states to exert covert and malign influence on UK policy, democracy and public opinion through attempts to influence social media, journalism and political figures. In December 2023, the British Government called out an FSB (Russian Federal Security Service)-linked cyber unit (known as STARBLIZZARD) for its persistent attempts to "*hack and leak*" material relating to UK

political issues. Similarly, in September 2024 the British Government joined the United States in calling out Russian State media channel RT as a mouthpiece of Russian disinformation, including for its role in seeking to influence democratic processes in Moldova. In March 2023, Yang Tengbo was excluded from the UK on the grounds that the relationship he developed with Prince Andrew could be used for political interference purposes by the Chinese State; this judgement was upheld following appeal by the Special Immigration Appeals Commission in December 2024. Additionally, in December 2024 the Investigatory Powers Tribunal dismissed complaints brought by Christine Lee, who was subject to an MI5 Interference Alert to Parliamentary Authorities in January 2022 following an investigation confirming her links to the United Front Work Department.

A number of steps have been taken to strengthen the response to hostile activity by foreign states. This includes the National Security Act, which came into law on 20 December 2023. This has introduced new measures to protect the public, give MI5 and its policing partners a greater range of tools and make the UK a harder operating environment.

### *The threat to the UK from terrorism*

The UK National Threat Level is currently 'SUBSTANTIAL: *an attack is likely*', and it has remained at that level throughout the reporting period. Since the Westminster Bridge attack of 22 March 2017 and 31 March 2025, MI5 and police partners disrupted 43 terrorist attack plots in the UK.

It continues to be most likely that an Islamist terrorist, Extreme Right-Wing Terrorism (ERWT) or Left-Wing, Anarchist and Single-Issue Terrorism (LASIT) attack would emanate from self-initiated terrorists radicalised online, who plan and conduct attacks without formal association or practical support from a domestic or international terrorist group. Personalised motivations and a widening spectrum of underlying grievances mean that the shape of these extremist ideologies continues to be complex, volatile and unpredictable.

The conflict between Israel and Hamas resonated among Islamist extremists in the UK, and it represents a further grievance narrative that may entrench extremist views in the UK, now and in the future. We remain focused on identifying any emergent threats linked to the conflict.

There has been one successful ERWT attack in the UK this reporting period. A 31-year-old British national stabbed an asylum seeker at the Pear Tree Inn, Worcester, on 2 April 2024. The attacker almost certainly held ERWT beliefs and conducted his attack in furtherance of his anti-immigration beliefs.

The primary role of overseas Islamist terrorist groups and transnational ERWT online communities in driving domestic threat is through inspiring UK-based individuals to carry out terrorist activity. Geopolitical and domestic events have been exploited to fuel extremist narratives and grievances. Al-Qaeda (AQ) and Islamic State (IS) both attempted to capitalise on the conflict between Israel and Hamas, situating it within wider global jihadist narratives to drive engagement with their terrorist agendas. Leveraging such events as a means of encouraging individuals to carry out attacks is highly likely to continue.

### *Northern Ireland-related terrorism*

In March 2024, the Threat Level in Northern Ireland from Dissident Republican groups was lowered to 'SUBSTANTIAL: *an attack is likely*'. The level of threat is now broadly stable after several years of gradual decline, with greatly reduced numbers of Dissident Republican attacks or attempted attacks. However, constant security agency pressure will continue to be required to keep the threat suppressed at this level.

The most serious national security threat in Northern Ireland remains that posed by the New Irish Republican Army (New IRA). Dissident Republican groups retain stated intent to conduct attacks. However, during the reporting period there have been no attacks, although in February 2024, media reporting indicated that a group referring to themselves as 'ANP' (Arm Na Poblachta) claimed to a media outlet that it had thrown two devices at a police patrol. One device was recovered.

The focus of Loyalist paramilitary groups remains in criminality rather than activity of national security concern, which falls within the remit of the Police Service of Northern Ireland (PSNI).

### *The Cyber Threat*

The UK continues to face real and enduring threats from states and cyber criminals to steal information, data and intellectual property. In the last two years, we have also seen the spillover of the Cyber Threat from Russia's war in Ukraine and conflict in the Middle East, inspiring non-state threat actors to carry out cyber attacks against Western critical national infrastructure (CNI). These threat actors are not subject to formal or overt state control, which makes their activities less predictable.

The most prevalent Cyber Threat to the UK is almost certainly cyber espionage; however, ransomware attacks continue to pose the most immediate and disruptive threat to our CNI, with some state-linked cyber groups now targeting the industrial control systems on which infrastructure relies.

Russia continues to act as a capable, motivated and irresponsible threat actor in cyberspace. Russian threat actors almost certainly intensified their cyber operations against Ukraine and its allies in support of their military campaign and wider geopolitical objectives. China continues to be a highly sophisticated and capable threat actor, targeting a wide range of sectors and institutions across the globe, including in the UK. Iran-based threat actors remain aggressive in cyberspace and continue to achieve their objectives through less sophisticated cyber techniques (including prolific use of 'spear-phishing'), but also targeting industrial control systems.

The UK General Election in July 2024 presented an attractive target for a range of threat actors, due in part to the UK's membership of NATO, the G7 and our continued support for Ukraine. Threats against UK officials and election candidates – particularly their personal devices and accounts, seen as a softer target by adversaries – were highlighted in public attributions.

Many nation-state threat actors and cyber criminals are already using artificial intelligence (AI) to increase the volume, and heighten the impact, of cyber attacks. Generative AI (that is, AI tools that can produce different types of content, including text, images and video)

will make it harder for defenders to identify social engineering attacks without the development of new mitigations. Highly capable state actors, in terms of both AI and cyber operations, will most likely be able to exploit the potential of AI to create more advanced cyber attacks.

Over the next five years, the expected increased demand for commercial cyber tools and services, coupled with a permissive operating environment in less-regulated regimes, will almost certainly result in an expansion of the global commercial cyber intrusion sector. The real-world effect of this will be an expanding range and number of victims to manage, with attacks coming from less-predictable types of threat actor. Many of these will have access to commodity cyber tools that require low skill to weaponise and will be operating from countries with scant regard for international norms and regulations.

### *Proliferation of Weapons of Mass Destruction*

HMG continues to take measures at home and to engage internationally in efforts to counter the proliferation of equipment and materials related to weapons of mass destruction.

# ANNEX B: EXPENDITURE, ADMINISTRATION AND POLICY – 2022/23

<table>
<tr><th colspan="2">Single Intelligence Account</th></tr>
<tr><td colspan="2">Expenditure in 2022/23</td></tr>
<tr><td>Total budget and out-turn</td><td>
<table>
<tr><th>£'000</th><th>Resource spending</th><th>Capital spending</th><th>TOTAL</th></tr>
<tr><td>Budget</td><td>3,313,914</td><td>1,172,426</td><td>4,486,340</td></tr>
<tr><td>Out-turn</td><td>3,208,600</td><td>1,156,257</td><td>4,364,857</td></tr>
</table>
</td></tr>
<tr><td>Expenditure by category</td><td>• Staff pay: £1.33bn<br>• Other expenditure: £2.44bn<br>• Capital spending: £1.16bn</td></tr>
</table>

The figures above represent the combined budgets of MI5, SIS, GCHQ, *** and NSS costs for managing the Single Intelligence Account (SIA) as already published in the Single Intelligence Account. The Resource and Capital figures above include Departmental Expenditure Limits and Annually Managed Expenditure, as published in the SIA Annual Resource Accounts.

The Committee has been provided with the individual figures for each Agency; however, these have been redacted in the subsequent pages, since to publish them would allow the UK's adversaries to deduce the scale and focus of the Agencies' activities and effort more accurately. This would enable them to improve their targeting and coverage of the Agencies' personnel and capabilities, and to seek more effective measures to counter the Agencies' operations against them.

## MI5 (Security Service)

### *Expenditure in 2022/23*[1]

**Total budget and out-turn**

| £'m | Resource spending | Capital spending | TOTAL |
|---|---|---|---|
| Budget | *** | *** | *** |
| Out-turn | *** | *** | *** |

**Expenditure by category**

- Staff costs (including R&D staff costs CDEL[2]): ***
- Other revenue costs (including professional services, accommodation, research and development, and IT systems): ***
- Capital costs (excluding R&D staff costs): ***

### *Administration*

**Staff numbers**[3]

| | Total staff | SCS[4] | Non-SCS |
|---|---|---|---|
| 31 March 2022 | 5,526.5 | 91.5 | 5,435 |
| 31 March 2023 | 5,384.5 | 86 | 5,298.5 |

**Recruitment in 2022/23**

- MI5 recruited 625[5] staff, against a target of 602 in 2022/23.
- This compares with recruiting 608 new staff against a target of 507 in 2021/22.

**Major projects in 2022/23**

- Preparation for MI5's adoption of a Cloud platform: In 2022/23, work continued to build the platform itself, and to migrate data across to the new system. MI5 also continued to work on: the financing of the project; compliance; and behaviour change, in order to maximise staff use of the platform once it is complete.
- TRANSFORMING CORPORATE SERVICES: The programme to deliver all corporate services to the Agencies (such as finance, commercial services and human resources), the transfer of Agency staff into a cross-community team, and the creation of a new set of digital platforms for the use of corporate services continues. At the end of the 2022/23 financial year, the programme had completed two out of three of its objectives: establishing the cross-community team and moving Agency staff onto the associated digital platform. Work on the programme's third objective – to deliver a set of new digital capabilities to improve how the organisation operates – continued during the 2022/23 financial year, with a target of July 2023 for these capabilities to 'go live'.

[1] As reported to the Committee in MI5's end-year report for the 2022/23 financial year.
[2] Research and development staff costs account for staff who occupy roles that are categorised as research and development activity. They count as Capital Departmental Expenditure Limit (CDEL) expenditure and are separate to Resource Departmental Expenditure Limit (RDEL) staff costs. When combined, the two figures account for total staff cost.
[3] These figures refer to the number of full-time equivalent (FTE) staff as at the end of each financial year. MI5 also employed a number of contractors/consultants. These figures are not included but have estimated costs of *** million in 2022/23 and *** million in 2023/24.
[4] Senior Civil Service.
[5] Figures provided are of staff headcount rather than FTE.

| | |
|---|---|
| | ● Counter Terrorism Operations Centre (CTOC): This programme seeks to bring together the counter-terrorism (CT) elements of the UK Intelligence Community with Counter Terrorism Policing (CTP). At the end of the 2022/23 financial year, the programme was on track to be delivered on time and within budget. In October 2022, the first four floors of the CTOC became operational. |
| Diversity and inclusion 2022/23 | ● Recruitment of staff from under-represented groups rose during the 2022/23 financial year. MI5 exceeded national representation levels in both the recruitment of women and ethnic minorities, achieving rates of 60% and 22% respectively.<br>● MI5, alongside SIS and GCHQ, changed the parental nationality rules for applications to Agency roles, removing the requirement for at least one parent of an applicant to be British or from an approved list of countries. The change was made to try and widen the pool of individuals eligible to join the Agencies.<br>● MI5 expanded its Summer Diversity Internship Programme in 2023, with opportunities for *** interns, a quarter of whom were of Black heritage – a key target of the programme.<br>● MI5 and SIS launched a 'Disability and Neurodivergence in the UK Intelligence Services' electronic brochure, which has been made available to every candidate applying to MI5 and SIS.<br>● MI5 worked with recruitment contractor *** to deliver initiatives that promote diverse recruitment, such as data-led decision-making and targeted Equality, Diversity and Inclusion (EDI) outreach. |
| ***Policy*** | |
| Allocation of effort at 31 March 2023 | ● Counter-terrorism (all categories except NIRT): 54%<br>● Counter State Threats: 29%<br>● Northern Ireland-related terrorism (NIRT): 17% |
| Major achievements reported to the Committee for 2022/23 | ● MI5 disrupted two Extreme Right-Wing Terrorist (ERWT) and three Islamist terrorist plots between April 2022 and March 2023.<br>● The UK–US Data Access Bilateral Agreement came into force in October 2022, allowing more data to be obtained from US communications service providers.<br>● MI5 and the Centre for the Protection of National Infrastructure (CPNI)[6] provided advice and supported the operational response to the death of HM Queen Elizabeth II (Operation LONDON BRIDGE[7]). This was the largest protective security operation ever conducted in the UK.<br>● MI5 supported the delivery of protective security briefings and advice to individuals, including Members of Parliament, who had been sanctioned by the Iranian Government. |

[6] On 13 March 2023, CPNI was renamed the National Protective Security Authority (NPSA), as part of the announcement of HMG's Integrated Review Refresh. NPSA has absorbed the responsibilities of CPNI but with a broader remit, reflecting the fact that the threats that the UK faces today extend far beyond those to critical national infrastructure.

[7] Operation LONDON BRIDGE refers to the Government's funeral plan for the death of the late HM Queen Elizabeth II.

## *Crisis response impact 2022/23*

- MI5 continued to respond to the Ukraine crisis during this time. Some of the resource requirements for the initial short-term response subsided; however, additional resourcing was still required to support areas that had increased in significance due to the crisis (for example, the Russia Team within the Joint State Threats Assessment Team).
- In the Committee's Annual Report 2022–2023, we noted that some areas of MI5's Counter State Threat Mission had been affected by the Ukraine crisis; the effects of the crisis were mitigated during this period and work on these areas was able to resume.

## Secret Intelligence Service (SIS)

### *Expenditure in 2022/23*[8]

**Total budget and out-turn**

| £'m | Resource spending | Capital spending | TOTAL |
|---|---|---|---|
| Budget | *** | *** | *** |
| Out-turn | *** | *** | *** |

**Expenditure by category**

- Staff costs: ***
- Other costs: ***
- Capital costs: ***
- Conflict, Security and Stability Fund: ***[9]
- National Cyber Security Programme: ***[10]

### *Administration*

**Staff numbers**[11]

| | Total staff | SCS | Non-SCS |
|---|---|---|---|
| 31 March 2022 | 3,673.2 | 85.68 | 3,587.52 |
| 31 March 2023 | 3,752.96 | 91.91 | 3,661.05 |

**Recruitment in 2022/23**

- SIS recruited *** new staff against a target of *** in 2022/23.
- This compares with the recruitment of *** staff against a target of *** in 2021/22.

**Major projects in 2022/23**

- Capability Portfolio: SIS continued to invest in this programme, which aims to ensure that SIS's data, knowledge, communications and technical operational capabilities remain effective, efficient, compliant and secure. These capabilities are delivered through a number of capability centres, each with a specific focus, such as *** and ***. The programme is listed within the Government Major Projects Portfolio, reflecting its scale and complexity, and it has external assurance, including input from the Infrastructure Projects Authority. However, as noted in the Committee's Annual Report 2022–2023, the risk posed by a lack of resource is rated 'red' for both probability and potential impact; this continued to be the case in the 2022/23 financial year.
- Preparation for the adoption of a Cloud platform: In 2022/23, SIS engaged commercial partners to provide additional delivery capacity for the project and selected a number of systems to be migrated as a priority (known as the 'First Five' systems). However, delays to the project, resulting from a reassessment of the requirements needed to enable the adoption of the Cloud platform, cost an estimated £16.9m during this period.

[8] As reported to the Committee in SIS's end-year report for the 2022/23 financial year.
[9] Separate funding stream.
[10] Separate funding stream.
[11] These figures refer to the number of FTE staff as at the end of each financial year. SIS also employed a number of contractors/consultants. These figures are not included but have estimated costs of *** in 2022/23 and *** in 2023/24.

| | |
|---|---|
| | • The Science, Technology and Engineering Programme (STEP): This will fund research and development across the Agencies over a four-year window. The programme has three strategic objectives, which are: delivering against the challenges presented by Chinese technology; accessing new disruptive science and technology; and rebuilding talent and infrastructure within the Agencies. Following work in 2021/22 to develop a cross-Agency strategy for science, technology and innovation, the strategy was formally agreed in 2022/23. For SIS, this led the organisation to pivot towards China-related work, and to focus on key technologies such as ***, *** and ***. |
| Diversity and inclusion 2022/23 | • The proportion of new staff recruited from under-represented groups increased during the 2022/23 financial year: 22% of new staff were of an ethnic minority background, exceeding the national representation level.<br>• SIS continued its Summer Diversity Internship: in summer 2023, 72% of the cohort were women and 45% were of Black heritage.<br>• Working with MI5 and GCHQ, SIS delivered over 150 outreach initiatives, targeting audiences including school children and experienced industry professionals.<br>• SIS worked with recruitment contractor *** to deliver initiatives that promote diverse recruitment, such as data-led decision-making and targeted EDI outreach. |
| ***Policy*** | |
| Allocation of effort at 31 March 2023 | • Key operational activities, including: counter-terrorism; cyber and access generation; global themes;[12] and prosperity and economic stability – 36.3%<br>• Operational support, including: global network enabling; covert operations; data exploitation; operational security; and operational technology – 35.2%<br>• Corporate services, including: legal and private offices; human resources; finance; estates and business change; IT infrastructure; security and compliance; science, research and innovation; and policy, requirements and communications – 28.5% |
| Major achievements reported to the Committee for 2022/23 | • SIS provided significant support to the Ukrainian government to enable it to push back Russian forces and address critical threats from Russia (***).<br>• SIS informed the Joint Terrorism Analysis Centre's (JTAC) assessment of the emerging Islamic State (IS) threat in an African country (***). This reportedly had direct consequences for HMG's work in that country, avoiding large-scale disruption and costs associated with reducing HMG's presence there.<br>• SIS provided insights into how the Iranian Intelligence Services (***) target individuals they consider a threat to regime stability. This assisted wider HMG work to counter malign Iranian activity directed towards EU countries. |

[12] 'Global themes' include defence technology and counter-proliferation.

## *Crisis response impact 2022/23*

- SIS moved its response to the war in Ukraine from a crisis footing to business as usual.
- SIS continued to host a small team (*** officers from across the Agencies) to support Afghan relocation and resettlement.
- Relevant teams co-located for three days at the height of the Sudan crisis in April 2023 (this did not impact wider resourcing as the crisis response only involved existing staff).

## Government Communications Headquarters (GCHQ)

### *Expenditure in 2022/23*[13]

**Total budget and out-turn**

| £'m | Resource spending | Capital spending | TOTAL |
|---|---|---|---|
| Budget | *** | *** | *** |
| Out-turn | *** | *** | *** |

**Expenditure by category**

- Staff costs: ***
- Other costs: ***
- Capital costs: ***

### *Administration*

**Staff numbers**[14]

| | Total staff | SCS | Non-SCS |
|---|---|---|---|
| 31 March 2022 | 7,082.1 | 114.7 | 6,967.4 |
| 31 March 2023 | 7,162.08 | 120.51 | 7,041.57 |

**Recruitment in 2022/23**

- GCHQ recruited 586 new staff against a target of 820 in 2022/23.[15] GCHQ also recruited 132 students for short-term placements in this period.
- This compares with recruiting 386 new staff against a target of 739 in 2021/22 (with 258 students for short-term placements).

**Major projects in 2022/23**

- Computer Network Exploitation (CNE) Growth: This project aims to increase GCHQ's capability to deliver CNE operations and is driven by a new set of demands for additional capacity from two sources: ***[16] and the ***. Delivery of this programme is measured through milestones that represent the increasing provision of CNE capacity. During the 2022/23 financial year, out of a total of five planned milestones, four were delivered and one was cancelled.
- Cloud Adoption: This is a project preparing GCHQ for the adoption of a new Cloud platform. Delivery of the programme is measured through milestones: five project milestones were delivered in the 2022/23 financial year.
- Continuous At-Sea Deterrent (CASD) programme: This project aims to improve the assurance that the UK Intelligence Community can provide for the UK's CASD. During this period, the project was reported as making '*** progress' against its target framework.

[13] As reported to the Committee in GCHQ's end-year report for the 2022/23 financial year.

[14] These figures refer to the number of FTE staff as at the end of each financial year. GCHQ also employed a number of contractors/consultants. These figures are not included but have estimated costs of *** in 2022/23 and *** in 2023/24.

[15] Recruitment target reduced to 601 in-year due to recruitment and vetting capacity issues.

[16] ***

| | |
|---|---|
| Diversity and inclusion 2022/23 | • GCHQ's median ethnicity pay gap increased from 9.2% in 2021/22 to 11.5% in 2022/23. Similarly, GCHQ's median gender pay gap increased from 10.9% in 2021/22 to 12.6% in 2022/23.<br>• A member of staff in the National Cyber Security Centre (NCSC) was recognised by EqualityX[17] as one of the Top 10 Most Influential Muslims in Technology.<br>• The Whittaker Initiative, GCHQ's Inclusive Practice Programme, worked with over 800 staff to enable them to understand how they can shape the organisation's culture.<br>• GCHQ began collecting data from staff – on a voluntary basis – to understand whether there are systemic organisational biases that are influencing how people join and progress within the organisation.<br>• GCHQ launched its new Accessibility Leadership Programme, a four-day face-to-face programme aimed at all staff with a disability, invisible illness or neurodivergence. |
| ***Policy*** | |
| Allocation of effort at 31 March 2023 | • Mission-specific programmes, including: counter-terrorism; offensive cyber; serious organised crime; and counter-proliferation – ***<br>• Capability exploitation – 18%<br>• Engineering – 18%<br>• IT services – 11%<br>• Cyber security – ***<br>• Corporate services (including human resources and finance) – 12% |
| Major achievements reported to the Committee for 2022/23 | • GCHQ hosted a workshop that brought together a number of international Signals Intelligence (SIGINT) agencies to discuss the challenges presented by China.<br>• GCHQ provided support and expertise to the Home Office and Department for Culture, Media and Sport throughout the passage of the Online Safety Act 2023.<br>• GCHQ provided insight into China's potential response to ***.<br>• GCHQ continued to produce reporting on Russia's war in Ukraine. This included providing insights into ***, as well as insights on Russian efforts to *** in Ukraine.<br>• GCHQ provided linguist support to operations in relation to missing UK nationals ***. |
| ***Crisis response impact 2022/23*** | |
| The war in Ukraine increased the resourcing pressure on GCHQ's Russia Mission. It therefore had to reduce other areas of Intelligence and Effects work that were not related to ***. This represented a re-deployment of around *** of GCHQ's operational Intelligence and Effects workforce into Russia/Ukraine crisis-response work during this period. However, GCHQ was able to move from an initial 'surge' footing to an established effort by the end of this period.<br><br>More widely, GCHQ reported that ***, which was created in response to the ***, ceased work. | |

[17] EqualityX is an organisation that celebrates Muslim talent and champions the achievements of Muslims.

## Defence Intelligence (DI)

### *Expenditure in 2022/23*[18]

**Total budget and out-turn**[19]

| £'000 | Resource spending | Capital spending | TOTAL |
|---|---|---|---|
| Budget | *** | *** | *** |
| Out-turn | *** | *** | *** |

**Expenditure by category**

- Operational staff costs: ***
- Research and development: ***
- Other operational costs: ***
- Other administrative costs: ***
- Against this, DI received an income of ***

**DI core spending – total budget and out-turn**[20]

| £'000 | Resource spending | Capital spending | TOTAL |
|---|---|---|---|
| Budget | 359,332 | 36,733 | 396,065 |
| Out-turn | 364,892 | 36,766 | 401,658 |

### *Administration*

**Staff numbers**[21]

**DI staffing figures *****[22]

| | Total staff | Total civilian staff | Total Armed Forces staff | Armed Forces | | Civilian staff | |
|---|---|---|---|---|---|---|---|
| | | | | SCS | Non-SCS | SCS | Non-SCS |
| 31 March 2023 | *** | *** | *** | *** | *** | *** | *** |

**DI core personnel**

| | Total staff | Total civilian staff | Total Armed Forces staff | Armed Forces | | Civilian staff | |
|---|---|---|---|---|---|---|---|
| | | | | SCS | Non-SCS | SCS | Non-SCS |
| 31 March 2022[23] | 4,252 | 1,500 | 2,752 | 8 | 2,744 | 9 | 1,491 |
| 31 March 2023 | 4,012 | 1,408 | 2,604 | 7 | 2,597 | 11 | 1,398 |

[18] As reported to the Committee in DI's end-year report for the financial year 2022/23.

[19] DI subsequently reported that between 2023 and 2024, some RDEL expenditure was reclassified, which artificially reduced RDEL costs by £10 million.

[20] ***

[21] These figures refer to the number of FTE staff as at the end of each financial year. DI also employed a number of contractors/consultants. These figures are not included but have estimated costs of £28.904 million in 2022/23 and £31.092 million in 2023/24.

[22] ***

[23] DI has now informed the Committee that due to a transition between different HR systems, the 31 March 2022 figures published in the Committee's Annual Report 2022–2023 were incorrect. The figures included above are the correct figures for 31 March 2022.

| | |
|---|---|
| Recruitment in 2022/23 | ● DI recruited 168 new civilian staff in 2022/23, up from 143 in 2021/22. |
| Major projects in 2022/23 | ● PRIDE: This project aims to consolidate the DI estate, with the Defence Geographic Centre (DGC) at Feltham transferring its operations to RAF Wyton, and MoD Feltham being released from the Ministry of Defence (MoD) estate. During the 2022/23 financial year, a workforce strategy was designed to sustain operations during the move of personnel to RAF Wyton.<br>● DI was unable to provide any information as to what it had delivered against its other two major projects this year. The two projects in question are: RAF Digby and Defence Intelligence Consolidation.[24] |
| Diversity and inclusion 2022/23 | ● DI created a 'Culture Action Plan' to address five key themes: Clarity, Confidence, Capability, Continuous Improvement and Collaboration.<br>● DI expanded its Diversity and Inclusion (D&I) Adviser network by training new advisers and improving signposting for people to access this resource.<br>● DI implemented the 'Green Dot'[25] behaviour intervention campaign and held online sessions in March 2023. DI reported that this had high uptake levels from its staff.<br>● DI established a Neuro-Inclusivity Network and a Mental Health and Wellbeing Network. |
| ***Policy*** | |
| Allocation of effort at 31 March 2023 | ● Total operational and analysis effort – 83.66%. This comprises:<br>– All source analysis and assessment – 9.2%<br>– Collection and analysis – 74.46%<br>● Operational support – 11.58%. This comprises:<br>– Security and intelligence training – 9.55%<br>– Intelligence policy and future capability development – 1.54%<br>– Reserves – 0.49%<br>● Central support – 4.74% |

[24] DI provided a late update on these two projects after the Report had been written. Regarding RAF Digby, DI confirmed that the winning tender's bid had to be terminated due to contracting issues. However, the re-tendering of the entire project was avoided as DI was able to secure an exemption for a single source delivery. On the Defence Intelligence Consolidation project, an assessment study was completed, and a decision was made to change the location of some of the requirements. This additional work extended the timelines for the programme approvals plan.

[25] Green Dot is an initiative that seeks to encourage staff to raise concerns about any behaviour that makes them feel uncomfortable or excluded.

| | |
|---|---|
| Major achievements reported to the Committee for 2022/23 | ● DI helped to ***. This helped to inform HMG's understanding of potential *** and address counter-intelligence concerns.<br>● DI continued its 'daily tweeting' campaign to counter Russia's narrative on the war in Ukraine; in terms of dissemination, DI reported that these tweets were the most successful social media campaign by UK Defence ever conducted.<br>● DI tracked *** vessels within several naval theatres ***, providing situational awareness of *** vessels and contributing to wider Five Eyes understanding of *** naval patterns.<br>● UK Defence, including DI, provided significant support to the security around the FIFA World Cup in Qatar. DI delivered multiple threat assessments, drawing on a range of capabilities (***). |

## *Crisis response impact 2022/23*

In 2023, DI's primary focus was on supporting the Ukrainian counter-offensive; however, it also supported a number of other crisis events, including the evacuation of personnel from Sudan in April 2023 and the UK response to the Niger coup in July 2023.

## National Security Secretariat (NSS)

### *Expenditure in 2022/23*[26]

**Total budget and out-turn**

| £'000 | Resource spending | Capital spending | TOTAL |
|---|---|---|---|
| Budget | 17,190.0 | 0 | 17,190.0 |
| Out-turn | 18,835.5 | 0 | 18,835.5 |

**Expenditure by category**

- Operational staff costs: £15.2m
- Operational IT costs: £1.7m
- Other operational costs: £1.9m
- National Cyber Security Programme: £1.2m[27]

### *Administration*

**Staff numbers**[28]

| | Total staff | SCS[29] | Non-SCS |
|---|---|---|---|
| 31 March 2022 | 196 | 23 | 173 |
| 31 March 2023 | 189.4 | 29.1 | 160.3 |

**Recruitment in 2022/23**

- NSS recruited 112 new staff in 2022/23, up from 46 in 2021/22.

**Major projects in 2022/23**

- None reported.

**Diversity and inclusion 2022/23**

- NSS conducted a bullying, harassment and discrimination staff survey and used the data to develop five actions that ranged from mandatory training for senior management to implementing a standardised approach for new staff joining NSS.
- NSS took part in the wider Cabinet Office pilot of an anonymous reporting tool, the bullying, harassment and discrimination Anonymous Speak Up Portal.

### *Policy*

**Allocation of effort at 31 March 2023**

- Policy teams and private office: 91%
- Corporate services for NSS: 9%

[26] As reported to the Committee in NSS's end-year report for financial year 2022/23.
[27] Separate funding stream.
[28] These figures refer to the number of FTE staff as at the end of each financial year. NSS also employed a number of contractors/consultants. These figures are not included. The estimated costs for these contractors were not available for 2022/23, but were estimated at £161,610 for 2023/24.
[29] Includes one SCS 4 – the National Security Adviser.

| | |
|---|---|
| Major achievements reported to the Committee for 2022/23 | • NSS led the national security elements of Operation LONDON BRIDGE following the death of HM Queen Elizabeth II. It worked closely with the Home Office, the Agencies and law enforcement to identify national security risks to the lying in state and the state funeral, and to produce protective security plans for each event.<br>• NSS contributed to the Integrated Review Refresh, which was published by the Cabinet Office on 13 March 2023, updating the Government's security, defence, development and foreign policy priorities to reflect changes in the global context since the 2021 Integrated Review.<br>• NSS worked with the Department for Culture, Media and Sport and the Department for Education to develop options for increasing the uptake of computer science as a subject in schools in order to increase the number of individuals with cyber skills. |

## *Crisis response impact 2022/23*

NSS moved staff around within their own team structures to provide more support to priority areas. For example, at one point during the 2022/23 financial year, the majority of staff in the International Affairs Unit were deployed to work on the Russia/Ukraine response.

## Joint Intelligence Organisation (JIO)

### *Expenditure in 2022/23*[30]

**Total budget and out-turn**

| £'000 | Resource spending | Capital spending | TOTAL |
|---|---|---|---|
| Budget | 11,500 | 2,000[31] | 13,500 |
| Out-turn | 11,029 | 1,616 | 12,645 |

**Expenditure by category**[32]

- Staff costs: £8.9m
- Other operational costs: £196,000
- The remaining out-turn is accounted for primarily by accommodation/ estates, staff training, supplies and services, and other administrative costs.

### *Administration*

**Staff numbers**[33]

| | Total staff | SCS | Non-SCS |
|---|---|---|---|
| 31 March 2022 | 106 | 10 | 96 |
| 31 March 2023 | 97.6 | 9 | 88.6 |

**Recruitment in 2022/23**

- JIO recruited 13 new staff against a target of 61 in 2022/23, down from 31 in 2021/22.[34]

**Major projects in 2022/23**

- The INDEX (Information and Data Exchange) system: This project aims to create a cross-departmental platform for sharing analysis and assessment. INDEX will use machine learning to help analysts identify content most relevant to their subject of interest. The platform was being developed during the 2022/23 financial year.

**Diversity and inclusion 2022/23**

- JIO diversity data: 39% female; 13% ethnic minority background (23% did not declare their ethnic background); 6% LGBT (30% did not declare their sexual orientation); and 10% disabled (20% did not declare whether or not they had a disability).
- JIO produced an assessment of culture, diversity and inclusion in the national security community in January 2023. The assessment concluded that, despite some areas of progress, a faster and greater change of culture was needed across the national security community to deliver the Integrated Review's outcomes, and to respond to complex global challenges.

[30] As reported to the Committee in JIO's end-year report for the 2022/23 financial year.
[31] JIO received £2 million in funding from the Agencies for its INDEX programme.
[32] JIO also received an income of £364,000 from course fees and other Government departments in 2022/23.
[33] These figures refer to the number of FTE staff as at the end of each financial year. JIO also employed a number of contractors/consultants. These figures are not included but have estimated costs of £101,671.56 in 2023/24. JIO reported no contractors/consultants in 2022/23.
[34] The reduction in the number of staff recruited into JIO was due to a Cabinet Office recruitment freeze.

| | |
|---|---|
| | ● Internally, JIO worked to improve its own culture. This included providing opportunities for staff to articulate their desired working culture, particularly in relation to shared values and behaviours.<br>● JIO participated in national security community activities, including providing mentors to a wide range of cross-Government initiatives (such as the National Security Race Strategy). |
| ***Policy*** | |
| Allocation of effort at 31 March 2023 | ● Total operational activity: 92%<br>● Corporate services: 8% |
| Major achievements reported to the Committee for 2022/23 | ● JIO issued 51 Joint Intelligence Committee (JIC) Assessments, 32 Intelligence Briefs and 173 JIO Spotlights.<br>● The JIC Chair briefed NATO's North Atlantic Council on the geopolitical implications of the Russia–Ukraine war.<br>● In September 2022, the JIO hosted the annual South Asia Five Eyes analytical conference in London. |
| ***Crisis response impact 2022/23*** | |
| Russia/Ukraine dominated JIO resources and outputs during 2022/23, with periods where staff had to be moved across to this area as intelligence reporting and the demand for assessment increased. JIO also moved two staff from work on professionalisation and tradecraft to increase resilience in their assessment teams. | |

## Homeland Security Group (HSG)

### *Expenditure in 2022/23*[35]

**Total budget and out-turn**

| £'m | Resource spending | Capital spending | TOTAL |
|---|---|---|---|
| Budget | 1,171 | 180 | 1,351 |
| Out-turn | 1,129 | 166 | 1,295 |

**Expenditure by category**[36]

- Staff costs: £85.5m
- Other costs: £1,281.1m
- Against this, HSG received an income of £237.8m, and funding from:
  - Conflict, Security and Stability Fund: £3m
  - National Security Council (Nuclear): £16.9m

### *Administration*

**Staff numbers**[37]

| | Total staff | SCS | Non-SCS |
|---|---|---|---|
| 31 March 2022 | 1,113 | 33 | 1,080 |
| 31 March 2023 | 1,211 | 34 | 1,177 |

**Recruitment in 2022/23**

- HSG recruited 251 new staff in 2022/23, up from 214 in 2021/22.

**Major projects in 2022/23**

- Radiological & Nuclear Change Programme: This seeks to improve the UK's defences against radiological and nuclear terrorism, and its preparedness for such risks. In 2022/23, HSG deployed 270 new radionuclide identification devices (RIDs)[38] across 65 sites and replaced obsolete mobile radiation detection units. It also began to replace electronics across 85 Cyclamen System 1 & 2 portals – which are border detection systems designed to target radioactive and nuclear materials – to extend their lifespans.
- Targeted Interception Programme: This programme seeks to deliver a replacement to the existing law-enforcement mission management system for the targeted interception of communications, in order to keep pace with evolving technology. The Outline Business Case for the programme was due to be reviewed by the Financial Investment Committee in November 2022. However, this milestone was delayed so that HSG could check if there was a commercial off-the-shelf system that would be more cost-effective and less risky. In January 2023, it was agreed that the bespoke system was still the best option.

[35] As reported to the Committee in HSG's end-year report for the financial year 2022/23.
[36] The vast majority of HSG expenditure is administered via grants mechanisms, and CT policing grants generally constitute over 75% of HSG's net budget.
[37] These figures refer to the number of FTE staff as at the end of each financial year. HSG also employed a number of contractors/consultants. These figures are not included but have estimated costs of £4.6 million in 2022/23 and £4.9 million in 2023/24.
[38] These are portable devices that can detect, locate and identify radioactive materials by analysing the gamma radiation they emit.

| | |
|---|---|
| | ● Internet Connection Records (ICR)[39] Project: This project was established in April 2022 and focuses on enabling public authorities to obtain ICR data in order to effectively investigate internet-enabled/ dependent crimes. In August 2022, concerns around the affordability and feasibility of the project were raised. In response, HSG changed the technical approach to the programme and began to work with Telecommunications Operators to explore cost-effective and sustainable options for collecting ICRs within their networks. Detailed designs for such options were completed in March 2023. |
| Diversity and inclusion 2022/23 | ● HSG undertook a refresh of its Diversity and Inclusion Strategy to align with strategies in the wider national security community and Home Office. |
| ***Policy*** | |
| Allocation of effort at 31 March 2023 | ● National Security Directorate (including arm's length bodies): 33%<br>● Directorate of State Threats and Cyber: 9%<br>● PREVENT and Research and Information Communication Unit: 11%<br>● PROTECT, PREPARE, CBRNE and science (including the Joint Security and Resilience Centre): 18%<br>● Data, Information and Operations: 14%<br>● Central Directorate (formerly CONTEST): 8%<br>● Economic Crime Directorate: 7% |
| Major achievements reported to the Committee for 2022/23 | ● The Security Minister announced the establishment of the 'Defending Democracy Taskforce' in November 2022. The taskforce aims to ensure that the UK's democratic processes and institutions are resilient against threats of foreign interference.<br>● HSG contributed to Operation LONDON BRIDGE, including the co-ordination and security of the event.<br>● HSG worked with MI5 and policing partners to identify and address national security threats to the 2022 Commonwealth Games. |
| ***Crisis response impact 2022/23*** | |
| HSG responded to a number of major events including:<br>● the death of HM Queen Elizabeth II (Operation LONDON BRIDGE);<br>● ongoing instability in Ukraine; and<br>● the Western Jet Foil Immigration terrorist attack in October 2023.<br><br>The initial response to Ukraine required the redeployment of staff; however, the remainder of these crises were managed within existing business areas. HSG maintained a volunteer cadre of 30 staff to ensure that resource could be deployed to crisis roles at short notice. | |

[39] Internet Connection Records (ICRs) are a form of Communications Data. They represent a record of an event held by a Telecommunications Operator about the service to which a customer has connected on the internet. They contain data about access to internet services but do not include content information about the activity. For example, an ICR might show that an individual has used a chat application but not what the message was that they sent or who they sent it to.

# ANNEX C: EXPENDITURE, ADMINISTRATION AND POLICY – 2023/24

<table>
<tr><th colspan="2">Single Intelligence Account</th></tr>
<tr><td colspan="2">Expenditure in 2023/24</td></tr>
<tr><td>Total budget and out-turn</td><td>
<table>
<tr><th>£’000</th><th>Resource spending</th><th>Capital spending</th><th>TOTAL</th></tr>
<tr><td>Budget</td><td>3,518,085</td><td>1,378,780</td><td>4,896,865</td></tr>
<tr><td>Out-turn</td><td>3,498,605</td><td>1,372,096</td><td>4,870,701</td></tr>
</table>
</td></tr>
<tr><td>Expenditure by category</td><td>• Staff pay: £1.49bn<br>• Other expenditure: £2.72bn<br>• Capital spending: £1.37bn</td></tr>
</table>

The figures above represent the combined budgets of MI5, SIS, GCHQ, *** and NSS costs for managing the Single Intelligence Account (SIA) as already published in the Single Intelligence Account. The Resource and Capital figures above include Departmental Expenditure Limits and Annually Managed Expenditure, as published in the SIA Annual Resource Accounts.

The Committee has been provided with the individual figures for each Agency; however, these have been redacted in the subsequent pages, since to publish them would allow the UK’s adversaries to deduce the scale and focus of the Agencies’ activities and effort more accurately. This would enable them to improve their targeting and coverage of the Agencies’ personnel and capabilities, and to seek more effective measures to counter the Agencies’ operations against them.

## MI5 (Security Service)

### *Expenditure in 2023/24*[40]

**Total budget and out-turn**

| £'m | Resource spending | Capital spending | TOTAL |
|---|---|---|---|
| Budget | *** | *** | *** |
| Out-turn | *** | *** | *** |

**Expenditure by category**

- Staff costs (including R&D staff costs CDEL):[41] ***
- Other revenue costs (including professional services, accommodation, research and development, and IT systems): ***
- Capital costs (excluding R&D staff costs CDEL): ***

### *Administration*

**Staff numbers**[42]

| | Total staff | SCS[43] | Non-SCS |
|---|---|---|---|
| 31 March 2023 | 5,384.5 | 86 | 5,298.5 |
| 31 March 2024 | 5,664.9 | 71 | 5,593.9 |

**Recruitment in 2023/24**

- MI5 recruited 726[44] staff, against a target of 797 in 2023/24.
- This compares with recruiting 625 new staff against a target of 602 in 2022/23.

**Major projects in 2023/24**

- Preparation for MI5's adoption of a Cloud platform: An Outline Business Case was presented to, and approved by, the Resource Council in May 2024. The Spending Review approved funds (of ***) for financial year 2024/25 to enable progress relating to the migration of data.
- TRANSFORMING CORPORATE SERVICES: Work continued on the final objective of the programme to establish a cross-community Corporate Services team. In July 2023, MI5 met a key 'go-live' date in relation to these new digital capabilities (implementing a new digital Human Resources platform) and reviewed lessons learned from this process in February 2024.
- Counter Terrorism Operations Centre (CTOC): The programme continued on track and within budget, with four floors operating as business as usual at the end of March 2024, and construction for all 15 floors completed on schedule. A Gateway Review in July 2023 assessed the status of the project as 'amber', with further work required but an overall positive trajectory towards completion.

[40] As reported to the Committee in MI5's end-year report for the 2023/24 financial year.

[41] Research and development staff costs account for staff who occupy roles that are categorised as research and development activity. They count as Capital Departmental Expenditure Limit (CDEL) expenditure and are separate to Resource Departmental Expenditure Limit (RDEL) staff costs. When combined, the two figures account for total staff cost.

[42] These figures refer to the number of full-time equivalent (FTE) staff as at the end of each financial year. MI5 also employed a number of contractors/consultants. These figures are not included but have estimated costs of *** million in 2022/23 and *** million in 2023/24.

[43] Senior Civil Service.

[44] Figures provided are of staff headcount rather than FTE.

| | |
|---|---|
| Diversity and inclusion 2023/24 | ● While MI5 continued to focus on recruitment of individuals from under-represented groups, the proportion of new female and ethnic minority staff declined from 2021/22. New joiners were 58% female (down from 60%), and 13% from an ethnic minority background (down from 22%).<br>● MI5 published its Diversity and Inclusion Report, which consolidates previous reporting on pay gaps for gender, ethnicity, sexual orientation and disability. In 2023, MI5 reported that the median gender pay gap decreased for the second consecutive year to 14.1%, falling below the UK national average for the first time. Meanwhile in 2023, the median ethnicity pay gap increased to 12.3% from 7%.[45]<br>● In June 2024, MI5 launched its Equality, Diversity and Inclusion (EDI) strategy to 2030. This set out a range of objectives to improve inclusion and behaviour, and to embed EDI into MI5 decision-making.<br>● MI5 continues to run its Summer Intelligence Internship: The 2024 scheme provided opportunities to *** people, 56% of whom were female.<br>● In December 2023, MI5 reconfirmed its Disability Confident Leader status.<br>● In June 2024, MI5, SIS and GCHQ launched 'Upstander' Training to encourage staff to challenge inappropriate behaviours in the workplace. MI5 aims to have delivered training to 30% of staff by the end of the 2025/26 financial year. |
| ***Policy*** | |
| Allocation of effort at 31 March 2024[46] | ● Counter-terrorism (except NIRT): 57%<br>● Counter State Threats: 27%<br>● Northern Ireland-related terrorism (NIRT): 16% |
| Major achievements reported to the Committee for 2023/24 | ● MI5 disrupted one Islamist terrorist attack, two Extreme Right-Wing Terrorist (ERWT) attacks, and one Left-Wing, Anarchist and Single-Issue Terrorist (LASIT) attack between April 2023 and March 2024.<br>● MI5 and the Police Service of Northern Ireland (PSNI) investigated the attempted murder of off-duty PSNI officer John Caldwell. PSNI has arrested a number of individuals in connection with the attempted murder.<br>● ***<br>● MI5 and the National Protective Security Authority (NPSA, formerly CPNI – Centre for the Protection of National Infrastructure) supported work to ensure the security of the 2024 UK General Election. This included: delivering security videos and guidance on personal safety for candidates; providing guidance on protecting pedestrian queues; mail screening of suspect packages at polling stations; and raising awareness of signs of malicious activities by state actors. |

[45] MI5 noted that high rates of recruitment amongst ethnic minorities could have contributed to the increase in the ethnicity pay gap, as new recruits are more likely to start in junior positions, and thus have lower salaries.
[46] Operational allocation of effort (by FTE, to the nearest per cent).

## *Crisis response impact 2023/24*

During this period, MI5 supported the Government's response to a heightened threat from Iran:

- Iran increased its targeting of individuals that it views as threats to the regime as a result of the protests which first started in the country in 2022.
- MI5's Iran Mission has particularly focused on understanding the effect that the Gaza conflict, and the subsequent escalation in hostilities between Israel and Iran, has had on Iranian intent towards the UK.
- ***

MI5 also supported the Government's response to the Israel/Gaza conflict:

- MI5 supported the UK Government's response to the 7 October 2023 attack on Israel by Hamas. This included supporting the UK Government ***. This affected ***; however, this returned to business as usual from ***.
- Following the 7 October attack on Israel by Hamas, MI5 experienced an increase in unsolicited reporting. This reporting required triaging to determine whether it met the threshold for further investigation. The majority did not meet the threshold for further investigation. ***.

MI5 continued to support the Government's response to the Russian invasion of Ukraine:

- A combination of work to support Ukraine's security and an increase in the direct threat posed by the Russian Intelligence Services towards the UK has contributed to resource pressures across MI5.
- Elements of the direct threat to the UK included: the threat of assassination; political interference activity; cyber threats; and the emergence of sabotage directed by Russia against the UK and UK interests overseas.

## Secret Intelligence Service (SIS)

### *Expenditure in 2023/24*[47]

**Total budget and out-turn**

| £'m | Resource spending | Capital spending | TOTAL |
|---|---|---|---|
| Budget | *** | *** | *** |
| Out-turn | *** | *** | *** |

**Expenditure by category**

- Staff costs: ***
- Other costs: ***
- Capital costs: ***
- Conflict, Security and Stability Fund: ***[48]
- National Cyber Security Programme: ***[49]

### *Administration*

**Staff numbers**[50]

| | Total staff | SCS | Non-SCS |
|---|---|---|---|
| 31 March 2023 | 3,752.96 | 91.91 | 3,661.05 |
| 31 March 2024 | 3,933.55 | 94.40 | 3,839.15 |

**Recruitment in 2023/24**

- SIS recruited *** new staff against a target of *** in 2023/24.
- This compares with recruiting *** new staff against a target of *** in 2022/23.

**Major projects in 2023/24**

- Capability Portfolio: A Gateway Review in 2023 made three 'critical' recommendations for the project and two 'essential' recommendations. The most urgent recommendations included: improving financial tracking and controls across all Capability Centres; relaunching P3M[51] approaches for a specific part of the programme; and clearer communication to the Capability Centres to increase engagement and understanding of the need for change.
- Science, Technology and Engineering Programme (STEP): The programme provided expertise and *** of research and development investment to the Government's AI Taskforce to support the UK's work on foundation artificial intelligence (AI) models and to accelerate the adoption of AI within the UK national security community. A Gateway Review in December 2023 called it a "*well-led, impactful programme*". However, financial uncertainty created by the Spending Review meant that the programme was assessed as 'amber', rather than 'green'.
- Project ***: A project to improve SIS's *** for ***. The Full Business Case for this project was approved in March ***, with the capability intended to be deployed to *** by ***.

[47] As reported to the Committee in SIS's end-year report for the financial year 2023/24.
[48] Separate funding stream.
[49] Separate funding stream.
[50] These figures refer to the number of FTE staff as at the end of each financial year. SIS also employed a number of contractors/consultants. These figures are not included but have estimated costs of *** in 2022/23 and *** in 2023/24.
[51] Portfolio, Project and Programme Management.

| | |
|---|---|
| Diversity and inclusion 2023/24 | ● SIS's median pay gap for gender and ethnicity rose from 6–7% to 13–15%. There was a significant drop in representation of those from under-represented groups at the more senior grades.<br>● In 2023, *** candidates took part in SIS's Summer Intelligence Officer Internship programme: all *** candidates took the option to sit the SIS assessment centre, with *** passing and being offered permanent SIS roles. In 2024, SIS increased the number of internships available from *** to ***.<br>● SIS launched a sponsorship scheme for ethnic minority colleagues at non-SCS grades.<br>● SIS worked with a youth-specialist social enterprise to undertake local outreach and recruitment for their Change, Analysis and Projects Apprenticeship.<br>● During this period, 10% of the SIS workforce reported experiencing bullying. SIS took steps to address this issue, including a plan to roll out 'Upstander' training across the organisation, which encourages staff to raise any concerns about inappropriate behaviour. |
| ***Policy*** | |
| Allocation of effort at 31 March 2024 | ● Key operational activities, including: counter-terrorism; cyber and access generation; global themes; and prosperity and economic stability – 35.0%<br>● Operational support, including: global network enabling; covert operations; data exploitation; operational security; and operational technology – 34.8%<br>● Corporate services, including: legal and private offices; human resources; finance; estates and business change; IT infrastructure; security and compliance; science, research and innovation; and policy, requirements and communications – 30.2% |
| Major achievements reported to the Committee for 2023/24 | ● SIS worked with *** partners to *** Russian officials and *** hostile Russian actors in the ***.<br>● SIS provided insight into the *** and contributed extensively to Joint Intelligence Committee (JIC), COBR and other deliberations on the UK's policy response to the aborted rebellion by the *** in *** 2023.<br>● SIS delivered a range of support to Ukrainian partners – *** – which has allowed Ukraine to continue to defend itself against the Russian invasion.<br>● SIS engaged with a range of international partners (***) to understand and co-ordinate work on the global risks of potential destabilisation in the South China Sea.<br>● SIS shared details of a possible ISKP (Islamic State – Khorasan Province) plan to attack the ***, in time for defensive measures to be taken.<br>● SIS delivered reporting on *** position and intent, which informed UK and US policy-makers involved in hostage negotiations. |

## *Crisis response impact 2023/24*

- SIS moved their response to the conflict between Israel and Gaza from a crisis footing to business as usual.
- In this period, the cross-Agency team supporting Afghan relocation and resettlement efforts reduced from *** officers to ***. Plans were also in place to reduce the team to *** officers in early 2024/25.

## Government Communications Headquarters (GCHQ)

### *Expenditure in 2023/24*[52]

**Total budget and out-turn**

| £'m | Resource spending | Capital spending | TOTAL |
|---|---|---|---|
| Budget | *** | *** | *** |
| Out-turn | *** | *** | *** |

**Expenditure by category**

- Staff costs: ***
- Other costs: ***
- Capital costs: ***

### *Administration*

**Staff numbers**[53]

| | Total staff | SCS | Non-SCS |
|---|---|---|---|
| 31 March 2023 | 7,162.08 | 120.51 | 7,041.57 |
| 31 March 2024 | 7,549.13 | 120.97 | 7,428.16 |

**Recruitment in 2023/24**

- GCHQ recruited 774 new staff against a target of 1,131 in 2023/24.[54] GCHQ also recruited 212 students in this period for short-term placements.
- This compares with GCHQ recruiting 586 new staff against a target of 820 in 2022/23 (and 132 students).

**Major projects in 2023/24**

- Computer Network Exploitation (CNE) Growth: Building on the progress in 2022/23 – in which four out of five milestones for that year were achieved – this project met all five of its planned milestones for the 2023/24 financial year.
- Continuous At-Sea Deterrent (CASD): This project aims to enhance the UK Intelligence Community's provision of assurance of the UK's CASD. The Full Business Case for this project, approved by HM Treasury, was ***.
- Structured Data Engineering: This capability will facilitate collaboration across the Intelligence Community by ensuring that a wide range of information can be accessed securely and efficiently, and will enable Target Discovery, Tracking and Development. During the 2023/24 financial year, GCHQ's *** was upgraded and GCHQ's *** was replaced.

[52] As reported to the Committee in GCHQ's end-year report for the 2023/24 financial year.

[53] These figures refer to the number of FTE staff as at the end of each financial year. GCHQ also employed a number of contractors/consultants. These figures are not included but have estimated costs of *** in 2022/23 and *** in 2023/24.

[54] This recruitment target was reduced to 911 in-year due to recruitment and vetting capacity issues.

| | |
|---|---|
| Diversity and inclusion 2023/24 | ● GCHQ introduced a single central Equality, Diversity and Inclusion Action Plan, which brings together their previous separate Ethnicity, Gender and Inclusion Action Plans. This will enable better co-ordination of EDI deliverables.<br>● In Q3–4 of 2023/24, 41% of the applicants that GCHQ attracted were female, and 32% were from an ethnic minority background. However, GCHQ noted that it expected that the statistics would be different for new joiners. GCHQ's projection for 2024/25 was that 39% of their new joiners would be female and 17% would be from an ethnic minority background.<br>● A cohort of GCHQ staff participated in the inaugural Five Eyes EDI Summit, hosted by the ***.<br>● GCHQ's campaign to encourage staff to share their diversity information, 'Count Me In', resulted in an increase in declaration rates for every recorded diversity characteristic, providing a more detailed picture of the demographics of the organisation.<br>● GCHQ formed the Workplace Adjustment Task Force in conjunction with the Agencies' new cross-community Corporate Services team. This is a cross-directorate community to resolve the most complex workplace adjustment issues. |
| ***Policy*** | |
| Allocation of effort at 31 March 2024 | ● Mission-specific programmes including: counter-terrorism (CT); offensive cyber; serious organised crime; and counter-proliferation – ***<br>● Capability exploitation – 19%<br>● Engineering – 19%<br>● IT services – 11%<br>● Cyber security – ***<br>● Corporate services (including human resources and finance) – 12% |
| Major achievements reported to the Committee for 2023/24 | ● GCHQ supported the Department for Science, Information and Technology and the AI Taskforce[55] to plan and deliver the Prime Minister's AI Safety Summit in November 2023.<br>● GCHQ supported cross-Government planning to ensure that the 2024 UK General Election was free from interference. In particular, the National Cyber Force and National Cyber Security Centre (NCSC) participated in a Cabinet Office-led UK Election Security preparation exercise, which sought to increase the Government's preparedness for any critical cyber incidents.<br>● NCSC provided support to the Foreign, Commonwealth and Development Office's (FCDO) Ukraine Cyber Programme, which aims to improve the resilience of Ukraine's critical national infrastructure.<br>● GCHQ considered the *** in 2024 and provided insights on ***.<br>● The NCSC published its sixth annual report on the Active Cyber Defence programme in July 2023.[56] |

[55] The AI Taskforce assesses the risks and opportunities posed by artificial intelligence.
[56] Active Cyber Defence seeks to reduce the harm from commodity cyber attacks by providing protective tools and services.

## *Crisis response impact 2023/24*

Further prioritisation (via the 2023 Intelligence Outcomes Prioritisation process) towards intelligence work on *** and *** required a decrease in GCHQ's *** effort, with approximately *** of GCHQ's *** workforce being redeployed.

GCHQ's operational response to various crises in the Middle East meant reprioritising work for staff in GCHQ's operational, legal, policy, international relationships and other teams; however, there was no long-term surge of staff to work on the Middle East.

## Defence Intelligence (DI)

### *Expenditure in 2023/24*[57]

**Total budget and out-turn**

| £'000 | Resource spending | Capital spending | TOTAL |
|---|---|---|---|
| Budget | *** | *** | *** |
| Out-turn | *** | *** | *** |

**Expenditure by category**

- Operational staff costs: ***
- Research and development: ***
- Other operational costs: ***
- Other administrative costs: ***
- Against this, DI received an income of ***

**DI core spending – total budget and out-turn**[58]

| £'000 | Resource spending | Capital spending | TOTAL |
|---|---|---|---|
| Budget | 384,675 | 31,830 | 416,505 |
| Out-turn | 374,538 | 40,702 | 415,240 |

### *Administration*

**Staff numbers**[59]

**DI staffing figures *****[60]

| | Total staff | Total civilian staff | Total Armed Forces staff | Armed Forces | | Civilian staff | |
|---|---|---|---|---|---|---|---|
| | | | | SCS | Non-SCS | SCS | Non-SCS |
| 31 March 2023 | *** | *** | *** | *** | *** | *** | *** |
| 31 March 2024 | *** | *** | *** | *** | *** | *** | *** |

**DI core personnel**

| | Total staff | Total civilian staff | Total Armed Forces staff | Armed Forces | | Civilian staff | |
|---|---|---|---|---|---|---|---|
| | | | | SCS | Non-SCS | SCS | Non-SCS |
| 31 March 2023 | 4,012 | 1,408 | 2,604 | 7 | 2,597 | 11 | 1,398 |
| 31 March 2024 | 3,968 | 1,452 | 2,516 | 7 | 2,509 | 11 | 1,441 |

[57] As reported to the Committee in DI's end-year report for financial year 2023/24.

[58] ***

[59] These figures refer to the number of FTE staff as at the end of each financial year. DI also employed a number of contractors/consultants. These figures are not included but have estimated costs of £28.904 million in 2022/23 and £31.092 million in 2023/24.

[60] ***

| | |
|---|---|
| Recruitment in 2023/24 | ● DI recruited 240 new civilian staff in 2023/24,[61] up from 168 in 2022/23. |
| Major projects in 2023/24 | ● PRIDE2: The contract award for the infrastructure needed to integrate the Defence Geographic Centre with RAF Wyton was completed in March 2024. MoD Feltham was partially disposed of with approximately 17% of the land being handed over to the Department for Education.<br>● RAF Digby: The infrastructure for the new technical infrastructure facility is currently being designed. A contract was also agreed to provide the new Single Living Accommodation for junior staff. However, the deadlines for both projects slipped: the accommodation is not now expected to be ready until January 2026, and the technical facility in November 2029.<br>● Defence Intelligence Consolidation: In December 2023, the Ministry of Defence (MoD) formally announced the closure and disposal of MoD Chicksands (actual disposal is not expected to be before 2030). |
| Diversity and inclusion 2023/24 | ● DI developed a 'Distressing Materials and Psychological Risk Management' policy and produced associated resources to support and provide guidance to staff working with distressing material.<br>● DI's Mental Health First Aiders Network was created in October 2023. This enabled trained personnel from DI to meet monthly, to share experience and resources and hear from guest speakers.<br>● The DI Diversity and Inclusion (D&I) Advisers and Practitioners (DIAP) Network was established in February 2024. The group meets regularly to facilitate discussion and ensure the distribution of information on D&I issues. |
| ***Policy*** | |
| Allocation of effort at 31 March 2024 | ● Total operational and analysis effort – 83.26%. This comprises:<br>– All source analysis and assessment – 9.55%<br>– Collection and analysis – 73.77%<br>● Operational support – 12.08%. This comprises:<br>– Security and intelligence training – 9.80%<br>– Intelligence policy and future capability development – 1.69%<br>– Reserves – 0.59%<br>● Central support – 4.66% |

[61] Armed Services manning is conducted centrally and the DI military staff is subject to the posting policy of the three Armed Services. DI does not recruit military staff directly.

| | |
|---|---|
| Major achievements reported to the Committee for 2023/24 | ● To support DI's work internationally, DI published a paper on 'China's influence playbook'. The paper assesses how and why China projects its international influence, and the implications of its actions.<br>● Working closely with JIO, DI provided assessments regarding the Wagner rebellion. DI also *** key figures in the Russian and Wagner Group leadership.<br>● The Chief of Defence Intelligence visited an overseas partner (***) to work with them on exposing Russian malign activity ***.<br>● DI provided insight into the scale and nature of the Taliban threat to candidates for the Afghanistan Relocation and Assistance Policy, supporting MoD and wider cross-Government efforts to maintain the scheme. |

## *Crisis response impact 2023/24*

DI provided support to Ukraine and work in relation to the Middle East following the Hamas attack against Israel on 7 October 2023.

An alternative resourcing model was used to meet an increase in demand for intelligence during: the Iranian attack on Israel (April 2024); Houthi activity in the Red Sea (January–June 2024); the Morocco earthquake (September 2023); and flooding in Libya (September 2023).

## National Security Secretariat (NSS)

### *Expenditure in 2023/24*[62]

**Total budget and out-turn**

| £'000 | Resource spending | Capital spending | TOTAL |
|---|---|---|---|
| Budget | 18,890 | 0 | 18,890 |
| Out-turn | 19,852 | 0 | 19,852 |

**Expenditure by category**

- Operational staff costs: £15.5m
- Operational IT costs: £1.8m
- Other operational costs: £2.5m
- National Cyber Security Programme: £1.2m[63]

### *Administration*

**Staff numbers**[64]

| | Total staff | SCS[65] | Non-SCS |
|---|---|---|---|
| 31 March 2023 | 189.4 | 29.1 | 160.3 |
| 31 March 2024 | 233.47 | 23.62 | 209.85 |

**Recruitment in 2023/24**

- NSS recruited 64.62 new staff in 2023/24, down from 112 in 2022/23.

**Major projects in 2023/24**

- None reported.

**Diversity and inclusion 2023/24**

- NSS refreshed its Diversity and Inclusion (D&I) Strategy following the results of their 2023/24 People Survey. This included embedding D&I into business-as-usual activities such as recruitment and induction processes, and tackling bullying, harassment and discrimination.
- NSS set up a monthly D&I newsletter, which signposts Civil Service-wide resources and events.
- NSS launched a reverse mentoring scheme for staff.

### *Policy*

**Allocation of effort at 31 March 2024**

- Policy teams and private office: 94%
- Corporate services for NSS: 6%

[62] As reported to the Committee in NSS's end-year report for financial year 2023/24.
[63] Separate funding stream.
[64] These figures refer to the number of FTE staff as at the end of each financial year. NSS also employed a number of contractors/consultants. These figures are not included. The estimated costs for these contractors were not available for 2022/23 but were estimated at £161,610 for 2023/24.
[65] Includes one SCS 4 – the National Security Adviser.

| | |
|---|---|
| Major achievements reported to the Committee for 2023/24 | ● The Counter State Threats Strategy received cross-Government collective agreement in April 2023. Work was carried out to implement the Strategy, and governance structures were also agreed.<br>● NSS led the national security elements of Operation GOLDEN ORB (supporting the Coronation of HM King Charles III), working closely with the Home Office, the Agencies and law enforcement to ensure public safety and reduce the possibility of security incidents. |

## *Crisis response impact 2023/24*

In the early stages of the Israel/Gaza conflict, NSS moved to a "*crisis posture*" and moved a large number of staff (primarily from within the organisation) across to provide resilience in response to the increased workload.

NSS temporarily increased its headcount to bring in staff from the FCDO, Home Office and the MoD to maintain resilience and provide a multi-department approach to the crisis-response work on the Middle East.

## Joint Intelligence Organisation (JIO)

### *Expenditure in 2023/24*[66]

**Total budget and out-turn**

| £'000 | Resource spending | Capital spending | TOTAL |
|---|---|---|---|
| Budget | 13,850 | 2,000 | 15,850 |
| Out-turn | 13,705 | 1,806 | 15,511 |

**Expenditure by category**[67]

- Staff costs: £9.5m
- Other operational costs: £297,000
- The remaining out-turn is accounted for primarily by accommodation/ estates, staff training, supplies and services, and other administrative costs.

### *Administration*

**Staff numbers**[68]

| | Total staff | SCS | Non-SCS |
|---|---|---|---|
| 31 March 2023 | 97.6 | 9 | 88.6 |
| 31 March 2024 | 116 | 8 | 108 |

**Recruitment in 2023/24**

- JIO recruited 53 new staff against a target of 76 in 2023/24, up from 13 in 2022/23.

**Major projects in 2023/24**

- None reported.

**Diversity and inclusion 2023/24**

- JIO diversity data: 42% female; 13% ethnic minority background (36% did not declare their ethnic background); 9% LGBT (37% did not declare their sexual orientation); and 15% disabled (34% did not declare whether or not they had a disability).
- JIO hosted a delegation from *** Equality, Diversity, Inclusion and Accessibility Team to discuss the value of data in tracking under-representation.

### *Policy*

**Allocation of effort at 31 March 2024**

- Total operational activity: 93%
- JIO corporate services: 7%

[66] As reported to the Committee in JIO's end-year report for the 2023/24 financial year.
[67] JIO also received an income of £610,000 from course fees and other Government departments in 2023/24.
[68] These figures refer to the number of FTE staff as at the end of each financial year. JIO also employed a number of contractors/consultants. These figures are not included but have estimated costs of £101,671.56 in 2023/24. JIO reported no contractors/consultants in 2022/23.

| | |
|---|---|
| Major achievements reported to the Committee for 2023/24 | ● JIO produced 47 Joint Intelligence Committee (JIC) Assessments, 22 Intelligence Briefs and 166 Spotlights.<br>● JIO provided bespoke training to the government of Somalia, to introduce them to the process of intelligence assessment.<br>● JIO supported the national security response to the 2024 UK General Election. |

## *Crisis response impact 2023/24*

JIO played a significant role in:

- HMG's crisis work on Sudan and the subsequent evacuation of British nationals;
- HMG's response to the war in Ukraine; and
- HMG's response to events in the Middle East, including the Hamas terrorist attacks on Israel, the subsequent conflict in Gaza, and broader regional tensions.

In particular, JIO reported that its Middle East and Russia/Ukraine teams were working under high pressure for much of 2023/24. These teams were supported during points of crisis by analysts from other teams within JIO. The redeployment of staff and increased demands affected the delivery of JIO's corporate and organisational development activities (such as diversity and inclusion initiatives).

## Homeland Security Group

### *Expenditure in 2023/24*[69]

**Total budget and out-turn**

| £'m | Resource spending | Capital spending | TOTAL |
|---|---|---|---|
| Budget | 1,207 | 280 | 1,487 |
| Out-turn | 1,244 | 242 | 1,486 |

**Expenditure by category**[70]

- Staff costs: £97.2m
- Other costs: £1,374.9m
- Against this, HSG received an income of £228.7m and funding from:
  - Conflict, Security and Stability Fund: £3m
  - National Security Council (Nuclear): £18.4m

### *Administration*

**Staff numbers**[71]

| | Total staff | SCS | Non-SCS |
|---|---|---|---|
| 31 March 2023 | 1,211 | 34 | 1,177 |
| 31 March 2024 | 1,229 | 35 | 1,194 |

**Recruitment in 2023/24**

- HSG recruited 186 new staff in 2023/24, down from 251 new staff in 2022/23.

**Major projects in 2023/24**

- Radiological & Nuclear Change Programme: This project seeks to improve the UK's defences against radiological and nuclear terrorism. During this period, the 2024 Business Case for this programme was being developed – although it is not going to be submitted until Autumn 2024.
- Targeted Interception Services Programme: In May 2023, a Gateway Review of the programme rated its progress as 'amber'.
- Internet Connection Records: A Business Case was submitted to establish a pilot with a Telecommunications Operator and develop a central system (the pilot was due to be completed in September 2024).

**Diversity and inclusion 2023/24**

- HSG developed a new Diversity and Inclusion Action Plan, which had the following objectives: reducing disparities in promotion and progression; reducing disparities in reward and recognition; and addressing disparities linked to the capabilities of line managers.
- HSG created a new staff site, which brought together HSG-specific and Home Office resources on diversity, inclusion and wellbeing into one place, so that staff can access the resources as needed.

[69] As reported to the Committee in HSG's end-year report for the financial year 2023/24.

[70] The vast majority of HSG expenditure is administered via grants mechanisms, and CT policing grants generally constitute over 75% of HSG's net budget.

[71] These figures refer to the number of FTE staff as at the end of each financial year. HSG also employed a number of contractors/consultants. These figures are not included but have estimated costs of £4.6 million in 2022/23 and £4.9 million in 2023/24.

| ***Policy*** | |
|---|---|
| Allocation of effort at 31 March 2024 | ● National Security Directorate (including arm's length bodies): 32%<br>● Directorate of State Threats and Cyber: 10%<br>● PREVENT and Research and Information Communication Unit: 11%<br>● PROTECT, PREPARE, CBRNE and Science (including the Joint Security and Resilience Centre): 19%<br>● Data, Information and Operations: 10%<br>● Central Directorate (formerly CONTEST): 8%<br>● Economic Crime Directorate: 10% |
| Major achievements reported to the Committee for 2023/24 | ● HSG led on the National Security Act, which received Royal Assent in July 2023. As outlined in the main body of this Report, the Act modernises counter-espionage laws to address evolving state threats to national security.<br>● HSG published a Fraud Strategy in May 2023. This includes 52 actions that the Government, law enforcement and industry will deliver with the overall aim of cutting fraud levels by 10%.<br>● HSG led on the Economic Crime and Corporate Transparency Act 2023, which received Royal Assent in October 2023. This Act reformed the role of Companies House and expanded law-enforcement powers to tackle economic crime and protect national security. |

## *Crisis response impact 2023/24*

HSG contributed to the Government response to a number of major events and crises, including:

- the manhunt for Daniel Khalife in September 2023;
- Hamas's attack on Israel on 7 October 2023 and the subsequent and ongoing conflict;
- incidents in the Red Sea and wider Middle East throughout 2023 and 2024;
- the response to the Hartlepool terrorist attack in October 2023;
- the July 2024 General Election; and
- nationwide riots in July and August 2024.

A new Israel/Hamas Hub was established to manage the medium to long-term implications of the conflict in Gaza.

# ANNEX D: INQUIRY DEADLINES

In its Annual Report 2022–2023, the Committee noted that it had been severely hampered by the failure of the UK Intelligence Community to meet standard deadlines as part of the ISC Inquiry process. The Committee had therefore hosted a substantive meeting in November 2022 where it called upon the heads of the organisations it oversees to provide assurances on a suitable way forward. As a result of this meeting, the Committee decided to operate a two-tier approach to its Inquiries, granting additional time for commissions in relation to a small number that fall into the tightly defined category of 'Exceptional Inquiries'.

The Committee continues to observe the operation of this two-tier approach: if it is not satisfied that the criteria are being used appropriately or that either set of deadlines is being met, then the Committee has agreed that it will revert to the previous – single – set of Standard Inquiry deadlines. We will therefore record, in each subsequent Annual Report, those deadlines set and met.

The following table covers only those Inquiry deadlines set during the time period covered by this Report.

| Inquiry | Commission | Deadline |
|---|---|---|
| Iran | Contested redaction requests | (a) An extension was requested by six organisations. The Committee agreed that one organisation's rationale provided was reasonable and granted the extension. The other organisations were granted a partial extension.<br>(b) Five other organisations failed to fully meet the deadline, submitting some of their contested redaction requests late. These requests could not be considered within the usual processes and had to be dealt with afterwards, between the Committee and the Prime Minister. |

ISBN 978-1-5286-6092-1
E03492825