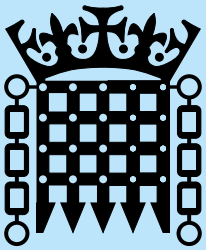

Intelligence and Security Committee of Parliament

Annual Report 2022–2023

Chairman:
The Rt Hon. Sir Julian Lewis MP

HC 287

Intelligence and Security Committee of Parliament

Annual Report 2022–2023

Chairman:
The Rt Hon. Sir Julian Lewis MP

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 5 December 2023

HC 287

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: isc.independent.gov.uk

ISBN 978-1-5286-4463-1

E02988480 12/23

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 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 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.

The 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

[*] Throughout the Report, the term 'Intelligence Community' is used to refer to the seven organisations that the Committee oversees; the term '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 Committee oversees operations subject to the criteria set out in section 2 of the Justice and Security Act 2013.

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).

CONTENTS

THE WORK OF THE COMMITTEE

1. **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.**

2. This Report summarises the work of the ISC for the period from April 2022 to March 2023 in carrying out its oversight of the Intelligence Community. The term 'Intelligence Community' currently refers to the three intelligence Agencies (MI5, SIS and GCHQ) and some of the parts of those policy departments which deal with intelligence and security matters (Ministry of Defence, Cabinet Office and Home Office). **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 – is addressed later in this Report.**

Membership during the period covered by this Report

3. On 14 December 2022, the Rt Hon. Stewart Hosie MP notified the Chairman of his intention to step down from his role on the Committee. Following a consultation process, as set out in the Justice and Security Act 2013, Owen Thompson 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 7 February 2023.

Work programme

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

- held 24 full Committee meetings, including evidence sessions with Government Ministers, senior officials from across the Intelligence Community and external experts, and briefing on the situation in Ukraine;
- conducted one visit to the Intelligence Community;
- held bilateral discussions with counterparts from the Parliaments of the Czech Republic and the Republic of South Africa, and from the Government of New Zealand; and
- held one other meeting.

[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.

Reports

Extreme Right-Wing Terrorism

5. The Committee began an Inquiry into Extreme Right-Wing Terrorism (ERWT) in October 2019, following the decision in 2018 that MI5 would take over from Counter Terrorism Policing (CTP) as the lead for this threat. MI5 assumed full responsibility for ERWT in 2020, after the UK counter-terrorism structures were reviewed. The Committee therefore considered it important to review how the transition from CTP to MI5 has worked and what MI5 is now doing to tackle this increasingly complex threat.

6. During the Inquiry, the Committee found that the ERWT threat was on an upward trajectory. It was therefore seriously concerned to find that MI5 has had to absorb responsibility for tackling ERWT without any commensurate increase in resources. ERWT and Left-Wing, Anarchist and Single-Issue Terrorism casework – accounting for around a fifth of all counter-terrorism investigations – can only be undertaken at the expense of other MI5 work. As a result, MI5 has been unable to expand its work, as it had intended, in other areas. This situation is untenable. While MI5, rightly, allocates its resources on what it assesses to be the highest-priority work based on its expert knowledge of the threat, it cannot be expected simply to absorb this new responsibility. The Committee concluded that MI5 must be given additional funding to enable it to tackle ERWT without other areas of its work suffering as a consequence. The Committee's Report was published on 13 July 2022.

7. On 22 February 2023, the Chairman of the ISC, the Rt Hon. Kevan Jones MP and the Rt Hon. Theresa Villiers MP spoke at a panel event organised by the Royal United Services Institute (RUSI) to discuss the Committee's ERWT Report. The panel discussed the Committee's recommendations and conclusions, before a broader question-and-answer session with those attending both in person and online. The Committee is grateful to RUSI for facilitating the event and providing a platform to address this issue.

8. Disappointingly, by the time of that event, the Committee had still not received the Government response to its Report. The Memorandum of Understanding (MoU) between the Committee and the Prime Minister states, "*HMG will aim to respond substantively to any report by the ISC within 60 days*". In the case of the ERWT Report, that period expired on 11 September 2022 without the Government providing a substantive response. **The Committee is concerned that the Government did not provide a substantive response until 30 March 2023, 261 days after the Report was published, and that no explanation has been provided as to the reasons for the delay. The Committee hopes that the Government will provide more timely responses to the Committee's Reports in future, and respect the timeline set out in the MoU.**

9. In terms of the response itself, the Committee would highlight the following considerations:

- With regard to the forthcoming introduction of online safety legislation, the Committee had identified the urgent need to ensure that Ofcom, as the independent regulator, develops the necessary capabilities to hold technology companies to account. In that light, the Government's commitment to work closely with Ofcom to identify how it can continue to build the full range of necessary capabilities is an encouraging development. However, more broadly with regard to the online space,

the Committee is perplexed that, whilst Director General MI5 made it clear to the Committee that there was a particular challenge in determining Extreme Right-Wing activity online which could translate into 'real-world' terrorist activity, the Government response appears to play down this problem, noting only, "[we] *judge that the majority of ERWT activity of concern (short of actual terrorist attacks) is likely to occur online in the years to come*".

- The current vetting processes for candidates applying to join the police was also a feature of the Report, in particular the need to scrutinise online activity as part of that process. The Government reports that work is now being undertaken to ensure that measures being taken on vetting are sufficiently robust, including through technological solutions to assist with the emerging risk around social media. This is a welcome development, particularly in light of recent events regarding the Metropolitan Police Service.

- However, the Committee is disappointed that the Government has failed to provide a positive response to the Committee's call for MI5 to be given the additional funding it needs, having taken over primacy for ERWT from CTP. The generic and somewhat evasive response by the Government that MI5 had benefited from an overall increase in the funding of the Single Intelligence Account in 2021 and that it "*deploys its resources flexibly across all areas of the national security threat*" is not adequate. This is a situation we will continue to monitor.

- In a similar vein, the Committee notes the Government's failure to commit to a dedicated review of the current proscription process. The Committee expressed concern in the Report that a number of groups did not meet the terrorism threshold for proscription, but it had been assured during the course of the Inquiry that CTP and the Home Office were considering a review of the process – this was duly highlighted as a welcome development by the Committee. In its response, the Government has, however, failed to commit to undertaking such a review, simply responding that "*the impact of proscription is kept under constant review*". **The Committee hopes that the Government will undertake a dedicated review of the proscription process to ensure that it is fit for purpose.**

Annual Report 2021–2022

10. The Committee published its Annual Report for 2021–2022 on 13 December 2022, summarising the work of the Committee from August 2021 to March 2022.[2] This included the publication of one Report and one statement, and contributions to four pieces of legislation. The Report noted that the Committee had, during the period in question, been "*severely hampered*" by the failure of the Intelligence Community to provide responses to the Committee in accordance with long-established standard deadlines (developments since then are covered later in this Report).

11. The Report reiterated the concerns expressed in the Committee's previous Annual Report (for 2019–2021) over the erosion of Parliamentary oversight as a result of the Committee's current MoU not being updated to cover all intelligence and security activities

[2] The Annual Report 2021–2022 covered a shorter period than usual as delays to the Committee's Annual Report 2019–2021 meant that that Report had covered an extended period.

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*". (This issue is also addressed further later in this Report.)

Legislation

12. During the period covered by this Report, there have been five pieces of legislation before Parliament with which the ISC has engaged at a Committee level.

National Security Bill

13. The Committee strongly welcomed the introduction of the National Security Bill (which, at the time of writing, had not yet completed its passage through Parliament): the Committee has been calling for such legislation for many years. In its *Russia* Report of 2020,[3] for example, the Committee stated that the Official Secrets Acts regime was outdated and not fit for purpose. The Committee is therefore pleased that the National Security Bill seeks to modernise the Official Secrets Acts 'espionage' regime and create important new offences, such as sabotage, foreign interference and assisting a foreign intelligence service.

14. The Committee has been heavily engaged in scrutinising the Bill. The Committee has considered classified information – on behalf of Parliament – from the Government and held constructive sessions with the Intelligence Community to allow them to explain the rationale behind key parts of the Bill. The Committee has focused on ensuring that the Bill is as effective as possible, providing the Intelligence Community and law enforcement with the required tools whilst incorporating the necessary safeguards. The key aspects are outlined below.

(i) Reform of the Official Secrets Acts

15. The Committee has long called for the reform of the entire Official Secrets Acts regime; however, the Bill only reforms the Official Secrets Acts 'espionage' regime; it does not reform the Official Secrets Act 1989 – as recommended by the ISC and by the Law Commission in its 2020 Report into the *Protection of Official Data*.[4] This is disappointing, given that the Government's 2021 public consultation committed that "*the legislative proposals being developed by the Government will therefore include, at a minimum … reform of the Official Secrets Act 1989*".

16. This fundamental omission means that the current problems with the Official Secrets Act 1989 – which have already been acknowledged by the Government – will persist. This includes the requirement to prove damage for 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. During Second Reading of the Bill in the House of Commons, Members of the ISC sought assurances that reform of the Official Secrets Act 1989 would be brought forward with "*some urgency*"; however, the Government did not commit to a timeline for this reform.

---

[3] *Russia*, HC 632, 21 July 2020.
[4] '*Protection of Official Data* Report', Law Commission, 1 September 2020.

(ii) Defence against extra-territorial offences

17. The Committee has focused particularly on Clause 31 of the Bill (originally Clause 23 when the Bill was introduced). As first drafted, this would have amended 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*")[5] where these actions were necessary for the proper exercise of their functions. The Committee had serious concerns about this Clause on a number of grounds, including the unnecessary breadth of the immunity, the lack of a proportionality requirement and the lack of accountability safeguards.

18. At Committee Stage in the Commons, the Bill Committee recognised that there may be classified information underpinning the Government's rationale for the Clause, which could not be disclosed to it, and the Government committed to provide the ISC with this evidence. This was subsequently provided to this Committee, and after considering it we held several sessions with the Intelligence Community.

19. The Committee concluded that there was potentially a legitimate problem, namely that despite the existing legislative protection, there may still be a risk of criminal liability for junior members of the Intelligence Community even when acting within the remit of their duties, and this could potentially have an impact on operations.

20. However, while the ISC recognised the potential issue, it was firmly of the opinion that the Clause as drafted was not appropriate, going considerably beyond what was needed. The Committee's view was that there was no justification for such a broad automatic exemption with limited accountability. Indeed, the Government admitted during Committee Stage in the Lords that the 'exemption' as originally drafted would have meant that, in some cases, authorisation by the Secretary of State for encouraging or assisting an offence overseas would no longer be required. The Committee found this acknowledgement extremely concerning, demonstrating that the Government was willing to undermine existing Ministerial and oversight provisions set out in statute. It also highlighted the importance of ensuring the right balance between enabling the Intelligence Community to undertake its critical role and incorporating sufficient safeguards.

21. The ISC therefore made a series of recommendations to the Intelligence Community as to what, in its view, would constitute a proportionate solution to the problem identified. Notably, the Committee suggested that the Intelligence Community consider whether, instead of an automatic 'exemption', the Bill might introduce a limited 'defence' for the intelligence services (and the Armed Forces) in relation to offences overseas (specifically, encouraging or assisting the commission of an offence) where their act is necessary for the 'proper' exercise of their functions. The Committee also noted that the 'proper' exercise of a function should incorporate proportionality, i.e. that an act could not be within the 'proper' exercise if it is not proportionate. It was agreed that the Intelligence Community and the Home Office would revise the Clause to take into account these recommendations, mindful of the wider context of concerns raised in Parliament. On 18 January 2023, the Chairman wrote to the Security Minister formally requesting that the Government provide the ISC with the draft amendment in advance of it being tabled, with sufficient time for the ISC to scrutinise it and make any further recommendations. This was essential given the serious concerns with the Clause that

[5] As set out in Part 2 and Schedule 4 of the Serious Crime Act 2007.

had been raised in both Houses, the unique ability of the ISC to review classified material on behalf of Parliament and the very late stage in Parliament's consideration of the Bill.

22. While the ISC received interim updates from the Intelligence Community on the overarching direction of travel with regard to an amended Clause, the ISC received no response from the Security Minister, or any other Home Office Minister. The draft amendment was provided to the Committee by the Security Minister only on 20 February, with it being tabled in Parliament the next day, leaving no time for the Committee to scrutinise the draft amendment – and indeed ahead of an already scheduled session to discuss the proposed amendment. The Home Office therefore tabled its amendment as a 'fait accompli' with little regard for the need for effective Parliamentary engagement and scrutiny to take place. This failure in handling – for no good reason – completely undermined the requests the Committee had received from the Intelligence Community for assistance with the Bill and belied any assurances that the matter was being taken seriously.

23. In terms of the amended Clause itself, it replaces the automatic 'exemption' with a more limited 'defence' for the intelligence services (and the Armed Forces) in relation to offences overseas (specifically, encouraging or assisting the commission of an offence) where their act is necessary for the 'proper' exercise of their functions – as the Committee had recommended. Unlike the previous 'exemption', the 'defence' will require the facts of any case to be put forward and considered properly in a court. The new Clause also introduces a level of senior official and ministerial accountability: it requires the heads of each intelligence service to have in place internal safeguarding arrangements designed to ensure that their staff act in a way that is necessary for the proper exercise of their service's functions. The relevant Secretary of State must also be content with these arrangements. Again, this is in line with the recommendations made by this Committee.

24. The Committee discussed the amended Clause with the Intelligence Community and noted that it was an improvement when compared with the previous version. However, the Committee made clear to the Community that it still had concerns – notably that:

- the "*proper*" exercise of a function of an intelligence service must incorporate proportionality – i.e. that an act could not be within the "*proper*" exercise if it is not proportionate;

- the Government must set out in sufficient detail what was meant by the "*arrangements*" that the heads of each intelligence service are expected to establish;

- "*proper*" exercise must be connected to the internal oversight arrangements that each head of an intelligence service is expected to establish – i.e. that an act could not be considered within the "*proper*" exercise of the function of an intelligence service if it does not comply with the internal oversight arrangements; and

- unlike the previous 'exemption', this new 'defence' must not lead to fewer ministerial authorisations needing to be sought for Intelligence Community activity or less daily oversight from Ministers and/or judicial commissioners.

25. Given that the Government had formally tabled the amendment without providing the Committee with sufficient time to scrutinise it, there was no opportunity to revise the proposed amendment further to address these concerns. The Committee made clear to the

Government that it therefore required several assurances from the Government at the despatch box if it were to be in a position to support the new Clause. The Committee tabled its own amendment to the Government's proposed Clause, in the event that these assurances were not forthcoming.

26. The Government provided these critical assurances at Report Stage in the Lords on 1 March. The Minister confirmed at the despatch box that:

- "*where the intelligence services or Armed Forces do not apply proportionality consistent with their legal or policy obligations, that would not be a proper exercise of their functions… to be completely clear, a person's lack of compliance with their legal and policy obligations could be considered by the prosecution and would impact the availability of the defence – that includes proportionality*";

- the arrangements would ensure that the intelligence services and Armed Forces applied "*rigorous safeguards, standards and internal processes for determining that activity is lawful and properly exercised*", including that "*operational decisions are recorded, taken at appropriate seniority and made with the benefit of advice from specialist legal advisers to ensure compliance with domestic and international law; all personnel receive mandatory training on their legal obligations;* [and] *policy documents set out specific requirements for different activities, including what authorisations are required and how to decide whether activity is necessary, reasonable and proportionate. Compliance with these requirements ensure*[s] *that acts are within the proper exercise of the functions of the organisation concerned. Some of these policies have been published, such as the Fulford principles, where the passing and receipt of intelligence relates to detainees, the compliance of which is assessed by the Investigatory Powers Commissioner's Office… Arrangements can also go beyond pure legal considerations, with ethics counsellors in post to discuss the difficult decisions we sometimes take when balancing risk. To go back to Secretaries of State, they are accountable for the work of the intelligence services and the Armed Forces in Parliament. A central part of their obligations will remain authorising the required operational activity at the appropriate time*";

- "*where a member of the intelligence services or the Armed Forces conducted activity that did not comply with the arrangements – namely, the rigorous safeguards, standards and internal processes that I described earlier – this breach of the arrangements could be scrutinised by the proper oversight mechanisms; for example, an error would be reported to IPCO for a breach of the Fulford principles. It could be considered by the prosecution and would impact the availability of the defence*"; and that

- "*the introduction of this new defence, in and of itself, will not lead to fewer ministerial authorisations sought by the intelligence services or to less daily oversight from Ministers and/or judicial commissioners over intelligence activity*".

27. Given these assurances, the ISC was content to support the inclusion of the amended Clause 31 as part of the Bill. It was subsequently agreed by the Lords on 1 March 2023. The Committee is content that this defence now finds a better balance between providing the necessary protection for intelligence officers whilst also maintaining a sufficient level of accountability and oversight. **The Committee also considers this to be a good example**

of positive and constructive engagement with the Intelligence Community (despite the poor handling by the Home Office). It demonstrates the benefits of an effective oversight Committee, which is used to scrutinising classified information on behalf of Parliament and the public and understands the context within which such information is used.

(iii) Foreign Influence Registration Scheme

28. In its Report on the hostile state threat posed by Russia, published in July 2020, the ISC recommended new legislative powers to tackle foreign interference, including to defend against the agents of hostile foreign powers (the Committee saw value in a scheme such as the US Foreign Agents Registration Act). The Committee was clear that such powers (or such a scheme) were required to counter Russian influence in the UK. Despite a commitment by HMG in its 2021 public consultation that the legislation would "*include, at a minimum ... the creation of a Foreign Influence Registration Scheme* [FIRS]", the FIRS did not appear in the National Security Bill when it was introduced to Parliament. It appears that the FIRS was either not ready or thought not to be required – which would have been a significant missed opportunity. However, after the Bill was introduced in Parliament, the Security Minister assured the Committee that the FIRS would be introduced via amendment, and the Home Secretary committed in Parliament that the provisions would be introduced in time for Committee Stage in the House of Commons. While the ISC welcomed the eventual introduction of the FIRS (via amendment, at the end of the Commons Committee Stage), it remains concerned that this was introduced at such a late stage, and therefore allowed only limited time for Parliament to scrutinise the scheme effectively.

29. The Committee considers that the establishment of the FIRS will help UK law enforcement and the Intelligence Community to tackle the complex and varied threats posed by hostile state actors. It will increase the transparency of those threats and help to make the UK a more difficult operating environment for foreign intelligence services. This should help to deter hostile state actors from undertaking harmful activity and disrupt it at a much earlier stage. However, the ISC is concerned that, at the time of writing, there remain key issues with the FIRS that will undermine its potential utility:

- The FIRS is unnecessarily complex, being split into two tiers. Whilst the primary tier – the 'Political Influence Tier' – requires the registration of political influencing activities directed by a foreign power, the secondary 'Enhanced Tier' requires the registration of any specified activity beyond political influencing but only where the Government lists in secondary legislation the foreign state or entity directing such activity. The Committee expects that listing countries or entities will be challenging in practice. It will take time for the Government to agree which countries to add or remove when flexibility and pace may be required. It is unclear whether a country could be removed or added multiple times, undermining certainty for potential registrants. In practice, these flaws will inevitably lead to the 'Enhanced Tier' – which could have been a valuable tool – not being used.

- The 'Political Influence Tier' itself is now so narrow as to undermine its utility. Due to widespread Parliamentary concerns about burdens on foreign businesses, charities and educational bodies operating within the UK, ahead of Report Stage in the House of Lords, the Government significantly reduced the scope of the 'Political Influence Tier' so that it now only requires registration of political influencing

activity directed by a foreign power and no longer requires the registration of political influencing activity directed by a foreign company. The Committee is concerned that these changes have gone too far, inadvertently creating loopholes – for instance, it appears that foreign powers may still be able to avoid the registration of their political influencing activity (and the resultant transparency) by directing it through opaque intermediary commercial structures (thereby obscuring the link between the foreign power ultimately in control and the commercial entity directing the political influencing activity).

- There is a potential lack of transparency, particularly in relation to the secondary 'Enhanced Tier', and the ability of the Home Office to resource the FIRS properly, which will be essential for scrutinising submitted documents, identifying any risks and updating the register.

30. In summary, the ISC is disappointed that such a complex and inconsistent scheme has been established. This was an important opportunity, which has been broadly missed. The Committee is of the view that it would have been more effective to have one tier that applies to all countries automatically and a broader range of covert activity. Whilst this would have required a greater number of exemption categories – to cover charities, educational establishments and legitimate business, for example – it would have been a simpler and more practical system of registration. **Given these concerns, the Committee considers that the Government should keep the effectiveness of the FIRS under review and report to Parliament on its operation within the next two years.**

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

31. We note that, during consideration of the Bill by the Lords, an amendment was proposed by the Opposition to require the Government to update the MoU between the ISC and the Prime Minister, if the National Security Bill leads to the creation of any new teams outside the organisations already subject to the scrutiny of the ISC. This update would ensure that the ISC could oversee the entirety of the new national security regime being implemented by the Bill, helping to 'future-proof' the oversight provisions.

32. At the time of drafting (March 2023), this amendment had been agreed by the Lords and was awaiting the Commons' consideration of the Lords' amendments. Whilst the amendment relates only to matters within the scope of the Bill, it has a bearing on the wider problem referred to in the ISC's previous Annual Reports: namely that the Committee's MoU is out of date and urgently needs to be updated to ensure that the Committee can – on behalf of Parliament – effectively scrutinise matters relating to intelligence and security. This is discussed further under the section later in the Report on 'Other Issues'.

33. Whilst the Committee has previously commented at Report Stage in the Lords on the Government's handling of the Bill – which has left much to be desired – after considerable Parliamentary scrutiny, the Bill has been much improved since its introduction. The Committee is also pleased to see that the Government has incorporated various changes recommended by Members of the ISC. At the time of drafting (March 2023), the Bill has returned to the Commons and is awaiting the Commons' consideration of the Lords' amendments.

Other legislation

34. During the period covered by this Report, the Committee also considered the following pieces of legislation, legislative guidance and legislative reports:

- The *Economic Crime and Corporate Transparency Bill*, which was introduced in Parliament on 23 September 2022. This follows the recommendation in the Committee's *Russia* Report of 2020 for a new statutory framework which – amongst other areas – would help to tackle the illicit financial dealings of the Russian elite and the 'enablers' who support this activity.

- The Government's introduction of a *national security-related amendment to the Product Security and Telecommunications Infrastructure Bill* during Report Stage in the House of Lords. This amendment changes the Electronic Communications Code, which currently allows telecom providers to ask landowners – including those with national security, law enforcement and defence equities – for the right to carry out surveys as well as the right to install telecommunications equipment. The proposed amendment will provide relevant Secretaries of State with the power to intervene and stop such rights being imposed where necessary, by issuing a certificate to the court (although the threshold for issuing such a certificate will be high and all other routes to a mutually agreed solution must have been exhausted).[6]

- The *Statutory Instrument bringing into force the revised 'Covert Human Intelligence Sources: Code of Practice' and the revised 'Interception Code of Practice'*. This Code of Practice provides guidance on authorisations for the use or conduct of covert human intelligence sources pursuant to the Covert Human Intelligence Sources (Criminal Conduct) Act 2021 and Interception (Code of Practice) Regulations 2022. The Committee understands that these have been prepared with input from the Investigatory Powers Commissioner, but that the revised Code of Practice does not change the policy or primary legislation that was approved by Parliament on the use of Covert Human Intelligence Sources and Criminal Conduct Authorisations.

- The *report laid by the Home Secretary in Parliament on 9 February 2023 – as required under section 260 of the Investigatory Powers Act 2016 (IPA) – relating to the operation of the IPA and the recommendations for reform*. The Committee noted the Home Secretary's announcement that Lord Anderson will undertake an independent review of the IPA and assess the case for legislative change. At the time of writing, the Committee awaits the conclusions of Lord Anderson's review, which it will consider before deciding what further action to take.

Areas of inquiry

International Partnerships

35. The Committee began its Inquiry into International Partnerships in October 2019. Once the Committee had completed its Inquiry, it followed the well-established process to prepare its Report for publication, as part of which it considers requests from the Intelligence Community

[6] The Product Security and Telecommunications Infrastructure Act was subsequently passed in December 2022.

for the redaction of text which the Community considers would harm their capabilities. In such cases, the Committee requires the Community to demonstrate clearly what harm would be caused by the publication of the text. The Committee considers each request from the perspective of national security: where the Committee agrees that the information would damage national security, it is redacted from the report. The Committee aims to ensure that only the minimum of text is redacted from each report. If an organisation considers that any of the redaction requests that the Committee has rejected would cause serious damage to national security if published, the head of that organisation must appear before the Committee at a Contested Redactions session, to explain exactly why publication would be so damaging. This is discussed between the Committee and the head of the organisation concerned and, at that meeting, agreement is reached as to the text which can be published in the final version of the report.

36. In relation to the International Partnerships Report, the Committee held two Contested Redactions sessions in July 2022, reaching agreement as to the text for publication, and subsequently sending its Report to the Prime Minister[7] on 6 September 2022, requesting confirmation that there was no material in the Report which would prejudice the discharge of the functions of the Agencies. **By convention, the deadline requested for the Prime Minister to provide such a confirmation is ten working days. However, at the time of writing, the Committee has still not received a response from the Prime Minister, 144 working days later.**

37. Instead, on 20 September 2022 – the deadline for the Prime Minister to have given confirmation – the Committee received a letter from the Deputy National Security Adviser (DNSA) stating that the response would be delayed because the Intelligence Community needed to engage with international partners. The Committee was surprised by this, given that the Community had already asked for additional time earlier in the process for them to engage with international partners, and the Committee had already provided this. It was not clear, therefore, why there needed to be any further delay. More disappointing still was the fact that the Community then took a further 37 working days to come back to the Committee – it was not until 11 November 2022 that the DNSA wrote again to the Committee to inform it that international partners had requested three redactions (two of which the Community had previously requested for redaction but which the Committee had rejected) and one factual amendment.

38. However, at that point it became clear that the Community had not relayed the Committee's rationale for having rejected the Community's initial request for those two redactions (during the redactions process) – for example, in one case the Committee considered that the material was already in the public domain and had cited where it could be found. The Committee therefore insisted that the Community relay those rationales to the partners concerned to see if that would resolve their concerns. On 14 February 2023 (a further 64 working days since the DNSA had written to the Committee stating that international partners had raised concerns), the Committee received a letter from GCHQ stating that the Intelligence Community "*had now*" conveyed the Committee's reasoning for rejecting those requests previously, however partners' positions remained unchanged.

[7] The ISC sends its Reports to the Prime Minister of the day. On 6 September 2022, Boris Johnson MP stepped down as Prime Minister and on the same day Liz Truss MP was invited to form a Government. Subsequently, on 25 October 2022, Liz Truss stepped down as Prime Minister and Rishi Sunak MP was invited to form a Government.

39. At the time of writing, therefore, the Committee has been advised by GCHQ that there are three redaction requests and one factual amendment request from international partners outstanding. A further factual amendment request from the Community has also now been sent to the Committee for consideration. However, as the Intelligence Community's role in the process concluded when the Report was sent to the Prime Minister, it is for the Prime Minister now to consult with the Committee if he considers that this material would prejudice the discharge of the functions of the Agencies, were it to be published. As noted previously, at the time of writing, the Committee has still not received a response from the Prime Minister – six months after the Report was sent.[8] The Committee looks forward to a swift response, in order that it may now publish the completed Report without any further unnecessary delay.

China

40. In 2019, the Committee began taking evidence in connection with its Inquiry into national security issues relating to China. During the period covered by this Annual Report, the completed Report has been going through the process of factual amendment and redaction requests.[9]

Cloud Technologies

41. In May 2021, the Committee commenced an Inquiry into Cloud Technologies. During the period covered by this Annual Report, the Committee received written evidence and held oral evidence sessions with the Intelligence Community. We have been supported in this Inquiry by the NAO and we wish to express our thanks once again to the Comptroller and Auditor General and his team for their assistance, and the excellent work carried out.

Iran

42. In November 2021, the Committee announced that it will be undertaking an Inquiry into national security issues relating to Iran. During the period covered by this Annual Report, the Committee received written evidence and held oral evidence sessions with external experts on the threat from Iran, including academics, former civil servants, and former UK and US Government representatives.

Areas of scrutiny

43. Following the publication of the third volume of the Manchester Arena Inquiry, the Committee again expressed its deepest sympathies for the families whose lives have been permanently affected by this tragic event. The Committee welcomed the Inquiry Report, which it committed to consider thoroughly, and noted the statement by the Inquiry Chair, Sir John Saunders, that the ISC is the most suitable body to monitor any closed recommendations he might make. Once these recommendations are finalised and – noting the wider remit of the Inquiry – the Committee will consider what further action by the ISC might be necessary.

---

[8] We note that we were only provided with confirmation on 20 July 2023, the day that Parliament adjourned for the summer recess.
[9] The Report was subsequently published on 13 July 2023. As this falls outside the period covered by this Annual Report, it will be covered in our 2023–2024 Annual Report.

44. The Committee has been briefed as the situation in Ukraine has developed. It has heard from, and questioned, the Intelligence Community on the military and political situation, the Government's objectives, the work being done by the UK Intelligence Community and the impact of Western weapons. The Committee was also briefed on Russia's objectives and its targeting of Ukraine's critical national infrastructure.

45. Following the withdrawal of forces from Afghanistan, the Committee requested from the Government any intelligence assessments which covered the outlook for the regime with regards to the final withdrawal of US and coalition forces from Afghanistan. Subsequently, in November 2021, the Committee requested additional information on the Intelligence Community's role in the UK's withdrawal from Afghanistan. The Committee continues to consider the evidence provided by the Intelligence Community.

46. In accordance with its broader oversight function, the Committee has continued this year to monitor the expenditure, administration and policy of the seven organisations it oversees through the Quarterly Reports it receives from them and the end-of-year information covering the 2021/22 financial year. The threat assessment is summarised in Annex A, and the key facts and major developments for each organisation in 2021/22 are summarised in Annex B.

OTHER ISSUES

Erosion of Parliamentary oversight of intelligence and security matters

47. For the past three years, the Committee has continued to highlight 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 Intelligence and Security Committee of Parliament (ISC) and the Prime Minister. Intelligence and security matters are increasingly devolved to policy departments, but these departments have not been added to the Committee's MoU. 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*". 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*".

48. During the passage of the National Security and Investment (NSI) Act 2021, the Committee sought assurances about the oversight of the Investment Security Unit (ISU) that would be created by the Act. The ISU receives input from the Intelligence Community in order to advise the responsible Minister (formerly the BEIS Secretary of State, and at the time of writing the Chancellor of the Duchy of Lancaster) on national security risks to the UK from foreign investments or acquisitions, and on whether it is appropriate to 'call in' transactions for a national security assessment or to apply remedies to address national security risks. During the passage of the NSI Act, the Committee was informed that, despite the ISU relying on classified information, oversight would instead be undertaken by the BEIS Select Committee. However, such oversight can only be undertaken effectively by the ISC – as the only Committee of Parliament with regular access to classified information, and to which the UK Intelligence Community has a statutory duty to provide information. When the House of Lords considered the NSI Bill, it repeatedly amended it to provide for appropriate ISC oversight of the ISU, only for this to be overturned by the Government in the House of Commons.

49. **The Committee has raised the issue of its statutory remit with the National Security Adviser (NSA) on a number of occasions, both in correspondence and in meetings. As stated in our 2021–2022 Annual Report, the NSA relayed to the Chair in January 2022 that the Government did not feel bound by the statements made by the then Security Minister in July 2012, and the assurances given by him to Parliament, as referenced above. The Committee is deeply disappointed and concerned that the Government has taken this approach – which prevents effective scrutiny by Parliament of national security issues across Government. Select Committees are not equipped to handle classified material, so when the Government informs the Committee that a matter involving security and intelligence activities falls within the remit of those Committees, it is clear that this topic will not be subject to effective oversight.**

50. In relation to the ISU, the Government announced in February 2023 that the ISU would move from BEIS to the Cabinet Office, as part of wider machinery of government changes. The Committee presumed that the ISU would therefore be subject to oversight by the ISC – thereby resolving the impasse over the Committee's remit. We were therefore taken aback to receive a letter from the Minister of State for Investment Security and Minister of State for Business and Trade on 21 March 2023, informing us that the BEIS Select Committee would continue to conduct oversight and scrutiny of the ISU, subject to an MoU between the BEIS Select Committee and the Government.

51. The Deputy National Security Adviser (DNSA) wrote to the Committee on 23 March 2023 to explain the Government's reasoning for this decision. He stated the Government's position that the ISC's remit under the current MoU "*does not automatically extend to the activities of* [the Chancellor of the Duchy of Lancaster]*, as the Secretary of State with responsibility for the work of the ISU*". However, this argument is invalid, as the BEIS Select Committee's remit did not – at that point – extend to oversight of the activities of the Chancellor of the Duchy of Lancaster either. Furthermore, if the ISU is to be located within the National Security Secretariat (NSS), as its remit would indicate, the MoU clearly states that the ISC shall oversee the activities of the NSS in relation to matters of intelligence and security.

52. The DNSA further stated that "*there is no barrier to any Select Committee receiving classified information*". However, during the passage of the National Security Bill, Lord Coaker asked how Select Committee members who do not hold the necessary security clearance "*could possibly look at and scrutinise classified material on Parliament's behalf*", and the Minister responded that "*if they do not have the necessary security clearances, they obviously cannot*". It is clear, therefore, that the ISC is the only Committee of Parliament that can perform this vital oversight role, as the only Parliamentary body with the necessary security infrastructure to scrutinise the material that underpins national security decisions. At the time of writing, the Committee is considering its response.

53. It is not just a matter of the ISU: there are far wider implications than just this one area of work. The issue of the ISC's MoU was, yet again, the subject of much discussion in the House of Lords this year – this time, during the passage of the National Security Bill, as mentioned earlier in this Report. The Committee has previously noted that none of the arguments put forward by the Government as reasons for refusing to put in place effective scrutiny have borne scrutiny themselves. We note, therefore, the comments by the Rt Hon. Lord Butler of Brockwell, the former Cabinet Secretary and former Member of the ISC, in March 2023, that the MoU had not been brought up to date not only for "*no good reason*", but for a "*bad reason*" – that the Government "*have taken a dislike to the ISC*" and "*have tried to restrict its activities*". Lord Butler offered the view that "*if the Government are not going to use the ISC properly, they should save money and abolish it*".

54. **This certainly raises the question as to what the Government regards as the point and purpose of the ISC – indeed why it was established in 1994, and why it was reformed in 2013. If the ISC is to carry out its function to scrutinise the Government's work on intelligence and security matters on behalf of Parliament, then the ISC must be able to oversee such work in its entirety, without exception, in order to provide meaningful assurance to Parliament and the public. If the Government thinks that highly classified material can be given to Select Committees, then presumably it could go down that path in relation to all highly classified material, giving oversight of the intelligence Agencies**

and those departments currently overseen by the ISC to Select Committees. Certainly, we note that its current stance has led to increased calls from Select Committees such as the Foreign Affairs Committee, the Home Affairs Committee and the National Security Strategy (Joint Committee) to receive briefings from the Agencies. While this is understandable, and the ISC always seeks to collaborate constructively with Select Committees, we do question whether the Government has really thought through the consequences of its current position.

55. The Committee therefore welcomed the amendment proposed by the Opposition during the passage of the National Security Bill, as mentioned above, which would require the Government to update the MoU between the ISC and the Prime Minister, if the Bill leads to the creation of any new teams outside the organisations already subject to the scrutiny of the ISC. The Government opposed this amendment on the grounds that it did not think it "*appropriate to mandate the Prime Minister to update the MoU in a specific timeframe, particularly so soon after a change has been proposed, and while there is an established practice of the ISC proposing such changes via its Annual Report*". However, the amendment was supported by the Lords, on the grounds that if the Government were to use the ISC for the purpose for which it was established, then it must update the MoU. The Committee considers that each piece of new legislation devolving such matters away from the bodies already overseen by this Committee should come with a commensurate amendment to this Committee's MoU. It would appear – on the grounds of the debate on the National Security Bill – that this would receive the support of the House of Lords.

56. In the Committee's Annual Report 2019–2021, we committed to publishing the current MoU each year to ensure it would not be allowed to fall out of date in the future. The current MoU, negotiated in 2013, can be found at Annex C. However, the changes which the Committee considers must be made are shown in the proposed MoU at Annex D.

57. **During the passage of the Justice and Security Act 2013 (JSA), the 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.*"[10] We again, therefore, urge the Prime Minister to meet the commitments made to Parliament, and to the public, during the passage of the JSA, when the Security Minister told Parliament that it was *"the intention of the Government 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"*.[11]**

Meeting with the Prime Minister

58. 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 has not had a meeting with a Prime Minister since December 2014. This was the subject of discussion in the House of Lords during the passage of the National Security Bill, where the Rt Hon. Lord Beith highlighted the issue of "*the disengagement of Prime Ministers from the Committee*", and Lord Coaker stated that for the Prime Minister

[10] Justice and Security Bill [HL]. (31 January 2013). [Hansard].
[11] Justice and Security Bill [HL]. (31 January 2013). [Hansard].

not to have met the Committee since 2014 was "*simply unacceptable*": both called for annual meetings between the Committee and the Prime Minister to resume.

59. **The Committee did receive an invitation to meet the then Prime Minister in October 2022, prior to her resignation. Unfortunately, although the Committee requested a date for this meeting, it did not receive a further response. The Committee therefore urges the Prime Minister to meet with it as a matter of priority. There are matters of significant constitutional importance at stake.**

The provision of evidence

60. In its previous Annual Report 2021–2022, the Committee noted that it had been "*severely hampered*" over the previous year by the failure of the UK Intelligence Community to meet standard deadlines as part of the ISC inquiry process. Lack of timely provision of evidence is a very serious issue, as it prevents the Committee from effectively performing its statutory oversight role. Moreover, as the NSA himself acknowledged, "*the Intelligence Community's licence to operate is dependent on credible oversight*".[12] The Agencies were granted increased powers under the JSA on the basis of the ISC being given increased powers – in the same legislation – to oversee them. The two are firmly linked. **If the ISC's oversight is frustrated, then the ISC cannot provide any assurance to the public or Parliament that the intelligence Agencies are acting appropriately, and therefore that they merit the licence to operate that Parliament has given them through their statutory powers.**

61. The Committee therefore hosted a substantive meeting in November 2022 where it called upon the heads of the seven organisations it oversees to provide assurances on a suitable way forward. The Committee was reassured that the Intelligence Community Heads appeared to have recognised the need to address the situation. The Chief of SIS particularly underlined the importance of the Committee's role in ensuring that the Agencies retain their licence to operate and for his staff to retain confidence in the democratic legitimacy of their activities. The Joint Intelligence Committee Chair assured the Committee that the Community recognised that it was for the Committee to set the timescales for the provision of evidence by the Intelligence Community, and reiterated that the Intelligence Community would meet the deadlines which the Committee determined to be appropriate. **The Committee welcomed this positive and constructive approach, and the clear demonstration by the Community of the recognition of the importance of this Committee in providing them with a mandate from the UK public.**

62. Following this meeting, the Committee decided to operate a two-tier approach to its inquiries – broadly in line with what the Intelligence Community had proposed, but with some tightening of the criteria which would merit extended deadlines. The Committee has agreed that in relation to a small number of its inquiries, which fall into a category of 'Exceptional Inquiries', additional time will be granted, if all three of the following criteria are clearly met:

I. The focus of the inquiry is on current or developing aspects of the Community's operationally focused work, relating to information, activities, policy, sensitive relationships or capabilities. This does not include administrative, corporate or commercial issues.

[12] Letter from National Security Adviser to Chair – 23 February 2022.

II. The subject requires an exceptional level of cross-Community collaboration – above and beyond the usual levels of such working by the Intelligence Community. The inquiry significantly engages a majority of the organisations overseen by the Committee and there is a requirement for significant joint responses due to overlapping or independent activity. This does not apply if an inquiry engages multiple organisations, but Agencies and departments are able to provide individual evidential responses. The same will apply if the subject requires an exceptional level of consultation with a range of international partners – above and beyond the usual levels of such working by the Intelligence Community. (The fact that the Intelligence Community is working with international partners on the subject matter of an inquiry is not sufficient for the inquiry itself to meet this criterion.)

III. The inquiry captures the full scope of a broadly defined strategic mission (e.g. 'the Russia mission'). This does not apply if an inquiry looks only at a specific aspect of a mission.

63. It will be important to observe how this two-tier arrangement works: if the Committee 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. This arrangement will therefore need to be kept under close review. In future reports we will therefore – in the interests of transparency – record the deadlines set and met: we do this for the first time this year, in Annex E.

64. **On a related note, the Committee has noted on a number of occasions over the past year a lack of advance notice from some parts of the Intelligence Community of significant policy announcements.** By way of example, the Committee was not made aware ahead of time about the Security Minister's announcement to the House on 1 November 2022 that a taskforce would be formed to secure and defend the democracy and institutions of the UK. Given the ISC's role in highlighting such threats – including most recently in our 2020 *Russia* Report – the Committee is encouraged that the Government is taking action on this important issue. However, as Members of the Committee stated in Parliament in response to the Security Minister's statement, the ISC is the only Committee that can properly scrutinise any elements of the taskforce's activities that involve access to classified information. It is therefore disappointing that the Government did not engage with the ISC prior to the establishment of the taskforce. As noted earlier, the Committee has faced similar issues during its engagement with the Government on the National Security Bill, during which vital information or proposals have arrived too late for Members to consider them in depth – on one occasion arriving the night before Report Stage. **The ISC has historically been able to offer advice, and perhaps support, to the Government when national security matters are before Parliament; however, it cannot do so if it is not kept informed.**

Business appointments

65. In our Annual Report 2019–2021, the Committee reflected on the need for further thought and scrutiny regarding the obligations of former (senior) members of the Intelligence Community – particularly when they sought to build a career in the private sector or as a commentator on security issues, using the knowledge they had gained.

66. The Committee continues to be concerned by the issue of former senior members of the Intelligence Community taking up positions in the private sector. In the period covered by this Annual Report, the Committee was made aware that Dr Ian Levy – Technical Director at the National Cyber Security Centre – was resigning to take up a security architecture role at Amazon UK Services.

67. Responding to the Committee's concerns about this 'revolving door', Director GCHQ stated that such movement was desirable in allowing GCHQ to refresh skills, build strong relationships with the private sector, and attract talent. He acknowledged that there were risks to manage, but assured the Committee that GCHQ had the framework and policies in place to do this appropriately, including through the Business Appointment Rules process, and the maintenance of a good relationship with previous staff members as a way to reduce 'insider risks'.

68. **The Committee nevertheless considers that further thought and scrutiny are needed with regard to the obligations, including contractual obligations, of former senior members of the Intelligence Community. The Committee will continue to take an active interest in such cases.**

GCHQ recruitment and vetting

69. Over the past year, the Committee has been made aware of two incidents that raise questions regarding GCHQ's security culture and systems.

70. In late 2022, GCHQ wrote to the Committee to inform it about an ongoing investigation into ***, caused by ***.[13] Investigations concluded that *** has had a significant effect on ***. GCHQ concluded that, as per its equities process, it had no option but to *** to ensure that *** an unacceptable cyber-security risk.

71. **The incident raises concerns regarding GCHQ's approach to recruitment and vetting, as well as the stringency of *** protocols in place to ***. The Committee is particularly concerned with regard to ***.** The Committee intends to scrutinise this issue further.

72. The Committee was similarly concerned to note that an individual, who was reported in the media to have been working on secondment at GCHQ, was attacked and seriously injured in Cheltenham in March 2023. (GCHQ wrote to the Committee to confirm that the individual attacked was an employee of the US National Security Agency on secondment to GCHQ.) At the time of writing, we understand that Counter Terrorism Policing was leading the investigation into this incident, and that a suspect had been arrested for attempted murder under the Police and Criminal Evidence Act 1984 and under Section 41 of the Terrorism Act (2000) on suspicion of preparing acts of terrorism under Section 5 of the Terrorism Act (2006).[14] GCHQ informed the Committee that the suspect is a former member of GCHQ who left the organisation in November 2022, and that it understands that the suspect may have targeted the victim as a result of her employment with GCHQ. The Committee awaits an update on this incident once the investigation has concluded.

---

[13] The response to this incident was code-named Operation ***.

[14] We note that the suspect subsequently pleaded guilty to attempted murder, and to a further charge of assault occasioning actual bodily harm, in August 2023.

Committee resources

73. In April 2022, at the beginning of the 2022/23 financial year, the Committee was provisionally allocated its full budget of £1.84 million. It was not until November 2022 that final budget allocations were confirmed and the Committee's budget was inexplicably reduced to £1.635 million. At the time of writing, no explanation has yet been received as to the reasons for this reduction.

74. The Committee has again made clear that its budget for financial years 2023/24 and 2024/25 must be the full allocation of £1.84 million. Taken together with the failure of the Government to update the Committee's remit, any budget cut raises significant concerns as to whether there is now a concerted effort being made to undermine the democratic scrutiny of the UK Intelligence Community put in place by Parliament. At the time of writing, no allocation information has yet been received.

LIST OF WITNESSES

Officials

CABINET OFFICE

Sir Simon Gass KCMG CVO – Chair, Joint Intelligence Committee

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

Other officials

FOREIGN, COMMONWEALTH AND DEVELOPMENT OFFICE (FCDO)

Mr Thomas Drew CMG – Director General Defence and Intelligence

Other officials

GOVERNMENT COMMUNICATIONS HEADQUARTERS (GCHQ)

Sir Jeremy Fleming KCMG CB – Director GCHQ

Other officials

HOME OFFICE

Ms Chloe Squires – Director General Homeland Security Group

Other officials

MINISTRY OF DEFENCE (MoD)

Mr Adrian Bird CB – Chief of Defence Intelligence

Other officials

SECRET INTELLIGENCE SERVICE (SIS)

Sir Richard Moore KCMG – Chief, SIS

Other officials

SECURITY SERVICE (MI5)

Mr Ken McCallum – Director General MI5

Other officials

Expert external witnesses

Professor Ali Ansari, Professor of Iranian History, University of St Andrews

Baroness Ashton of Upholland LG GCMG, High Representative of the European Union for Foreign Affairs and Security Policy (2009-2014)

Ambassador John Bolton, United States National Security Adviser (2018-2019)

Sir Richard Dalton KCMG, UK Ambassador to Iran (2002-2006)

Professor Anoush Ehteshami, Professor of International Relations, Durham University

Dr Sanam Vakil, Director, Middle East and North Africa Programme, Chatham House

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, Left-Wing, Anarchist and Single-Issue Terrorism and Northern Ireland-related terrorism, Hostile State Activity, the Cyber Threat and Nuclear Proliferation. The Intelligence Community work to counter these threats. The following is a summary of their threat assessment for the period 1 April 2022 to 31 March 2023.

The threat picture

The threat to the UK from hostile activity by states

The threat to the UK from hostile activity by states is multi-faceted and complex. Attempts by foreign intelligence services to conduct espionage to obtain UK government and defence sector secrets continue; in February 2023 a British security guard, who had been recruited by the Russians while working in the British Embassy in Berlin, was sentenced to 13 years for eight offences under the Official Secrets Act. Espionage is similarly conducted to access economic information, including intellectual property, research and development, and scientific academic research.

The threat to the UK from hostile activity by states 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.

There is a growing threat of state-sponsored assassination, attacks and abductions of those perceived as dissidents. Since the start of 2022, there have been at least 15 credible threats to kill or kidnap British or UK-based individuals by the Iranian regime. In October 2022, a pro-democracy protester appeared to be the subject of violence outside the Chinese consulate in Manchester. The threat to dissidents in the UK from the Russian state, which we saw manifest in the attempted assassination of Sergey Skripal in 2018, has not abated.

The government is strengthening its response to hostile activity by foreign states. This includes: the National Security Bill, which will introduce 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 continued development of a whole of system response; and a concerted Counter State Threats strategy, bringing together expertise and tools from across government.

The threat to the UK from terrorism

The UK National Threat Level is currently 'SUBSTANTIAL': an attack is likely, and has remained at that level throughout the reporting period.

It continues to be most likely that an Islamist terrorism, Extreme Right-Wing Terrorism (ERWT) or Left-Wing, Anarchist and Single-Issue Terrorism attack would emanate from self-initiated terrorists radicalised online, who plan and conduct attacks independently of any formal association with a wider terrorist group. A widening spectrum of underlying personal grievances – which are not necessarily directly linked to core extremist narratives

– increases the difficulty of anticipating the focus of, and underlying ideologies and drivers behind, terrorist attacks.

There has been one terrorist attack in the UK during this period: on 30 October 2022, British national Andrew Leak carried out an ERWT attack against an immigration centre in Dover, which we assess was motivated by a cultural nationalist mindset that incorporated anti-Muslim grievances.

There have been no successful Islamist terrorist attacks during this period; however, three Islamist plots have been disrupted since 31 March 2022.

The threat to the UK from overseas continues to diversify. Pressure on Al-Qaeda (AQ) and Islamic State in Iraq and the Levant (ISIL) means that these groups no longer wield centralised operational infrastructure. In response, AQ and ISIL have entrenched affiliate branches in conflict zones around the globe: they operate in more theatres than ever before. The threat from affiliate networks primarily manifests against Western interests overseas, but both ISIL and AQ retain the intent to attack Western countries, including the UK.

Islamist terrorist groups based overseas, as well as transnational ERWT online communities, have continued to play an important role in driving the terrorist threat to the UK, primarily through inspiring individuals to carry out terrorist activity.

Northern Ireland-related terrorism

In March 2023, the threat level in Northern Ireland (NI) from Dissident Republican (DR) groups was raised to 'SEVERE: *an attack is highly likely*'. Whilst the number of national security attacks and attempted attacks by DRs in NI had been in decline, we have recently seen a shift in the threat, which has resulted in several attacks and attempted attacks.

The most serious threat in NI remains that posed by violent DR groups, specifically the new IRA, the Continuity IRA, and a new variant of the group calling themselves Arm Na Poblachta (ANP). There remains a minority who aim to destabilise the peace settlement, and their activity causes harm to communities across NI.

During the reporting period, the new IRA conducted a shooting attack against an off-duty police officer, leaving him in a critical condition, and separately deployed a command wire improvised explosive device (IED) against a police patrol car in Strabane. The group were also responsible for shots fired at Police Service Northern Ireland (PSNI) officers policing an anti-internment bonfire in Londonderry. ANP also attempted an attack, hijacking a civilian vehicle to deploy an IED against a PSNI station in Londonderry. The device did not function. These incidents demonstrate the continued intent and potential severity of the threat in NI from DR groups who continue to aspire to mount attacks, typically against the PSNI, prison officers and military personnel.

Loyalist paramilitary groups have in recent years been predominantly involved in criminality, but there is a risk that discontent in the loyalist community, which has previously given rise to episodes of violent disorder, could escalate again. The past year has primarily seen peaceful protest as the means for loyalist communities to express opposition to the NI

Protocol, with loyalists maintaining a 'wait and see' approach to negotiations regarding the Windsor Framework.

The Cyber Threat

Cyber is a vector used by both state actors and criminals to steal information, data and intellectual property; it represents a significant and increasing threat to the UK.

Over the past year, the global cyber-security landscape has evolved significantly. In the National Cyber Security Centre (NCSC) Annual Review 2022, the Chief Executive Officer of NCSC explained that the most profound change came with Russia's invasion of Ukraine. What has been seen is a very significant conflict in cyberspace. As Director GCHQ explained in March 2022: "*we have seen the Russian state try to align and coordinate cyber capabilities alongside more traditional facets of military power… The country's use of offensive cyber tools has been irresponsible and indiscriminate.*"

Chinese activity has become ever more sophisticated and pervasive in cyberspace; a substantial global espionage campaign seeks to meet political, socio-economic and strategic objectives. They are increasingly targeting third-party technology and service supply chains, as well as successfully exploiting software vulnerabilities. China has also identified several existing and emerging technologies as being vital to its future national security, notably artificial intelligence, quantum computing, and semiconductors. It has continued to direct significant resources into research and development and continues to push for technical supremacy. In January 2023, FBI Director Christopher Wray judged that China has "*a bigger hacking program than that of every other major nation combined*".

Iran remains an aggressive cyber actor with a range of espionage, disruptive and destructive cyber capabilities. Cyber actors associated with the Iranian State have also been implicated in attacks against victims in many countries. An example of this approach was Iran's attacks against the government of Albania in mid-2022, which the UK Government condemned in September.

Proliferation of weapons of mass destruction

HMG continues to support efforts both domestically and internationally to counter the proliferation of equipment and materials related to weapons of mass destruction.

ANNEX B: EXPENDITURE, ADMINISTRATION AND POLICY – 2021/22

<table>
<tr><th colspan="2">Single Intelligence Account</th></tr>
<tr><td colspan="2">Expenditure in 2021/22</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>3,016,916</td><td>951,433</td><td>3,968,349</td></tr>
<tr><td>Out-turn</td><td>2,936,425</td><td>919,035</td><td>3,855,460</td></tr>
</table>
</td></tr>
<tr><td>Expenditure by category</td><td>● Staff pay: £1.20bn
● Other expenditure: £2.31bn
● Capital spending: £919m</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 seek more effective measures to counter the Agencies' operations against them.

Cross-Agency major projects in 2021/22	● TRANSFORMING CORPORATE SERVICES – a 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. While the cross-community team ***, the Agencies had requested additional funding to pursue the shared set of digital platforms, having already had to draw down on contingency funds to address "*issues caused by COVID-19*" and a "*delay… that was not recoverable*". In December 2021, HM Treasury approved an adjusted Full Business Case Addendum following a re-planning exercise. This increased the programme's Whole Life Cost, comprising an increase in the base cost, and including a contingency. The Agencies expect that adjustments to the plan will necessitate the use of some of this contingency funding. The extent of this is subject to commercial negotiation, but is expected to remain within the authorised total. ● The cross-community initiative to deliver IT requirements to the Agencies (such as hardware, access management, storage and information sharing), to align IT infrastructure, platforms and practices across the Agencies, and to create new (and share existing) "*mission applications*". During the financial year 2021/22, the next stage of the cross-community infrastructure was delivered, with a focus on the National Security Platform. The initiative has also maintained mission capability across all Agencies through the support of critical infrastructure, and delivered critical infrastructure to support communications with HM Government (HMG) and partners in support of the UK response to Russia's invasion of Ukraine.

MI5 (Security Service)

Expenditure in 2021/22[1]

Total budget and out-turn

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

Expenditure by category

- Staff costs: ***
- Other revenue costs (including professional services, accommodation, research and development, and IT systems): ***
- Capital costs: ***
- National Cyber Security programme (NCSP): ***

Administration

Staff numbers[2]

	Total staff	SCS[3]	Non-SCS
31 March 2021	5,259	62.5	5,196.5
31 March 2022	5,526.5	91.5	5,435

Recruitment in 2021/22

- MI5 recruited 608[4] staff, against a target of 507 in 2021/22.
- This compares with recruiting 318 new staff against a target of 260 in 2020/21.

Major projects in 2021/22

- Work has continued on a project to establish a new Counter-Terrorism (CT) Operations Centre combining the CT elements of the Agencies with Counter Terrorism Policing (CTP). This aims to improve joint working between the Agencies and CTP, including in operational responses. The status of this programme was at Amber/Red as of March 2022 due to *** resourcing and global procurement issues, and therefore it was escalated to the Agencies' top-level governance body (***). As a result, since March 2022, resourcing has been prioritised for this project.
- A project preparing MI5 for the adoption of a Cloud platform. This focuses on working practices and the use of data, and is led by MI5's Cloud Adoption Portfolio team. The Outline Business Case was presented to, and endorsed by, the Resource Council.

[1] As reported to the Committee in MI5's end-year report for the 2021/22 financial year.
[2] These figures refer to the number of full-time equivalent (FTE) staff as at the end of the financial year. MI5 also engaged a number of contractors and/or consultants. These figures are not included but have estimated costs for 2021/22 of ***.
[3] Senior Civil Service.
[4] Figures provided are of staff headcount rather than FTE.

Diversity and inclusion 2021/22	● MI5 publishes a Gender Pay Gap Report (internally and externally) and an Ethnicity Pay Gap Report (internally only) on an annual basis. MI5 has undertaken to measure both its disability and sexual orientation pay gaps in 2022, in advance of publishing full reports in 2023 or 2024. ● MI5 significantly exceeded its target for female representation at SCS levels, and met its target for ethnic minority representation at SCS levels. ● MI5 introduced targeted 'Registrations of Interest' across a number of its recruitment campaigns, allowing applicants from under-represented groups to register their interest before a campaign opens formally, with the aim of increasing applications from women and from ethnic minorities. ● The first cohort from MI5's Diversity Internship arrived in summer 2021. The internship was reported to have been a success, with interns gaining significantly from the experience. ● With SIS and GCHQ, MI5 is piloting a Cabinet Office initiative supporting ethnic minority members of the Civil Service to obtain Developed Vetting status before applying for a role in the Intelligence Community. ● With SIS and GCHQ, MI5 attended the National Student Pride's Careers Fair and sponsored the LGBT Awards and the National Diversity Awards, to increase visibility and showcase the organisations' values to the wider public. ● OneCS, on behalf of the three Agencies, signed a new recruitment contract with *** in April 2022, which brings in numerous new initiatives to promote diverse recruitment, such as Equality, Diversity and Inclusion (EDI) being measured by specific key performance indicators.
Policy	
Allocation of effort at 31 March 2022[5]	Allocation of effort across three operational themes: ● CT – 59% ● Northern Ireland-related terrorism – 22% ● Counter State Threats[6] – 19%

[5] Operational allocation of effort (by FTE, to the nearest per cent).
[6] Previously referred to as 'Hostile State Activity'.

Major achievements reported to the Committee for 2021/22	● MI5 disrupted one Islamist terrorist plot and one Extreme Right-Wing Terrorism (ERWT) plot in this period. ● MI5, working with CTP and other partners, delivered a range of interventions to disrupt individuals and networks engaged in activity of national security concern. In many cases, these interventions have led to prosecution under the Terrorism Act. ● MI5's Russia mission supported the Intelligence Community response to Russia's invasion of Ukraine, continuing its work to degrade Russian Intelligence Services capability and co-ordinate the expulsion of Russian Intelligence Services officers across Europe. ● MI5 supported HMG as it considered domestic response options and provided advice to the Home Office on the national security considerations relevant to visa and border policy choices resulting from Russia's invasion of Ukraine and the potential for the Russian state to attempt to exploit refugee routes. ● Following a successful joint UK Intelligence Community German investigation, David Smith, a Russian agent within the British Embassy in Berlin, was arrested and later charged with nine offences under Section 1 of the Official Secrets Act. ● MI5 issued an interference alert in relation to Christine Lee, who had been involved in political interference activity on behalf of China's United Front Work Department (UFWD). The case provoked significant press attention and parliamentary debate, assisting not only in disrupting Lee's activity, but also in raising wider awareness of the threat from the UFWD and risks from foreign interference activity. ● The Centre for the Protection of National Infrastructure (CPNI)[7] provided protective security assets and advice for the COP26 summit hosted by the UK in Glasgow, ensuring that it was delivered safely and securely.

Covid-19 impact

- Covid-19 continued to have an impact on MI5's building capacity throughout the 2021/22 reporting year. At the outset of the reporting year, building capacity stood at approximately ***. Capacity was increased gradually in April (to ***) and May (to ***), before restrictions were fully removed in August.
- The impact of these capacity restrictions was reduced by MI5 employees being able to conduct some work from home, up to OFFICIAL-SENSITIVE, using devices supplied by GCHQ through its GOLO programme.
- MI5 continued to supply lateral flow tests for all staff throughout the year, and encouraged all those attending the workplace to test regularly, even if asymptomatic.

[7] On 13 March 2023, the CPNI was renamed as 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 the UK faces today extend far beyond critical national infrastructure.

Crisis response impact

- MI5 has supported the cross-Intelligence Community response to Russia's invasion of Ukraine in 2022, including:
  - managing the threat to the UK and the UK's interests;
  - degrading Russian Intelligence Services (RIS) capability in the UK and Europe;
  - supporting sanctions work against Russian state-linked individuals and enterprises; and
  - strengthening MI5's upstream effort to better detect threats projected by Russia from overseas.
- This has been resourced by staff from a range of capabilities in MI5 including ***, from a range of missions in an effort to minimise the impact of redeploying staff on the rest of the organisation.
- However, there was a consequent impact on several other workstreams across MI5 ***. This included:
  - stopping the testing of some new capabilities, preventing these from being deployed to investigators;
  - ***;
  - ***; and
  - ***.
- Following Russia's invasion of Ukraine, the Joint State Threats Assessment Team Russia team temporarily surged analytical capability in response to additional demand. This ***% increase in capability on Russia led to ***.
- In response to the changing security situation following the military withdrawal from Afghanistan, MI5 was also required to reprioritise some overseas investigative CT activity. CT resources were also surged in support of the wider UK Government resettlement effort through the tracing of individuals applying to relocate to the UK, with a short-term impact on MI5's *** functions.

Secret Intelligence Service (SIS)

Expenditure in 2021/22[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: ***
- NCSP: ***

Administration

Staff numbers[9, 10]

	Total staff	SCS	Non-SCS
31 March 2021	3,644	76.4	3,567.6
31 March 2022	3,673	85.68	3,587.52

Recruitment in 2021/22

- SIS recruited *** new FTE staff against a target of *** in 2021/22.
- This compares with the recruitment of *** new staff against a target of *** in 2020/21.

[8] As reported to the Committee in SIS's end-year report for the 2021/22 financial year.
[9] These figures refer to the number of FTE staff as at the end of the financial year. SIS also employed a number of contractors and/or consultants. These figures are not included but have estimated costs for 2021/22 of ***.
[10] These figures include *** staff.

Major projects in 2021/22	● A project preparing SIS for the adoption of a new IT platform. This aims to co-ordinate and enable the delivery of capabilities, services and processes, and implement the required cultural changes across the organisation, to ensure that SIS is ready to adopt and use the new platform. During the 2021/22 financial year, SIS *** and established a team to co-ordinate the migration to the new platform. SIS began onboarding this team in 2022. ● SIS continued to invest in its 'Capability Portfolio', 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 ***. This programme has external assurance, including input from the Infrastructure and Projects Authority. The programme currently lacks sufficient funding to meet its objectives, but expects to make up any shortfall through funding from cross-Community programmes including Digital Transformation and Science and Technology. ● A Science, Technology and Engineering programme has been established to fund research and development across the Agencies. Since the programme started, SIS has developed its strategy alongside the completion of the 2021 Spending Review process and the development of national science and technology priorities under the National Science and Technology Council. For instance, more resource has been allocated to the growing threat from China, and more investment has been allocated into key technologies (such as ***). However, significant risks remain that have been assessed as both high-probability and high-impact, such as *** insufficient commercial capacity.
Diversity and inclusion 2021/22	● SIS introduced targeted Registrations of Interest across a number of its recruitment campaigns, allowing applicants from under-represented groups to register their interest before a campaign opens formally, with the aim of increasing applications from women and from ethnic minorities. ● The first cohort from SIS's Diversity Internship arrived in summer 2021. The internship was reported to have been a resounding success, with interns gaining significantly from the experience. ● With MI5 and GCHQ, SIS is piloting a Cabinet Office initiative supporting ethnic minority members of the Civil Service to obtain Developed Vetting status before applying for a role in the Intelligence Community. ● With MI5 and GCHQ, SIS attended the National Student Pride's Careers Fair and sponsored the LGBT Awards and National Diversity Awards, to increase visibility and showcase the organisations' values to the wider public.

Policy	
Allocation of effort at 31 March 2022	• Key operational activities including: CT; cyber and access generation; defence technology and counter proliferation; and prosperity and economic stability – 31% • Operational support including: global network enabling; covert operations; data exploitation; operational security; and operational technology – 38% • 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 – 31%
Major achievements reported to the Committee for 2021/22	• SIS provided intelligence illuminating Russian intent towards Ukraine before and during its invasion in February 2022, enabling HMG to formulate appropriate policy responses. SIS responded to new requirements as the Ukraine crisis developed, producing reporting on the situation in Ukraine including on ***. • SIS delivered a range of support to Ukrainian partners, which enabled them to counter hostile RIS and military activity before and after the invasion. • SIS held dialogues on China with a wide range of international partners, and produced a range of intelligence reporting to inform HMG's policy development, including on ***. • SIS continued to provide intelligence that contributed to the detection and disruption of terrorist activity. SIS reporting on a planned attack in a capital city resulted in the arrest of two individuals by local authorities in the country concerned. • SIS intelligence was the main contributor to HMRC fraud systems, detecting a large-scale attack which, had it gone undetected and been successful, could have led to losses of over £50m.

Covid-19 impact

- Overseas Stations followed local Covid-19 laws and restrictions; however, SIS also developed a Global Network plan for Stations which outlined best practice on vaccinations and prevention measures.
- Operational activity with some liaison partners was delayed or curtailed due to ongoing local restrictions.
- SIS ensured that Stations were not understaffed for significant periods while staff on 'hardship postings' received regular 'breather' breaks. Staff required managed quarantine and self-isolation exemption letters to be able to have a full break in the UK.
- Exemption letters were also exceptionally issued to staff in order to return to the UK to conduct essential operational business, on the grounds of national security, which had to be authorised by a senior officer. However, the number of exemption letters significantly decreased with the relaxation of UK travel restrictions and a negligible number were issued during the reporting year.
- The Committee has not been provided with building capacity details for the Headquarters.

Crisis response impact

- SIS's response to Russia's invasion of Ukraine was resourced by staff from a range of areas across the organisation, including the Russia mission, other operational teams, linguists, open-source specialists, and military. Overall, *** staff were moved into a central operational hub over the course of *** days.
- SIS also responded to the military withdrawal from Afghanistan, during which a central operational hub was rapidly expanded to provide 24-hour coverage and include a 'communications team' of linguists. Overall, *** officers were involved over the *** period of the evacuation.

Government Communications Headquarters (GCHQ)

Expenditure in 2021/22[11]

Total budget and out-turn

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

Expenditure by category

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

Administration

Staff numbers[12]

	Total staff	SCS	Non-SCS
31 March 2021	7,181.2	102.5	7,078.7
31 March 2022	7,082.1	114.7	6,967.4

Recruitment in 2021/22

- GCHQ recruited 386 staff against a target of 588 in 2021/22.
- This compares with recruiting 377 new staff against a target of 859 in 2020/21.

[11] As reported to the Committee in GCHQ's end-year report for the 2021/22 financial year.
[12] These figures refer to the number of FTE staff as at the end of the financial year. GCHQ also employed a number of contractors and/or consultants. These figures are not included but have estimated costs for 2021/22 of ***.

Major projects in 2021/22	● Computer Network Exploitation (CNE) Growth – this project follows on from the CNE Scaling programme referenced in the 2021–2022 Annual Report. This is driven by a new set of demands from two sources, the first and largest being *** and the second being ***. The programme aims to significantly increase GCHQ's capacity to deliver CNE operations. It will deliver a range of capabilities – from physical facilities to complex software development – which, combined with an increase in skilled resources, will allow CNE to undertake operational tasking. Delivery of the programme is measured through milestones that represent the increasing provision of CNE capacity. During the 2021/22 financial year, one out of three delivery milestones was reached, with the other two being deferred. ● Analysis Convergence Unit (ACU) – this aims to improve and drive collaboration within Analysis across the UKIC, to rationalise and build a streamlined set of capabilities within Analysis, and to scale low-side analysis. The ACU is the principal portfolio for delivering the Digital Transformation of Data and Analytic capabilities committed to in the Spending Review. During the 2021/22 financial year, the programme had an underspend of £*** and delivered milestones including a transition from end-of-life legacy systems onto a new system for reading and publication of JSTAT assessments. ● Continuous At-Sea Deterrent (CASD) programme – this aims to enhance the Intelligence Community's provision of assurance on the UK's CASD. This received funding at the 2021 Spending Review to complete the final three years of the seven-year uplift programme. The Full Business Case is awaiting final approval and sign-off from the Treasury.

Diversity and inclusion 2021/22	● GCHQ's Gender Action Plan was endorsed in July 2022, and working groups have been set up to deliver against the priority areas. As part of this, GCHQ's Board agreed a new female recruitment ambition of 50% for the financial year 2021/22 (36% for technical capabilities). ● GCHQ published its fourth Gender Pay Gap Report in November, covering the year 2021. The Report showed that its gender pay gap had fallen for the second consecutive year (the mean gender pay gap fell from 12.5% in 2019 to 11.7% in 2021). ● GCHQ's first Ethnic Minority Action Plan reached the end of its 18-month timeframe. The majority of actions originally in scope were completed, including a reduction in the median pay gap, and improving ethnic minority recruitment rates. ● In line with the recommendations of a study of security clearance refusals for ethnic minority applicants, referred to in the Committee's 2021–2022 Annual Report, EDI training was introduced into GCHQ's Vetting Officer Development Programme. ● With MI5 and SIS, GCHQ is piloting a Cabinet Office initiative supporting ethnic minority members of the Civil Service to obtain Developed Vetting status before applying for a role in the Intelligence Community. ● With MI5 and SIS, GCHQ attended the National Student Pride's Careers Fair and sponsored the LGBT Awards and National Diversity Awards, to increase visibility and showcase the organisations' values to the wider public. ● GCHQ launched its Inclusion Action Plan this year, taking a 'whole system approach' to inclusion based on the three elements of organisational culture: physical artefacts, espoused values, and underlying beliefs.
Policy	
Allocation of effort at 31 March 2022	● Mission-specific programmes including: CT; Offensive Cyber; serious organised crime; and counter-proliferation – ***% ● Capability exploitation – 19% ● Engineering – 19% ● IT services – 11% ● Cyber security – ***% ● Corporate services (including human resources and finance) – 13%

Major achievements reported to the Committee for 2021/22	● GCHQ and the National Cyber Force (NCF)[13] have supported HMG's response to Russia's invasion of Ukraine. GCHQ intelligence was fundamental to the UK's assessment of the risk of conflict, and to efforts to build a coalition of Western nations to respond to the crisis. GCHQ also provided a greatly enhanced level of support to the UK presence based out of the Embassy in Kyiv. ● GCHQ and the National Cyber Security Centre (NCSC) worked with partners to build an intelligence picture of the first known destructive cyber-attack against Ukraine in the run-up to Russia's invasion, and to attribute this publicly to Russian military intelligence. ● NCSC and partners identified the significant compromises of Solar Winds and Mimecast, leading to a cross-government response and to the public attribution of this major cyber attack to Russia. ● GCHQ intelligence contributed to the senior decision-making process during the UK's military evacuation from Afghanistan. GCHQ reporting was a key factor in revising the severity of the threat assessment for Kabul airport, ultimately affecting how British Forces were deployed at Kabul airport and having a significant impact in reducing casualties and saving lives in relation to the suicide attack that took place. ● GCHQ intelligence collection resulted in overseas partners being warned about a specific plot linked to the Islamic State in Iraq and the Levant to conduct suicide attacks. This intelligence was identified as the result of investigation into other attack plots that were in the planning stages. ● Following the successful launch of the National Cyber Strategy in December 2021, the NCF has been supporting cross-government work to identify how best to achieve the Strategy's objectives and further the UK's position as a responsible democratic cyber power.
Covid-19 impact	
● The performance of GCHQ's investment portfolio continued to be affected by Covid-19 in the financial year 2021/22. There were early indications of Total Departmental Expenditure Unit underspend due to supply chain issues, protracted lead times and delays in mobilisation due to delivery management shortages. ● Many of GCHQ's Covid-19 countermeasures were close to being fully withdrawn by the end of the period covered by this Report, including the requirement to wear a face covering when moving around GCHQ's buildings and the routine asymptomatic testing of staff. ● The building occupancy level was raised, with a ceiling maintained for non-Covid reasons; this reflects the number of people that GCHQ considers can be accommodated without returning to previous levels of overcrowding.	

[13] NCF is a partnership between GCHQ and the Ministry of Defence primarily (although it also includes elements from SIS and the Defence Science and Technology Laboratory), and its work is therefore reflected under GCHQ and Defence Intelligence in this Annex.

Crisis response impact

- GCHQ's response to Russia's invasion of Ukraine has had a consequent resourcing impact on other lines of work. This includes GCHQ's work on ***.
- This has also led to a reduction in strategic reporting on ***; a reduction in ***, and prioritisation of ***.
- During the military withdrawal from Afghanistan, there was minimal need for GCHQ to reallocate resource from other areas within the organisation, although the demands on ***.

Defence Intelligence (DI)

Expenditure in 2021/22[14]

Total budget and out-turn

£'000	Resource spending	Capital spending	TOTAL
Budget	351,268	20,001	371,269
Out-turn	354,061	17,265	371,326

Expenditure by category

- Operational staff costs: £261.5m
- Research and development: £39.6m
- Other operational costs: £92.3m
- Other administrative costs: £11.5m
- Against this, DI received income of £33.6m

Administration

Staff numbers[15]

	Total staff	Total civilian staff	Total Armed Forces staff	Armed Forces		Civilian staff	
				SCS equivalent	Non-SCS equivalent	SCS	Non-SCS
31 March 2021	4,115	1,536	2,579	10	2,569	9	1,527
31 March 2022	4,194	1,587	2,607	8	2,599	9	1,578

Recruitment in 2021/22

- In 2021/22, DI recruited 143 civilian personnel, compared with 149 in 2020/21.[16]

[14] As reported to the Committee in DI's end-year report for the 2021/22 financial year.
[15] These figures refer to the number of FTE staff as at the end of the financial year. DI also employed a number of contractors and/or consultants. These figures are not included but have estimated costs for 2021/22 of £20.1m.
[16] 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 projects 2021/22	● PRIDE2 – this project, as set out in our Annual Report 2019–2021 and Annual Report 2021–2022, aims to consolidate the DI estate, and will support the Government's 'Places for Growth' policy by contributing to housing targets. During the 2021/22 financial year, DI worked to prepare the Outline Business Case for the programme and designed a workforce strategy to sustain output during the move of personnel from the Defence Geographic Centre in Feltham, to RAF Wyton. ● RAF Digby redevelopment – this project aims to replace ageing technical and domestic infrastructure at RAF Digby. This programme continued to progress and these upgrades are currently expected to be operational before 2030. ● DI Cyprus Consolidation – this project[17] is *** to rebuild an operations facility in Cyprus and bring *** missions under one facility. When evidence was submitted, infrastructure work was ongoing and due to be completed by September 2022, with network and security work due to be completed by February 2023 and the facility's internal infrastructure likely to be completed in June 2023.
Diversity and inclusion 2021/22	● The first year of DI's Diversity and Inclusion Strategy 2021–26 has been completed, and an action plan for the second year has been identified. ● The three key outputs for the second year are: a session of workshops in support of ongoing work to develop an inclusive culture; strengthening DI's Diversity and Inclusion Adviser resource; and educating managers and staff to create a culture of respect through the 'Green Dot' training programme (a programme developed by the Joint Intelligence Organisation, which seeks to encourage staff to raise a concern about any behaviour that makes them feel uncomfortable or excluded).
Policy	
Allocation of effort at 31 March 2022	● Total operational and analysis effort – 82%. This comprises: – All source analysis and assessment – 9% – Collection and analysis – 73% ● Operational support – 14%. This comprises: – Armed Forces security and intelligence training – 11% – Armed Forces intelligence policy and future capability development – 2% – Reserves – 1% ● Central support – 5%

[17] Project BRIGHTSIDE.

Major achievements reported to the Committee for 2021/22	● DI provided substantial analysis and assessment on Russia's invasion of Ukraine, including providing forewarning of Russian intent to customers across government, to international partners, and to parliamentarians and the general public. DI's work has informed decisions made by Ministers and Armed Forces chiefs on the UK's posture towards Russia, and the provision of lethal and non-lethal aid to Ukraine. ● Some of DI's reporting has been produced for public release. The impact of DI's daily Ukraine Twitter campaign, with an unprecedented level of activity and presence on Twitter, was substantial. In terms of penetration, this has become the best performing social media campaign of the Ministry of Defence (MoD). ● DI supported planning for the withdrawal of UK forces from Afghanistan, providing a range of assessments covering the strategic intent, capability and activities of the Taleban. In August 2021, DI temporarily reallocated resource to support the air evacuation of entitled persons under the UK Afghanistan Relocation and Assistance Policy. ● The NCF[18] also supported the military drawdown and evacuation from Afghanistan, rapidly developing cyber options to provide force protection measures. ● DI has continued to produce analysis on the potential of, and scenarios for, a Chinese invasion of Taiwan, including a substantial set of briefing papers and scenarios for the National Security Council. DI also continued to provide extensive support to the Royal Navy's Carrier Strike Group during its deployment to the Far East.
Covid-19 impact	
● All DI staff requiring access to systems above OFFICIAL-SENSITIVE have returned to the office, and desk utilisation at DI's main sites is mostly back to pre-Covid levels.	
Crisis response impact	
● DI temporarily reprioritised tasking across the organisation during Russia's invasion of Ukraine, in order to free up resources and to scale up intelligence collection and production capacity. ● In addition to refocusing efforts within business units to free up staff internally, an additional *** personnel augmented both DI's Russia and Eurasia Centre and Production and Engagement Team.	

[18] NCF is a partnership between GCHQ and the MoD primarily (although it also includes elements from SIS and the Defence Science and Technology Laboratory), and its work is therefore reflected under GCHQ and Defence Intelligence in this Annex.

National Security Secretariat (NSS)

Expenditure in 2021/22[19]

Total budget and out-turn

£'000	Resource spending	Capital spending	TOTAL
Budget	15,097.8	0	15,097.8
Out-turn	17,128.7	0	17,128.7

Expenditure by category

- Operational staff costs: £14.9m
- Operational IT costs: £2.1m
- National Cyber Security Programme (NCSP): £3.2m

Administration

Staff numbers

	Total staff[20]	SCS[21]	Non-SCS
31 March 2021	238	25	213
31 March 2022	196	23	173

Recruitment in 2021/22

- NSS recruited 46 staff in 2021/22.
- This compares with 77 staff in 2020/21.

Major projects in 2021/22

- None reported.

Diversity and inclusion 2021/22

- NSS hosts a small team from across the national security community to focus on driving change and progress on culture, diversity and inclusion for the whole community.
- The National Security Vetting Diversity Initiative launched this year, to improve recruitment and representation for organisations and roles requiring Developed Vetting security clearance.
- NSS contributed to the production and launch of the refreshed 'Mission Critical' toolkit of inclusive best practice.
- NSS is carrying out further work to build line management capability and introduce the 'Green Dot' campaign to improve behaviours.

Policy

Allocation of effort at 31 March 2022

- Policy teams and private offices – 87%
- Corporate services – 13%

Major achievements reported to the Committee for 2021/22

- In response to Russia's invasion of Ukraine, NSS established crisis response structures to lead on co-ordination and support ministerial decision-making.
- NSS led on the implementation of the Government's Integrated Review with the aim of ensuring that the UK's security, defence, development and foreign policy architecture keeps pace with the evolving international environment.

[19] As reported to the Committee in NSS's end-year report for the 2021/22 financial year.
[20] These numbers are in relation to all NSS staff excluding the Civil Contingencies Secretariat and NCSP-funded posts.
[21] Includes one SCS 4 – the National Security Adviser.

Covid-19 impact
● Limitations on building occupancy, travel restrictions and self-isolation requirements continued to have an impact. In November 2021, most Cabinet Office buildings lifted lockdown restrictions; however, NSS has not provided occupancy details to the Committee.
Crisis response impact
● During the course of 2021/22, NSS dedicated significant resource to work on Afghanistan, peaking during the evacuation, and on Ukraine in the run-up to and during Russia's invasion.

Joint Intelligence Organisation (JIO)

Expenditure in 2021/22[22]

Total budget and out-turn

£'000	Resource spending	Capital spending	TOTAL
Budget	11,500	0	11,500[23]
Out-turn	11,056	846	11,902

Expenditure by category

- Staff costs: £8.8m
- Travel: £85,000
- The remaining out-turn is accounted for primarily through accommodation/estates, staff training, supplies and services, and other administrative costs.

Administration

Staff numbers[24]

	Total staff	SCS	Non-SCS
31 March 2021	110	10	100
31 March 2022	106	10	96

Recruitment in 2021/22

- The JIO recruited 31 new staff in 2021/22, ***.
- This compares with 16 staff recruited in 2020/21, ***.

Major projects in 2021/22

- Development of the Information and Data Exchange (INDEX) system – this is a project to bring together cross-government reporting at the classification OFFICIAL-SENSITIVE onto one shared platform. The INDEX system uses 'smart search' technology to enable analysts to access relevant analysis, both from inside and outside the government, quickly and securely. During the 2021/22 financial year, the JIO secured additional funding to extend the INDEX service to other intelligence assessment departments across government.

[22] As reported to the Committee in the JIO's end-year report for the 2021/22 financial year.
[23] In the financial year 2021/22, JIO's budget was £11.5m but with access to a 'contingency fund' shared with NSS of up to £2.5m, should it be required. At the end of the financial year, with additional investment in the INDEX programme (which also accounts for the Capital Departmental Expenditure Unit spend when none was originally budgeted) the total JIO budget spend was £402,000 over the core £11.5m, drawing on the contingency fund for that value.
[24] These figures refer to the number of FTE staff as at the end of the financial year.

Diversity and inclusion 2021/22	● The JIO's Diversity and Inclusion Network meets each month to align national security community efforts with those throughout the Cabinet Office. All JIO staff have a mandatory Diversity and Inclusion objective as a way to mainstream the work across the organisation. ● JIO launched an Action Plan in late 2021, bringing together various strands of work under various themes (e.g. recruitment, culture, transparency). ● JIO's 'Yellow Dot' campaign – which seeks to encourage staff to raise a concern about any behaviour that makes them feel uncomfortable or excluded – has been rolled out across the wider national security community and rebranded as 'Green Dot'. ● JIO has sponsored some of the posts in the National Security Vetting Diversity Initiative.
Policy	
Allocation of effort at 31 March 2022	● Total operational activity – 93% ● Corporate services – 7%
Major achievements reported to the Committee for 2021/22	● JIO issued 43 Joint Intelligence Committee (JIC) Assessments, 45 Intelligence Briefs, and 205 JIO Spotlights. ● JIO supported the cross-government response to Russia's invasion of Ukraine, working closely with Five Eyes and other international partners. JIO issued assessments on a range of issues, including the risk to UK personnel in Ukraine, nuclear safety and security in Ukraine, and Russia's domestic and economic prospects as affected by the crisis. ● JIO chaired the NATO Civilian Intelligence Committee's Economic panel in July 2021, and briefed NATO's North Atlantic Council in December 2021 on the key findings. ● The Professional Head of Intelligence Assessment (PHIA) worked to develop a red team challenge function for the JIO, which seeks to give additional challenge and rigour to JIC judgements.
Covid-19 impact	
● JIO implemented a staff rota and used its emergency fallback site *** in order to continue to operate at close to full capacity. ● When distancing restrictions relaxed, JIO increased office presence to near 100%. JIO is still enabling hybrid working in part, in order to make effective use of its working environment and avoid disruption to those staff who require access to higher-classification systems.	
Crisis response impact	
● The response to Russia's invasion of Ukraine dominated JIO's resources and outputs between January and March 2022, and analysts and capability staff were temporarily reallocated from across the organisation into a Russia–Ukraine crisis team. ● During the early stages of 2022, JIO moved to shift working to sustain a frequent rhythm of assessed insights throughout the reporting period.	

Homeland Security Group (HSG)

Expenditure in 2021/22[25]

Total budget and out-turn

£'m	Resource spending	Capital spending	TOTAL
Budget	1,128.3	206.9	1,335.2
Out-turn	1,021.8	190.3	1,212.1

Expenditure by category

- Staff costs: £73m
- Grants spending: £989.4m[26]
- Other costs: £84.7m
- Conflict, Security and Stability Fund: £2.7m
- Additional funding allocated by the National Security Council (Nuclear): £15.8m
- Against this, HSG received an income of £259.4m

Administration

Staff numbers[27]

	Total staff	SCS	Non-SCS
31 March 2021	1,061	30	1,031
31 March 2022	1,113	33	1,080

Recruitment in 2021/22

- HSG recruited 214 staff in 2021/22, compared with 161 staff in 2020/21.

Major projects in 2021/22

- The Radiological and Nuclear Security Portfolio – this will deliver enhancements across the end-to-end system for nuclear security. At the 2021 Spending Review, the Treasury approved an overall funding envelope of £401m for the programme.
- Reform of the Suspicious Activity Reporting Regime – work continued on this programme to update the Regime to address the scale of the threat faced in the UK. This will be delivered through a staffing uplift, a new digital service and legislative change.

Diversity and inclusion 2021/22

- HSG's Diversity and Inclusion Action Plan focuses on improving outcomes for Black, Asian and Minority Ethnic (BAME) staff, particularly with a view to increasing representation at more senior grades.
- A Diversity and Inclusion Board meets regularly, with SCS leads across all protected groups each developing and driving clear actions for change and support.
- A 'Career Watch' sponsorship programme has been relaunched, available to all BAME staff and staff with disabilities. All SCS must sponsor at least two BAME staff/staff with disabilities.

[25] As reported to the Committee in the HSG end-year report for the 2021/22 financial year.
[26] The vast majority of HSG expenditure is administered via Grants mechanisms, and CT policing grants constitute over 75% of HSG's net budget.
[27] These figures refer to the number of FTE staff as at the end of the financial year.

Policy	
Allocation of effort at 31 March 2022	● National Security Directorate (including arm's length bodies) – 31% ● Directorate of State Threats and Cyber – 7% ● PREVENT and Research and Information Communication Unit – 13% ● PROTECT PREPARE (CBRNE) and science and technology (including the Joint Security and Resilience Centre) – 17% ● Data, Information and Operations – 16% ● CONTEST Directorate – 9% ● Economic Crime Directorate – 7%
Major achievements reported to the Committee for 2021/22	● HSG contributed to the cross-government response to Russia's invasion of Ukraine and its domestic implications for the UK, primarily through cross-government work on state threats resilience and preparedness. HSG also supported wider Home Office efforts to ensure that British nationals and other eligible persons were able to leave Ukraine and return to the UK. ● HSG continued to lead negotiations with the US on the UK–US Data Access Bilateral Agreement, and to work with operational partners to ensure readiness to make use of the agreement following its entry into force. ● HSG continued preparations for the introduction of the National Security Bill to Parliament. The Economic Crime (Transparency and Enforcement) Act received Royal Assent in March 2022. ● Following the death of Sir David Amess MP, HSG worked with CTP and the Parliamentary Security Department to review protective security arrangements for Members of Parliament.

Covid-19 impact
● During 2021/22, workplace attendance was governed by Government advice and the imposition and relaxation of restrictions. In March 2022, HSG's offices were brought back to full capacity, although hybrid working was also introduced. Under hybrid working, HSG staff are expected to spend at least 40% of their contracted time in the office.

Crisis response impact
● The HSG Operations team co-ordinated the Home Office's response to Russia's invasion of Ukraine. Increased demands were met through a volunteer cadre to provide resilience to the core team. As the demand on the department has become less acute, staffing has returned to business as usual. ● HSG also provided temporary resourcing assistance to the Foreign, Commonwealth and Development Office's Sanctions Taskforce established in the wake of the invasion. These have now returned to their regular assignments. ● HSG continues to contribute to cross-government responses through the Russia Domestic Co-ordination Cell.

ANNEX C: MEMORANDUM OF UNDERSTANDING UNDER THE JUSTICE AND SECURITY ACT 2013

Introduction

1. The Justice and Security Act 2013 ("the Act") provides for the oversight of the intelligence and security activities of HM Government (HMG) by the Intelligence and Security Committee of Parliament (ISC).

2. The Act states that any memorandum of understanding (MoU) for the purposes of the Act must be agreed between the Prime Minister and the Intelligence and Security Committee of Parliament. The ISC shall publish the MoU and lay a copy before Parliament (see section 2(6) of the Act).

3. In addition to addressing certain particular matters specified by the Act,[1] this MoU also sets out the overarching principles which will govern the relationship between the ISC and those parts of Government it oversees.

The Intelligence and Security Committee of Parliament

4. The ISC is a Committee of Parliament created by statute and comprising members of each House of Parliament.[2] For the purposes of its work, the ISC has a staff, known as the ISC Secretariat.

5. Parliament appoints the members of the ISC, by vote on a motion of the relevant House. Candidates for membership must first have been nominated by the Prime Minister. The ISC elects its own Chair from amongst the appointed members of the Committee.

6. The ISC makes its reports to Parliament, subject to the requirement that material must be redacted from a report if the Prime Minister considers that its inclusion would prejudice the functions of the Security Service, the Secret Intelligence Service, the Government Communications Headquarters (collectively, "the Agencies") or of other parts of the intelligence and security community. The ISC may also, as appropriate, report to the Prime Minister.

7. All members of the ISC, and their staff, are notified under the Official Secrets Act 1989 (section 1(1)(b) and 1(6)). They may not, without lawful authority, disclose any information related to security or intelligence which has come into their possession as a result of their work on, or for, the ISC.

---

[1] The activities of HMG that the ISC shall oversee; the principles governing the ISC's consideration of operational matters; the arrangements by which the Agencies and other government Departments will make information available to the ISC; and the relevant Ministers of the Crown responsible for providing information to the ISC.

[2] The Standing Orders of the House of Commons and House of Lords, which govern the procedures of their Select Committees in general, do not apply to the ISC. The ISC has the power to hear evidence on oath, but it is expected that this will only be used exceptionally.

Remit

8. The Act provides that the ISC may oversee the expenditure, administration, policy and operations of the Agencies; and that it may examine or otherwise oversee such other activities of HMG in relation to intelligence or security matters as are set out in a memorandum of understanding. The ISC is the only committee of Parliament that has regular access to protectively marked information that is sensitive for national security reasons: this means 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.[3] In addition to the expenditure, administration, policy and (subject to paragraphs 11–17) operations of the Agencies, the ISC and HMG have agreed that the ISC shall also oversee the following activities:

a) MOD:

   i The strategic intelligence activities undertaken by the Chief of Defence Intelligence, including intelligence collection, analysis and training.[4]

   ii Offensive cyber.

b) Cabinet Office:

   i The activities of the National Security Adviser and National Security Secretariat in relation to matters of intelligence and security. In practice this will include the activities of the Cabinet Office: in providing support to the Prime Minister in his role as Minister with overall responsibility for intelligence and security matters; coordinating intelligence policy issues of strategic importance and public scrutiny of intelligence matters; managing the Single Intelligence Account; and certain activities (relating to matters of intelligence and security) of the Office of Cyber Security and Information Assurance (OCSIA).

   ii The activities of the Joint Intelligence Organisation.

c) Home Office: the activities of the Office for Security and Counter-Terrorism (OSCT).

9. There are a number of other individuals or bodies that oversee intelligence and security matters. For example: the Independent Reviewer of Terrorism Legislation; the Intelligence Services Commissioner; and the Interception of Communications Commissioner. The ISC will continue to have a relationship with those bodies and should cooperate with them so far as is reasonable to avoid any unnecessary duplication in their respective remits.

10. Likewise, the ISC will seek to avoid unnecessary duplication with the work of courts or tribunals (such as the Investigatory Powers Tribunal) which may, from time to time, have cases before them concerned with intelligence and security matters.

---

[3] This will not affect the wider scrutiny of departments such as the Home Office, FCO and MOD by other parliamentary committees. The ISC will aim to avoid any unnecessary duplication with the work of those Committees.
[4] In respect to operational matters, addressed in paragraphs 11–17, general military operations conducted by the MOD are not part of the ISC's oversight responsibilities.

Oversight of Operational Matters

11. The ISC may consider or otherwise oversee the operational activities[5] of the Agencies and the specified activities of other Government Departments referred to in paragraph 8 above ("the Departments"). The ISC may consider particular operational matters in three sets of circumstances:

a. Where the ISC and the Prime Minister are satisfied that the matter is not part of any ongoing intelligence or security operation and is of significant national interest and the consideration of the matter is consistent with any principles set out in, or with any other provision made by, the MoU (see section 2(3)(a) and 2(4) of the Act); or

b. Where the Prime Minister has asked the ISC to consider the matter and the consideration of the matter is consistent with any principles set out in, or with any other provision made by, the MoU (see section 2(3)(b) and 2(4) of the Act); or

c. Where consideration of an operational matter is not covered by (a) or (b) above, but information is nevertheless provided voluntarily to the ISC by the Agencies or a Department, whether or not in response to a request by the ISC (see section 2(3)(c) of the Act).

Further detail regarding the ISC's oversight of operational matters in these circumstances is set out below.

12. The ISC recognises the sensitivity of intelligence and security operations. Its role overseeing such operational activity will therefore be governed by the following overarching principles:

a. this work must not jeopardise the success of an operation or compromise the security and safety of those involved; and

b. the ISC's examination of an operational matter must not unduly impede the operational effectiveness of an Agency or Department.

13. Where there are legal proceedings (criminal or civil), inquiries[6] or inquest proceedings, the ISC and HMG will consider carefully whether it is appropriate to proceed with an investigation.

14. Under section 2(3)(a) of the Act, the ISC's power to oversee operational activity is retrospective and on matters of significant national interest. When considering whether an activity 'is not part of any ongoing intelligence or security operation', the ISC and the Prime Minister will take into account:

a. Whether the main objectives of the particular operation have been achieved or whether there is now no reasonable prospect of further operational activity to seek to achieve the main objectives in the near future;

---

[5] Certain long-running 'operations' may be considered within the ISC's remit, for example, where the entire intelligence gathering effort for a particular country is undertaken for long periods under the guise of a single operational code word.
[6] Including statutory inquiries or other independent judge-led inquiries.

b. That the operational activity of the Agencies and Departments can vary greatly in scope, type and magnitude and in some cases it may not be clear when a particular operation has ended. Deciding whether a matter is or is not part of 'any ongoing intelligence or security operation' will be a matter of judgement for the Prime Minister and the ISC;

c. When two or more operational activities may be separated in time but closely linked in objective, the ISC will be entitled to have retrospective oversight of such operations that have been completed, unless such oversight would jeopardise the success of such future operations; and

d. The ISC and HMG are agreed that the operational activity or event in question will only be regarded as 'of significant national interest' if it raises issues of wider significance or raises serious questions relating to Agency or Departmental conduct, competence, resourcing and policy in the operational context, including in situations where there is, or is likely to be, significant parliamentary or public interest in relation to such issues or questions.

15. The Prime Minister will nominate the National Security Adviser and his deputy for intelligence matters to consider, on his behalf, whether the conditions for such oversight are met. The final decision will rest with the Prime Minister, in conjunction with the ISC.

16. Under section 2(3)(b) of the Act, the Prime Minister may, at his discretion, consider it appropriate to invite the ISC to consider an operational matter which falls outside the 'retrospective' and 'significant national interest' criteria.

17. Under section 2(3)(c) of the Act, the ISC may consider operational matters not covered by sections 2(3)(a) or 2(3)(b) where information is provided voluntarily to the ISC by the Agencies or a Department, whether or not in response to a request by the ISC.

Provision of Information

18. The ISC requires information from HMG in order to carry out its oversight function. The importance of the ISC's oversight role is recognised by the fact that, while officials and Ministers are able to provide information to the ISC, only a Secretary of State has the power to withhold it. This is reflected in paragraph 4 of Schedule 1 to the Act.

19. The duty to provide information to the ISC rests, for the Departments, with the relevant Minister of the Crown (this may, but need not necessarily, be a Secretary of State)[7] and for the Agencies, with the Heads of the Agencies.

20. In practice there will be a range of methods which the ISC may use in order to obtain the information it requires from HMG, including:

---

[7] For the following Departments, the relevant Ministers of the Crown, for the purposes of making information available to the ISC (paragraphs 4(3) and 4(7) of Schedule 1) are as follows:

a. Cabinet Office: Any Minister of the Crown in a relevant Government department;

b. MOD: Secretary of State for Defence;

c. Home Office: Secretary of State for the Home Department;

d. Foreign and Commonwealth Office: Secretary of State for Foreign and Commonwealth Affairs.

a. oral evidence sessions with Ministers, Agency Heads and other senior officials. These sessions allow the ISC to ask detailed questions about particular issues within their remit, but also to get a broader sense of the issues that Agencies, Departments and Ministers are facing and to decide whether any particular issue might need further scrutiny;

b. Written material, both regular briefs on agreed lines of reporting and responses to specific questions. HMG and the Agencies will keep the ISC fully and promptly informed of any significant matters falling within the ISC's remit;

c. Members of the ISC's staff working with the Agencies and the Departments to obtain information on the ISC's behalf, ensuring that the ISC has all the information it needs to do its job in relation to matters consistent with its remit.

21. The responsibility for ensuring the ISC has access to relevant information consistent with its remit will fall to the appropriate Agency or Department, who will make available the information the ISC needs. The ISC will work together with the Agencies and Departments to ensure that the provision of such information does not involve disproportionate cost or diversion of effort.

22. The Committee may seek confirmation from HMG of the factual accuracy or completeness of information it has gathered before drawing on it in its reports.

23. Committee members may, as part of their work, undertake visits to the Agencies and Departments that the ISC oversees, to familiarise themselves with the broader context of their work. Information provided to Committee members in the course of such visits will not constitute formal evidence gathering unless it is agreed as such by both parties either in advance or retrospectively.

24. On occasion the Prime Minister may write to the ISC specifically to draw to the Committee's attention an area of work it may wish to scrutinise.

25. In common with the practice for departmental select committees, the ISC should be informed of impending Ministerial statements or announcements which are relevant to its current enquiries or general remit in good time. The ISC will also be informed in advance of the appointments of the heads of the Agencies, the Chief of Defence Intelligence and the Chair of the Joint Intelligence Committee (JIC).

26. The ISC will seek to keep HMG informed as to its future work plans, as far as that is possible and reasonable. The ISC, in consultation with the Agencies and Departments, will set reasonable deadlines when it makes requests for information. Where it becomes clear that, exceptionally, HMG is unable to meet a particular deadline set by the ISC for provision of information, then the Agency or Department concerned will notify the ISC and provide a written explanation in advance of the deadline.

Protection and Handling of Sensitive Information

27. The ISC is responsible for ensuring that information disclosed to it is handled in accordance with HMG's document handling, storage and security procedures. The ISC

will be provided with appropriate accommodation and facilities for this purpose and/or the requisite resources.

28. The Act sets out restrictions on the ISC's ability to publish or disclose information (section 3(4) of, and paragraph 6 of Schedule 1 to, the Act). In practice, the ISC and HMG agree that these provisions of the Act will only prevent the ISC publishing or disclosing information if it is information of the kind that it could not include in one of its reports to Parliament.

29. Paragraph 1(3) of Schedule 3 to the Act allows the ISC created by the Act to access documents or other information provided by or belonging to the previous Intelligence and Security Committee (i.e. the Committee established by section 10 of the Intelligence Services Act 1994). The ISC in a new Parliament will inherit the documents, and will be able to continue the ongoing work, of its predecessor in the preceding Parliament (paragraphs 1(6) and (7) of Schedule 1 to the Act). The Committee's staff will continue in post notwithstanding a dissolution of Parliament.

Withholding Information

30. The ISC regularly sees protectively marked material in the course of their work but there may, exceptionally, be circumstances in which it would not be appropriate for the ISC to see particular information, as set out in paragraph 4 of Schedule 1 to the Act. The power to withhold information from the ISC can only be exercised by a Secretary of State (given the ISC's remit this will generally be the Foreign, Home or Defence Secretaries).

31. It is agreed by HMG and the ISC that no decision will be taken to withhold information from the ISC without the ISC being informed of that decision. If the Secretary of State, after considering advice from the Agencies and/or the Departments, decides that there is reason to withhold certain information, the relevant Minister will discuss the matter with the ISC Chair, if requested.

32. The power to withhold information from the ISC under paragraph 4(4)(b) of Schedule 1 is discretionary,[8] and one that it is expected will be required to be exercised very rarely. In exercising this discretion the Secretary of State will have particular regard to the provisions that the ISC has for keeping material confidential. In some cases, having regard to those provisions and other features of the ISC that distinguish it from select committees, the Minister might well consider it appropriate that information be provided to the ISC. For example, the ISC has in the past received information about matters sub judice and/or contained in papers of a previous administration.

[8] In considering whether to withhold information on these grounds the Secretary of State will have regard to any guidance issued by a Minister of the Crown or a Department concerning the provision of evidence by civil servants to Select Committees (paragraph 4(5) of Schedule 1). Currently, this means the Cabinet Office Guide "Departmental Evidence and Response to Select Committees" (July 2005) (sometimes referred to as the "Osmotherly Rules"). The Osmotherly Rules outline the categories of information where it may sometimes be appropriate to decline to provide information to Select Committees. These include information: as to officials' personal views (as distinct from views of Ministers) on policy options; requiring substantial research be carried out by a Department or which could only be supplied at excessive cost; about matters *sub judice*; about the conduct of particular individuals, where the Committee's line of questioning appears to be not just to establish facts but with the implication of allocating individual blame; and contained in papers of a previous administration.

Oral Evidence Sessions: Closed

33. The ISC's evidence sessions are generally with Ministers (Home Secretary, Foreign Secretary) and senior officials (Heads of Agencies, National Security Adviser, Chair of the JIC, Chief of Defence Intelligence, Head of OSCT). This is not an exhaustive list, and the ISC may invite any Minister or senior official to give evidence.

34. During an evidence session, if witnesses consider that answering a question put to them would disclose information that a Minister might consider ought properly to be withheld from the ISC, in accordance with paragraph 4(4) of Schedule 1 to the Act, then the witnesses should state that they will need to take further advice before answering the question. A response must be provided to the ISC in writing as soon as possible after the evidence session (generally within 14 days). This will take the form of a substantive response to the question, or a response setting out the Secretary of State's decision, informing the ISC that they will be exercising the power to withhold the information.

35. The Committee will supply witnesses giving oral evidence with copies of their verbatim transcripts as soon as possible after their appearance (generally within 14 days). This is to enable witnesses to check that the transcript is an accurate record of what they said and, if necessary, provide corrections.

Open Sessions

36. HMG and the ISC are committed to enabling occasional evidence sessions in public on matters agreed by both parties. The nature of the Committee's work and the need for it to consider protectively marked material in carrying out its functions means that the majority of sessions will continue to be held in private. HMG and the ISC will agree adequate safeguards (including on physical security, attendance, and arrangements for broadcast) in advance of each public session. This will allow them to take place without risking disclosure of protectively marked information, while still enabling a substantive hearing. The ISC will provide those giving evidence with an indication of the main issues to be discussed, in keeping with the practice of Parliamentary Select Committees.

Reporting

37. Whilst the Act provides that information must be redacted from a report if the Prime Minister considers its inclusion would be prejudicial to the continued discharge of the functions of the Agencies or of the wider intelligence and security community, HMG will work constructively with the ISC to ensure that as much of its reports that can be published, is published. HMG and the ISC will work together to apply a reasonable process for identifying, in consultation with the ISC, sensitive material that must be removed from ISC reports prior to publication.

38. HMG will aim to respond substantively to any report by the ISC within 60 days.

39. The ISC will provide information on its staffing and budget in its published reports.

ANNEX D: PROPOSED MEMORANDUM OF UNDERSTANDING UNDER THE JUSTICE AND SECURITY ACT 2013

(SHOWING THE CHANGES, IN UNDERLINED ITALICS, REQUIRED TO BRING IT UP TO DATE AND WHICH HAVE BEEN PUT TO THE GOVERNMENT)

Introduction

1. The Justice and Security Act 2013 ("the Act") provides for the oversight of the intelligence and security activities of HM Government (HMG) by the Intelligence and Security Committee of Parliament (ISC).

2. The Act states that any memorandum of understanding (MoU) for the purposes of the Act must be agreed between the Prime Minister and the Intelligence and Security Committee of Parliament. The ISC shall publish the MoU and lay a copy before Parliament (see section 2(6) of the Act).

3. In addition to addressing certain particular matters specified by the Act[1], this MoU also sets out the overarching principles which will govern the relationship between the ISC and those parts of Government it oversees.

The Intelligence and Security Committee of Parliament

4. The ISC is a Committee of Parliament created by statute and comprising members of each House of Parliament.[2] For the purposes of its work, the ISC has *a dedicated independent staff*, known as the Office of the ISC, *headed by the Director*.

5. Parliament appoints the members of the ISC, by vote on a motion of the relevant House. Candidates for membership must first have been nominated by the Prime Minister. The ISC elects its own Chair from amongst the appointed members of the Committee.

6. The ISC makes its reports to Parliament, subject to the requirement that material must be redacted from a report if the Prime Minister considers that its inclusion would prejudice the functions of the Security Service, the Secret Intelligence Service, the Government Communications Headquarters (collectively, "the Agencies") or of other parts of the intelligence and security community. The ISC may also, as appropriate, report to the Prime Minister.

---

[1] The activities of HMG that the ISC shall oversee; the principles governing the ISC's consideration of operational matters; the arrangements by which the Agencies and other government Departments will make information available to the ISC; and the relevant Ministers of the Crown responsible for providing information to the ISC.

[2] The Standing Orders of the House of Commons and House of Lords, which govern the procedures of their Select Committees in general, do not apply to the ISC. The ISC has the power to hear evidence on oath, but it is expected that this will only be used exceptionally.

7. All members of the ISC, and their staff, are notified under the Official Secrets Act 1989 (section 1(1) (b) and 1(6)). They may not, without lawful authority, disclose any information related to security or intelligence which has come into their possession as a result of their work on, or for, the ISC.

Remit

8. The Act provides that the ISC may oversee the expenditure, administration, policy and operations of the Agencies; and that it may examine or otherwise oversee such other activities of HMG in relation to intelligence or security matters as are set out in a memorandum of understanding. The ISC is the only committee of Parliament that has regular access to protectively marked information that is sensitive for national security reasons: this means 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 will not affect the wider scrutiny of *those* departments by other parliamentary committees. The ISC will aim to avoid any unnecessary duplication with the work of those Committees. In addition to the expenditure, administration, policy and (subject to paragraphs 11-17) operations of the Agencies, the ISC and HMG have agreed that the ISC's oversight of intelligence and security matters across Government entails, as at *[date to be added]*:

a. MOD:

   (i) The strategic intelligence activities undertaken by the Chief of Defence Intelligence, including intelligence collection, analysis and training.[3]

   (ii) Offensive cyber.

b. Cabinet Office:

   (i) The activities of the National Security Adviser and National Security Secretariat in relation to matters of intelligence and security. In practice this will include the activities of the Cabinet Office: in providing support to the Prime Minister in his role as Minister with overall responsibility for intelligence and security matters; coordinating intelligence policy issues of strategic importance and public scrutiny of intelligence matters; managing the Single Intelligence Account; and certain activities (relating to matters of intelligence and security) of the Office of Cyber Security and Information Assurance (OCSIA).

   (ii) *The activities of the Investment Security Unit.*

   (iii) The activities of the Joint Intelligence Organisation.

c. Home Office: the activities of *Homeland Security Group*.

d. *Department for Science, Innovation and Technology:*

   (i) *The activities of the Telecoms Security and Resilience Team.*

[3] In respect to operational matters, addressed in paragraphs 11 – 17, general military operations conducted by the MOD are not part of the ISC's oversight responsibilities.

(ii) *The Counter Disinformation Unit.*

e. *Department for Culture, Media and Sport: the activities of the Office of Communications.*

f. *Department for Transport: the activities of the Transport Security, Resilience and Response Group.*

g. *Foreign Commonwealth and Development Office: the activities of the Intelligence Policy Department.*

9. There are a number of other individuals or bodies that oversee intelligence and security matters. For example: the Independent Reviewer of Terrorism Legislation and the *Investigatory Powers Commissioner*. The ISC will continue to have a relationship with those bodies and should cooperate with them so far as is reasonable to avoid any unnecessary duplication in their respective remits.

10. Likewise, the ISC will seek to avoid unnecessary duplication with the work of courts or tribunals (such as the Investigatory Powers Tribunal) which may, from time to time, have cases before them concerned with intelligence and security matters.

Oversight of Operational Matters

11. The ISC may consider or otherwise oversee the operational activities[4] of the Agencies and the specified activities of other Government Departments referred to in paragraph 8 above ("the Departments"). The ISC may consider particular operational matters in three sets of circumstances:

a) Where the ISC and the Prime Minister are satisfied that the matter is not part of any ongoing intelligence or security operation and is of significant national interest and the consideration of the matter is consistent with any principles set out in, or with any other provision made by, the MoU (see section 2(3)(a) and 2(4) of the Act); or

b) Where the Prime Minister has asked the ISC to consider the matter and the consideration of the matter is consistent with any principles set out in, or with any other provision made by, the MoU (see section 2(3)(b) and 2(4) of the Act); or

c) Where consideration of an operational matter is not covered by (a) or (b) above, but information is nevertheless provided voluntarily to the ISC by the Agencies or a Department, whether or not in response to a request by the ISC (see section 2(3)(c) of the Act).

Further detail regarding the ISC's oversight of operational matters in these circumstances is set out below.

[4] Certain long-running 'operations' may be considered within the ISC's remit, for example, where the entire intelligence gathering effort for a particular country is undertaken for long periods under the guise of a single operational code word.

12. The ISC recognises the sensitivity of intelligence and security operations. Its role overseeing such operational activity will therefore be governed by the following overarching principles:

a) this work must not jeopardise the success of an operation or compromise the security and safety of those involved; and

b) the ISC's examination of an operational matter must not unduly impede the operational effectiveness of an Agency or Department.

13. Where there are legal proceedings (criminal or civil), inquiries[5] or inquest proceedings, the ISC and HMG will consider carefully whether it is appropriate to proceed with an investigation.

14. Under section 2(3)(a) of the Act, the ISC's power to oversee operational activity is retrospective and on matters of significant national interest. When considering whether an activity ' is not part of any ongoing intelligence or security operation', the ISC and the Prime Minister will take into account:

a) Whether the main objectives of the particular operation have been achieved or whether there is now no reasonable prospect of further operational activity to seek to achieve the main objectives in the near future

b) That the operational activity of the Agencies and Departments can vary greatly in scope, type and magnitude and in some cases it may not be clear when a particular operation has ended. Deciding whether a matter is or is not part of 'any ongoing intelligence or security operation' will be a matter of judgement for the Prime Minister and the ISC

c) When two or more operational activities may be separated in time but closely linked in objective, the ISC will be entitled to have retrospective oversight of such operations that have been completed, unless such oversight would jeopardise the success of such future operations; and

d) The ISC and HMG are agreed that the operational activity or event in question will only be regarded as 'of significant national interest' if it raises issues of wider significance or raises serious questions relating to Agency or Departmental conduct, competence, resourcing and policy in the operational context, including in situations where there is, or is likely to be, significant parliamentary or public interest in relation to such issues or questions.

15. The Prime Minister will nominate the National Security Adviser and his deputy for intelligence matters to consider, on his behalf, whether the conditions for such oversight are met. The final decision will rest with the Prime Minister, in conjunction with the ISC.

16. Under section 2(3)(b) of the Act, the Prime Minister may, at his discretion, consider it appropriate to invite the ISC to consider an operational matter which falls outside the 'retrospective' and 'significant national interest' criteria.

---

[5] Including statutory inquiries or other independent judge-led inquiries.

17. Under section 2(3)(e) of the Act, the ISC may consider operational matters not covered by sections 2(3)(a) or 2(3)(b) where information is provided voluntarily to the ISC by the Agencies or a Department, whether or not in response to a request by the ISC.

Provision of Information

18. The ISC requires information from HMG in order to carry out its oversight function. The importance of the ISC's oversight role is recognised by the fact that, while officials and Ministers are able to provide information to the ISC, only a Secretary of State has the power to withhold it. This is reflected in paragraph 4 of Schedule 1 to the Act.

19. The duty to provide information to the ISC rests, for the Departments, with the relevant Minister of the Crown (this may, but need not necessarily, be a Secretary of State)[6] and for the Agencies, with the Heads of the Agencies.

20. In practice there will be a range of methods which the ISC may use in order to obtain the information it requires from HMG, including:

a) Oral evidence sessions with Ministers, Agency Heads and other senior officials. These sessions allow the ISC to ask detailed questions about particular issues within their remit, but also to get a broader sense of the issues that Agencies, Departments and Ministers are facing and to decide whether any particular issue might need further scrutiny;

b) Written material, both regular briefs on agreed lines of reporting and responses to specific questions. HMO and the Agencies will keep the ISC fully and promptly informed of any significant matters falling within the ISC's remit;

c) Members of the ISC's staff working with the Agencies and the Departments to obtain Information on the ISC's behalf, ensuring that the ISC has all the information it needs to do its job in relation to matters consistent with its remit.

21. The responsibility for ensuring the ISC has access to relevant information consistent with its remit will fall to the appropriate Agency or Department, who will make available the information the ISC needs. The ISC will work together with the Agencies and Departments to ensure that the provision of such information does not involve disproportionate cost or diversion of effort.

22. The Committee may seek confirmation from HMG of the factual accuracy or completeness of information it has gathered before drawing on it in its reports.

---

[6] For the following Departments, the relevant Ministers of the Crown, for the purposes of making information available to the ISC (paragraphs 4(3) and 4(7) of Schedule (I) are as follows:

a. Cabinet Office: Any Minister of the Crown in a relevant Government department;
b. MOD: Secretary of State for Defence;
c. Home Office: Secretary of State for the Home Department;
d. *Foreign Commonwealth and Development Office: Secretary of State for Foreign, Commonwealth and Development Affairs;*
e. *DSIT: Secretary of State for Science, Innovation and Technology;*
f. *DCMS: Secretary of State for Culture, Media and Sport; and*
g. *Department for Transport: Secretary of State for Transport.*

23. Committee members may, as part of their work, undertake visits to the Agencies and Departments that the ISC oversees, to familiarise themselves with the broader context of their work. Information provided to Committee members in the course of such visits will not constitute formal evidence gathering unless it is agreed as such by both parties either in advance or retrospectively.

24. On occasion the Prime Minister may write to the ISC specifically to draw to the Committee's attention an area of work it may wish to scrutinise.

25. In common with the practice for departmental select committees, the ISC should be informed of impending Ministerial statements or announcements which are relevant to its current enquiries or general remit in good time. The ISC will also be informed in advance of the appointments of the heads of the Agencies, the Chief of Defence Intelligence and the Chair of the Joint Intelligence Committee (JIC).

26. The ISC will seek to keep HMG informed as to its future work plans, as far as that is possible and reasonable. The ISC, in consultation with the Agencies and Departments, will set reasonable deadlines when it makes requests for information. Where it becomes clear that, exceptionally, HMG is unable to meet a particular deadline set by the ISC for provision of information, then the Agency or Department concerned will notify the ISC and provide a written explanation in advance of the deadline.

Protection and Handling of Sensitive Information

27. The ISC is responsible for ensuring that information disclosed to it is handled in accordance with HMG's document handling, storage and security procedures. The ISC will be provided with appropriate accommodation and facilities for this purpose and/or the requisite resources.

28. The Act sets out restrictions on the ISC's ability to publish or disclose information (section 3(4) of, and paragraph 6 of Schedule 1 to, the Act). In practice, the ISC and HMG agree that these provisions of the Act will only prevent the ISC publishing or disclosing information if it is information of the kind that it could not include in one of its reports to Parliament.

29. Paragraph I (3) of Schedule 3 to the Act allows the ISC created by the Act to access documents or other information provided by or belonging to the previous Intelligence and Security Committee (i.e. the Committee established by section 10 of the Intelligence Services Act 1994). The ISC in a new Parliament will inherit the documents, and will be able to continue the ongoing work, of its predecessor in the preceding Parliament (paragraphs 1 (6) and (7) of Schedule I to the Act). The Committee's staff will continue in post notwithstanding a dissolution of Parliament.

Withholding Information

30. The ISC regularly sees protectively marked material in the course of their work but there may, exceptionally, be circumstances in which it would not be appropriate for the ISC to see particular information, as set out in paragraph 4 of Schedule I to the Act. The power to withhold information from the ISC can only be exercised by a Secretary of State (given the ISC's remit this will generally be the Foreign, Home or Defence Secretaries).

31. It is agreed by HMG and the ISC that no decision will be taken to withhold information from the ISC without the ISC being informed of that decision. If the Secretary of State, after considering advice from the Agencies and/or the Departments, decides that there is reason to withhold certain information, the relevant Minister will discuss the matter with the ISC Chair, if requested.

32. The power to withhold information from the ISC under paragraph 4(4)(b) of Schedule 1 is discretionary[7], and one that it is expected will be required to be exercised very rarely. In exercising this discretion the Secretary of State will have particular regard to the provisions that the ISC has for keeping material confidential. In some cases, having regard to those provisions and other features of the ISC that distinguish it from select committees, the Minister might well consider it appropriate that information be provided to the ISC. For example, the ISC has in the past received information about matters *sub judice* and/or contained in papers of a previous administration.

Oral Evidence Sessions: Closed

33. The ISC's evidence sessions are generally with Ministers (Home Secretary, Foreign Secretary) and senior officials (Heads of Agencies, National Security Adviser, Chair of the JIC, Chief of Defence Intelligence, Head of *HSG*). This is not an exhaustive list, and the ISC may invite any Minister or senior official to give evidence.

34. During an evidence session, if witnesses consider that answering a question put to them would disclose information that a Minister might consider ought properly to be withheld from the ISC, in accordance with paragraph 4(4) of Schedule 1 to the Act, then the witnesses should state that they will need to take further advice before answering the question. A response must be provided to the ISC in writing as soon as possible after the evidence session (generally within 14 days). This will take the form of a substantive response to the question, or a response setting out the Secretary of State's decision, informing the ISC that they will be exercising the power to withhold the information.

35. The Committee will supply witnesses giving oral evidence with copies of their verbatim transcripts as soon as possible after their appearance (generally within 14 days). This is to enable witnesses to check that the transcript is an accurate record of what they said and, if necessary, provide corrections.

Open Sessions

36. HMG and the ISC are committed to enabling occasional evidence sessions in public on matters agreed by both parties. The nature of the Committee's work and the need for it to consider protectively marked material in carrying out its functions means that the majority of

[7] In considering whether to withhold information on these grounds the Secretary of State will have regard to any guidance issued by a Minister of the Crown or a Department concerning the provision of evidence by civil servants to Select Committees (paragraph 4(5) of Schedule I). Currently, this means the Cabinet Office Guide "Departmental Evidence and Response to Select Committees" (July 2005) (sometimes referred to as the "Osmotherly Rules"). The Osmotherly Rules outline the categories of information where it may sometimes be appropriate to decline to provide information to Select Committees. These include information: as to officials' personal views (as distinct from views of Ministers) on policy options; requiring substantial research be carried out by a Department or which could only be supplied at excessive cost; about matters *sub judice;* about the conduct of particular individuals, where the Committee's line of questioning appears to be not just to establish facts but with the implication of allocating individual blame; and contained in papers of a previous administration.

sessions will continue to be held in private. HMG and the ISC will agree adequate safeguards (including on physical security, attendance, and arrangements for broadcast) in advance of each public session. This will allow them to take place without risking disclosure of protectively marked information, while still enabling a substantive hearing. The ISC will provide those giving evidence with an indication of the main issues to be discussed, in keeping with the practice of Parliamentary Select Committees.

Reporting

37. Whilst the Act provides that information must be redacted from a report if the Prime Minister considers its inclusion would be prejudicial to the continued discharge of the functions of the Agencies or of the wider intelligence and security community, HMG will work constructively with the ISC to ensure that as much of its reports that can be published, is published. HMG and the ISC will work together to apply a reasonable process for identifying, in consultation with the ISC, sensitive material that must be removed from ISC reports prior to publication.

38. HMG will aim to respond substantively to any report by the ISC within 60 days.

39. The ISC will provide information on its staffing and budget in its published reports.

ANNEX E: INQUIRY DEADLINES

The following table covers only those Inquiry deadlines occurring since the new system was agreed on 20 December 2022.

Inquiry	Commission	Deadline
China	Contested redaction requests	(a) Six of the seven organisations met the set deadline. (b) An extension was requested by one organisation. The Committee agreed that the rationale provided was reasonable and granted the extension. The revised deadline was met.

E02988480
978-1-5286-4463-1