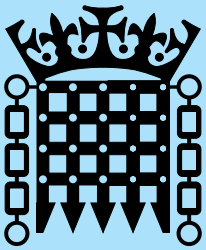

Intelligence and Security Committee of Parliament

Annual Report 2021–2022

Chairman:
The Rt Hon. Dr Julian Lewis MP

HC 922

Intelligence and Security Committee of Parliament

Annual Report 2021–2022

Chairman:
The Rt Hon. Dr 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 13 December 2022

HC 922

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 978-1-5286-3758-9

E02813160 12/2022

Printed on paper containing 40% recycled fibre content minimum

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

THE INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT

The Rt Hon. Dr Julian Lewis MP (Chairman)

Maria Eagle MP
(from 9 February 2022)

The Rt Hon. Sir John Hayes CBE MP

The Rt Hon. Stewart Hosie MP

The Rt Hon. Dame Diana Johnson DBE MP
(until 14 January 2022)

The Rt Hon. Kevan Jones MP

The Rt Hon. Mark Pritchard MP
(until 27 January 2022)

Colonel The Rt Hon. Bob Stewart DSO MP

The Rt Hon. Theresa Villiers MP

Admiral The Rt Hon. Lord West of Spithead GCB DSC PC

The Rt Hon. Sir Jeremy Wright KC MP
(from 9 February 2022)

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

---

[*] Throughout the report, the term 'Intelligence Community' is used to refer to the seven organisations that the Committee oversees. The term 'Agencies' (or, on occasion, 'the intelligence Agencies') refers to MI5, SIS and GCHQ as a collective; and the term 'Departments' refers to the intelligence and security parts of the Ministry of Defence, Cabinet Office and the Home Office (DI, JIO, National Security Advisor (NSA), NSS and Homeland Security Group) as a collective, unless specified otherwise.

[†] From 1 April 2021, the Home Office moved to a new structure "*based around missions and capabilities*". Homeland Security Group (one of the new missions) comprises what was formally known as the Office for Security and Counter-Terrorism, along with three departments from Serious Organised Crime Group (Economic Crime, Cyber Policy and the Serious Organised Crime Capability team).

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

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

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

CONTENTS

THE WORK OF THE COMMITTEE

1. This Report summarises the work of the Intelligence and Security Committee of Parliament (ISC) for the period August 2021 to March 2022 in carrying out its oversight of the Intelligence Community.[1]

Membership during the period covered by this Report

2. On 14 and 27 January 2022 respectively, the Rt Hon. Dame Diana Johnson DBE MP and the Rt Hon. Mark Pritchard MP notified the Chairman of their intent to step down from their roles on the Committee. Following a consultation process, as set out in the Justice and Security Act 2013, Maria Eagle MP and the Rt Hon. Sir Jeremy Wright KC MP were nominated for membership of the Committee by the Prime Minister, and were appointed as members of the Committee by the House of Commons on 9 February 2022.

Work programme

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

- held 13 full Committee meetings, including evidence sessions with Government Ministers, senior officials from across the Intelligence Community, and external experts;
- conducted one visit to the Intelligence Community;
- held bilateral discussions with counterparts from the Parliament of Australia and United States Congress; and
- held three other meetings.

Reports

4. The Committee published its Annual Report 2019–21 on 10 December 2021. It covered a longer period than usual (due to the Intelligence Community having missed the deadline for the 2019–2020 Report), summarising the work of the Committee from July 2019 to July 2021. This included the publication of five Reports and three statements, and contributions to three pieces of legislation. The Annual Report 2019–2021 also addressed the serious concerns the Committee had around the behaviour of senior staff within the Intelligence Community and of some senior staff once they left post, and outlined the changes required to the Committee's Memorandum of Understanding to ensure that intelligence and security activity across Government does not evade scrutiny.

[1] This Annual Report covers a shorter period than usual as delays to the Committee's Annual Report last year meant that Report covered an extended period.

Statements

5. In July 2020, the Committee published its *Russia* Report, in which it made clear that the UK had been welcoming Russian money for many years with few questions – if any – being asked about the provenance of this considerable wealth. The Committee highlighted the urgent need for the UK Government to disrupt this illicit financial activity, questioning the efficacy of the existing measures.

6. On 14 March 2022, the Economic Crime (Transparency and Enforcement) Act received Royal Assent. The next day, the Committee issued a statement making clear its support for the legislation, which is the first step towards addressing its concerns. The Committee considers, however, that in order to give the authorities – and in particular the National Crime Agency which leads on this effort – the necessary clout and greater powers required to ensure the UK is no longer a safe haven for the oligarchs and their enablers, the legislation will need to be accompanied by the appropriate financial support.

Legislation

7. During the period covered by this Report, there have been four pieces of legislation before Parliament to which the Intelligence and Security Committee has contributed collectively:

(i) The Telecommunications (Security) Act 2021 received Royal Assent on 17 November 2021. This legislation establishes a new telecommunications security framework, giving HMG new powers to regulate and issue codes of practice, including limiting or removing high-risk vendors (such as Huawei) from the UK telecommunications network, assigning responsibilities to Ofcom, and introducing new penalties for non-compliance.

As with the National Security and Investment (NSI) Act 2021 (on which we commented in our 2019–2021 Annual Report), the Committee is supportive of the principle behind the Act, but is concerned about the lack of parliamentary oversight of those aspects of the legislation that cannot be effectively scrutinised by Select Committees due to the classification of the material (in this case, the Digital, Culture, Media and Sport (DCMS) Select Committee would be responsible for oversight of any actions taken by the Secretary of State under the powers granted by this Act). This 'oversight gap' is addressed in more detail later in this Report.

(ii) The Economic Crime (Transparency and Enforcement) Act 2022 received Royal Assent on 15 March 2022. This is a vital piece of legislation and – as noted previously – will go some of the way to addressing the recommendations included in the Committee's *Russia* Report. The Act – which had the Committee's full support – was expedited through Parliament, having been introduced following Russia's invasion of Ukraine. The legislation will allow the Government to move more quickly to impose sanctions against oligarchs already designated by allied countries.

(iii) The Online Safety Bill was introduced in Parliament on 17 March 2022, following the Draft Online Safety Bill (Joint Committee) report in December 2021. The Bill will regulate online content by imposing a regulatory framework for internet firms to tackle harmful content, which will be overseen by Ofcom.

The Committee had highlighted in its *Russia* Report the potential threat to elections and democracy from foreign interference online – agreeing with the DCMS Select Committee that "*the UK is clearly vulnerable to covert digital influence campaigns*".[2] It is too soon to tell whether organised hostile state action, such as the spreading of disinformation without an explicit incitement to violence, will be adequately addressed by this legislation.

(iv) The Election Bill was introduced in Parliament on 5 July 2021 and at the time of writing is in the Committee Stage in the House of Lords, which began on 10 March 2022. The Bill aims to increase the transparency and security of elections, including restrictions on how foreign third-party campaigners raise funding for elections. Such restrictions were identified by the Committee in its *Russia* Report, which has been referenced throughout the passage of the Bill in Parliament.

8. As at March 2022, legislation was still awaited to reform the Official Secrets Acts – which the Home Secretary, in evidence before this Committee in 2019, had described as "*completely out of date.*"[3] Legislation is also still awaited on an equivalent to the US Foreign Agents Registration Act, which requires anyone other than accredited diplomats – including both US and non-US citizens – who represents the interests of "*foreign principals who are engaged in political activities*"[4] in a political capacity to register with the Department of Justice, disclosing their relationship with the foreign government.

Areas of inquiry

Extreme Right-Wing Terrorism

9. In October 2019, the Committee began an Inquiry into the threat from 'Right-Wing Terrorism' (subsequently renamed 'Extreme Right-Wing Terrorism', or ERWT), 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. ERWT is now therefore assessed alongside the Islamist terror threat, and it forms part of the overall UK Threat Level assessment. 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.

10. The Committee completed its Report on 26 July 2021, and all the factual checks and redaction stages had been completed by 5 January 2022. However, while the Report was being prepared for publication, there was an exceptional breach of procedure as the Committee received additional requests for redactions from the Intelligence Community which had been missed during the redaction process itself. The Committee was concerned that the Intelligence Community had failed to identify sensitive intelligence material through the established processes, and therefore risked such information being published. We also note that, as a result, the Prime Minister was wrongly advised by the Intelligence Community that the material in the version of the Report that he reviewed would not prejudice the discharge of the functions of the Agencies. As a result of these last-minute delays, as at the time of writing

[2] DCMS Select Committee, *Disinformation and 'Fake News'*, HC1791, 18 February 2019.
[3] Oral evidence – Home Secretary, 31 January 2019.
[4] The US Department of Justice website, Foreign Agents Registration Act, justice.gov/nsd-fara

this Report, the Extreme Right-Wing Terrorism Report is still awaiting publication – although it is hoped that it can be laid before Parliament shortly.

11. Turning to the substance of our Inquiry, the Committee found that the number of ERWT investigations, disruptions and Prevent referrals have all increased steadily since 2017. Of the 25 attacks prevented by the Intelligence Community and CTP between March 2017 and January 2020, eight (just under 30% of the total) were motivated by an ERWT ideology. In terms of where the threat is coming from, the Committee found that there has clearly been a shift in the age, demographic and backgrounds of those associated with ERWT. The new ERWT threat is fragmented and complex, increasingly driven by the internet and characterised by a technologically aware demographic of predominantly young men, many of them still in their teens, who are typically 'Self-Initiated Terrorists'. Crucially, few of these individuals belong to organised groups, and they are difficult to identify and monitor. Their motivation can be highly individualistic, according to their particular personal circumstances, the nature of their grievances and perceptions of their own capabilities – determining how, why and when they may choose to attack is therefore particularly challenging.

12. Extreme Right-Wing Terrorists often display an interest in military culture, weaponry and the Armed Forces or law enforcement organisations. Individuals often seek to join the military, and groups seek to recruit within the military (military experience remains a source of legitimacy among EWRT groups). The fact that the Armed Forces do not provide clear direction to service personnel regarding the membership of any organisation, let alone an extremist one, would therefore appear to be something of an anomaly: it appears a somewhat risky approach, given the sensitive roles of many service personnel. There is a similar risk from the insider threat in relation to the police – brought into sharp focus in April 2021 when a Metropolitan Police Officer was convicted of membership of National Action. This case highlighted issues around the current vetting processes for candidates applying to join the police – the lack of thorough background checks is a particular concern.

13. In terms of drivers, it is clear that the online space is key. Historically, a journey into ERWT entailed real-world contact with organised groups and individuals in-person: the internet has removed these barriers. Self-Initiated Terrorists are now radicalised, and can radicalise others, online from the seclusion of their bedrooms. Online content such as videos of terrorist attacks, manifestos, propaganda and ideological literature can all be found on a variety of platforms and at different levels of encryption – progressing from mainstream social media sites through to fringe networking sites, gaming sites, dedicated extremist websites and Secure Messaging Applications. Potential recruits can be channelled into 'echo chambers' isolated from opposing viewpoints – although not everyone will be guided through the system by a recruiter. Some find their own way through to the more extreme material.

14. The Home Office is still developing its understanding of the volume of ERWT material online and which categories are most widely accessed. It appears to be more difficult to tackle than Islamist terrorism propaganda, perhaps because of the wider lack of understanding of the ERWT threat, and concerns regarding freedom of speech (particularly in the US, where material on US-owned platforms can go unchallenged owing to the US Constitution's First Amendment). There is also the particular challenge of determining whether Extreme Right-Wing activity online might translate into 'real world' terrorist activity. It is clear that the ERWT online environment poses a new challenge for the Intelligence Community and there is a long way to go when it comes to tackling what is largely an ungoverned space.

15. The Committee found that a further key factor – given that Extreme Right-Wing Terrorists tend to be tech-savvy, and their conspiracy-theorist, anti-government outlook tends to reinforce the idea that their internet use is being monitored – is that they tend to use encrypted platforms, Virtual Private Networks (VPNs) and 'dark net' sites. In this respect, as the Head of CTP put it, "*end-to-end encryption is a disaster*".[5] MI5 has called on Communications Service Providers (CSPs) to allow the Agencies to have exceptional access to encrypted messaging.

16. However, what is more fundamental perhaps is that the CSPs – the companies that host these platforms – must ensure that this material cannot be viewed and shared in the first place. The Committee first identified this problem in 2014, but little progress appears to have been made since. While the major CSPs may be finally taking steps (Facebook reports removing 8.7 million pieces of terrorist content over a three-month period), the smaller organisations – many of which are particularly influential in the ERWT space – appear reluctant to step up. The Online Safety Bill will provide sweeping new powers for Ofcom, but we are concerned as to whether Ofcom has the capability to exercise this ambitious new remit.

17. The UK is not alone in facing these challenges: technology and ease of communication means that ERWT is a threat without borders, and in most cases without affiliation. International co-operation is therefore important in tackling ERWT, although the disparity in approach and legal thresholds for defining the threat makes this challenging. It is therefore encouraging that the strong operational relationships built up over the years by the Intelligence Community and police with their European counterparts continue in the post-Brexit era – although it is important to ensure that alternative arrangements are put in place to avoid potential loss of access to some key capabilities.

18. During the Inquiry, the Committee found that the ERWT threat was on an upward trajectory. The ERWT space is now populated by an increasing number of young people – a significant percentage of MI5's Subjects of Interest (SOIs) are under 24. There are reports that groups and individuals have sought to co-opt the Covid-19 pandemic using conspiracy theories and exploiting grievances to radicalise and recruit. While the full impact of the global pandemic has yet to be seen, we are assured that the Intelligence Community and the police have recognised the impact that events such as the pandemic and Black Lives Matter protests may have had on the extremist lives of individuals and the possibility that this will lead to an increase in the threat. We were therefore seriously concerned to find that MI5 have had to absorb responsibility for tackling ERWT without any commensurate resources. ERWT and Left-wing, Anarchist and Single-Issue Terrorism (LASIT) 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. MI5 must be given additional funding to enable it to tackle ERWT without other areas of its work suffering as a consequence.

[5] Oral evidence – CTP, 29 April 2021.

International partnerships

19. The Committee began an Inquiry into international partnerships in October 2019. Since November 2021, the completed Report has been going through the factual checks and redaction processes.

China

20. In 2019, the Committee began taking evidence in connection with its Inquiry into national security issues relating to China. The Committee published a Statement in relation to the first of its workstrands – the UK Telecommunications Sector – in July 2019. Once the Committee was reconstituted in July 2020, it resumed taking evidence on the remaining workstrands. Progress on this Inquiry has been disrupted by the national lockdowns due to the Covid-19 pandemic, and the excessive delay in reconstituting the Committee after the December 2019 election.

Cloud technologies

21. In May 2021, the Committee commenced an Inquiry into cloud technologies, and is currently in the process of taking evidence. The Committee has been supported in this Inquiry by the National Audit Office, and we wish to express our thanks to the Comptroller and Auditor General and his team for their excellent work.

Iran

22. In November 2021, the Committee announced that it will be undertaking an Inquiry into national security issues relating to Iran. The initial evidence provided was insufficient: despite a full response being requested, as at the end of March 2022 this has still not been received.

Other areas

23. 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. In November 2021, the Committee requested further information on the Intelligence Community's role in the UK's withdrawal from Afghanistan.

24. 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 2020/21 financial year. The threat assessment is summarised in Annex A, and the key facts and major developments for each organisation in 2020/21 are summarised in Annex B.

OTHER ISSUES

The provision of evidence

25. The Committee has been severely hampered over the past year by the failure of the UK Intelligence Community to meet standard deadlines as part of the ISC Inquiry process. In the Committee's Annual Report 2019–2021, we attributed this to their reduced resources during the pandemic and their need to focus on immediate national security threats. However, this is no longer a credible explanation.

26. This is a very serious issue, as it prevents the Committee from effectively performing its statutory oversight role. Moreover, as the National Security Adviser said, "*the Intelligence Community's licence to operate is dependent on credible oversight*".[6] The Agencies were granted increased powers under the Justice and Security Act 2013 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 being 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.** Despite numerous complaints, the situation has not improved and, if anything, has got worse. The Committee has called on the Heads of the seven organisations it oversees to account for these failures, and to provide assurances on a suitable way forward.

Increased media presence

27. The Committee has noted that the Heads of the intelligence Agencies are increasingly making appearances in the media, with a far higher profile than their predecessors. Recent examples of this include the Director-General MI5's interview in the *Daily Mail* newspaper about his career, the Director GCHQ's interview and podcast features in *The Times*, and the Chief of SIS's Twitter account. While the majority of media is undertaken by the heads of the organisations, there have also been anonymised interviews with more junior staff. For example, The *Daily Telegraph* published an interview with MI5's Director K, and the *Sunday Times* featured interviews with a number of junior GCHQ staff. This is a clear step-change for the Agencies, who have traditionally shied away from such exposure – particularly of junior staff.

28. While the Committee recognises the important role public outreach can play in attracting employees by opening up about the culture and working practices in such secret organisations, it must be undertaken in a strategic and considered manner. The Committee is concerned that, if media engagement strategies go too far, they risk trivialising the important work of the Agencies and diverting their focus from national security priorities. Social media is also known to be a battleground for covert hostile state action, so any enhanced media engagement should not undermine the Agencies' ability to act covertly and keep the UK safe.

[6] *Letter to Chairman – National Security Adviser, 23 February 2022.*

Meeting with the Prime Minister

29. 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. In the previous Annual Report, we stated that we would seek a meeting with the Prime Minister this year; unfortunately, despite requests for suitable dates, we are yet to receive a response from the Prime Minister. The Committee urges the Prime Minister to meet with it as a priority.

Committee resources

30. As set out in our Annual Report 2019–2021, the Committee's budget was – exceptionally – reduced in the 2019/20 financial year, but assurances had been received that the full budget would be reinstated in the 2020/21 financial year. Unfortunately, the Committee's budget remained at the reduced level of £1,328,000 – which was insufficient to operate at a fully staffed level.

31. At the beginning of the 2021/22 financial year, the Committee once again received only a partial allocation – insufficient to cover the full staffing and administrative running costs for the Committee and its Office (unlike in the case of Select Committees of the House of Commons, the Chairman receives no salary). After representations were made, this was eventually increased to £1,550,000. However, this still did not include sufficient funding to operate at a fully staffed level, and the Committee also forwent any overseas travel in order to reduce costs. The Committee is assured that, for the 2022/23 financial year, it will receive the full budget of £1,834,000.

Proposed changes to the Memorandum of Understanding

32. In the Committee's Annual Report 2019-2021, we highlighted that the current Memorandum of Understanding (MoU) between the Prime Minister and the Committee is out of date and requires updating. The Government had given a clear undertaking to Parliament during the passage of the Justice and Security Act 2013 when the then Security Minister – who was leading the Bill – 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"*. The Security Minister also 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."*[7]

33. However, as intelligence and security activities are increasingly being devolved to policy departments – under what was the Fusion Doctrine and is now referred to as the framework of the UK Integrated Review – those departments are not being added to this Committee's MoU, as expected, and therefore oversight is being eroded. During the passage of the National Security and Investment (NSI) Bill, the Committee sought assurances about the oversight of the Investment Security Unit (ISU) which the legislation would create in the Department

[7] Justice and Security Bill [HL]. (19 July 2012). [Hansard]. (Volume 738). parliament.uk/Lords/2020-07-09/debates

for Business, Energy and Industrial Strategy (BEIS). We were informed that, despite the Unit relying on classified information, oversight would 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.

34. The issue of the Committee's statutory remit has been raised with the National Security Adviser on a number of occasions, both in correspondence and in meetings. In January 2022, the National Security Adviser met the Chairman of the Committee and relayed the Government's latest position – which is that they do 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.

35. We are deeply disappointed and concerned that the Government has taken this view, and is therefore actively avoiding the effective scrutiny by Parliament of national security issues across Government. **The absence of proper scrutiny, which can only be carried out by the ISC, is genuinely troubling.**

36. Select Committees are not equipped to handle classified material, and therefore when the Government informs the Committee that a classified topic falls within the remit of those Committees, it is clear that this topic will not be subject to effective oversight. This is of course no reflection on the ability of Select Committees to provide effective oversight on all other matters.

37. **The only avenue for effective parliamentary oversight of security and intelligence matters is this Committee. Each piece of new legislation devolving such matters away from the bodies already overseen by this Committee should therefore come with a commensurate expansion to this Committee's MoU.**

38. In our 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. The changes which the Committee considers must be made are shown in the proposed MoU (as first published in our Annual Report 2019–2021), at Annex D.

LIST OF WITNESSES

Officials

CABINET OFFICE

Sir Stephen Lovegrove KCB – National Security Adviser

Sir Simon Gass KCMG CVO – Chair, Joint Intelligence Committee

Other officials

MINISTRY OF DEFENCE (MoD)

Lieutenant General Sir Jim Hockenhull KBE – then Chief of Defence Intelligence

Other officials

SECRET INTELLIGENCE SERVICE (SIS)

Officials

SECURITY SERVICE (MI5)

Officials

NATIONAL AUDIT OFFICE (NAO)

Gareth Davies – Comptroller and Auditor General

Other officials

Expert external witnesses

David Ferbrache – Chief Technology Officer, Cyber, KPMG UK

Dr Wai Kuan Hon – Counsel, Dentons law firm

ANNEX A: THREAT ASSESSMENT

The threat to the UK and its interests overseas comes from a number of different sources, as outlined in previous Annual Reports, including Islamist terrorism, Extreme Right-Wing Terrorism (ERWT), Left-wing, Anarchist and Single-Issue Terrorism (LASIT) and Northern Ireland-related terrorism (NIRT), 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 August 2021 to 31 March 2022.

The threat picture

The UK National Threat Level[8] is currently 'SUBSTANTIAL: an attack is likely'. Within this reporting period, the UK National Threat Level was raised on 15 November 2021 from SUBSTANTIAL to 'SEVERE: an attack is highly likely', following two terrorist attacks in quick succession. On 9 February 2022, the UK National Threat Level was lowered to 'SUBSTANTIAL: an attack is likely', reflecting the assessment that, despite these attacks, the nature and scale of the UK terrorist threat was consistent with a 'SUBSTANTIAL' Threat Level.

The UK continues to face a high level of terrorist threat, from increasingly diverse ideological influences. There were two UK terrorist attacks during this period: the Islamist terrorist-inspired murder of Sir David Amess MP in October 2021 by Ali Harbi Ali, which was the first UK terrorist attack since the attack at Forbury Gardens, Reading, in June 2020, and an explosion outside Liverpool Women's Hospital in November 2021 (where the ideological motivation for this attack remains unclear). These attacks continue to reflect the complex, volatile and unpredictable nature of the terrorist threat in the UK.

In the UK, the primary terrorist threat continues to be from UK-based, self-initiated Islamist terrorists or small groups, 'inspired' to conduct attacks following radicalisation from Islamist extremist propaganda, often accessed online. Extremist ideologies are increasingly diverse, reflecting the expanding reach and range of radicalising narratives online, consumed by a broadening demographic. Terrorist attacks are increasingly likely to be characterised by rapid escalation to violence and low-sophistication methodologies, such as the use of bladed weapons and vehicles.

Overseas, there remains an enduring threat from Al-Qaeda, Islamic State in Iraq and the Levant (ISIL) and their affiliates, who aspire to direct attacks against the UK and its interests overseas. Al-Qaeda and ISIL have exploited unstable conditions in failed or failing states to grow their networks via affiliate branches; they now operate in more theatres of conflict than ever before. The majority of jihadist violence overseas is focused on sustaining insurgent efforts against 'near enemy' regimes and their Western partners locally. The present threat from Al-Qaeda and ISIL is primarily manifest against UK and Western interests overseas rather than in Western countries themselves. But external

[8] The Joint Terrorism Analysis Centre (JTAC) is responsible for the UK National Threat Level; which incorporates the threat from Islamist terrorism, Extreme Right-Wing Terrorism (ERWT), Left-wing, Anarchist and Single-Issue Terrorism (LASIT) in the UK, and Northern Ireland-related terrorism (NIRT) in mainland Great Britain. MI5 is responsible for setting the threat level from NIRT in Northern Ireland. There are five tiers to the threat level system: CRITICAL (an attack is highly likely in the near future); SEVERE (an attack is highly likely); SUBSTANTIAL (an attack is likely); MODERATE (an attack is possible but not likely); and LOW (an attack is unlikely).

operations against the West still have a role in Al-Qaeda's and ISIL's long-term strategies – even if they arise from more diverse sources. As leadership attrition has made centrally controlled plots against the West harder, Al-Qaeda and ISIL have encouraged and enabled more opportunistic threats from their supporters.

Separately, there is a persistent threat from ERWT in the UK and, to a lesser extent, LASIT. ERWT ideologies are becoming increasingly indistinct and blended with other ideological beliefs, as individuals form and pursue their own grievance narratives, independent from organised groupings or other clear influences. The threat posed by these widening avenues to radicalisation is further exacerbated by the ease with which extremist narratives, violent content and instructional material (including for the creation of homemade explosives and 3D printed firearms) can be found online. This extremist propaganda is finding its way to individuals with complex needs, including minors, and those with mental ill-health, and urging them to contemplate violent acts. It continues to be most likely that an Islamist terrorist, ERWT or LASIT attack would emanate from Self-Initiated Terrorists radicalised online, who plan and conduct attacks independently of any formal association with a wider terrorist group.

NIRT

In March 2022, the threat level in Northern Ireland (NI) from dissident republican (DR) groups was lowered from 'SEVERE: an attack is highly likely' to 'SUBSTANTIAL: an attack is likely'. The level of threat is now broadly stable after several years of gradual decline; constant security force pressure will be required to keep the threat suppressed at this level.

DR and loyalist paramilitary groups remain a feature of life in NI. The most serious threat in NI remains that posed by violent DR groups, specifically the new IRA and Continuity IRA (CIRA). In addition, new IRA, CIRA and other dissident groups who are no longer assessed to pose a national security threat are all involved in other types of harmful serious criminal activity, violence and intimidation that threaten local communities. There remains a minority who aim to destabilise the peace settlement, and their activity causes harm to communities across NI.

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 given rise to episodes of violent disorder, could escalate again. In the last year, we have seen discontent about issues such as the NI Protocol result in incidents including the hijacking and burning of local buses, as well as a sophisticated hoax aimed to disrupt an event at which the Irish Foreign Minister was present.

During the reporting period, the new IRA attempted an attack which targeted a police officer and her child, leaving an improvised explosive device (IED) under the car. Although the device failed to function, the incident demonstrates the continued intent and potential severity of the threat in NI from DR groups who continue to aspire to mount attacks typically against the Police Service of Northern Ireland (PSNI), and prison officers and military personnel.

The threat to the UK from Hostile State Activity

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. Espionage is similarly conducted to access economic information, including intellectual property, research and development and scientific academic research. It 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 also exists a continuing threat of state-sponsored assassination, attacks and abductions of those perceived as dissidents.

The National Security and Investment Act has given the UK greater powers to investigate and intervene in foreign direct investment that could threaten UK national security. The Government is also seeking to ensure that the security and law enforcement agencies have the necessary tools and legal authority to tackle the evolving threat of hostile activity by foreign states through the recently introduced National Security Bill.

Cyber threat

Cyber is a vector used by state and criminal actors to steal information, data and intellectual property, and it is a significant threat to the UK. In the digital age, the UK's own cyber power will be an even more important lever for delivering our national goals.

The Covid-19 pandemic, which continued into this reporting period as well as our last, demonstrated how reliant the UK is on cyberspace, to keep our society, economy and technology safe. This is significant, as the existence of cyberspace makes it easier for our adversaries to perpetrate their activity at scale and across borders.

Throughout last year, the ransomware threat grew, with Russian-speaking cyber criminals responsible for the most serious incidents, such as the Colonial Pipeline attack (May 2021) which impacted US energy supplies. The Conti ransomware attack against Ireland's Health Service Executive (May 2021) was the most serious cyber incident ever against a nation's healthcare system. Full recovery from the incident took Ireland several months. Foreign states and cybercriminals will continue to exploit known or undiscovered vulnerabilities in software libraries to target popular applications and services, similar to how organisations worldwide were impacted by the critical vulnerability in the Log4j Java library (December 2021).

Cyber and technology have continued to be used to degrade international human rights of privacy and freedom of thought and expression; authoritarian states will look to increase their control of the internet through increased legislation, technical measures, and influence within international digital standards shaping bodies. This increases the cyber threat to communications and data transiting these systems. Throughout the year, public exposures showed the scale of commercial cyber capabilities on offer. The proliferation of these commercial tools has enhanced the capabilities of nation states not traditionally viewed as advanced threats in the cyber landscape.

The Russian cyber threat to the UK continues to be closely monitored, and organisations are strongly encouraged to follow National Cyber Security Centre (NCSC) guidance on steps to increase their cyber resilience. Since the start of the Russia–Ukraine conflict (February 2022), we have seen Russia use cyber as a tool to support its wider military objectives, and

it has almost certainly been responsible a series of cyber-attacks against Ukraine, including against Viasat. Although the primary target is believed to have been the Ukrainian military, other customers were affected, such as personal and commercial internet users.

As revealed in a speech by the Director GCHQ (May 2022), since the National Cyber Force (NCF) stood up in April 2020, it has mounted operations to undermine the networks of cybercriminals, preventing them from profiting from their crimes, as well as denying them access to their cyber tools and malware. In real life, this has meant tens of millions of pounds in potential fraud against the UK economy has been avoided. Hundreds of thousands of stolen credit cards were made worthless to the criminals, and countless potential victims of crime around the world have had their data and accounts safeguarded.

With the publication of the National Cyber Strategy (NCS) (December 2021), HMG is taking a new, comprehensive approach to strengthening the UK's position as a responsible and democratic cyber power. The strategy takes a 'whole of cyber' approach and, for the first time, broadens the scope beyond cyber security to consider the full range of capabilities available to the UK. This will transform the UK's ability to develop, integrate and utilise these capabilities alongside diplomatic, economic and military levers of power and optimise them to deliver effect in order to keep the country safe, protecting and promoting the UK's interests at home and abroad. While the UK will not routinely talk about individual cyber operations, the NCF, along with the NCSC, could be used to support and advance a wide range of HMG priorities relating to national security and the prevention of serious crime.

WMD/Counter-proliferation

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 – 2020/21

<table>
<tr><th colspan="2">Single Intelligence Account</th></tr>
<tr><td colspan="2">Expenditure in 2020/21</td></tr>
<tr><td>Total budget and outturn</td><td>
<table>
<tr><th>£'000</th><th>Resource spending</th><th>Capital spending</th><th>TOTAL</th></tr>
<tr><td>Budget</td><td>2,901,202</td><td>810,041</td><td>3,711,243</td></tr>
<tr><td>Outturn</td><td>2,859,811</td><td>794,967</td><td>3,654,778</td></tr>
</table>
</td></tr>
<tr><td>Expenditure by category</td><td>● Staff pay: £1.19bn
● Other expenditure: £1.53bn
● Capital spending: £795m</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 SIA. 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 2020/21	● TRANSFORMING CORPORATE SERVICES – a programme to deliver all corporate services to the Agencies (such as finance, commercial services and human resources), ***, and the creation of a new set of digital platforms for the use of corporate services. ***, but the Agencies are in the process of requesting 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"*. ● The cross-community IT 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*". As of the financial year 2020/21, a shared team has been established within GCHQ as the "*first large scale collaborative Directorate General*" across the Agencies, ***. This team "*maintained mission capability*" throughout Covid-19 with reduced access to offices, including by piloting a *** mobile desktop.

MI5 (Security Service)

Expenditure in 2020/21[9]

Total budget and outturn

£'000	Resource spending	Capital spending	TOTAL
Budget	***	***	***
Outturn	***	***	***

Expenditure by category

- Staff pay: ***
- Other revenue costs (including professional services, accommodation, research and development, and IT systems): ***
- Capital costs: ***

Administration

Staff numbers[10]

	Total staff	SCS[11]	Non-SCS
31 March 2020[12]	4,685.5	55.5	4630
31 March 2021	5,259	62.5	5,196.5

Recruitment in 2020/21

- MI5 recruited 318 staff against a target of 260 in 2020/21.
- This compares with recruiting 458 new staff against a target of 345 in 2019/20.

Major projects in 2020/21

- Work has continued on a project to establish a new Counter-Terroism (CT) Operations Centre combining the CT elements of the Agencies with CT Policing. This aims to improve joint-working between the Agencies and CT Policing, including in operational responses.
- A project preparing MI5 for the adoption of a Cloud platform was led by MI5's newly formed Cloud Adoption Portfolio team. This focused on working practices and the use of data.

Diversity and inclusion 2020/21

- MI5 published a Gender Pay Gap Report (internally and externally) and an Ethnicity Pay Gap Report (internally only) on an annual basis.
- MI5 exceeded its target for female representation but fell short of its target for ethnic minority representation.
- MI5 used thematic recruitment campaigns to improve representation, such as 'Women in Tech' and the MI5 Diversity Internship.
- MI5 launched its new social media account on Instagram, gaining 110,000 followers.

[9] As reported to the Committee in MI5's end-year report for the 2020/21 financial year.
[10] These figures refer to the number of full-time equivalent (FTE) staff as at the end of the financial year. MI5 also employed a number of contractors and/or consultants. These figures are not included but have estimated costs for 2020/21 of ***.
[11] Senior Civil Service.
[12] Previous figures provided by MI5 were incorrectly given as Headcount rather than FTE. As such, the 31 March 2020 figure is not the same as that used in the Annual Report 2019–2021.

Policy	
Allocation of effort at 31 March 2021[13]	Allocation of effort across three operational themes: ● International CT – 63% ● Northern Ireland-related terrorism – 20% ● Hostile State Activity – 16%
Major achievements reported to the Committee for 2020/21	● MI5 disrupted two Islamist terrorist plots and two Extreme Right-Wing Terrorist (ERWT) plots in this period. ● MI5, working with Counter Terrorism Policing (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. ● The Centre for the Protection of National Infrastructure (CPNI) worked to secure supply chains for vaccine producers authorised in the UK. ● CPNI was also involved in supporting HMG's response to an attempt by a company with links to the Chinese state and intelligence services to purchase a UK company working in a sensitive sector. ● MI5 provided resources to help protect the UK's Covid-19 response, including deploying a dedicated team to advise on the protection of the Nightingale Hospitals and working with universities and pharmaceutical companies to secure Covid-19 testing, treatment, vaccine research and development.

Covid-19 impact
● In late March 2020, MI5 significantly restricted full time employee numbers in buildings to critical staff only (approximately *** of total staff). ● MI5 employees worked from home up to OFFICIAL-SENSITIVE, using devices supplied by GCHQ through ***. Capacity was increased gradually in May (to ***), June (***) and July (***), and by December 2020 was at ***. In January 2021, a return to two-metre social distancing was mandated, with building capacity significantly reduced again, to approximately *** of total staff, until the end of the financial year. ● In February 2021, MI5 began to supply lateral flow tests for asymptomatic testing of staff in their buildings. ● MI5 participated in an HMT-led programme to reduce spending, with the savings going towards the pandemic response. ● Separately, a programme to improve joint-working between MI5 and CTP was stopped temporarily.

[13] Operational allocation of effort (by FTE, to the nearest percentage).

Secret Intelligence Service (SIS)

Expenditure in 2020/21[14]

Total budget and outturn

£'000	Resource spending	Capital spending	TOTAL
Budget	***	***	***
Outturn	***	***	***

Expenditure by category

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

Administration

Staff numbers[15] [16]

	Total staff	SCS	Non-SCS
31 March 2020	4,107	85	4022
31 March 2021	3,644	76.4	3567.6

Recruitment in 2020/21

- SIS recruited *** new FTE staff against a target of *** in 2020/21.
- This compares with the recruitment of *** new staff against a target of *** in 2019/20.

Major projects in 2020/21

- SIS continued to invest in their 'Capability Portfolio', which currently involves a number of capability centres, each focused on a set of related capabilities. This programme has external assurance, including input from the Infrastructure and Projects Authority.
- A Science, Technology and Engineering programme has been set up to fund research and development across the Agencies – this programme is still in its early stages.

Diversity and inclusion 2020/21

- Online recruitment strategies *"hyper-targeted"* under-represented groups through social media.
- Vetting teams conducted a review of BAME security clearance refusals and held cultural awareness workshops.
- The first online pilot of SIS's 'Inspiring Leaders' programme was launched in November 2020.
- Reverse mentoring programmes established 45 partnerships.
- Senior leaders attended a two-day 'Inclusive Leadership' workshop led by a consultancy firm for corporate culture.
- SIS's first BAME Pay Gap Report was published (internally) in January 2021, alongside their Gender Pay Gap Report.

[14] As reported to the Committee in SIS's end-year report for the 2020/21 financial year.
[15] 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 2020/21 of ***.
[16] These figures include ***.

Policy	
Allocation of effort at 31 March 2021	• Key operational activities including: Counter Terrorism; cyber and access generation; defence technology and counter proliferation; and prosperity and economic stability – 36% • Operational support including: global network enabling; covert operations; data exploitation; operational security; and operational technology – 28% • 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 – 36%
Major achievements reported to the Committee for 2020/21	• SIS reporting enabled the disruption of two credible attack plots: *** • SIS contributed to the Intelligence Community response and support to HMG on the potential kidnap of a vulnerable *** UK national. • A new *** capability *** has enabled law enforcement to secure prosecutions. • SIS continued to focus intelligence production to address the Chinese threat, including ***.

Covid-19 impact
• Premises: In January 2021, SIS buildings were at significantly restricted capacity (***). Overseas Stations followed local rules for Covid-19 if local healthcare provision was on par with the NHS, and UK rules when it was not. • People: Self-isolation periods were factored into breaks for those in hardship postings, and SIS worked to ensure that staff overseas were able to return to the UK at the end of their tour, taking into account restrictions on international travel. • Agents: Priority work continued ***. Operational teams were at *** capacity at the end of the financial year, slightly below pre-Covid levels.

Government Communications Headquarters (GCHQ)

Expenditure in 2020/21[17]

Total budget and outturn

£'000	Resource spending	Capital spending	TOTAL
Budget	***	***	***
Outturn	***	***	***

Expenditure by category

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

Administration

Staff numbers[18]

	Total staff	SCS	Non-SCS
31 March 2020	7,107	94	7,013
31 March 2021	7,181.2	102.5	7,078.7

Recruitment in 2020/21

- GCHQ recruited 397 staff against a target of 859[19] in 2020/21.
- This compares with recruiting 585 new staff against a target of 697 in 2019/20.[20]

Major projects in 2020/21

- GOLO – a project aiming to deliver better working systems at OFFICIAL-SENSITIVE across the Agencies, alongside connection to the internet. This included *** devices which facilitate home-working.
- Computer Network Exploitation (CNE) Scaling – this project, as stated in our Annual Report 2019–2021, aims to help GCHQ become more proactive in conducting operations on the internet.

[17] As reported to the Committee in GCHQ's end-year report for the 2020/21 financial year.
[18] 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 2020/21 of ***.
[19] This target was set prior to the Covid-19 pandemic, which has negatively impacted GCHQ recruitment.
[20] These figures differ from those included in the Annual Report 2019–2021 due to a changed methodology within GCHQ.

Diversity and inclusion 2020/21	● GCHQ moved to a new set of Equality, Diversity and Inclusion (EDI) Priorities for 2021. Their new priorities are 'innovating to deliver diversity', 'enabling all our people to flourish', 'making inclusion mission critical', and 'embedding a data-led approach to EDI'. ● GCHQ released the mission statement for their Ethnic Minority Action Plan in the autumn of 2020, which is now being implemented. ● A study of security clearance refusals for ethnic minority applicants was concluded, and changes such as introducing EDI training into GCHQ's Vetting Officer Development Programme were recommended as a result. ● GCHQ's recruitment campaign (ATTRACT) targeted ethnic minorities and women to raise awareness of the organisation as a desirable place to work. ● The first GCHQ-wide inclusion survey received over 2,500 responses. ● The third GCHQ Gender Pay Gap Report was released, and the first Board-level Champion for Social Mobility was appointed.
Policy	
Allocation of effort at 31 March 2021	● Mission-specific programmes including: counter-terrorism; offensive cyber; serious organised crime; and counter proliferation – *** ● Capability exploitation – 19% ● Engineering – 19% ● IT services – 12% ● Cyber security – *** ● Corporate services (including human resources and finance) – 13%
Major achievements reported to the Committee for 2020/21	● Two *** Extreme Right-Wing Terrorists – first identified by GCHQ reporting – were arrested as part of separate investigations into their attack planning. Similarly, following GCHQ operational support to UK agencies, a UK-based Islamist attack planner was given a life sentence with a minimum term of 19 years. ● GCHQ provided insights into the Child Sexual Abuse (CSA) threat, ***. ● GCHQ's contribution to HMRC *** fraud operations has prevented more than £1 billion in revenue loss. ● GCHQ reported on its work on Russia in the run-up to the conflict, including work to support HMG contingency planning, ***. ● Working with a Five Eyes SIGINT partner, the National Cyber Force (NCF) planned and executed an operation to disrupt an ERWT threat within 24 hours.[21] ● The NCF conducted an offensive cyber operation designed to degrade a range of platforms ***.

[21] NCF is a partnership between Defence Intelligence and GCHQ, and their work is therefore reflected under both organisations in this Annex.

Covid-19 impact

- GCHQ has not provided a breakdown of the proportion of its staff working from the office.
- GCHQ has collected data since September 2020 on the proportion of staff *'*available for core business*'*. This was 81% in September 2020, rose to 92% by the end of 2020, and then fell during the third lockdown in January 2021 to 82%, but it is not clear whether or not this measure includes access to highly classified information.
- GCHQ increased its spending on facilitating *** working in non-secure environments.
- By the end of the financial year, GCHQ had supplied devices to each Agency to facilitate home-working up to OFFICIAL-SENSITIVE for all staff, via their GOLO programme.

Defence Intelligence (DI)

Expenditure in 2020/21[22]

Total budget and outturn

£'000	Resource spending	Capital spending	TOTAL
Budget	349,235	334	349,569
Outturn	383,737	34	383,771

Expenditure by category

- Operational staff costs: £243.8m
- Other operational costs: £81.7m
- Research and development: £34.4m
- Administration: £28.9m
- Against this, DI received income of £25.7m

Administration

Staff numbers[23]

	Total staff	Total civilian staff	Total Armed Forces staff	Armed Forces		Civilian staff	
				SCS equivalent	Non-SCS equivalent	SCS	Non-SCS
31 March 2020	4,089	1,436	2,653	9	2,644	9	1,427
31 March 2021	4,115	1,536	2,579	10	2,569	9	1,527

Recruitment in 2020/21

- In 2020/21, DI recruited 149 civilian personnel, compared with 131 in 2019/20.[24]

Major projects 2020/21

- PRIDE2 – this project, as set out in our Annual Report 2019-2021, aims to consolidate the DI estate, and will support the HMG 'Places for Growth' policy by contributing to housing targets.

Diversity and inclusion 2020/21

- The DI Diversity & Inclusion Strategy 2021 – 2026 was published in early 2021, and a Wellbeing, Diversity and Inclusion Working Group was established to oversee its implementation.

[22] Information has been reported to the Committee from DI's end-year report for the 2020/21 financial year.
[23] These figures refer to the number of full-time equivalent (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 2020/21 of £8m.
[24] Military 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.

Policy	
Allocation of effort at 31 March 2021	● Total operational and analysis effort – 82%. This comprises: – All source analysis and assessment – 9% – Collection and analysis – 73 % ● Operational support – 13%. This comprises: – Armed Forces security and intelligence training – 10% – Armed Forces intelligence policy and future capability development – 2% – Reserves – 1% ● Central support – 4%
Major achievements reported to the Committee for 2020/21	● DI provided early warning of the build-up and then reduction of Russian forces on the Ukrainian border in 2020, including the context needed to consider response options. ● DI continued to monitor Russian efforts to produce new weapon capabilities, including anti-satellite missiles. This informed the UK position and narrative on responsible behaviours in space. ● DI continued to support the deployment of the UK's Carrier Strike Group (CSG) to the Far East, working with Permanent Joint Headquarters and the Carrier Support Force to improve intelligence understanding prior to deployment. ● Working with a Five Eyes SIGINT partner, NCF planned and executed an operation to disrupt an Extreme Right-Wing Terrorism threat within 24 hours. ● NCF has conducted an offensive cyber operation designed to degrade a range of platforms ***.[25]
Covid-19 impact	
● All DI staff requiring access to systems above OFFICIAL-SENSITIVE were able to return to the office by the end of the financial year. DI plans to offer a balance between home and office working going forwards. ● DI provided intelligence relating to the spread and impact of the pandemic to MoD, other departments and Five Eyes partners. This has assisted MoD diplomacy efforts, the formulation of MoD Covid-19 policy and operational planning, and government procurement of test kits.	

[25] NCF is a partnership between DI and GCHQ, and their work is therefore reflected under both organisations in this Annex.

National Security Secretariat (NSS)

Expenditure in 2020/21[26]

Total budget and outturn

£'000	Resource spending	Capital spending	TOTAL
Budget	15,528	0	15,528
Outturn	17,430	0	17,430

Expenditure by category

- Pay costs: £14.9m
- National Cyber Security Programme (NCSP): £2.5m

Administration

Staff numbers[27]

	Total staff[28]	SCS[29]	Non-SCS
31 March 2020	190	26	164
31 March 2021	238	25	213

Recruitment in 2020/21

- NSS recruited 77 staff in 2020/21.
- This compares with 49 staff in 2019/21.

Major projects in 2020/21

- None reported.

Diversity and inclusion 2020/21

- NSS hosts a cross-government National Security Culture, Diversity and Inclusion team that identifies ways to implement the findings of the National Security Culture Inquiries in 2019 and 2020.
- NSS is sponsoring an outreach campaign to drive recruitment of ethnically diverse talent.

Policy

Allocation of effort at 31 March 2021

- Operational (policy teams & private offices) – 85%
- Corporate services – 15%

Major achievements reported to the Committee for 2020/21

- The UK formally took up its Presidency of the Intelligence College of Europe (ICE) in February 2021. The UK's Presidential theme is "*Fusing Intelligence Policy to build resilience in the 21st century*" and members of the ICE have been invited to run seminars and workshops around this theme, that NSS will facilitate.
- The Government Security Group has added the ability to conduct videoconferencing at SECRET on Rosa, a cross-government IT platform.

[26] As reported to the Committee in NSS's end-year report for the 2020/21 financial year.
[27] These figures refer to the number of full-time equivalent (FTE) staff as at the end of the financial year. NSS also employed a number of contractors. These figures are not included but have estimated costs for 2020/21 of £412,500.
[28] These numbers are in relation to all NSS staff excluding the Civil Contingencies Secretariat and National Cyber Security Programme-funded posts, which were approximately 150 FTE.
[29] Includes one SCS 4 – the National Security Adviser.

Covid-19 impact

- NSS has not provided a breakdown of the proportion of its staff working from the office.
- NSS scaled back a "*substantial amount*" of non-critical work, and noted a "*loss of resilience*" in critical functions. Limited access to high-classification systems continued to affect NSS work throughout summer 2020.
- NSS has used the pandemic to identify work that can be taken forward using a hybrid model of flexible working.

Joint Intelligence Organisation (JIO)

Expenditure in 2020/21[30]

Total budget and outturn

£'000	Resource spending	Capital spending	TOTAL
Budget	10,055	0	10,055
Outturn	9,813	39	9,852

Expenditure by category

- Pay costs: £7.4m
- Travel: £0.025m
- The remaining outturn is accounted for primarily through accommodation/estates, refurbishment, staff training and other administrative costs.

Administration

Staff numbers[31]

	Total staff	SCS	Non-SCS
31 March 2020	111	11	100
31 March 2021	110	10	100

Recruitment in 2020/21

- The JIO recruited 16 new staff in 2020/21, ***.
- This compares with 43 staff recruited in 2019/20, ***.

Major projects in 2020/21

- None reported.

Diversity and inclusion achievements 2020/21

- The JIO's Diversity and Inclusion Network meets each month to align national security community efforts with those throughout the Cabinet Office.
- JIO has launched the 'Yellow Dot' campaign to encourage staff to raise concerns about any behaviour or phrase that is exclusionary.

Policy

Allocation of effort at 31 March 2021

- Total operational activity – 96.4%
- Corporate services[32] – 3.6%

[30] As reported to the Committee in the JIO's end-year report for the 2020/21 financial year.
[31] These figures refer to the number of full-time equivalent staff as at the end of the financial year.
[32] In previous years, 'corporate services' included those working within PHIA. The JIO now considers these staff as 'operational activity' rather than 'corporate staff'.

Major achievements reported to the Committee for 2020/21	● JIO issued 30 Joint Intelligence Committee (JIC) Assessments, 97 Intelligence Briefs and 216 JIO Spotlights. ● JIO supported the HMG response to Covid-19, issuing a series of JIO Spotlights on international vaccine diplomacy and vaccine security, including on the 'Global Covid Vaccine Race' and *** Vaccine Diplomacy. ● As Russia mobilised troops in Crimea and on the northern and eastern borders of Ukraine at the end of March 2021, JIO created a crisis response team which produced daily intelligence updates and short-notice JIC assessments on the military build-up. ● Five Eyes partners supported a number of papers, and JIO established virtual meetings dedicated to the strategic assessment ***. JIO also increased sharing of 'Reports Edited for Liaison Services' (RELS) assessments with a range of other allies ***. ● The JIC Chair briefed NATO Ambassadors *** in parallel with the Acting NSA.

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.
- Savings were made on travel, subsistence and training due to the pandemic – these savings were reallocated to security measures, mostly the installation of circle locks.

Homeland Security Group

Expenditure in 2020/21[33]

Total budget and outturn

£'000	Resource spending	Capital spending	TOTAL
Budget	1,048,700	111,100	1,107,500
Outturn	1,008,000	105,500	1,111,000

Expenditure by category

- Grants spending: £871.5m[34]
- Staff pay: £60.8m
- Other costs: £98.5m
- Against this, Homeland Security Group received an income of £22.8m

Administration

Staff numbers[35]

	Total staff	SCS	Non-SCS
31 March 2020	792	23	769
31 March 2021	1,061	30	1,031

Recruitment in 2020/21

- Homeland Security Group recruited 161 staff in 2020/21 against a target of 262.
- This compares with 166 employees in 2019/20 with no set recruitment target.

Major projects in 2020/21

- None reported.[36]

Diversity and inclusion 2020/21

- A Diversity and Inclusion Board has been established with SCS leads across all protected groups.
- A 'Career Watch' sponsorship programme has been launched, and made available to all BAME staff and staff with disabilities. All SCS must sponsor at least two members of staff.
- 'Let's Talk About Race' sessions were piloted and will be rolled out across Homeland Security Group.
- Advice and listening sessions were held following the murder of Sarah Everard.

[33] As reported to the Committee in the Homeland Security Group end-year report for the 2020/21 financial year.
[34] The vast majority of Homeland Security Group expenditure is administered via grants mechanisms, and CT policing grants constitute over 75% of Homeland Security Group's net budget.
[35] These figures refer to the number of full-time equivalent staff as at the end of the financial year. Homeland Security Group also employed a number of contractors and/or consultants. These figures are not included but have estimated costs for 2020/21 of just over £0.8m.
[36] Homeland Security Group has highlighted in previous returns that the Communications Capabilities Development Programme (CCD) transitioned from a programme into the Communications Data and Lawful Intercept (CDLI) service partnership on 1 April 2018. Therefore, Homeland Security Group was no longer running any major projects in 2020/21 as defined by the Infrastructure and Projects Authority's Government Major Projects Portfolio (GMPP).

Policy	
Allocation of effort at 31 March 2020	● National Security Directorate – 38% ● PREVENT and Research, Information and Communications Unit – 14% ● PROTECT, PREPARE (CBRNE) and science and technology – 15% ● Chief Operating Officer's directorate (including Communications Data Lawful Intercept, Planning and Resources Unit and the Joint Security and Resilience Centre) – 17% ● CONTEST (formerly known as Strategy, Planning and International) – 10% ● Economic Crime Directorate – 6%
Major achievements reported to the Committee for 2020/21	● Homeland Security Group secured multi-year funding to improve *'*protective capabilities*'* against a terrorist attack using a radiological or nuclear device. ● The Counter-Terrorism and Sentencing Act 2021 and the Covert Human Intelligence Sources (Criminal Conduct) Act 2021 strengthened the statutory powers of Homeland Security Group operational partners.
Covid-19 impact	
● Most staff worked from home throughout the financial year; a small number of staff were able to work from home at SECRET. Staff worked from the office "*with split team working in operation*" when it was critical. ● The risk to CT "*resilience and capability*" has been monitored by Homeland Security Group throughout the financial year in order to identify potential policy impacts from Covid-19, and to provide ministerial assurance.	

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,[37] 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.[38] 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.

---

[37] 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.

[38] 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.[39] 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.[40]

   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.

---

[39] 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.
[40] 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[41] 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[42] 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;

---

[41] 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.
[42] 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)[43] and for the Agencies, with the Heads of the Agencies.

[43] 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.

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. 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,[44] 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

[44] 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.

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 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[45], 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.[46] 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.

---

[45] 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.

[46] 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.[47]

   (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 *Homeland Security Group*.

d. BEIS: the activities of the Investment Security Unit.

e. Department for Digital, Culture, Media and Sport:

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

[47] 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 Office of Communications;*

(iii) *the Counter Disinformation Unit.*

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.

h. Department of Health: the activities of the Joint Biosecurity Unit.

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[48] 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.

[48] 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[49] 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.

[49] 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)[50] 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.

---

[50] 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. BEIS: Secretary of State for Business, Energy and Industrial Strategy.

f. DCMS: Secretary of State for Digital, Culture, Media and Sport.

g. Department for Transport: Secretary of State for Transport

h. Department of Health & Social Care: Secretary of State for Health and Social Care

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[51], 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 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

[51] 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.

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.

E02813160
978-1-5286-3758-9